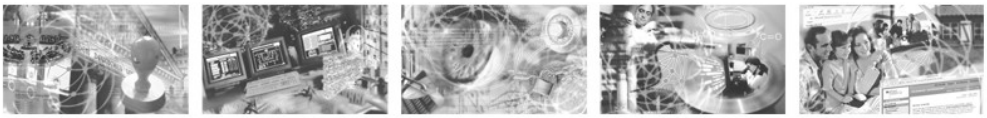
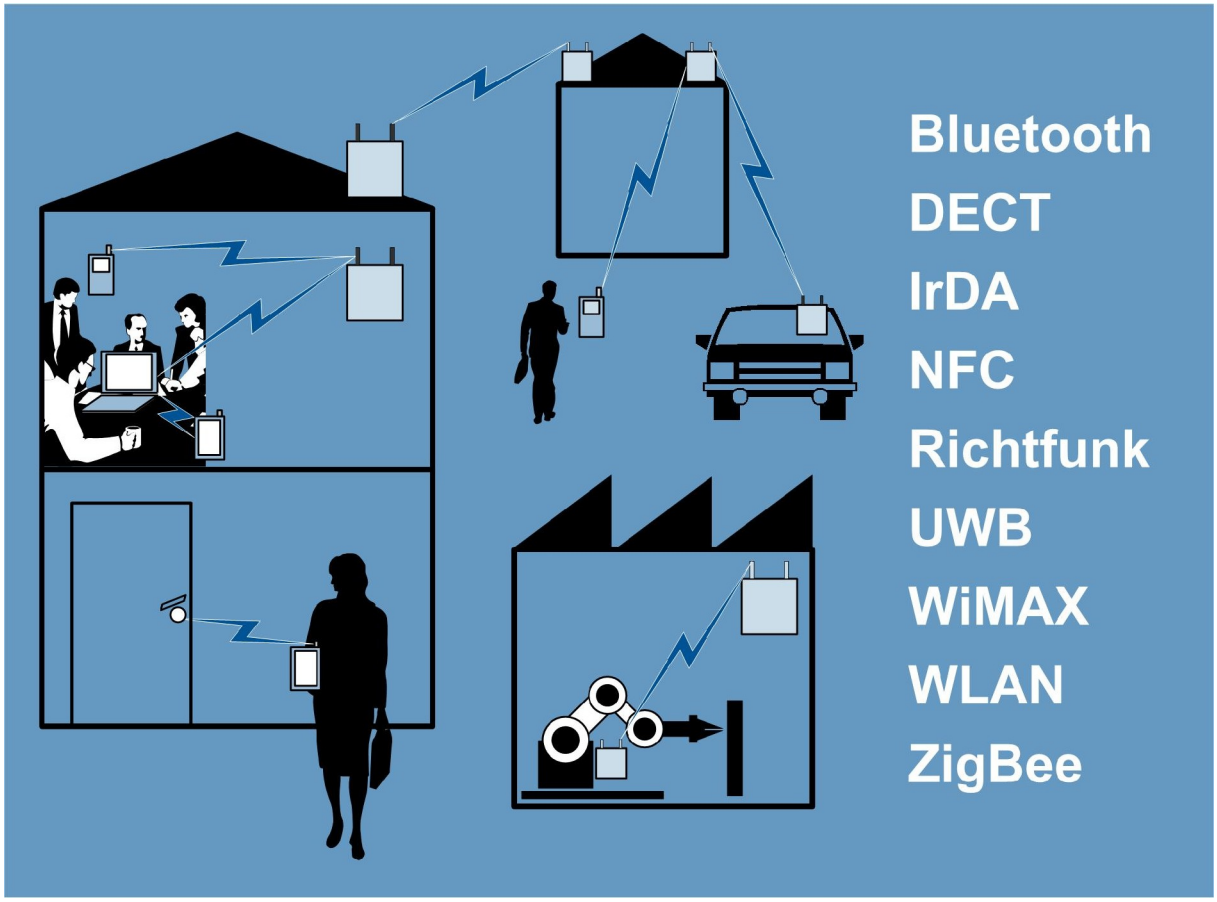
Bundesamt
für Sicherheit in der
Informationstechnik



Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte



Bundesamt für Sicherheit in der Informationstechnik

Diese Broschüre soll die Funktionsweise von drahtlosen Kommunikationssystemen darstellen, mögliche Gefährdungen der Informationssicherheit bei Nutzung dieser Systeme beschreiben sowie geeignete Schutzmaßnahmen aufzeigen. Das Dokument reflektiert den Stand der Technik bis September 2009.

An der Erstellung waren folgende Mitarbeiter des BSI beteiligt: Heinz Gerwing, Jörg Mattke, Dr. Wilhelm Pütz, Guido Reckhaus, Berthold Ternes. Weiterhin haben folgende Mitarbeiter der ComConsult Beratung und Planung mitgewirkt: Dr. Simon Hoff, Dietlind Hübner, Daniel Meinhold, Dr. Joachim Wetzlar.

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 (0) 228 99 95820
E-Mail: publikationen@bsi.bund.de
Internet: https://www.bsi.bund.de

Einleitung

Drahtlose Kommunikationssysteme finden bei zunehmender Produktvielfalt eine immer größere Verbreitung. Die Funkanbindung von stationären wie mobilen Endgeräten an das Telefonnetz, das Internet oder das lokale Netz in einem Unternehmen oder einer Behörde bietet neue Freiheiten bei der Nutzung der Netze und deren Dienste. Drahtlose Netze können ein effizienter Ersatz sein für ein aufwendiges Verlegen von Kabeln; Ad-hoc-Vernetzung per Funk ermöglicht den spontanen und mobilen Datenaustausch. Kabellose Eingabegeräte erhöhen den Bedienkomfort der IT-Systeme. Mit heute verfügbarer drahtloser Technik sind viele Mobilitätsansprüche der Nutzer von IT-Technik realisierbar.

Die wichtigsten technischen Systeme hierzu sind zurzeit:

- WLANs (Wireless Local Area Networks) nach den Standards der Serie IEEE 802.11 als Ergänzung der kabelbasierten lokalen Netze (Local Area Networks, LANs)
- Bluetooth zur Übertragung von Sprache und Daten in der unmittelbaren persönlichen Umgebung
- Sprach- und Datenkommunikationssysteme nach dem DECT-Standard (Digital Enhanced Cordless Telecommunications)
- WiMAX (Worldwide Interoperability for Microwave Access) zur drahtlosen Anbindung von Feststationen und für mobile Endgeräte
- Richtfunk-Techniken zur drahtlosen Überbrückung größerer Entfernungen zwischen Gebäuden
- ZigBee, basierend auf IEEE 802.15.4, für Sensor- und Steuernetzwerke
- UWB (Ultra Wideband) zur Anbindung von Peripheriegeräten mit hohen Datenraten
- NFC (Near Field Communication) zur drahtlosen Kopplung von Geräten in kurzen Entfernungen

Außerdem zeichnen sich bereits künftige Entwicklungen ab, die beispielsweise einem Endgerät einen systemübergreifenden Wechsel von Kommunikationsmedien ohne Abbruch der Ende-zu-Ende-Kommunikation ermöglichen (IEEE 802.21 – Media Independent Handover, MIH).

Ebenfalls sind ältere drahtlose Techniken weiterhin zu beachten, insbesondere

- Infrarot-Module nach IrDA zur Kommunikation mit Peripheriegeräten
- Drahtlose Tastaturen, Mäuse und andere Eingabegeräte

Alle diese Systeme bieten einen Gewinn an Komfort und Mobilität, jedoch birgt die Nutzung der drahtlosen Technik auch zusätzliches Gefährdungspotenzial für die Sicherheit der Informationen. Diese Gefährdungen sind bedingt durch die spezielle drahtlose Kommunikationstechnik, durch Schwächen der zugrunde liegenden Protokolle sowie durch falsche Konfiguration und Benutzung der Systemkomponenten.

Drahtlos heißt, dass Informationen mittels elektromagnetischer Wellen wie Funk oder Infrarot-Licht zwischen den Kommunikationspartnern übertragen werden. Hier fehlt also der physikalische Schutz des Mediums, den eine Leitung – sei es Kabel, Draht oder Lichtwellenleiter – bietet. Dies führt praktisch bei allen drahtlosen Kommunikationssystemen zu typischen Problemen:

Interferenzen und stark schwankende Kanalbedingungen können bis zum Verlust der Verfügbarkeit der Kommunikationsfähigkeit des Systems führen. Darüber hinaus können die ausgesendeten elektromagnetischen Wellen aber auch von Dritten empfangen, aufgezeichnet, ausgewertet und ggf. manipu-

liert werden. Mit Hilfe von leistungsfähiger Empfangstechnik, z.B. mit Richtantennen oder empfindlichen Empfängermodulen sind der Empfang und die Aufzeichnung der Informationen auch weit über die normale Nutzreichweite der funkbasierten Kommunikationssysteme möglich.

Damit die übertragenen Informationen vertraulich bleiben, sind sichere Verschlüsselungsverfahren notwendig, starke Authentisierungsverfahren sollen dem nicht autorisierten Dritten den Zutritt zum drahtlosen Kommunikationssystem verwehren, und Integritätsschutzmechanismen sollen dafür Sorge tragen, dass ausgesendete Informationen unverfälscht den Empfänger erreichen.

Im Folgenden werden in separaten autarken Kapiteln die wichtigsten drahtlosen Kommunikationssysteme dargestellt, mögliche Gefährdungen der Informationssicherheit bei Nutzung dieser Systeme beschrieben und ggf. geeignete Schutzmaßnahmen aufgeführt. Diese Informationsschrift möchte Administratoren, Sicherheitsbeauftragten und Endbenutzern drahtloser Kommunikationssysteme eine Hilfestellung zur Bewertung und sicheren Nutzung dieser Systeme bieten.

Gliederung des Dokumentes

A. Funk-LAN (WLAN, IEEE 802.11)

Inhaltsverzeichnis des Abschnitts

A.1 Grundlagen und Funktionalität

Wireless Local Area Networks (WLANs, manchmal auch als Funk-LANs bezeichnet), die auf dem 1997 vom Institute of Electrical and Electronics Engineers (IEEE) veröffentlichten und seitdem kontinuierlich weiterentwickelten Standard IEEE 802.11 basieren (siehe [IEEE07]), findet man als drahtlose Erweiterung eines traditionellen LAN (Local Area Network) sowohl in den Bereichen Büro, Industrie, Handel, Logistik und Medizin als auch im privaten Bereich. WLANs erlauben den für viele Anwendungsbereiche immer wichtiger werdenden drahtlosen Zugang zu Informationen.

Aufgrund der einfachen Installation werden WLANs auch für temporär zu installierende Netze (z.B. auf Messen) verwendet. Darüber hinaus werden über WLANs an öffentlichen Plätzen wie Flughäfen oder Bahnhöfen Netzwerkzugänge (sogenannte Hotspots) angeboten, um mobilen Benutzern Verbindungen in das Internet und hierüber z.B. per Virtual Private Network (VPN) einen Zugriff auf die heimatliche IT-Infrastruktur zu ermöglichen.

Die Kommunikation erfolgt bei WLANs über Funk, was prinzipiell immer die Gefahr der Abhörbarkeit, des unerlaubten Zugangs zum WLAN und der Störbarkeit von Übertragungen (beabsichtigt oder nicht) birgt.

Bereits Mitte 2001 sind massive Sicherheitslücken im Standard IEEE 802.11 bekannt geworden, die zu großen Sicherheitsproblemen geführt haben. Die ursprünglich spezifizierten kryptographischen Mechanismen haben sich als unzulänglich erwiesen, da der verwendete Verschlüsselungsalgorithmus in kürzester Zeit gebrochen werden kann. Der Zugang zu fremden WLANs wird außerdem noch durch frei verfügbare Werkzeuge erleichtert. Seit geraumer Zeit gibt es von der IEEE allerdings mit IEEE 802.11i eine Erweiterung des Standards, die deutlich verbesserte Sicherheitsmaßnahmen spezifiziert.

Bis heute basieren praktisch alle am Markt verfügbaren WLAN-Systeme auf dem genannten Standard IEEE 802.11 und seinen Ergänzungen, die im Folgenden kurz vorgestellt werden[1]. Eine besondere Rolle nimmt dabei das Hersteller-Konsortium Wi-Fi Alliance ein, das basierend auf IEEE 802.11 mit Wi-Fi einen Industriestandard geschaffen hat. Dabei bestätigt die Wi-Fi Alliance mit dem Wi-Fi-Gütesiegel, dass ein Gerät gewisse Interoperabilitäts- und Konformitätstests bestanden hat.

A.1.1 Allgemeiner Aufbau eines WLAN

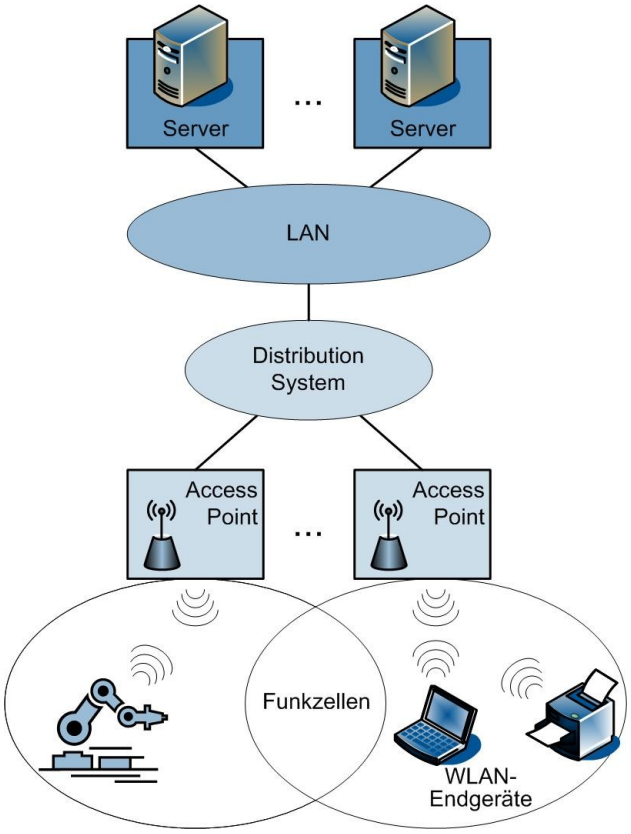
In WLANs werden zunächst zwei Formen der drahtlosen Kommunikation unterschieden.

Im Ad-hoc-Modus kommunizieren zwei oder mehr mobile Endgeräte (Clients), die mit einem WLAN-Adapter ausgestattet sind, direkt miteinander. WLANs im Ad-hoc-Modus sind in der Praxis eher selten.

Der größte Teil der WLAN-Installationen wird im Infrastruktur-Modus betrieben. Hier erfolgt die Kommunikation der Endgeräte über eine zentrale Funkbrücke, den sogenannten Access Point, über den auch die Anbindung an das kabelbasierte LAN erfolgt und der sich gemäß einer Bridge nach IEEE 802.1D verhält (siehe [IEEE04-1D] und Abbildung A-1).

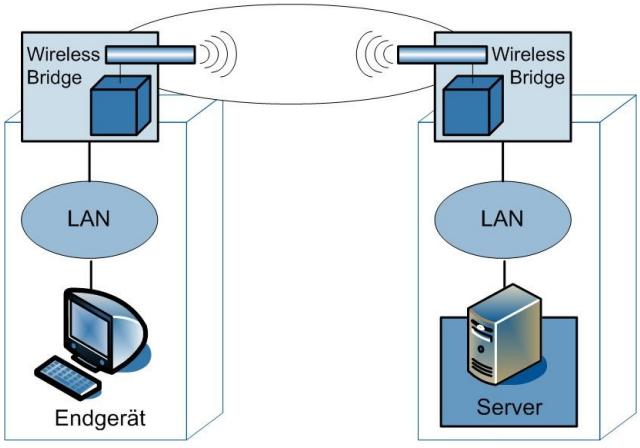
[1] Neben dem Standard IEEE 802.11 gibt es noch andere WLAN-Standards, die jedoch keine praktische Relevanz mehr haben, da diese Standards nicht weiterentwickelt werden und keine Produkte am Markt verfügbar sind. Zu nennen sind hier HomeRF und HIPERLAN/2 (High Performance Radio Local Area Network Type 2).

Abbildung A-1: Infrastruktur-Modus-Erweiterung kabelbasierter LANs



Bei der Verwendung entsprechender Komponenten (Richtantennen) an den Access Points, die dann oft als Wireless Bridge bezeichnet werden, kann ein WLAN auch zur Kopplung kabelbasierter LAN-Segmente wie eine Richtfunkstrecke eingesetzt werden. Dabei kommunizieren die Access Points über die Funkschnittstelle direkt miteinander, wie in Abbildung A-2 dargestellt.

Abbildung A-2: Infrastruktur-Modus - LAN-Kopplung



Der Standard IEEE 802.11 verwendet die Bezeichnungen Independent Basic Service Set (IBSS) für Funk-Netzwerke im Ad-hoc-Modus und Basic Service Set (BSS) für Konstellationen im Infrastruktur-Modus mit einem Access Point. Mehrere gekoppelte BSS werden als Extended Service Set (ESS) bezeichnet, das koppelnde Netzwerk wird Distribution System (DS) genannt.

Es kann durchaus vorkommen, dass an einem Ort WLANs unterschiedlicher Betreiber empfangen werden können. Zur Identifikation wird für ein WLAN daher ein Name vergeben, der sogenannte Service Set Identifier (SSID).

A.1.2 Funkschnittstelle

In IEEE 802.11 und seinen Erweiterungen (siehe [IEEE07][2]) werden verschiedene Varianten zur physikalischen Übertragung und ein gemeinsames Verfahren für den Kanalzugriff spezifiziert.

- Systeme des 1997 veröffentlichten Standards IEEE 802.11 übertragen die Daten mit einer Rate von 1 Mbit/s oder 2 Mbit/s mittels Bandspreizverfahren: entweder Frequency Hopping Spread Spectrum (FHSS) oder Direct Sequence Spread Spectrum (DSSS). Die Systeme nutzen das ISM-Frequenzband (Industrial, Scientific, and Medical) zwischen 2,4 und 2,48 GHz. Der Vollständigkeit halber sei erwähnt, dass IEEE 802.11 auch eine Infrarot-Übertragung definiert, die aber bisher in der Praxis bedeutungslos geblieben ist. DSSS- und FHSS-Systeme werden praktisch nicht mehr eingesetzt.

- Die Systeme der 1999 veröffentlichten Ergänzung IEEE 802.11b verwenden eine Erweiterung des DSSS-Verfahrens. Die Brutto-Datenübertragungsrate beträgt maximal 11 Mbit/s. Es wird ebenfalls das ISM-Frequenzband bei 2,4 GHz genutzt.

  Mit IEEE 802.11b haben sich WLANs enorm verbreitet, und auch heute werden Systeme nach IEEE 802.11b noch eingesetzt.

- Um Datenraten bis zu 54 Mbit/s und eine höhere Anzahl von parallel operierenden Systemen mit sich überlappenden Funkzellen anbieten zu können, verwenden Systeme nach der ebenfalls 1999 veröffentlichten Ergänzung IEEE 802.11a den 5-GHz-Bereich, der unter anderem in Europa von 5,15 bis 5,35 GHz und von 5,47 bis 5,725 GHz für die WLAN-Nutzung zugelassen ist. Als Übertragungstechnik wird Orthogonal Frequency Division Multiplexing (OFDM) genutzt.

- Systeme der im Juni 2003 veröffentlichten Ergänzung IEEE 802.11g operieren im ISM-Band bei 2,4-GHz und sind mit IEEE 802.11b abwärtskompatibel. Als Übertragungstechnik wird OFDM analog zu IEEE 802.11a verwendet, wodurch auch Datenraten bis 54 Mbit/s möglich sind.

- Mit der im September 2009 verabschiedeten Ergänzung IEEE 802.11n sollen durch Erweiterungen der physikalischen Übertragung Datenraten von bis zu 600 Mbit/s brutto erreicht werden. Für die physikalische Übertragung wird ein als Multiple Input Multiple Output (MIMO) bezeichnetes Verfahren genutzt, das es gestattet, mehrere parallele OFDM-Ströme sich überlagernd auf einem Frequenzkanal zu übertragen. Aktuell sind diverse Vorstandardprodukte – meist mit einer physikalischen Datenrate von brutto 300 Mbit/s – auf dem Markt verfügbar. Die Wi-Fi Alliance bietet seit geraumer Zeit auch ein eigenes Zertifizierungsprogramm basierend auf der Vorversion Draft 2.0 von IEEE 802.11n an, nach dem bereits eine größere Zahl von Produkten zertifiziert ist. Dieses Zertifizierungsprogramm wird in einem zweiten Schritt auf den verabschiedeten Standard IEEE 802.11n erweitert.

Im 2,4-GHz-Frequenzbereich stehen in Deutschland 13 Frequenzkanäle mit einem Frequenzabstand von 5 MHz für die Funkübertragung nach 802.11b/g zur Verfügung. Bei einer Kanalbandbreite von ca. 20 MHz für IEEE 802.11b/g können jedoch nur maximal 3 Kanäle gleichzeitig überlappungsfrei genutzt werden.

[2] In regelmäßigen Abständen konsolidiert die IEEE ihre Basisstandards. Die Auflage von 2007 des Standards IEEE 802.11 beinhaltet unter anderem die im Folgenden vorgestellten Ergänzungen IEEE 802.11a/b/e/g/h/i.

Im 5-GHz-Bereich sind unter anderem in Europa insgesamt 19 Kanäle in einem Frequenzabstand von 20 MHz unter Auflagen freigegeben worden (siehe [EC05]). Bei einer Kanalbandbreite von 20 MHz stören sich diese Kanäle untereinander nicht.

Für Systeme nach IEEE 802.11n (bzw. nach Draft 2.0) muss berücksichtigt werden, dass auch eine Kanalbandbreite von 40 MHz verwendet werden darf. Dies macht für flächendeckende WLANs allerdings nur bei 5 GHz Sinn, da nur hier das für WLAN nutzbare Spektrum ausreichend groß ist.

Die Rahmenbedingungen und Parameter für den Betrieb von WLANs in Deutschland sind in Verfügungen der Bundesnetzagentur festgelegt (siehe [BNA03] für den 2,4-GHz-Bereich und [BNA06] für WLANs bei 5 GHz).

Der Zugriff auf den Funkkanal (Medium Access Control, MAC) erfolgt bei allen Systemen einheitlich nach einem zufallsgesteuerten Verfahren, Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), das einen Best-Effort-Dienst liefert. Die entsprechende Komponente des WLAN MAC Layer wird in der Terminologie von IEEE 802.11 als Distributed Coordination Function (DCF) bezeichnet. Der Standard spezifiziert auch eine optionale Polling-basierte deterministische Kanalvergabe (Point Coordination Function, PCF), die jedoch in den wenigsten Produkten implementiert ist.

Eine Auswahl der weiteren Ergänzungen des Standards IEEE 802.11 (siehe [IEEE07]), die auch für die Sicherheitsbetrachtung von WLANs wichtig sind, ist im Folgenden aufgelistet:

- IEEE 802.11e

  Hier wird die MAC-Ebene von IEEE 802.11 um Dienstgütemechanismen (Quality of Service, QoS) erweitert, indem ein erweiterter Kanalzugriff spezifiziert wird, der unter anderem eine Priorisierung verschiedener Verkehrsklassen erlaubt.

- IEEE 802.11h – Ergänzung zu IEEE 802.11a

  Der 5-GHz-Bereich wird auch von militärischen und zivilen Radar- und Navigationsanwendungen genutzt. Um Störungen dieser Anwendungen durch ein WLAN zu vermeiden, darf das gesamte bei 5 GHz zur Verfügung stehende Spektrum nur dann durch ein WLAN genutzt werden, wenn im WLAN mindestens eine dynamische Frequenzwahl (Dynamic Frequency Selection, DFS) und optional auch eine Anpassung der Sendeleistung (Transmit Power Control, TPC) unterstützt werden[3]. IEEE 802.11h spezifiziert die hierfür notwendige Erweiterung des MAC Layer. Die Wi-Fi Alliance bietet auch die Zertifizierung von WLAN-Geräten nach IEEE 802.11h an.

- IEEE 802.11i

  Hier werden verbesserte Sicherheitsmechanismen spezifiziert, die notwendig waren, weil sich die ursprünglich in IEEE 802.11 festgelegten Verfahren als unzulänglich erwiesen haben. Die Verbesserungen betreffen Verschlüsselung, Integritätsschutz und Authentisierung. Die Elemente von IEEE 802.11i und der entsprechenden Konzepte der Wi-Fi Alliance werden in den folgenden Kapiteln noch genauer beschrieben.

- IEEE 802.11k

  Der Standard IEEE 802.11k definiert Erweiterungen für das Radio Resource Management. Dabei wird auch die Verteilung der WLAN-Endgeräte auf die zur Verfügung stehenden Access Points optimiert. IEEE 802.11k wurde 2008 verabschiedet (siehe [IEEE08-11k]).

3 Dies betrifft die Bereiche 5,25 GHz bis 5,35 GHz und 5,47 GHz bis 5,725 GHz. Die Nutzung des 100 MHz großen Abschnitts von 5,15 GHz bis 5,25 GHz ist nicht durch Auflagen hinsichtlich DFS und TPC reguliert.

- IEEE 802.11r

  Der Standard IEEE 802.11r (Fast BSS Transition) aus dem Jahr 2008 spezifiziert Funktionen für einen schnelleren Wechsel der Funkverbindung (Handover) bei der Bewegung eines Endgeräts zwischen Funkzellen (siehe [IEEE08-11r]).

- IEEE 802.11s – in Arbeit

  Das Thema dieser Erweiterung sind sogenannte Mesh-Netze, d.h. Access Points kommunizieren untereinander über Funk, um Pakete von WLAN-Endgeräten zu vermitteln. Pakete können auf diese Weise über mehrere solcher (als Hops bezeichnete) Funkstrecken an das Ziel gelangen. Dabei sind spezielle Routing-Verfahren notwendig, die für eine Paketübertragung aus der vermaschten Netzstruktur, welche sich aus der Vernetzung über Funk ergibt, geeignete Wege von Access Point zu Access Point ermitteln. Mesh-Netze können als eine Verallgemeinerung des Prinzips einer Punkt-zu-Punkt-Verbindung über WLAN, wie sie bei einer LAN-Kopplung genutzt wird, verstanden werden. Mesh-Netze eignen sich insbesondere für WLAN-Installationen, für die mit vertretbarem Aufwand kein (ausschließlich) kabelbasiertes Distribution System realisierbar ist.

- IEEE 802.11w – in Arbeit

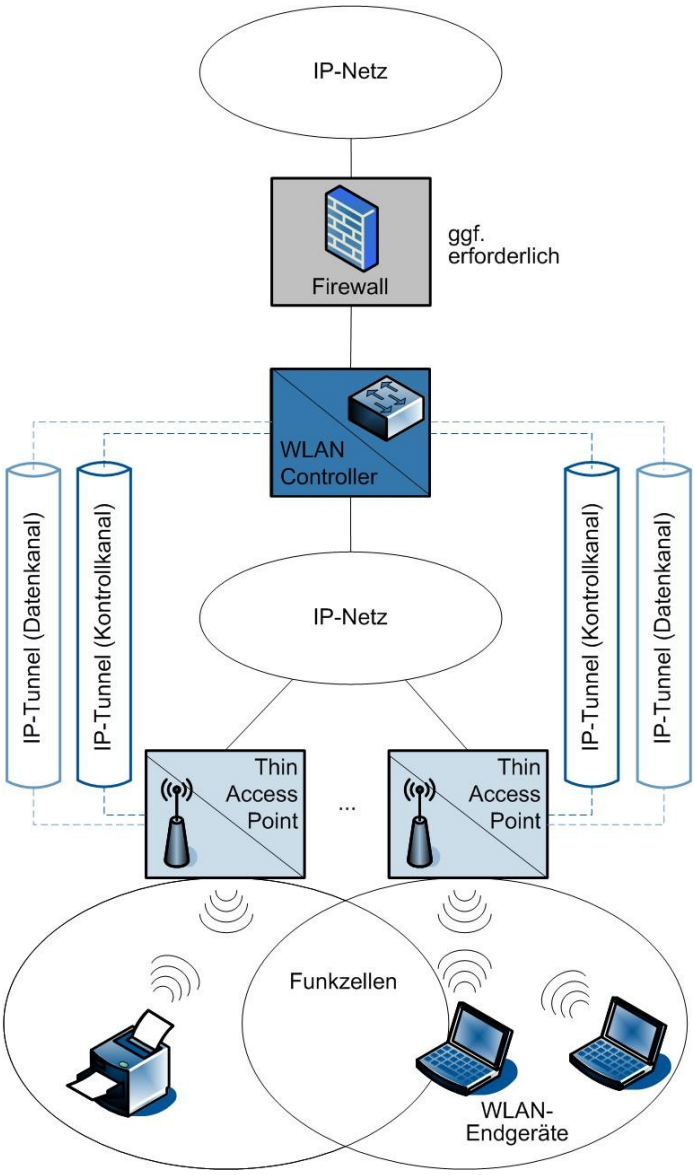
  Ein Sicherheitsrisiko, das IEEE 802.11i nicht beseitigt, geht von der Übertragung ungesicherter Management-Pakete (Management Frames) aus, die nicht verschlüsselt und nicht hinsichtlich ihrer Authentizität und Integrität geprüft werden. Die Absicherung solcher Management Frames soll mit IEEE 802.11w möglich werden.

In Arbeit sind noch weitere Erweiterungen, beispielsweise zur Verbesserung des Management von WLAN-Stationen (IEEE 802.11v).

A.1.3 Controller-basiertes WLAN-Design

Neben der Verwendung autonomer Access Points, die als Layer 2 Bridges direkt an ein kabelbasiertes LAN (Ethernet) angeschlossen werden, wird in WLAN-Installationen vermehrt das sogenannte Controller-basierte WLAN-Design eingesetzt. In einem Controller-basierten WLAN-Design werden WLAN-Funktionen durch zentral positionierte WLAN Controller realisiert und die Aufgaben der Access Points auf die reine Funkübertragung reduziert. Daher werden Access Points in einem Controller-basierten Design oft auch als Thin Access Points bezeichnet. Der WLAN Controller übernimmt die Aufgabe der zentralen Kontrolle und Überwachung der Thin Access Points. In der Internet Engineering Task Force (IETF) erarbeitet die Gruppe CAPWAP (Control and Provisioning of Wireless Access Points) die Standards für einen Controller-basierten WLAN-Aufbau.

Abbildung A-3: Controller-basiertes WLAN-Design



Die Kommunikation zwischen WLAN Controller und Thin Access Point erfolgt meist über IP-Tunnel (siehe Abbildung A-3). Über diese Tunnel können alle Daten für das Management der Thin Access Points sowie die gesamte Kommunikation von und zu den WLAN-Endgeräten (Nutzdaten) transportiert werden. Hiermit ist der Aufbau des WLAN als Overlay-Netz und damit verbunden eine Abstraktion von der Struktur des zugrunde liegenden Transportnetzes möglich. Dabei impliziert die Verwendung eines Tunnelmechanismus nicht automatisch eine Verschlüsselung der Kommunikation zwischen Thin Access Point und WLAN Controller.

Durch den Tunnelmechanismus für die Nutzdaten entsteht ein virtuelles Distribution System und die zugrunde liegende Netzstruktur zwischen Thin Access Points und WLAN Controller wird aus Sicht der WLAN-Endgeräte transparent. Diese Konzepte führen zu einem WLAN-Design, das sich deutlich von dem Aufbau mit traditionellen (sogenannten autonomen) Access Points unterscheidet. Bei der Verwendung von autonomen Access Points ist das Distribution System meist ein flaches Layer-2-

Netz, weil sich bei einem Layer-3-Netz Mobilitätseinschränkungen ergeben würden[4]. Dieses Problem kann durch den Einsatz von Tunnelmechanismen umgangen werden. Wird die Kommunikation eines WLAN-Endgeräts nämlich über das Distribution System getunnelt, merkt die Client-Applikation einen mobilitätsbedingten IP-Subnetzwechsel gar nicht, weil sie die zwischen Access Point und WLAN Controller liegende Netzstruktur nicht wahrnimmt.

WLAN Controller können also insbesondere eingesetzt werden, um ein WLAN in eine (beliebige) Layer-3-strukturierte LAN-Infrastruktur zu integrieren bzw. um das Distribution System als Layer-3-Netz aufzubauen.

Das Tunnel-Konzept der Nutzdaten in einer WLAN-Controller-Lösung hat in manchen Situationen auch Nachteile. Stellt man sich ein Filialszenario vor, bei dem WLAN Controller in der Zentrale aufgestellt sind und Thin Access Points in den Filialen über eine WAN-Strecke (Wide Area Network) angebunden werden, besteht das Problem, dass der lokale Verkehr erst in die Zentrale zum WLAN Controller und dann wieder zurück zur Filiale geleitet wird.

Zur Lösung dieses Problems bieten die meisten Hersteller die Möglichkeit, den Nutzdatenverkehr lokal am Thin Access Point auszukoppeln. Damit gehen aber die Eigenschaften eines Overlay-Netzes verloren.

Für den Tunnelmechanismus und die über den Tunnel ausgetauschten Daten liegt zwar seit März 2009 die CAPWAP Protocol Specification als RFC[5] 5415 vor (siehe [RFC5415]), aktuell sind aber oft noch herstellerspezifische Lösungen im Einsatz. In CAPWAP werden Kontroll- und Datenkanal über UDP (User Datagram Protocol) übertragen. Hierbei wird für Kontrollpakete der UDP-Port 5246 und für Datenpakete der UDP-Port 5247 genutzt.

Aus einer Sicherheitsperspektive ist das Controller-basierte Design außerdem aus folgenden Gründen interessant:

- Die Access Points erhalten ihre Konfiguration und bei Bedarf auch ein aktuelles Firmware Image grundsätzlich vom WLAN Controller. Für den gesicherten Austausch solcher Kontrolldaten fordert die CAPWAP-Spezifikation eine gegenseitig Authentisierung und eine Verschlüsselung zwischen Thin Access Point und WLAN Controller. Auf diese Weise kann das System vor einem unberechtigten Zugriff auf einen Access Point oder auf die zwischen Access Point und WLAN Controller ausgetauschten Kontrolldaten geschützt werden. Weiterhin ist das Risiko reduziert, dass ein Access Point mit unsicherer Default-Konfiguration versehentlich im Netz installiert ist. Allerdings muss an dieser Stelle darauf hingewiesen werden, dass bei CAPWAP eine Verschlüsselung der Nutzdaten zwischen Thin Access Point und WLAN Controller nur eine optionale Funktion darstellt, die aktuell nur von wenigen Produkten unterstützt wird.

- Die Zentralisierung von Sicherheitsfunktionen im WLAN Controller kann zu einer Leistungsverbesserung beitragen. Moderne Sicherheitsmechanismen für größere WLAN nutzen IEEE 802.1X für die Authentisierung und für die Verteilung von Sitzungsschlüsseln (siehe Kapitel A.2.4). Bei jedem Wechsel einer Funkzelle würde IEEE 802.1X eine erneute Authentisierung anstoßen. Dieser Aufwand kann erheblich reduziert werden, wenn die Authentisierung zentral auf dem WLAN Controller, der ja mehrere Thin Access Points (d.h. Funkzellen) bedient, durchgeführt wird.

- Durch die genannten Tunnelmechanismen wird auch die Kommunikation zwischen Endgeräten zunächst zum WLAN Controller geleitet und kann dort gefiltert werden. Dies erschwert Angriffe von einem Endgerät auf ein anderes Endgerät.

---

4 Auf Layer 3 bedingt ein Handover in ein anderes IP-Subnetz den Wechsel der IP-Adresse des WLAN-Endgerätes. Durch diesen Adresswechsel verliert der Client aber alle Kommunikationsbeziehungen, die auf seiner alten IP-Adresse beruhten. Dies macht gegebenenfalls den Neustart einer Anwendung oder sogar den Neustart des gesamten Client-Systems notwendig.

5 RFC steht für Request for Comments.

A.1.4 Mesh-Netze

Allgemein grenzen sich Mesh-Netze, die aktuell in IEEE 802.11s standardisiert werden, von einem traditionellen Infrastruktur-WLAN durch Benutzung der Luftschnittstelle zur Kommunikation zwischen Access Points ab. Die Access Points verfügen also nicht mehr grundsätzlich über eine kabelgebundene LAN-Anbindung. Stattdessen wird die Anbindung drahtlos per WLAN bereitgestellt. Die entsprechenden Access Points werden als Mesh Access Points (MAPs) bezeichnet. Die Funkvernetzung zwischen MAPs wird auch als Wireless Backhaul bezeichnet.

Zur Identifikation des Wireless Backhaul dient ein dem Mesh-Netz spezifisch zugeordneter SSID, der sogenannte Mesh SSID. Hierüber können die MAPs den Wireless Backhaul identifizieren und das Mesh-Netz aufbauen. Innerhalb des Wireless Backhaul stellt jeder MAP einen Knotenpunkt dar und sendet den Mesh SSID aus.

Bei der Kommunikation der MAPs untereinander ist wesentlich, dass Pakete auch über mehrere MAPs geleitet werden können (d.h. über mehrere sogenannte Hops), um das Ziel zu erreichen. Innerhalb dieser vermaschten Struktur findet Routing auf MAC-Ebene mit Hilfe zur Verfügung stehender Informationen über die Pfadkosten statt (Mesh Routing). Die hierbei berücksichtigten Informationen sind beispielsweise die verwendbaren Datenraten und die Anzahl der Hops zum Ziel. Als Koppelelemente in das kabelbasierte LAN kommen dedizierte Access Points mit einer LAN-Anbindung zum Einsatz, sogenannte Root Access Points (RAPs). MAPs assoziieren sich (teilweise über weitere Hops) an einem RAP und bilden so ein Mesh-Netz.

Neben der Funktion als Knotenpunkt innerhalb des Mesh-Netzes können MAPs auch für WLAN-Endgeräte einen Netzzugang zur Verfügung stellen. Dabei repräsentieren sie zum Endgerät einen Access Point analog zum traditionellen Infrastruktur-Modus. Aus dem Blickwinkel des Endgeräts ist die Mesh-Funktion somit transparent.

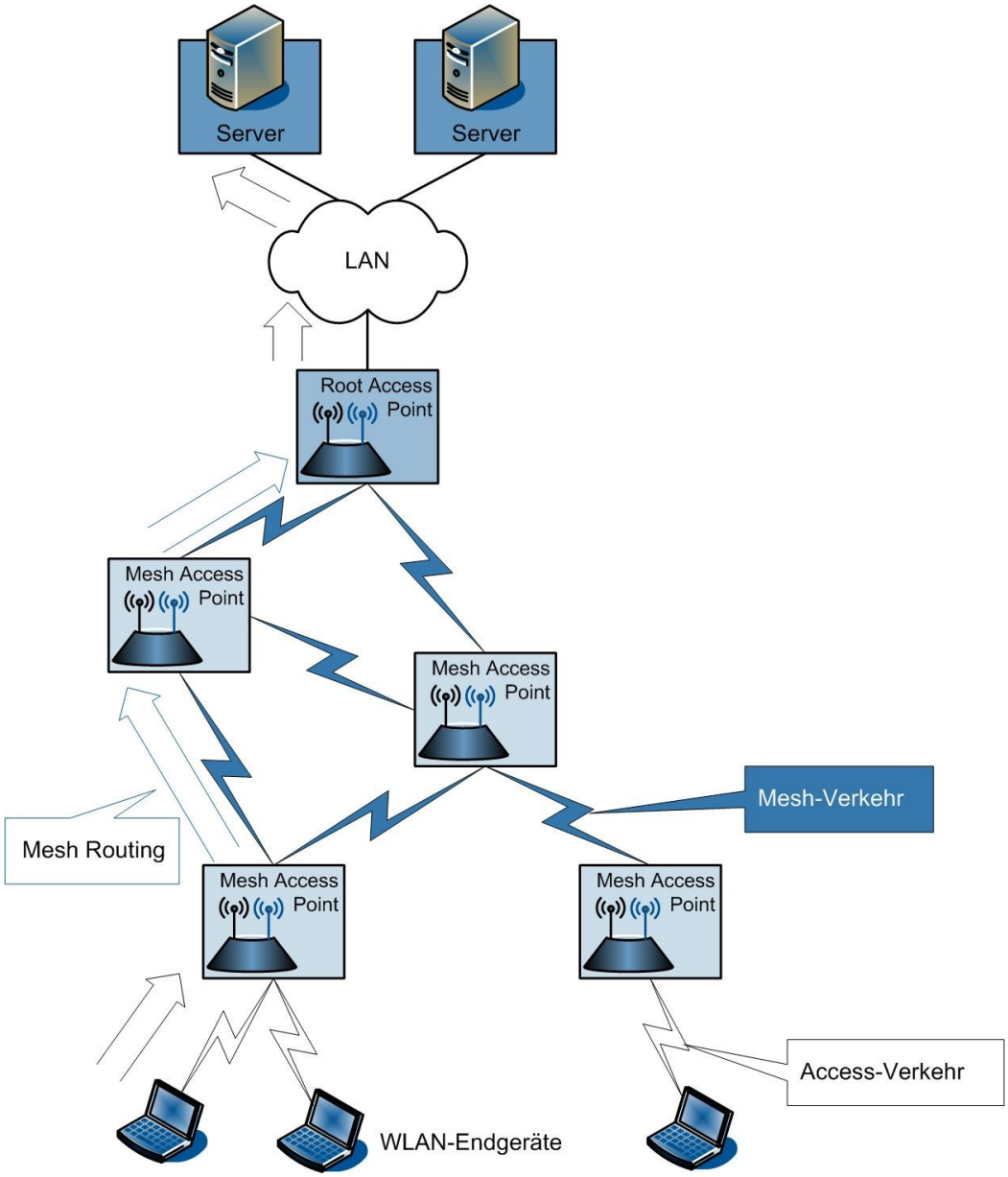
Insgesamt sind in einem Mesh-Netz zwei Typen von Kommunikationsverkehr zu unterscheiden:

- Mesh-Verkehr: Kommunikation zwischen MAPs
- Access-Verkehr: Kommunikation zwischen WLAN-Clients und MAPs

Die Trennung von Mesh-Verkehr und Access-Verkehr erfolgt oft durch die Nutzung unterschiedlicher Frequenzbereiche, beispielsweise könnte der Bereich bei 2,4 GHz für den Access-Verkehr und der 5-GHz-Bereich für den Mesh-Verkehr vorgesehen werden.

Die allgemeine Netztopologie ist in Abbildung A-4 zusammengefasst. Die Funkvernetzung von MAPs kann auch zur LAN-Kopplung (siehe Abbildung A-2) genutzt werden. Hauptgrund für die Verwendung der Mesh-Netze liegt in einen vergleichsweise kostengünstigen Aufbau des Netzes, falls der Versorgungsbereich kabeltechnisch nur schwer zu erschließen ist.

Abbildung A-4: Mesh-Topologie



A.1.5 Spezifische Anwendungen von WLAN

Folgende Anwendungsbereiche haben sich für WLAN entwickelt, die spezielle Anforderungen an Aufbau und Absicherung stellen:

- Voice over IP über WLAN
- Hotspots und der technologisch verwandte Bereich des Gastzugangs
- WLAN im Industriebereich

A.1.5.1 Voice over IP über WLAN

Für die Übertragung von Sprache mittels IP-Protokoll (Voice over IP, VoIP) über WLANs ist der ursprünglich in der Version des Standards von 1999 spezifizierte Kanalzugriff nicht zufriedenstellend geeignet. Der Grund ist zunächst, dass der Kanalzugriff in einem WLAN nach IEEE 802.11 ein zufallsgesteuerter Mechanismus ist, der weder eine Priorisierung unterschiedlicher Verkehrsklassen noch eine explizite Bandbreitenreservierung vorsieht. Als Konsequenz ist die Antwortzeit in einem WLAN nach IEEE 802.11 stets starken Schwankungen unterworfen. Diese Schwankungen sind neben der Qualität des Funkkanals abhängig von der Anzahl der Clients, die an einem Access Point assoziiert sind, und vom Verkehrsverhalten (also von den Anwendungen) dieser Clients.

Für die Übertragung von Sprache und anderen Daten, die höhere Anforderungen an das Antwortzeitverhalten haben, ist der Kanalzugriff daher mit IEEE 802.11e um Mechanismen zur Zusicherung von Dienstgüte (Quality of Service, QoS) erweitert worden. Auf einem Draft zu IEEE 802.11e basiert der Industriestandard Wi-Fi Multimedia (WMM) des Herstellerkonsortiums Wi-Fi Alliance, nach dem diverse WLAN-Produkte zertifiziert sind. Das Kernelement von IEEE 802.11e und WMM ist die abwärtskompatible Erweiterung des Kanalzugriffs um einen Priorisierungsmechanismus. Der grundsätzliche Zufallsmechanismus des Kanalzugriffs in WLANs bleibt aber erhalten. Es werden folgende Prioritätsklassen unterschieden: Voice Priority als höchste Priorität, gefolgt von Video Priority, dann Best Effort Priority und schließlich Background Priority.

Wird VoIP in einem flächendeckenden WLAN, bestehend aus mehreren überlappenden Funkzellen (Access Points) genutzt, bestehen hohe Anforderungen an den Zellwechsel (Handover). Gewisse Ausfallzeiten der Verbindung sind bei einem Handover unvermeidbar. Für VoIP müssen sich diese Ausfallzeiten in tolerablen, d.h. kaum wahrnehmbaren Grenzen bewegen. Standardisierte Handover-Mechanismen liegen mit Verabschiedung von IEEE 802.11r erst seit 2008 vor. IEEE 802.11r spezifiziert insbesondere ein für die Mobilität optimiertes Schlüssel-Management für IEEE 802.1X. Auf diese Weise kann die aufwendige Reauthentisierung bei einem Handover entfallen.

WLAN-Telefone sind seit geraumer Zeit am Markt verfügbar und werden als Alternativsystem zu DECT (Digital Enhanced Cordless Telecommunications) positioniert. WLAN-Telefone haben im Vergleich zu DECT derzeit noch einen deutlich höheren Stromverbrauch.

Moderne Mobiltelefone für GSM/UMTS haben oft neben Bluetooth auch eine WLAN-Schnittstelle. Wenn auf einem solchen Mobiltelefon (als Smartphone bezeichnet) eine VoIP-Anwendung (Softphone) installiert wird, kann grundsätzlich auch über WLAN telefoniert werden, wenn eine geeignete Anbindung an ein Telekommunikationssystem besteht.

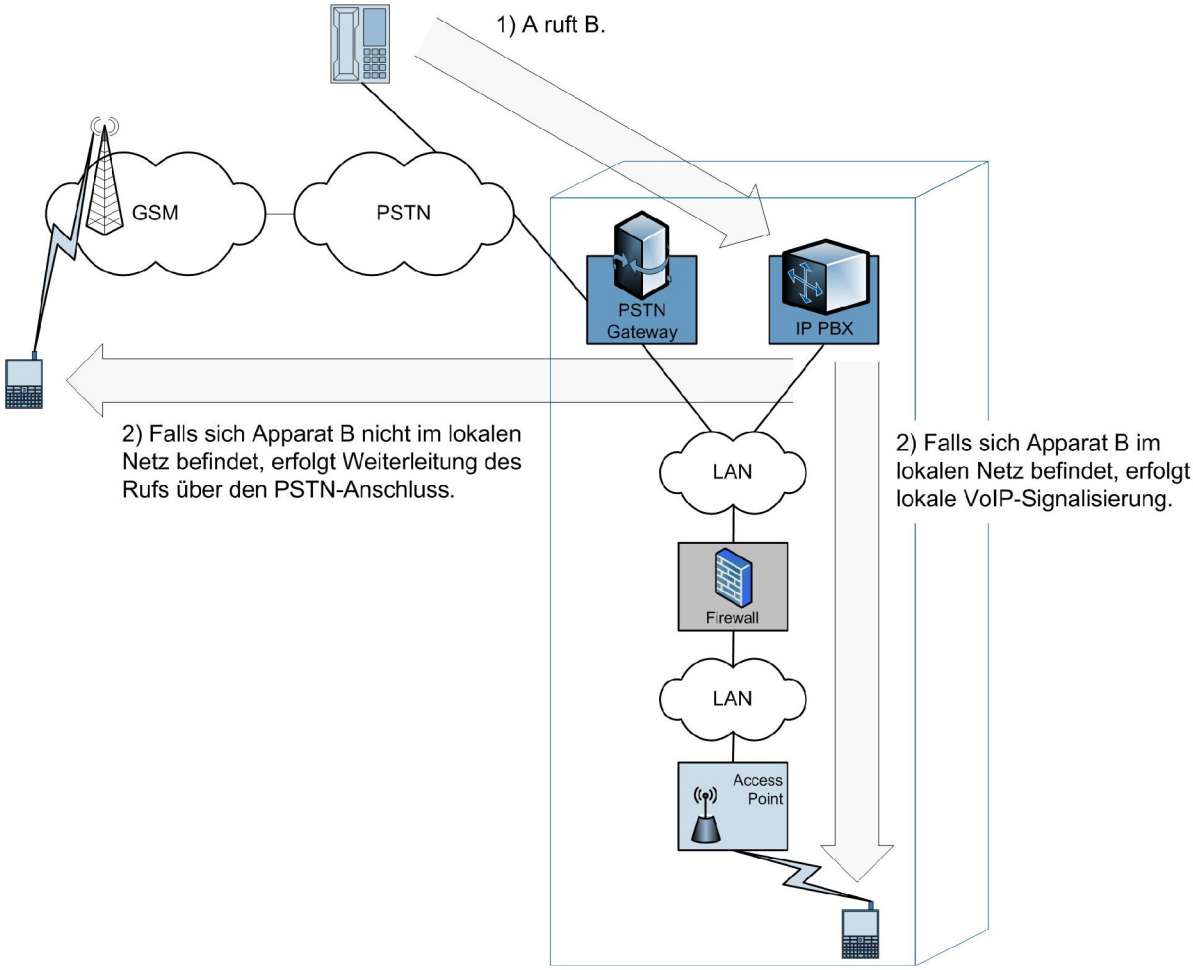
Unter Fixed Mobile Convergence (FMC) wird allgemein eine Verbindung zwischen einem Festnetz und einem Mobilfunknetz verstanden, die netzübergreifend Leistungsmerkmale zu einem einheitlichen Dienst integriert. Ein typisches Beispiel ist die Erreichbarkeit unter einer einzigen Rufnummer im Festnetz und im Mobilfunknetz. Dabei erfolgt eine Anbindung von GSM- bzw. UMTS-Mobiltelefonen an eine lokale TK-Anlage derart, dass der Teilnehmer einerseits am Mobiltelefon unter seiner Festnetznummer erreichbar ist und andererseits auf die vom Festnetzanschluss gewohnten Leistungsmerkmale zurückgreifen kann.

Bei Verwendung eines Smartphones mit einem Softphone gestatten es manche FMC-Lösungen, dass sich das Endgerät im Empfangsbereich des heimatlichen WLAN automatisch in dieses Netz einbucht und die Sprachkommunikation per VoIP automatisch über WLAN geführt wird. Bewegt sich das Mobiltelefon aus dem Abdeckungsbereich des WLAN hinaus, wird wieder über GSM/UMTS kommuniziert (siehe Abbildung A-5). Dabei kann auch eine nahtlose Gesprächsübergabe (Handover) zwischen WLAN und GSM/UMTS realisiert werden.

Weitere Informationen zur Verwendung von WLAN in der Telekommunikation und zum Themenbereich FMC können der „Technischen Leitlinie Sichere TK-Anlagen“ des BSI entnommen werden (sie-

he [TLSTK08]). Sicherheitsaspekte bei der Nutzung öffentlicher Mobilfunknetze (inklusive der Absicherung mobiler Endgeräte) werden in der Broschüre „Öffentliche Mobilfunknetze und ihre Sicherheitsaspekte“ analysiert (siehe [ÖMS08]).

Abbildung A-5: Rufvermittlung bei einer FMC-Lösung



A.1.5.2 Hotspots

Neben der Erweiterung der LAN-Infrastruktur im betrieblichen und privaten Umfeld haben sich öffentliche WLANs (Hotspots) als eine Nutzungsform der WLAN-Technik etabliert.

Für den Aufbau einer Hotspot-Lösung sind die Bereiche Absicherung des Hotspots gegen einen unautorisierten Zugang, Teilnehmerverwaltung, Authentisierung des Teilnehmers dem Netz gegenüber sowie Zahlungsabwicklung und Abrechnung zu betrachten. Da Hotspot-Anbieter im Sinne des Telekommunikationsgesetzes (TKG) als Telekommunikationsdienstleister auftreten, sind unter anderem die Auflagen bzgl. Sicherheit der Abrechnungs- und Benutzerdaten (Datenschutz, Speicherung von Verbindungsdaten) zu berücksichtigen (siehe [TKG04]).

Ein Nutzer, der sich an einem Hotspot anmelden möchte, führt zunächst eine Assoziierung des Endgeräts an einem entsprechenden Access Point des Hotspot durch. In der Regel erfolgt keine Verschlüsselung auf der Luftschnittstelle, um dem Endgerät einen möglichst unproblematischen Netzzugang zu ermöglichen. Eine IP-Adresse erhält das Endgerät automatisch über das Dynamic Host Configuration Protocol (DHCP). Wenn die Netzverbindung aufgebaut ist, startet der Nutzer einen Web-Browser und wird automatisch zur Startseite des Hotspot-Systems umgeleitet. Hier werden die Zahlungs- und Zu-

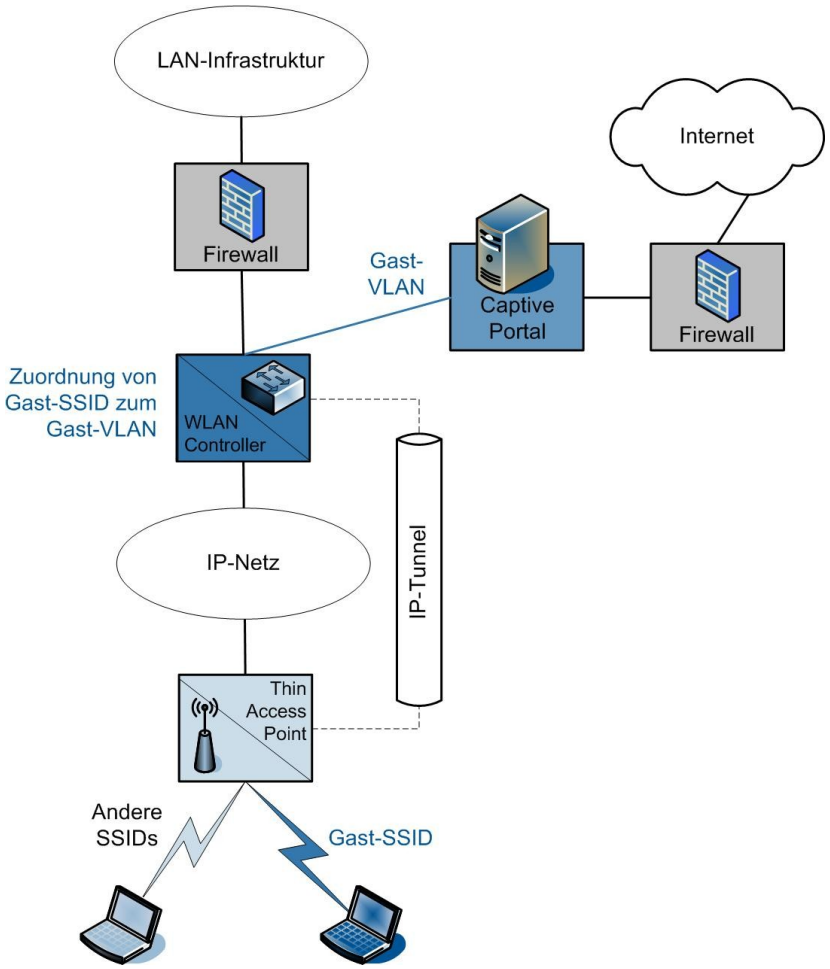
gangsmodalitäten geregelt. Die Zugangskontrolle an einem Hotspot erfolgt in den meisten Fällen durch Angabe eines Passworts in einem Feld einer Web-Applikation des Hotspot-Systems.

Leider ist bis heute keine einheitliche systemübergreifende Authentisierung, Anmeldung und Abrechnung für Hotspot-Systeme realisiert. Durch den Einsatz eines Clearing House oder durch direkte Kooperationen von Dienstanbietern ist dieses Problem inzwischen zwar deutlich gemildert, von der Umsetzung eines internationalen Standards ist man aber noch entfernt. Für größere Hotspot-Systeme hat sich jedoch der Trend durchgesetzt, ein GSM- bzw. UMTS-Netz für Authentisierung und Abrechnung zu nutzen, da diese elementaren Funktionen hier bereits implementiert sind.

A.1.5.3 Gastzugang

Bei dem Gastzugang soll über WLAN den Besuchern eines Unternehmens oder einer Behörde ein eingeschränkter Netzzugang (typischerweise reduziert auf einen reinen Zugang zum Internet) über die eigene Infrastruktur des Unternehmens bzw. der Behörde zur Verfügung gestellt werden. Für Projektgruppen, in denen firmen- bzw. behördenübergreifend zusammengearbeitet wird, bedeutet ein solcher WLAN-basierter Gastzugang zum Internet oft eine erhebliche Arbeitserleichterung. Über den Gastzugang kann ein Besucher dann beispielsweise per VPN auf die eigene Infrastruktur zugreifen.

Abbildung A-6: Exemplarischer Aufbau eines Gastzugangs in einem Controller-basierten Design



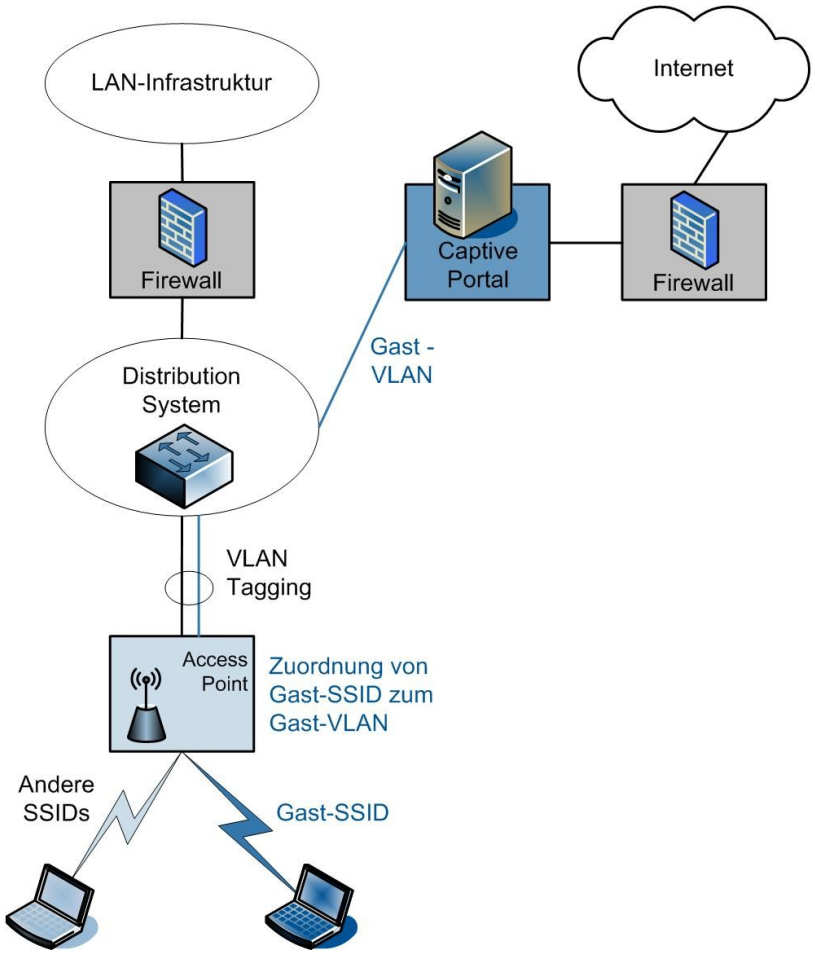
Dieser Zugang sollte natürlich zeitlich befristet und authentisiert werden. Die dabei eingesetzten Mechanismen basieren auf den Konzepten, die für WLAN-Hotspots eingesetzt werden. Kernelement der Infrastruktur für den Gastzugang ist ein Gateway, das den gesamten Verkehr eines Gast-Client abfängt

(Proxy-Funktion). An dem Gateway erfolgt eine Authentisierung mit Nutzername und Passwort. Dabei wird eine Browser-Anfrage eines noch nicht authentisierten Gastes zunächst auf eine Anmeldeseite geleitet (Redirect). Auf dieser Seite werden Nutzername und Passwort angegeben und bei einer positiven Prüfung wird der Gast auf die ursprünglich gewünschte Internet-Seite geleitet. Da ein nicht authentisierter Nutzer automatisch auf eine spezielle Web-Seite weitergeleitet wird, heißt dieser Mechanismus allgemein Captive Portal. Über das Captive Portal erfolgt auch eine eventuelle Bandbreiten- und Volumenbegrenzung für den Gastzugang.

Eine solche Lösung für einen Gastzugang kann Bestandteil der eigenen Infrastruktur als Komponente im WLAN Controller sein oder als separate Appliance (wie in Abbildung A-6 gezeigt) aufgebaut werden. Typischerweise wird der gesamte Verkehr der Gäste netztechnisch von anderen Nutzern getrennt (sogenanntes Gast-VLAN). Das Gast-VLAN kann aber auch (z.B. per VPN) zu einem Provider ausgekoppelt werden, der dann das Captive Portal und den Internet-Zugang bereitstellt.

Ein Gastzugang kann auch mit traditionellen autonomen Access Points aufgebaut werden, wie in Abbildung A-7 gezeigt. Die Trennung zwischen Gast-SSID und den anderen SSIDs für betriebliche WLAN-Anwendungen erfolgt in diesem Fall am Access Point.

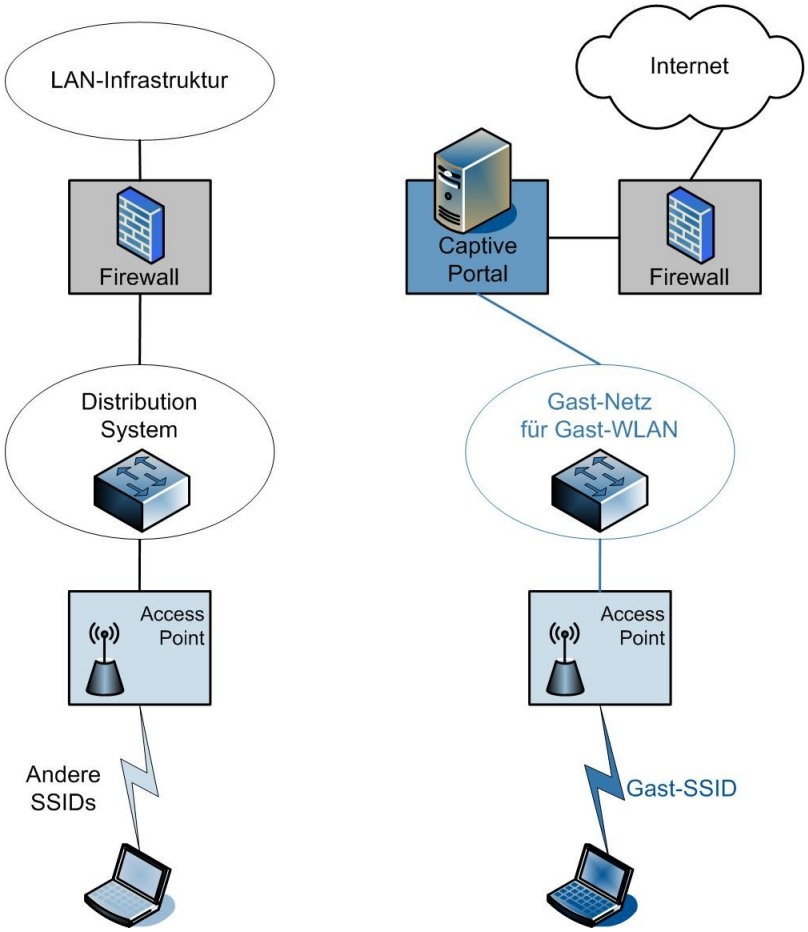
Abbildung A-7: Exemplarischer Aufbau eines Gastzugangs mit autonomen Access Points



Grundsätzlich ist auch eine vollständige physikalische Trennung von betrieblichem WLAN und einem WLAN für den Gastzugang möglich, wie in Abbildung A-8 illustriert. Dies ist aus einer Sicherheitsperspektive die beste, jedoch auch die teuerste Alternative. Dabei muss außerdem beachtet werden, dass es zu Interferenzen zwischen den Access Points für den Gastzugang und den Access Points für das betriebliche WLAN kommen kann, wenn (insbesondere bei 2,4 GHz) eine Überlappung der von

beiden WLANs aufgespannten Funkzellen besteht. Hierdurch ist eine deutlich aufwendigere Planung erforderlich.

Abbildung A-8: Physikalische Trennung des Gastzugangs



A.1.5.4 WLAN im Industriebereich

WLANs werden nicht nur im Logistikbereich (z.B. Barcode Scanner, Gabelstapler mit Auftragsvergabe per WLAN) und für produktionsnahe Anwendungen (z.B. drahtlose Bedienfelder), sondern auch in der Automatisierungstechnik eingesetzt. Hier werden unter anderem fahrerlose Transportsysteme, Einschienenhängebahnen, Kräne oder Roboter über WLAN gesteuert. Neben Anforderungen an die Robustheit der WLAN-Geräte hinsichtlich des Einflusses hoher Temperaturschwankungen, Wasser und Staub müssen Schwankungen der Antwortzeit und Paketverluste bei der WLAN-Übertragung besonders berücksichtigt werden. Weiterhin bestehen in Industrieumgebungen oft andere technische und organisatorische Rahmenbedingungen, die den Einsatz von Sicherheitsmechanismen erschweren können. Beispielsweise kann es vorkommen, dass die eingesetzten Spezialgeräte keine Authentisierung nach dem Stand der Technik unterstützen oder die Konfiguration von neuem Schlüsselmaterial mit einem erheblichen Aufwand verbunden ist.

A.1.5.5 Ortung und Positionsbestimmung per WLAN

Mit WLAN-Technik kann auch eine Ortung und Positionsbestimmung von WLAN-Geräten vorgenommen werden.

Dabei können zwei Perspektiven unterschieden werden: Unter Positionsbestimmung wird – analog zum Global Positioning System (GPS) – der Blickwinkel des Endgeräts verstanden („Wo bin ich?“). Bei der Ortung geht es um die Feststellung der Position eines WLAN-Geräts aus der Perspektive der Infrastruktur („Wo ist das WLAN-Gerät?“). Je nach Aufbau der Anwendung hängen Ortung und Positionsbestimmung eng miteinander zusammen.

Teilweise handelt es sich bei der Ortung um Spezialsysteme, die WLAN-ähnlich bei 2,4 GHz operieren, aber keine reine WLAN-Technik verwenden. In Abhängigkeit vom Einsatzszenario und der geforderten Genauigkeit können spezielle Endgeräte (sogenannte Tags) oder normale PCs genutzt werden. Grundsätzlich ist auch eine Ortung von WLAN-Geräten möglich, ohne dass auf dem Gerät eine spezielle Software zur expliziten Unterstützung der Ortungsanwendung abläuft.

Systeme zur groben Ortung von WLAN-Geräten sind inzwischen ein üblicher Bestandteil von WLAN-Controller- und WLAN-Management-Systemen. Für eine feinere Ortung beispielsweise mit einer Genauigkeit im Meterbereich sind die bereits erwähnten Spezialsysteme verfügbar.

Neben Anwendungen im Bereich der Logistik zur Bestimmung des aktuellen Aufenthaltsorts einer WLAN-Station (z.B. zur Optimierung einer Auftragsvergabe) liegen die Anwendungen im Bereich des Netz- und des Security Management. Eine typische Anforderung ist die Ortung eines fehlerhaften oder fremden WLAN-Geräts auf einem Grundriss des WLAN-Versorgungsbereichs. Solche Anwendungen gestatten grundsätzlich auch die Erstellung von Bewegungsprofilen und betreffen daher auch den Datenschutz.

Eine weitere Möglichkeit zur Positionsbestimmung durch ein WLAN-Endgerät liegt in der Auswertung von SSIDs und Signalpegeln der Access Points in der näheren Umgebung. Dabei erfolgt ein Abgleich der gemessenen Daten mit einem über das WLAN-Endgerät zugänglichen Kartenmaterial („Der Access Point x ist an Position y installiert.“) und einer daraus resultierenden Abschätzung der eigenen Position.

A.2 Sicherheitsmechanismen

In diesem Kapitel werden die wesentlichen Sicherheitsmechanismen vorgestellt, die zum Schutz der WLAN-Übertragung beitragen. Den Schwerpunkt bildet die Vorstellung der Ergänzung IEEE 802.11i (bzw. der entsprechenden Spezifikationen der Wi-Fi Alliance) und der Authentisierung über IEEE 802.1X. Weitere Sicherheitsmechanismen und detailliertere Ausführungen können dem Teil 1 der Technischen Richtlinie Sicheres WLAN entnommen werden (siehe [TR-S-W1]).

A.2.1 Netzwerkname (SSID)

Der Service Set Identifier (SSID) dient der Identifikation eines ESS, d.h. eines WLAN. Bei der Anmeldung an ein WLAN und beim Handover zwischen zwei benachbarten Funkzellen dient der SSID dazu, den nächsten Access Point zu finden. Die maximale Länge eines SSID beträgt 32 Byte. Der SSID wird auf Endgerät und Access Point konfiguriert. Die Endgeräte-Software unterstützt meist verschiedene Profile, die es erlauben, mehrere WLANs (d.h. mehrere SSIDs) zu konfigurieren.

Die Übertragung des SSID geschieht auf Layer 2 als Parameter in einem speziellen, in regelmäßigen Abständen übertragenen Paket, dem sogenannten Beacon Frame. Dieser Mechanismus wird auch als SSID Broadcast bezeichnet. In dem Beacon Frame übermittelt ein Access Point neben dem SSID die wesentlichen Übertragungsparameter inklusive der Sicherheitseinstellungen, wie z.B. das zu verwendende Verschlüsselungsverfahren.

Alternativ kann ein Endgerät explizit erfragen, ob ein Access Point mit einem gewissen SSID erreichbar ist. Hierzu sendet das Endgerät unter Angabe des gewünschten SSID ein spezielles Layer-2-Paket (Probe Request) und ein Access Point passender SSID antwortet mit einem Probe-Response-Paket. Verwendet der Client dabei den sogenannten Broadcast SSID (ein SSID der Länge 0), so bedeutet dies, dass der Client mit einem beliebigen Access Point kommunizieren möchte. Sofern es in der Konfiguration eines Access Point nicht unterdrückt wird, antwortet ein Access Point auf ein Probe Request, das einen Broadcast SSID enthält, durch ein Probe-Response-Paket mit dem SSID des Access Point.

Für nicht-öffentliche WLAN sollte an einem Access Point die Antwort auf eine Anfrage mit Broadcast SSID unterdrückt werden.

Da der SSID unverschlüsselt gesendet wird, kann ein Angreifer ihn mit einfachen Mitteln in Erfahrung bringen. Einige Access Points bieten die Möglichkeit, den SSID Broadcast zu unterbinden[6]. Ein Endgerät muss den SSID dann, wie eben beschrieben, explizit erfragen. Bevor die Broadcast-Übertragung des SSID am Access Point unterbunden wird, sollte überprüft werden, ob alle Endgeräte mit dieser Einstellung zurechtkommen, denn dies kann für manche Systeme zu Beeinträchtigungen in der Netzauswahl kommen. Hierzu gehören z.B. Microsoft Windows-XP-Systeme unter Service Pack 2, die über die Funktion Wireless Zero Configuration (WZC) konfiguriert werden.

A.2.2 MAC-Adresse

Jede Netzwerkkarte verfügt über eine eindeutige Hardware-Adresse, die im Normalfall als MAC-Adresse (Media Access Control Address) verwendet wird. Prinzipiell ist es möglich, an einem Access Point Listen anzulegen, in denen die MAC-Adressen derjenigen Endgeräte eingetragen werden, denen

[6] Es erfolgt weiterhin eine periodische Übertragung durch den Access Point. In dem entsprechenden Paket ist der SSID des WLAN jedoch nicht mehr aufgeführt.

es erlaubt ist, über den Access Point zu kommunizieren. Dieses Prinzip der Zugangssteuerung über eine Liste von MAC-Adressen wird auch als MAC-Adressauthentisierung bezeichnet. Die MAC-Adresslisten müssen manuell gepflegt werden, d.h. der Aufwand wächst generell mit der Anzahl der zugelassenen Adressen.

Die meisten Access Points (bzw. WLAN Controller) unterstützen die Verwendung des Remote Authentication Dial-In User Service (RADIUS, siehe [RFC2865]). Die MAC-Adressen werden dann auf einem zentralen RADIUS-Server gepflegt, und die Access Points fragen über RADIUS nach, ob eine angegebene Adresse verzeichnet ist.

Die Pflege von Adresslisten auf den Access Points ist bereits bei wenigen Endgeräten und Access Points sehr aufwendig. Dies ist meist nur für WLAN im Small-Office-Home-Office-Bereich eine mit vertretbarem Aufwand durchführbare Maßnahme. Für größere WLANs mit vielen Endgeräten sind auch zentrale Listen unter Verwendung von RADIUS nur schwer zu verwalten.

Hinzu kommt, dass eine MAC-Adressauthentisierung nur einen geringen Sicherheitsgewinn liefert.

Für einen Angreifer kann mit nicht nennenswertem Aufwand ein WLAN-Adapter auf eine andere MAC-Adresse umgestellt werden. Vermutet ein Angreifer, dass eine MAC-Adressauthentisierung eingesetzt wird, beobachtet er einfach das WLAN, zeichnet die MAC-Adressen von erlaubten Endgeräten auf und konfiguriert für einen Angriff den eigenen WLAN-Adapter mit einer der aufgezeichneten MAC-Adressen.

Die MAC-Adressauthentisierung kann also lediglich als flankierende Maßnahme gesehen werden, sofern der Aufwand akzeptabel ist.

A.2.3 Wired Equivalent Privacy

Vertraulichkeit, Integrität und Authentizität im WLAN wurden im ursprünglichen Standard IEEE 802.11 ohne die Erweiterung IEEE 802.11i durch einen als Wired Equivalent Privacy (WEP) bezeichneten Mechanismus gesichert. Allerdings ist WEP mittlerweile vollständig kompromittiert und für die Absicherung eines WLAN allein als ungenügend einzustufen, wie im Folgenden noch beschrieben wird.

WEP basiert auf der Stromchiffre RC4, mit der Klardaten paketweise abhängig von einem Schlüssel und einem Initialisierungsvektor (IV) in Chiffratdaten umgewandelt werden. Der Schlüssel ist dabei eine Zeichenkette von wahlweise 40 oder 104 Bit und muss den am WLAN beteiligten Endgeräten sowie dem Access Point vorab zur Verfügung gestellt werden. Dabei wird für das gesamte WLAN ein gemeinsamer Schlüssel verwendet. Der IV wird vom Absender gewählt und sollte für jedes übertragene Datenpaket unterschiedlich sein. Der IV wird dem verschlüsselten Datenpaket unverschlüsselt vorangestellt und über das WLAN übertragen.

Über WEP sollten folgendermaßen die Vertraulichkeit und die Integrität der übertragenen Daten gesichert sowie die Authentisierung des Endgeräts (nicht des Nutzers) durchgeführt werden:

- Vertraulichkeit: Aus dem Schlüssel und dem IV wird ein pseudozufälliger Bitstrom generiert. Die Chiffratdaten ergeben sich, indem die unverschlüsselten Daten bitweise mit dem Bitstrom XOR-verknüpft werden (XOR = exklusives Oder). Beim Empfänger werden die Klartextdaten wiederum aus den Chiffratdaten ermittelt, indem derselbe Bitstrom mit den Chiffratdaten XOR-verknüpft wird.

- Integrität: Für jedes zu übertragene Datenpaket wird eine 32-Bit CRC-Checksumme (Cyclic Redundancy Check) berechnet. Anschließend wird das Datenpaket und die angehängte Checksumme verschlüsselt. Der Empfänger entschlüsselt das Datenpaket und überprüft die Checksumme. Ist die Checksumme korrekt, wird das Datenpaket angenommen, andernfalls wird es verworfen.

Das verwendete Verfahren eignet sich zwar zur Erkennung von Bitfehlern durch Übertragungsstörungen, es ist jedoch für die Abwehr systematischer Paketfälschungen und damit für die Sicherstellung der Integrität ungeeignet.

- Authentisierung: In Verbindung mit der WEP-Verschlüsselung kann zwischen zwei Authentisierungsmodi gewählt werden – „Open“ (hierbei findet keine Authentisierung statt) und „Shared Key“. Für die Authentisierung im „Shared Key“-Modus wird ein Challenge-Response-Verfahren durchgeführt: Der Access Point generiert 128 zufällige Bytes und sendet diese in einem Datenpaket unverschlüsselt an einen Client (Challenge). Der Client verschlüsselt das Datenpaket und sendet es zurück zum Access Point (Response). Der Client hat sich erfolgreich authentisiert, wenn der Access Point die Response zur Challenge entschlüsseln kann. Der Authentisierungsprozess ist nur einseitig – der Access Point muss sich gegenüber den Clients nicht authentisieren. Zum Authentisieren wird derselbe Schlüssel verwendet wie zur Verschlüsselung der Nutzdaten.

WEP verschlüsselt die übertragenen Nutzdaten und die Integritäts-Checksumme. Management- und Steuersignale (Management Frames und Control Frames) werden auf der Funk-Schnittstelle jedoch nicht verschlüsselt.

Die in WEP festgelegte Bereitstellung des Schlüsselmaterials für RC4 hat sich schon vor einiger Zeit als ungenügend erwiesen. Hierzu sei insbesondere auf die Arbeit von Fluhrer, Mantin und Shamir (siehe [FMS01]) hingewiesen, welche die Grundlage für die heute frei verfügbaren Angriffswerkzeuge auf WEP geschaffen hat.

Moderne Werkzeuge können mit einer guten Zuverlässigkeit den eigentlich geheimen WEP-Schlüssel aus aufgezeichneten verschlüsselten Paketen in Minuten zurückrechnen. Hierzu werden unter anderem sogenannte Re-Injection-Angriffe genutzt, die das zur Ermittlung des Schlüssels benötigte Verkehrsvolumen durch eine aktive Aktion des Angreifers aus wenigen aufgezeichneten Paketen künstlich erzeugen. Dabei wird zunächst versucht, aus den verschlüsselten Übertragungen spezielle Pakete z.B. durch einen Längenvergleich zu erraten (etwa einen ARP Request[7]) und aufzuzeichnen. Dieser aufgezeichnete Verkehr wird wieder in das WLAN „injiziert“, der zugrunde liegende Protokollmechanismus wird erneut angestoßen, und Stationen im WLAN antworten (etwa mit einem ARP Response).

Es existieren noch weitere Schwächen in WEP. Beispielsweise gestattet es der in WEP verwendete CRC-Mechanismus, dass Pakete fast beliebig gefälscht werden können, ohne dass die Integritätsprüfung dies bemerkt.

Für die Absicherung eines WLAN ist WEP als ungenügend einzustufen. Ein WLAN muss also stets mit weitergehenden Mitteln abgesichert werden.

A.2.4 IEEE 802.11i

Die Erweiterung IEEE 802.11i entstand, um die aufgetretenen Sicherheitslücken von WEP zu schließen (siehe [IEEE07]). IEEE 802.11i umfasst die Bereiche Verschlüsselung, Authentisierung und Schlüssel-Management.

Da die in IEEE 802.11i verabschiedete Lösung abwärtskompatibel zu WEP sein musste, umfasst sie zwei verschiedene Verschlüsselungsverfahren:

- Temporal Key Integrity Protocol (TKIP) mit Integritätsprüfung Michael

  TKIP ist eine als Temporärlösung aufzufassende abwärtskompatible Lösung, die ursprünglich zur verbesserten Absicherung bereits bestehender WLANs gedacht war.

[7] Das Address Resolution Protocol (ARP) dient zur Ermittlung der MAC-Adresse, an die ein IP-Paket in einer Broadcast-Domäne geschickt werden soll, d.h. der Abbildung einer IP-Adresse auf eine MAC-Adresse.

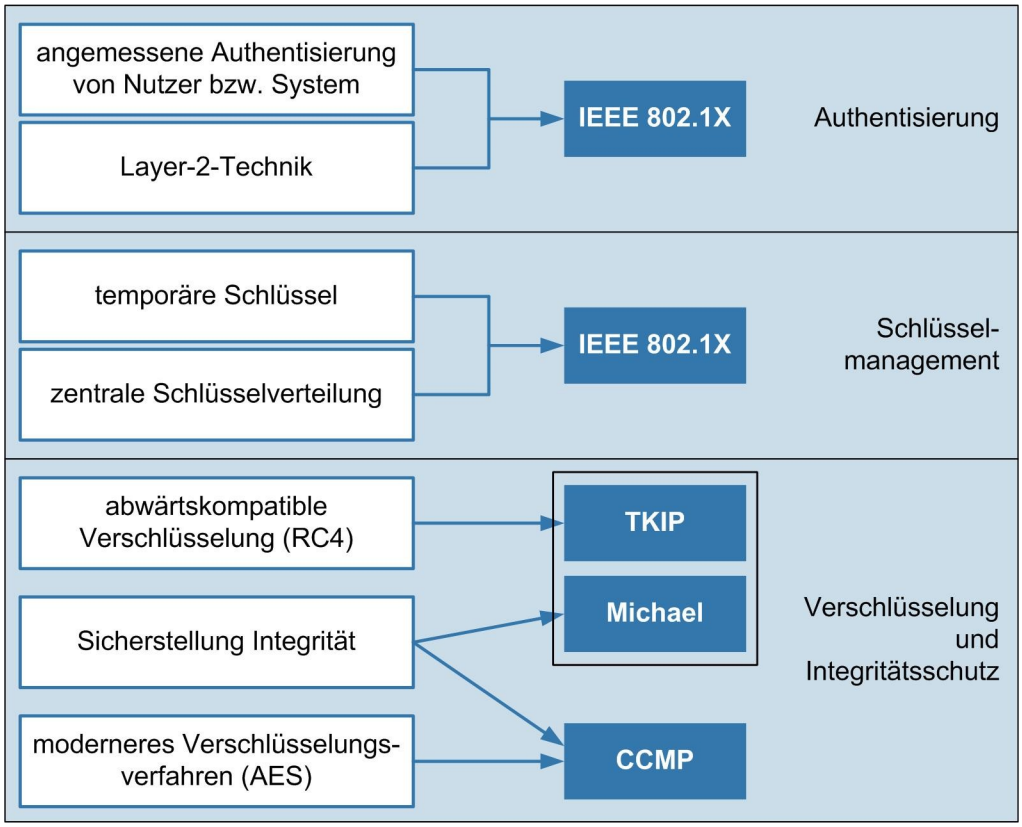
- Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)

  CCMP ist eine langfristige Lösung, die auf dem Advanced Encryption Standard (AES) basiert und eine entsprechende Hardware-Unterstützung erfordert.

Die Authentisierung erfolgt entweder über IEEE 802.1X (in diesem Fall erfolgt das Schlüsselmanagement auch über IEEE 802.1X, siehe Kapitel A.2.4.3) oder implizit über Pre-Shared Keys.

Ein WLAN, das ausschließlich eine durch die in IEEE 802.11i spezifizierten Sicherheitsmechanismen geschützte Kommunikation erlaubt, wird durch den Standard als Robust Security Network (RSN) bezeichnet. Abbildung A-9 zeigt die wesentlichen Bestandteile von IEEE 802.11i im Überblick.

Abbildung A-9: Bausteine von IEEE 802.11i im Überblick



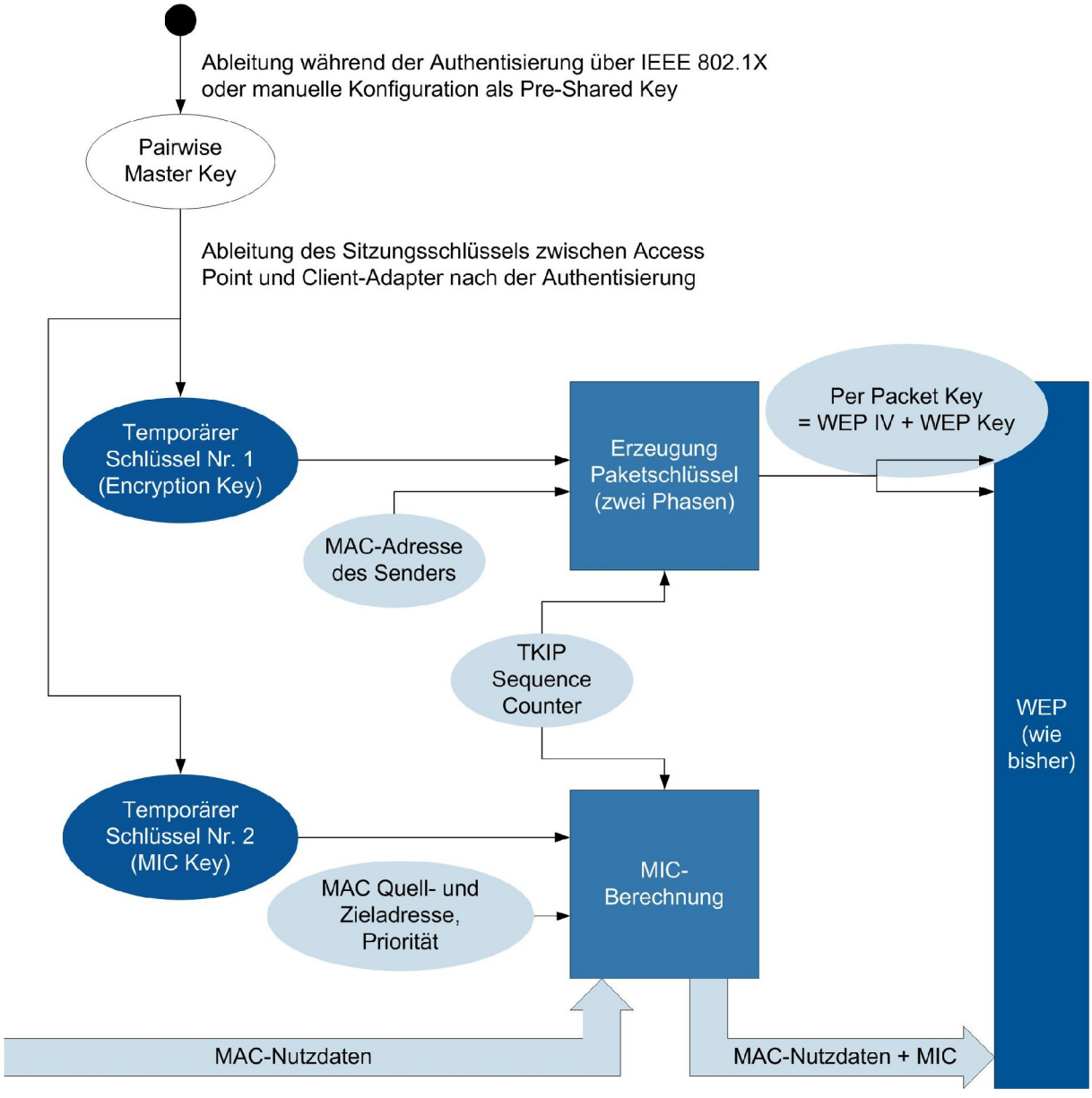
A.2.4.1 TKIP und Michael

Die zu WEP abwärtskompatible Verschlüsselungsmethode ist das Temporal Key Integrity Protocol (TKIP), das die bisher bekannten Schwächen von WEP bei der Auswahl und Erzeugung der Startwerte von RC4 eigentlich beseitigen sollte. Die effektive Schlüssellänge bei TKIP liegt weiterhin bei 104 Bit, da als Basis WEP verwendet wird. In TKIP wird pro Paket ein neuer Schlüssel erzeugt, um die bisher statischen WEP-Schlüssel zu vermeiden. Ein solcher Schlüssel entsteht durch Anwendung einer Hash-Funktion auf einen geheimen symmetrischen Sitzungsschlüssel, den Initialisierungsvektor und eine Paketsequenznummer. Der Sitzungsschlüssel wiederum wird aus einem gemeinsamen Schlüssel – Pairwise Master Key (PMK) genannt – abgeleitet, der entweder als Pre-Shared Key (PSK) auf den WLAN-Systemen voreingestellt ist oder der im Rahmen der Authentisierung eines WLAN-Endgeräts über IEEE 802.1X übermittelt wird (siehe Kapitel A.2.4.2 und A.2.4.4).

Da TKIP auf der gleichen Hardware basiert, die auch WEP nutzt, sind wesentliche Funktionen von TKIP in Software realisiert, wodurch sich bei älteren Geräten gegenüber WEP eine geringe Reduzierung des Datendurchsatzes ergeben kann.

Zur Beseitigung der mangelhaften Integritätsprüfung in WEP wird TKIP durch einen zusätzlichen Message Integrity Check (MIC, bezeichnet als Michael) ergänzt. Dieser berücksichtigt nicht nur die Nutzdaten, sondern auch eine Paketsequenznummer (TKIP Sequence Counter, TSC) sowie die Quell- und Zieladresse des MAC-Pakets und wird verschlüsselt übertragen. Beim Empfänger wird dann nach weitgehendem Ausschluss von zufälligen Übertragungsfehlern (korrekte CRC und passender Initialisierungsvektor) durch MIC die Integrität des Datenpakets bzw. des Absenders überprüft. Werden dabei innerhalb von 60 Sekunden mehr als zwei Pakete empfangen, deren MIC-Überprüfung fehlschlägt, geht TKIP von einem Angriff aus und blockiert für 60 Sekunden die Kommunikation, um im Anschluss neues Schlüsselmaterial auszuhandeln. Außerdem werden Replay-Attacken durch den TSC erschwert. Erkannte Angriffsversuch werden dem Netzmanagement gemeldet.

Abbildung A-10: Aufbau von TKIP (vereinfacht)



Im November 2008 wurden deutliche Schwächen von TKIP bekannt (siehe [BeTe09]). Dabei wurde eine bereits seit 2005 bekannte Angriffsform gegen WEP optimiert. Unter gewissen Rahmenbedingungen ist es damit möglich, einen mit TKIP verschlüsselten Verkehr ohne Kenntnis des Schlüssels zu entschlüsseln.

Der Angriff basiert unter anderem darauf, dass der Angreifer im Rahmen einer intelligenten Heuristik zur Prüfung, ob er einen Teil eines Pakets bereits richtig entschlüsselt hat, auch manipulierte Pakete an den Access Point schickt, die der Access Point nur dann akzeptiert, wenn die im Paket enthaltene Prüfsumme zum Paket passt. Verwirft der Access Point das Paket, weiß der Angreifer, dass er noch nicht richtig geraten hat und setzt den Prozess fort.

Gegen diese bekannte Angriffsform setzt TKIP (bzw. Michael) eigentlich die eben beschriebenen spezifischen Abwehrmaßnahmen ein. Diese werden aber in der optimierten Angriffsvariante umgangen, indem mit geringerer Intensität gesendet wird und so die Schranke von 60 Sekunden eingehalten wird sowie indem die Priorisierungsfunktion von WMM bzw. IEEE 802.11e ausgenutzt wird. Dabei erfolgt eine Aufteilung der Übertragung in verschiedene Prioritätsklassen und damit im Prinzip in logische Kanäle. Der Angreifer verwendet einfach unterschiedliche Prioritätsklassen in der Hoffnung, dass der TSC im Paket nicht kleiner oder gleich des für die entsprechende Prioritätsklasse im Access Point erwarteten TSC-Werts ist.

Der Angriff dauert in seiner ursprünglichen Fassung recht lang und auf dem Access Point muss WMM bzw. IEEE 802.11e aktiviert sein. Das Zeitintervall, in dem neues Schlüsselmaterial zwischen den Kommunikationspartnern ausgehandelt wird (Rekeying Interval), spielt eine besondere Rolle. Inzwischen wurde der Angriff über ein Man-in-the-Middle-Konzept weiter verfeinert. WMM muss dabei nicht mehr verwendet werden, und der Angriff benötigt nur noch in etwa eine Minute.

Auch wenn es sich hier nicht um die Angriffsqualität handelt, die gegen WEP möglich ist, muss davon ausgegangen werden, dass weitere Optimierungen und ggf. sogar weitere Schwachstellen bekannt werden. Daher wird von TKIP abgeraten und der Einsatz des im Folgenden beschriebenen CCMP empfohlen.

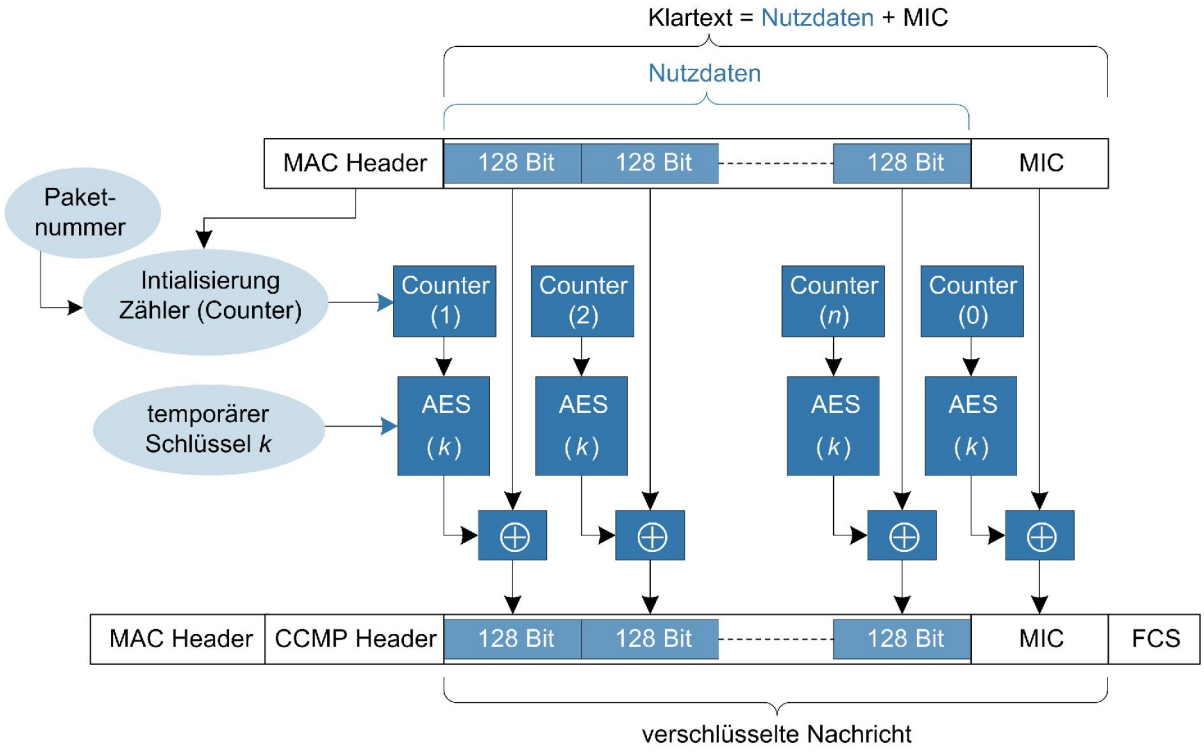
A.2.4.2 CCMP

Im zweiten langfristig zu nutzenden Verschlüsselungsverfahren von IEEE 802.11i wird der Advanced Encryption Standard (AES) im speziellen Modus Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) genutzt. Hierbei wird nicht direkt der Klartext mit AES verschlüsselt, sondern der Wert eines Zählers. Das eigentliche Verschlüsselungsergebnis entsteht dann aus der XOR-Verknüpfung eines Blocks des Klartextes mit dem AES-verschlüsselten Zähler, wie in Abbildung A-11 illustriert. Die Schlüssellänge beträgt 128 Bit. Die Bereitstellung des Schlüssels erfolgt über IEEE 802.1X oder über einen manuell konfigurierten Pre-Shared Key (siehe Kapitel A.2.4.2 und A.2.4.4). Die Integritätsprüfung geschieht durch die in CCMP genutzte Methode Cipher Block Chaining.

Der Einsatz von CCMP ist dringend zu empfehlen, da AES auch heute noch ein Verfahren auf dem Stand der Technik darstellt[8] und außerdem alle wesentlichen Elemente des Verschlüsselungsverfahrens in Hardware realisiert sind.

[8] In diesem Zusammenhang wird darauf hingewiesen, dass im Frühjahr/Sommer 2009 die Kryptoanalyse von AES gewisse Fortschritte erzielt hat (siehe [BDKKS09]). Die Ergebnisse haben jedoch noch keine praktische Relevanz. Weiterhin betreffen die gefundenen Schwachstellen die Variante von AES mit 256 Bit Schlüssellänge und nicht AES mit einer Schlüssellänge von 128 Bit, wie in WLAN genutzt. Die Empfehlung zur Nutzung von CCMP gemäß IEEE 802.11i gilt für WLAN daher bis auf Weiteres uneingeschränkt.

Abbildung A-11: Verwendung von AES in IEEE 802.11i (vereinfacht)



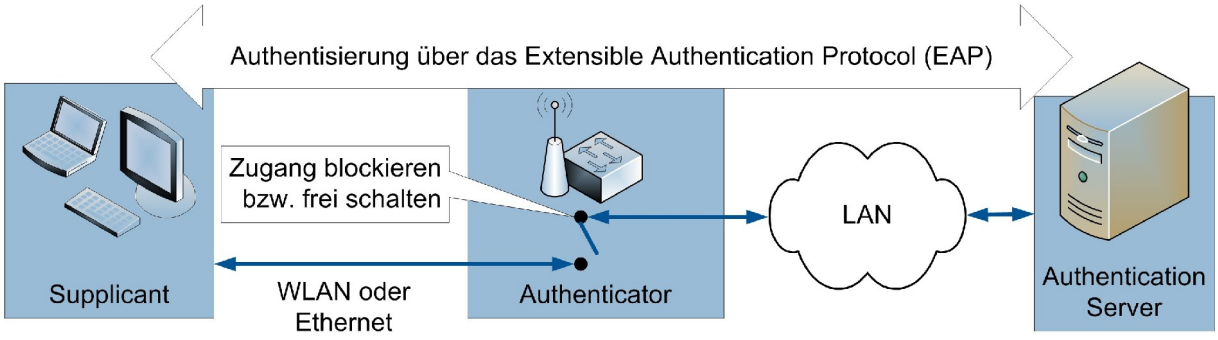
A.2.4.3 IEEE 802.1X

IEEE 802.1X spezifiziert eine standardisierte Methode zur portbasierten Netzwerkzugangskontrolle für kabelbasierte LAN und für WLAN (siehe [IEEE04-1X]).

IEEE 802.1X spezifiziert verschiedene Rollen der beteiligten Netzelemente (siehe Abbildung A-12):

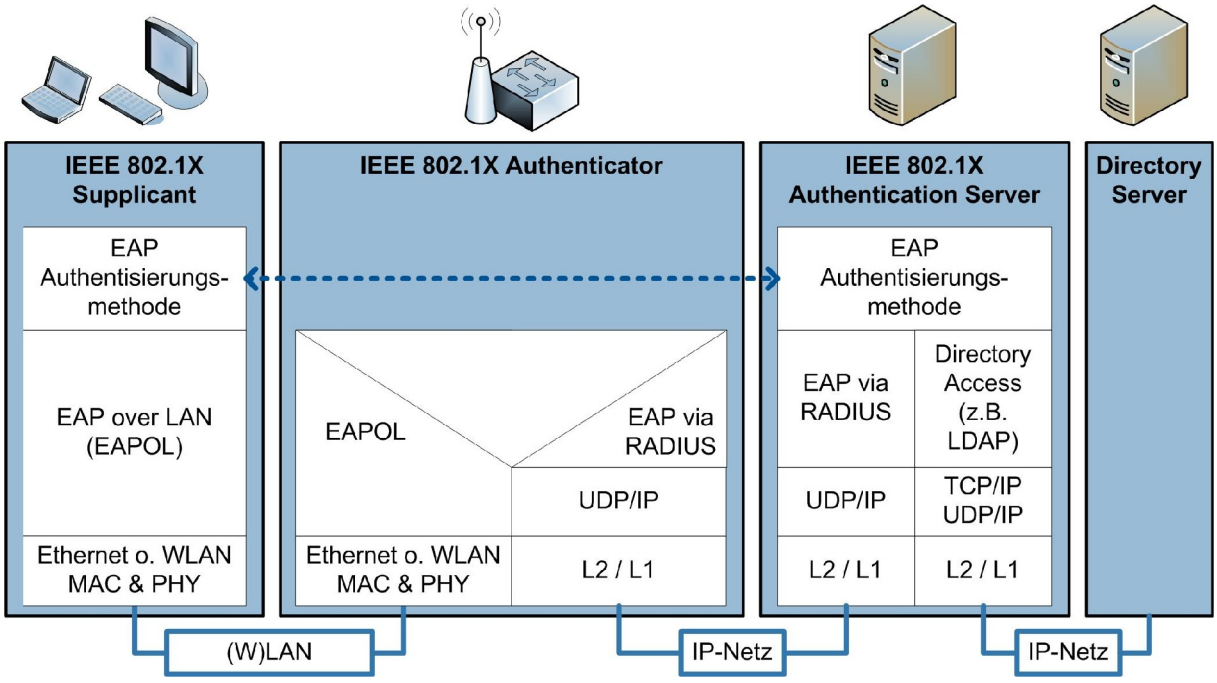
- Der Supplicant ist eine Software-Komponente im Endgerät, die den Netzwerkzugang anfordert.
- Das Gerät, das den Netzwerkzugang herstellt und eine Schnittstelle für die Authentisierung anbietet, heißt Authenticator. Im WLAN wird diese Funktion vom Access Point bzw. WLAN Controller wahrgenommen.
- Der Authentication Server ist das Gerät, welches den eigentlichen Authentisierungsdienst bereitstellt. Der Authenticator Server ist typischerweise ein RADIUS-Server (siehe [RFC3579]).

Abbildung A-12: Rollen in IEEE 802.1X



Die Authentisierung geschieht über das Extensible Authentication Protocol (EAP, siehe [RFC3748]). Dabei erfolgt die Kommunikation über die LAN- bzw. WLAN-Schnittstelle zwischen Supplicant und Authenticator mit der Variante EAP over LAN (EAPOL). EAPOL gestattet die Übertragung von EAP-Nachrichten auf Layer 2. Auf diese Weise wird eine Authentisierung am Netzzugangspunkt ermöglicht, bevor eine Kommunikation auf IP-Ebene und höheren Protokollebenen stattfinden kann. Die Kommunikation zwischen Authenticator und Authentication Server geschieht (typischerweise) über RADIUS, wobei die EAP-Nachrichten als RADIUS-Attribute übertragen werden. Für die Verwaltung der Daten der Geräte oder Nutzer, die sich mit IEEE 802.1X authentisieren, wird oft ein Verzeichnisdienst (Directory Service) wie z.B. LDAP (Lightweight Directory Access Protocol) verwendet, der vom RADIUS-Server angesprochen wird. Abbildung A-13 zeigt die genutzten Protokolle im Überblick.

Abbildung A-13: Protokolle in IEEE 802.1X



EAP ist modular und liefert einen Rahmen, in den die eigentlichen Authentisierungsverfahren, die sogenannten EAP-Methoden, eingebettet werden können. Damit EAP-Methoden für die Anwendung im WLAN geeignet sind, müssen sie zusätzlich auch die Möglichkeit der Erzeugung und Verteilung von Schlüsselmaterial (siehe Kapitel A.2.4.1 und A.2.4.2) bieten. Es gibt eine ganze Reihe von EAP-Methoden. Im Folgenden werden einige für die WLAN-Anwendung besonders relevanten Methoden beschrieben:

- EAP-TLS (siehe [RFC 5216])

  Diese EAP-Methode basiert auf der Authentisierung gemäß Transport Layer Security (TLS). Es wird eine gegenseitige Authentisierung anhand von X.509-Zertifikaten durchgeführt. Das bedeutet, dass eine Public Key Infrastructure (PKI) zur Verwaltung der Zertifikate (Ausstellung, Verteilung, Rückruf, Erneuerung usw.) benötigt wird, die wiederum einer sorgfältigen Planung bedarf. Dabei müssen für jeden zu unterstützenden Endgeräte-Typ Zertifikate ausgestellt und mit akzeptablem Aufwand verwaltet werden können.

  Bei EAP-TLS sendet der jeweils zu authentisierende Kommunikationspartner ein Zertifikat, das seinen öffentlichen Schlüssel enthält. Außerdem sendet er eine mit seinem privaten Schlüssel gebildete Signatur, sodass der Empfänger durch Anwendung des öffentlichen Schlüssels auf diese Signatur die Authentizität des Senders feststellen kann.

Während der Authentisierungsphase wird auch vom Client ein Master Session Key (MSK) generiert, der dem Server verschlüsselt durch seinen öffentlichen Schlüssel übermittelt wird. Aus diesem Master Session Key können dann sowohl Server als auch Client die für die weitere Verschlüsselung der Kommunikation nötigen Schlüssel wie z.B. den PMK von CCMP ableiten.

- EAP-TTLS (siehe [RFC 5281])

  Bei EAP-TTLS (Tunneled TLS) wird TLS nur zur Authentisierung des Server genutzt. Anschließend wird ein TLS-Tunnel zwischen Server und Client aufgebaut, in dem dann geschützt die Authentisierung des Client durch andere Methoden erfolgt, wie z.B. über eine EAP-Methode wie Generic Token Card (GTC) oder auch über ältere Standardprotokolle wie PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol) oder MSCHAP (Microsoft Challenge Handshake Authentication Protocol).

  Auch bei EAP-TTLS wird während der Authentisierungsphase ein MSK generiert, der für die Ableitung weiterer für die Verschlüsselung notwendiger Schlüssel genutzt wird.

- PEAP (IETF, Internet Draft)

  PEAP (Protected EAP) funktioniert ähnlich wie EAP-TTLS, nur dürfen im Tunnelinnern ausschließlich EAP-Methoden zur Authentisierung des Clients angewendet werden. Eine typische Kombination, die auch als PEAPv0 verzeichnet wird, ist PEAP mit innerer Authentisierungsmethode EAP-MSCHAPv2 (siehe [KaPa04]). EAP-MSCHAPv2 basiert auf der oft bei Windows-Clients genutzten PPP-Authentisierungsmethode MSCHAPv2. Über EAP-MSCHAPv2 können die für eine Domänenanmeldung üblichen Abfragen von Nutzername und Passwort erfolgen, sodass diese Methode gut zur Benutzerverwaltung in Windows-Lösungen passt.

- EAP-FAST (siehe [RFC 4851])

  EAP-FAST (Flexible Authentication via Secure Tunneling) basiert ebenfalls auf dem Prinzip des Aufbaus eines äußeren TLS-Tunnels. Es wird jedoch eine gegenseitige Authentisierung über sogenannte Protected Access Credentials (PACs) durchgeführt.

Wenn möglich, ist EAP-TLS gefolgt von EAP-FAST den anderen beschriebenen EAP-Methoden immer vorzuziehen, da durch die direkte gegenseitige Authentisierung von Server und Client auf jeden Fall ein höheres Sicherheitsniveau erreicht wird. Weiterhin ist EAP-TLS als RFC vergleichsweise solide standardisiert. EAP-TLS wird in den Tests für WPA2-Zertifizierungen (Wi-Fi Protected Access, siehe Kapitel A.2.5) als Referenzmethode benutzt und kann für WLAN daher durchaus als eine der am meisten getesteten EAP-Methoden bezeichnet werden[9]. EAP-TLS wird von praktisch allen Supplicants gängiger Betriebssysteme genauso wie von externen kommerziellen und Open Source Supplicants unterstützt. Die meisten modernen RADIUS-Server unterstützen EAP-TLS. Da auch auf der Seite der Netzbetriebssysteme eine geeignete Unterstützung der Verwaltung der Nutzerdaten vorliegt, ist EAP-TLS allgemein für WLAN im Behörden- und im Unternehmensbereich eine zu empfehlende Authentisierungsmethode.

A.2.4.4 Ableitung der Sitzungsschlüssel

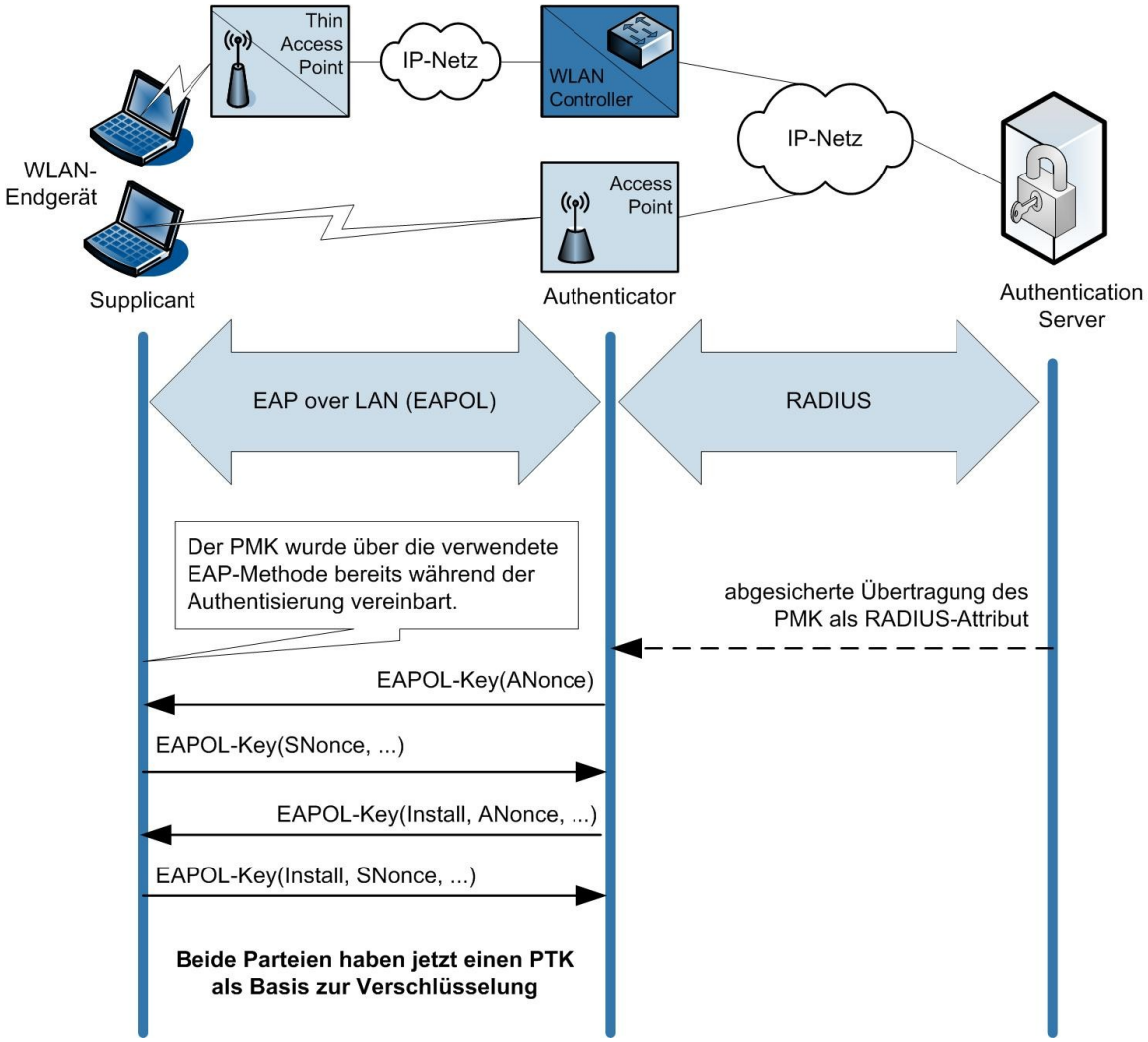
Über die genutzte EAP-Methode wird zwischen Supplicant und Authentication Server ein gemeinsamer geheimer Master-Schlüssel (Pairwise Master Key, PMK) vereinbart. Der PMK wird vom Authentication Server zum Authenticator (Access Point) übertragen. Der PMK hat eine Länge von 256 Bit.

Über EAPOL (siehe Kapitel A.2.4.2) können anschließend die verwendeten Sitzungsschlüssel ausgehandelt werden. Dabei werden Schlüsselinformationen zum Supplicant übertragen (Group Temporal

[9] Die Wi-Fi Alliance bietet seit April 2005 auch die Möglichkeit an, EAP-Methoden zu zertifizieren. Zu den Methoden, die zertifiziert werden können, gehören unter anderem auch EAP-TLS, EAP-FAST, EAP-TTLS und PEAP.

Key, GTK) und es wird ein gemeinsamer Schlüssel zwischen Supplicant und Authenticator abgeleitet (Pairwise Transient Key, PTK), wie in Abbildung A-14 gezeigt. Aus GTK und PTK werden dann die eigentlichen temporären Schlüssel für die Verfahren CCMP (bzw. TKIP) konstruiert. Die Länge dieser letztendlich verwendeten Schlüssel beträgt 128 Bit. Der GTK ist dabei die Grundlage für die Verschlüsselung von Broadcasts und Multicasts, während der PTK als Basis für die Verschlüsselung von Unicasts dient.

Abbildung A-14: PTK-Schlüsselgenerierung über EAPOL



Die Master-Schlüssel können auch als Pre-Shared Keys (PSKs) manuell auf den Komponenten konfiguriert werden. Bei Verwendung von PSKs wird die EAP-Authentisierung nicht genutzt, EAPOL kommt aber für die Ableitung von transienten Schlüsseln (PTK, GTK) weiterhin zum Einsatz.

Dieser Austausch von Schlüsselinformationen geschieht durch die in Abbildung A-14 gezeigte EAPOL-Key-Sequenz. Bei diesem sogenannten 4-Way-Handshake werden insbesondere zwei Pseudozufallszahlen (ANonce für den Authenticator und SNonce für den Supplicant) über EAPOL ausgetauscht, die als sitzungsspezifische Parameter in die Funktion zur Ableitung der PTK einfließen. Dies ist für eine sichere WLAN-Kommunikation bei IEEE 802.11i erforderlich, um einen statischen Schlüssel wie bei WEP zu vermeiden.

Bei lang andauernden WLAN-Sitzungen ist es sinnvoll, den PMK „aufzufrischen“. Hierzu sieht IEEE 802.1X die Funktion der regelmäßigen Reauthentisierung (Reauthentication) vor. Der vom Standard vorgeschlagene Wert ist eine Reauthentisierung alle 3600 Sekunden.

A.2.5 Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) ist ein 2003 veröffentlichter Industrie-Standard der Wi-Fi Alliance (siehe [WPA04]), der auf einem Draft zu IEEE 802.11i basierte und aufwärtskompatibel zu IEEE 802.11i ist. Bereits seit Ende August 2003 war WPA Bestandteil der Wi-Fi-Interoperabilitätstests.

Für WPA wurde TKIP zwingend vorausgesetzt, die Implementierung der Variante der AES-Verschlüsselung über CCMP war jedoch optional.

Im Jahr 2004 wurde WPA2, die Folgeversion von WPA, verabschiedet und im Sommer 2004 mit dem Zertifizierungsprozess begonnen. Seit Herbst 2006 ist eine WPA2-Zertifizierung zwingender Bestandteil einer Wi-Fi-Zertifizierung. WPA2 deckt alle zwingenden Anforderungen von IEEE 802.11i ab (inklusive AES-Modus CCMP).

Es gibt zwei Varianten von WPA2: WPA2-Enterprise für größere WLAN-Installationen, das für die Authentisierung und Schlüsselverwaltung IEEE 802.1X mit RADIUS nutzt, und WPA2-Personal für kleinere WLAN-Installationen und den SOHO-Bereich (Small Office – Home Office), das mit Pre-Shared Keys (PSK) operiert[10].

Abschließend zeigt Tabelle A-1 eine zusammenfassende Bewertung der Sicherheitselemente in IEEE 802.11i bzw. WPA und WPA2.

Tabelle A-1: Bewertung der Elemente von IEEE 802.11i bzw. WPA und WPA2

Funktion	Verfahren	Bewertung	Kommentar
Authentisierung	implizite Authentisierung durch Pre-Shared Key	**0**	Diese Bewertung gilt, sofern der Schlüssel zufällig gewählt ist bzw. aus einem Passwort hoher Komplexität mit einer Länge von mindestens 20 Zeichen erzeugt wird.
	IEEE 802.1X	**++**	Schlüsselmanagement und diverse Authentisierungsmethoden werden unterstützt. Die verwendete Authentisierungsmethode muss dem zu erreichenden Sicherheitsniveau angemessen gewählt sein. Nur für diesen Fall gilt die angegebene Bewertung.
Verschlüsselung (WPA)	TKIP	**-**	TKIP basiert auf WEP. Zwar erfolgt für jedes Paket eine kryptographische Erzeugung eines Schlüssels, jedoch wurden Ende 2008 eine Schwachstelle entdeckt, die unter gewissen Rahmenbedingungen eine Entschlüsselung der Übertragung durch einen Angreifer erlaubt.
Integritätsprüfung (WPA)	Michael	**0**	Ein DoS-Angriff ist möglich. Die Länge des MIC beträgt 64 Bit.
Verschlüsselung (WPA2)	CCMP	**++**	CCMP verwendet AES. AES erfordert entsprechende Hardware. Die verwendete Schlüssellänge beträgt 128 Bit. Nach dem Stand der Technik ist CCMP als sicheres Verfahren einzustufen.

[10] WPA2-Personal wird auch als WPA2-PSK bezeichnet.

Funktion	Verfahren	Bewertung	Kommentar
Integritätsprüfung (WPA2)	CBC-MAC	++	CBC-MAC ist ein Bestandteil von CCMP. Die Länge des MIC beträgt 64 Bit.

Legende:
"++" = sehr gut, "+" = gut, "0" = akzeptabel, "-" = mangelhaft, "--" = ungenügend

A.2.6 Wi-Fi Protected Setup

Wi-Fi Protected Setup ist ein weiterer Industrie-Standard der Wi-Fi Alliance, der speziell für den privaten WLAN-Einsatz Mechanismen zur vereinfachten Konfiguration einer WLAN-Absicherung anbietet. Hiermit wird das Problem adressiert, dass speziell im privaten Bereich manche Nutzer den Aufwand für die Konfiguration eines komplexen Kennworts für WPA2-Personal scheuen (von IEEE 802.1X in WPA2-Enterprise ganz zu schweigen) und daher ein ungeschütztes WLAN betreiben.

Neben einer vereinfachten Passwort-basierten Konfiguration spezifiziert Wi-Fi Protected Setup eine sogenannte Push-Button-Methode, also „Sicherheit auf Knopfdruck“. Dabei wird zunächst ein SSID automatisch vom Access Point erzeugt und den Endgeräten mitgeteilt. Anschließend wird am Access Point und dann am Endgerät ein „Knopf“ (z.B. per Mausklick) betätigt und hierdurch automatisch Schlüsselmaterial erzeugt und ausgetauscht. Der auf diese Weise ausgehandelte Schlüssel wird danach im verwendeten Verschlüsselungsverfahren, bei WPA2 beispielsweise von CCMP, verwendet.

Generell ist ein solches Verfahren natürlich in der Phase von Erzeugung des SSID bis zum Abschluss der Schlüsselaushandlung verwundbar. Die Aushandlung des Schlüsselmaterials erfolgt dabei zwar mit bewährten Verfahren (z.B. Diffie-Hellman), die Möglichkeit von Man-in-the-Middle-Angriffen kann aber nicht ausgeschlossen werden.

A.2.7 Absicherung der Kommunikation mit der LAN-Infrastruktur

Die Absicherung der Kommunikation mit IEEE 802.11i bzw. WPA2 bezieht sich auf den Schutz der Kommunikation auf der Luftschnittstelle. Ein Angreifer kann bei einem nach IEEE 802.11i abgesicherten Zugang keinen Zugriff auf das WLAN erhalten, ohne sich erfolgreich zu authentisieren und die Kommunikation kann bei Verwendung von CCMP nach dem aktuellen Stand der Technik nicht abgehört werden. Ohne weitergehende Mechanismen besteht jedoch kein Schutz auf der LAN-Schnittstelle des Access Point.

Hier sind zwei Aspekte zu unterscheiden:

- Schutz des kabelbasierten LAN-Zugangs vor unautorisiertem Zugang
- Schutz der Kommunikation zwischen Access Point und Infrastruktur

Der erste Punkt kann durch eine Netzzugangskontrolle abgedeckt werden. Manche Access Points unterstützen einen IEEE 802.1X Supplicant, der es gestattet, dass sich der Access Point selbst an dem Port eines Access Switches, an dem der Access Point angeschlossen ist, authentisiert.

Bei Verwendung eines Controller-basierten WLAN-Designs besteht noch eine weitere Möglichkeit, sofern die Pakete der WLAN-Endgeräte zum WLAN Controller getunnelt werden. An dem Port des Access Switches, an dem ein Thin Access Point angeschlossen ist, ist in diesem Fall nur die MAC-Adresse des Thin Access Point sichtbar. Hier kann also mit Port Security gearbeitet werden und der

Port des Access Switches an die MAC-Adresse des Thin Access Point gebunden werden. Bei einem normalen, autonomen Access Point ist dies nicht der Fall, da sich dieser als Bridge verhält und die MAC-Adressen der WLAN-Endgeräte daher am Access Switch sichtbar sind.

Für den zweiten Punkt können folgende Mechanismen in Betracht gezogen werden:

Bei einem Controller-basierten WLAN-Design gemäß CAPWAP erfolgt eine gegenseitige Authentisierung von Thin Access Point und WLAN Controller sowie die Verschlüsselung des per UDP übertragenen Kontrollkanals über Datagram TLS (DTLS). DTLS wurde im Jahr 2006 als RFC 4347 (siehe [RFC4347]) veröffentlicht und unterscheidet sich von TLS in den Bereichen, in denen der unzuverlässige Transport in UDP sich auswirkt. Dies beinhaltet unter anderem die folgenden Punkte:

- Durch die Möglichkeit von Neuübertragungen sorgt DTLS für die Zuverlässigkeit des initialen Handshake zur Authentisierung und zum Schlüsselaustausch. Bei TLS ist dies nicht notwendig, da bei Paketverlusten TCP automatisch für die Wiederholung sorgt.

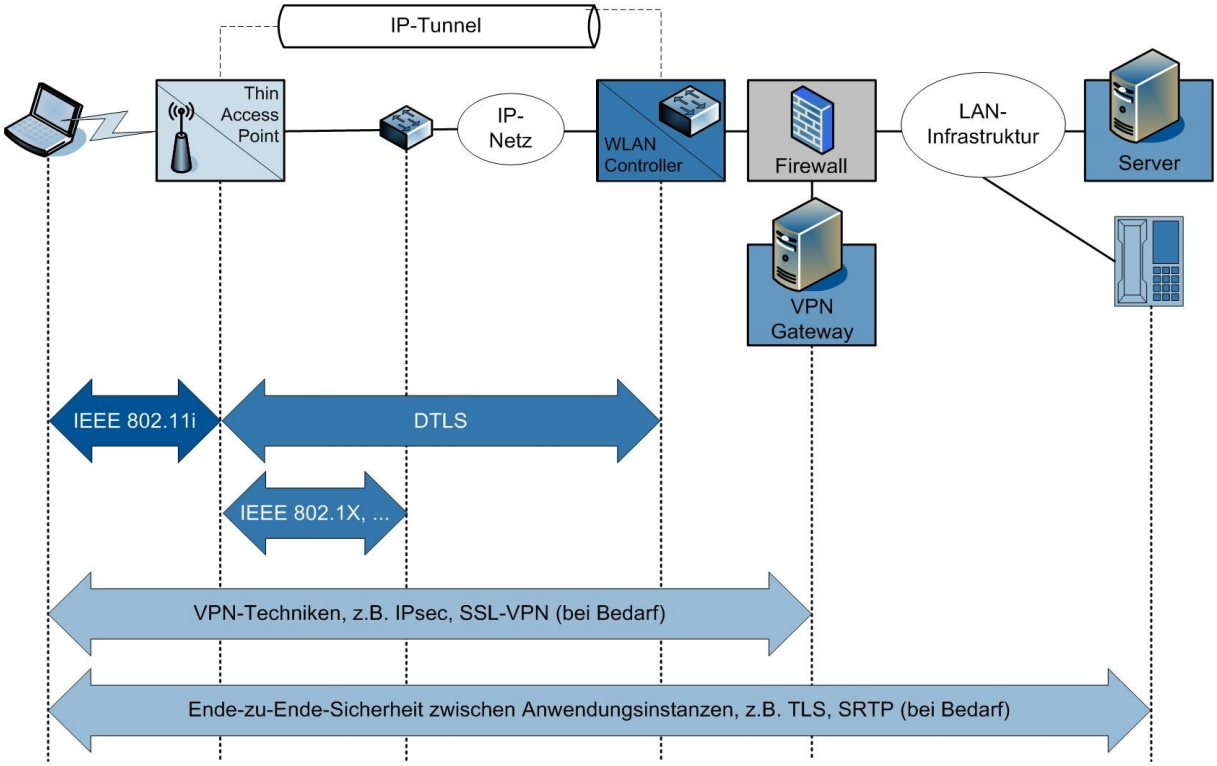
- DTLS nummeriert Pakete, damit bei einem Paketverlust nicht auf eine Integritätsverletzung (wie es bei TLS der Fall wäre) geschlossen wird.

Die Absicherung des Datenkanals, über den die Pakete der WLAN-Endgeräte transportiert werden, ist in der CAPWAP-Spezifikation als optionale Funktion vorgesehen und wird aktuell nur von wenigen Produkten unterstützt. Sofern die Übertragung von WLAN-Nutzdaten im kabelbasierten LAN über als unsicher klassifizierte Bereiche erfolgt, müssen bei entsprechend hohem Schutzbedarf weitergehende Sicherheitsmechanismen eingesetzt werden.

Hier kann zunächst eine Netztrennung für die WLAN-bezogene Kommunikation im LAN in Erwägung gezogen werden. Es besteht grundsätzlich auch die Möglichkeit bei entsprechendem Schutzbedarf die Kommunikation über VPN-Techniken (IPsec oder SSL-VPN) oder über eine Ende-zu-Ende-Sicherheit zwischen den beteiligten Anwendungsinstanzen abzusichern. Letzteres ist beispielsweise bei VoIP über WLAN eine Option. Der Medienstrom (also die Sprache) kann beispielsweise über das Secure Real-Time Transport Protocol (SRTP, siehe [RFC3711]) zwischen IP-Telefonen bzw. zwischen IP-Telefon und einem Gateway verschlüsselt übertragen werden. Dabei kommt ebenfalls AES zum Einsatz. SRTP wird von vielen Festnetz-IP-Telefonen, von einigen Softphones und auch von manchen WLAN-Telefonen unterstützt.

Eine Einordnung hinsichtlich des Wirkungskreises der genannten Sicherheitsmaßnahmen illustriert Abbildung A-15.

Abbildung A-15: Wirkungskreis der Sicherheitsmaßnahmen



A.2.8 Absicherung von Mesh-Netzen

Bei der Absicherung von Mesh-Netzen müssen Unterschiede zwischen Access-Verkehr und Mesh-Verkehr beachtet werden.

Für den Access-Verkehr gelten uneingeschränkt die mit IEEE 802.11i festgelegten Sicherheitsmechanismen.

Für den Mesh-Verkehr muss berücksichtigt werden, dass IEEE 802.1X für den Einsatz direkt verbundener Geräte spezifiziert ist und sich nicht unmittelbar auf die Verwendung in Multi-Hop-Netzen übertragen lässt. Aktuell sind seitens der Hersteller verschiedene Lösungen implementiert, die beispielsweise per Zertifikat oder Pre-Shared Key eine gegenseitige Authentisierung und mit AES eine Verschlüsselung durchführen. Bis zur Verabschiedung von IEEE 802.11s ist hier also eine Einzelfallbetrachtung erforderlich.

A.2.9 Absicherung der Übertragung von Management Frames

IEEE 802.11i berücksichtigt nicht die Absicherung der Übertragung von Management Frames auf der Luftschnittstelle, die beispielsweise eine Assoziation oder eine Authentisierung einleiten oder beenden. Diese Pakete werden aktuell nicht verschlüsselt und nicht hinsichtlich ihrer Authentizität und Integrität geprüft.

Daher sind DoS-Angriffe durch wiederholtes Senden bestimmter Steuer- und Management-Signale möglich (z.B. Deauthentication- bzw. Disassociation-Attacken).

Der in Arbeit befindliche Standard IEEE 802.11w (Protected Management Frames) wird die Absicherung von solchen Übertragungen unterstützen. Hierzu können einerseits gewisse Management Frames

statt über eine Broadcast-Übertragung als entsprechend viele Unicasts an in Frage kommende Empfänger übertragen werden. Hierdurch müssen zwar zunächst mehr Pakete geschickt werden, wenn jedoch zu einer Station bereits eine mit IEEE 802.11i abgesicherte Kommunikationsbeziehung besteht, kann das entsprechende Paket verschlüsselt werden. Andere Management Frames können mit einer kryptographischen Prüfsumme versehen werden, die der Empfänger auswerten kann und so entscheiden kann, ob es sich bei dem Paket um eine Fälschung oder ein Replay durch einen Angreifer handelt.

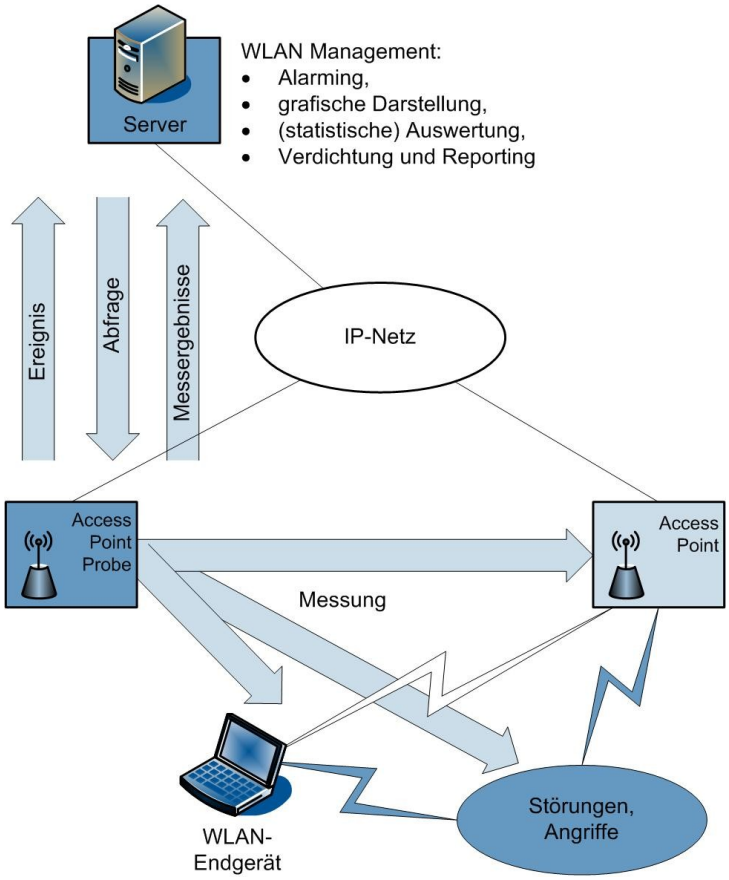
Da IEEE 802.11w noch in Arbeit ist, gibt es seitens der Hersteller auch noch keine einheitliche Implementierung dieser Funktionen.

A.2.10 Überwachung des WLAN

Eine Überwachung des WLAN ist Bestandteil des Netzmanagements und ist für WLAN-Installationen im Unternehmens- und Behördenbereich stets zu empfehlen. Dabei muss insbesondere eine Funktion zur Überwachung der Luftschnittstelle hinsichtlich Fehlern, Leistungsengpässen und Sicherheitsvorfällen unterstützt werden.

Diese Überwachung beinhaltet die regelmäßige Prüfung aller Funkkanäle bei 2,4 bzw. bei 5 GHz. Dabei erfolgt eine Messung von Leistungsparametern inklusive Feststellung der Qualität, mit der andere WLAN-Stationen (insbesondere andere Access Points) empfangen werden, sowie die Analyse der Übertragungen hinsichtlich Fehlern oder Angriffsmustern (siehe Abbildung A-16). Meldungen zu Fehlern und sicherheitsrelevanten Ereignissen sollten an eine zentrale Fehlerkonsole geschickt werden.

Abbildung A-16: Überwachung der Luftschnittstelle in einem WLAN



Bei der Überwachung der Luftschnittstelle muss beachtet werden, dass der Einsatz einer solchen Überwachungsfunktion auf den produktiv genutzten Access Points die Leistung des WLAN spürbar beeinträchtigen kann[11]. Wenn die zu erwartenden Leistungseinbußen nicht akzeptabel sind, kann für die Überwachung der Luftschnittstelle zumindest in kritischen Bereichen alternativ der punktuelle Einsatz von dedizierten Probes (d.h. Access Points, die ausschließlich eine Überwachungsfunktion haben) erfolgen.

Die Ergebnisse der Überwachung sollten auf einem Grundriss des Versorgungsgebiets dargestellt werden können, auf dem auch die Positionen von Access Points eingezeichnet sind.

Für die Überwachung im Bereich Security Management müssen insbesondere Abweichungen zwischen den erwarteten und den tatsächlichen Sicherheitsparametern der Endgeräte und der Access Points erkannt werden und gegebenenfalls zu einem entsprechenden Alarm führen. Eine Abweichung von Sicherheitsparametern kann auch auf eine fremde (rogue) WLAN-Station (Endgerät oder Access Point) hinweisen. Hierfür muss das Management-System Methoden zur Erkennung und Lokalisierung von fremden WLAN-Stationen bereitstellen und abhängig von der Position im Fall einer solchen Identifikation optional einen Alarm generieren.

Grundsätzlich kann ein WLAN-Management-System auch die Ortung und Darstellung von WLAN-Geräten (Endgeräte und Access Points) in einem Plan des WLAN-Versorgungsbereichs unterstützen.

Zusätzlich kann das WLAN-Management-System ein Wireless Intrusion Detection System (Wireless IDS), mit dem WLAN-spezifische Angriffe erkannt werden können, zur Verfügung stellen. Dabei kann beispielsweise erkannt werden, ob gehäuft die bereits erwähnten ungesicherten Management-Pakete (siehe Kapitel A.2.9) übertragen werden oder ob Angriffe gegen EAPOL durchgeführt werden.

11 Bei aktivierter Überwachungsfunktion schaltet ein Access Point regelmäßig vom Normalbetrieb für eine gewisse Zeitspanne in einen Messbetrieb um. Während dieses Messbetriebs kann der Access Point keine Nutzdaten mehr transportieren, und es kommt zu entsprechenden Verzögerungen (ggf. sogar zu Verlusten) bei der Übertragung. Häufigkeit und Dauer des Messbetriebs können herstellerspezifisch konfiguriert werden. Grundsätzlich können auch zusätzliche Access Points installiert werden, die eine reine Überwachungsfunktion für die produktiv genutzten Access Points haben.

A.3 Gefährdungen

Dieses Kapitel beschreibt typische Gefährdungen, denen ein WLAN ausgesetzt sein kann. Eine genauere Analyse der Gefährdungslage kann dem Teil 2 der Technischen Richtlinie Sicheres WLAN entnommen werden (siehe [TR-S-W2]).

A.3.1 Ausfall durch höhere Gewalt

Wie im kabelbasierten LAN kann es auch im WLAN z.B. durch Überspannungen zum Ausfall von WLAN-Komponenten kommen. Außerdem sind Außeninstallationen von WLAN-Komponenten zur Versorgung von Außenbereichen (z.B. Antennen) durch Blitz und Witterungseinflüsse gefährdet.

A.3.2 Mangelhafte Planung

Planungsfehler stellen sich oft als besonders schwerwiegend heraus, da leicht flächendeckende Sicherheitslücken geschaffen werden können, deren Beseitigung mit hohen Kosten verbunden ist.

Beispiele sind:

- Durch eine mangelhafte Planung können sich z.B. Leistungseinbußen ergeben, die durch Störungen oder auch durch Funklöcher entstehen können. Im Außenbereich kann eine mangelhafte Planung die Gefährdung von WLAN-Komponenten durch Blitzschlag oder Witterungseinflüsse zur Folge haben.
- Sind Authentisierungsverfahren und Schutz der hierzu notwendigen Informationen schlecht gewählt, kann dies neben dem Verlust der Vertraulichkeit und der Integrität der Kommunikation von WLAN-Endgeräten auch zu einer weitergehenden Kompromittierung der internen LAN-Infrastruktur führen.
- Durch Planungsfehler bei der Absicherung des LAN-Zugangs für Access Points und des Übergabepunkts zwischen WLAN Distribution System und LAN sind ebenfalls unberechtigte Zugriffe über den Ethernet-Anschluss eines Access Point möglich.

A.3.3 Fehlende Regelungen zur Nutzung von Frequenzen und unbeabsichtigte Störung durch Fremdsysteme

Ist die Nutzung des ISM-Bands bei 2,4 GHz nicht geregelt, und werden WLAN nach IEEE 802.11b bzw. IEEE 802.11g parallel zu anderen Funksystemen (wie z.B. Bluetooth[12], Bewegungsmeldern, Mikrowellenherden usw.) im selben Bereich genutzt, kann es zu signifikanten Störungen der Datenübertragung im WLAN kommen. Diese Störungen können auch durch einen anderen Nutzer (außerhalb der

[12] Mit Bluetooth 1.2 ist mit Adaptive Frequency Hopping (AFH) ein Mechanismus eingeführt worden, der die Koexistenz zwischen WLAN nach IEEE 802.11b bzw. IEEE 802.11g und Bluetooth verbessern soll. Bei manchen Bluetooth-Geräten kommt es aber trotz AFH noch zu signifikanten Störungen einer WLAN-Übertragung. Der Mischbetrieb zwischen Bluetooth und WLAN muss also bei Bedarf im Einzelfall getestet werden. Es gibt Hersteller, die für eine verbesserte Koexistenz mit WLAN auch weitergehende spezifische Mechanismen in ihre Bluetooth-Geräte implementieren. Weitere Hinweise zu diesem Thema finden sich in Kapitel B. Bluetooth.

Behörde oder des Unternehmens) verursacht werden, der berechtigterweise ebenfalls im 2,4-GHz-Bereich operiert, und müssen dann hingenommen werden.

Für den 5-GHz-Bereich ist zu beachten, dass Radar-Anwendungen (z.B. von Einrichtungen der zivilen Luftfahrt und des Militärs) in diesem Frequenzband Primärnutzer sind und Vorrang vor WLAN-Anwendungen genießen.

A.3.4 Unzureichende Regelungen zur Administration der WLAN-Infrastruktur

Aufgrund fehlender Regelungen zur Administration der WLAN-Infrastruktur kann es beispielsweise zu Fehlkonfigurationen der WLAN-Komponenten (z.B. Access Points) kommen. Probleme können sich auch ergeben, wenn es keine einheitliche Festlegung zur Dokumentation von Systemveränderungen gibt.

A.3.5 Fehlende Regelungen zur Überwachung der WLAN-Infrastruktur

Wurden keine Festlegungen zur Überwachung der WLAN-Infrastruktur getroffen und somit die entsprechenden finanziellen und personellen Ressourcen nicht bereitgestellt, werden Schwachstellen durch Fehlkonfigurationen und Angriffe auf das WLAN unter Umständen nicht erkannt.

A.3.6 Unzureichende Notfallvorsorge

Sofern für den Betrieb des WLAN keine Festlegungen zur Notfallbehandlung erfolgt sind, kann ein (ggf. bewusst herbeigeführter) Notfall die Grundlage für einen Angriff, beispielsweise verbunden mit einem Datenabfluss, bilden. Der Sicherheitsvorfall wird zwar vielleicht bemerkt, Gegenmaßnahmen können aber nicht zeitnah (innerhalb von Minuten) eingeleitet werden, da nicht auf entsprechend vorbereitete Maßnahmenkataloge, geregelte Abläufe und Befugnisse zu notwendigen Eingriffen zurückgegriffen werden kann.

Weiterhin kann es je nach Nutzung eines WLAN vorkommen, dass es nicht möglich ist, im Notfall auf ein Ausweichmedium (z.B. eine kabelbasierte Anbindung oder ein anderes Funksystem) auszuweichen. Hier kann sich eine effektive Notfallvorsorge als (wirtschaftlich oder technisch) schwer umsetzbar erweisen. Diese Gefährdung wirkt sich umso stärker aus, je mehr kritische Anwendungen über das WLAN betrieben werden.

A.3.7 Sicherheitskritische Grundeinstellung

Im Auslieferungszustand sind die WLAN-Komponenten häufig so konfiguriert, dass keine oder nur einige der Sicherheitsmechanismen aktiviert sind. So kann schon ein einziger Access Point oder ein einziges WLAN-Endgerät, die nicht gemäß geltender Sicherheitsrichtlinie konfiguriert wurden, zu einer Kompromittierung des gesamten WLAN führen.

A.3.8 Fehlkonfiguration von WLAN-Komponenten

Mittlerweile bieten Access Points bzw. WLAN Controller eine Vielzahl von Konfigurationseinstellungen, die insbesondere auch die Nutzung von Sicherheitsfunktionen betreffen. Werden hier falsche Einstellungen vorgenommen, ist entweder keine Kommunikation über einen Access Point möglich oder

die Kommunikation erfolgt ungeschützt bzw. mit einem zu geringen Schutzniveau, obwohl der Nutzer von einem vorhandenen Schutz ausgeht.

A.3.9 SSID Broadcast

Ein Access Point teilt durch ein regelmäßig ausgestrahltes Paket (das sogenannte Beacon Frame) seine Anwesenheit und seine Kommunikationsparameter mit. Dabei wird im Normalfall auch der SSID übertragen. Über die Angabe des SSID erfolgt die Anmeldung eines Endgeräts an einem WLAN. Die Kenntnis des SSID ist daher auch eine Grundlage für einen missbräuchlichen Zugriff auf ein WLAN. Einige Access Points bieten die Möglichkeit, das Senden des SSID im Beacon Frame zu unterbinden, um das WLAN vor Unbefugten zu verstecken (oft als Closed System bezeichnet). Dieser Schutz wirkt gegen manche frei verfügbare Werkzeuge, jedoch kann mit einem WLAN-Protokollanalysator auch in diesem Falle der SSID aus anderen Management- und Steuersignalen ermittelt werden.

A.3.10 Manipulierbare MAC-Adressen

Die MAC-Adressen von WLAN-Stationen können relativ einfach abgehört werden und ein Angreifer kann durch Verwendung einer anderen MAC-Adresse eine fremde Identität vorspielen. MAC-Adressfilter, die in Access Points oder WLAN Controller zum Zweck des Zugriffsschutzes häufig unterstützt werden, sind daher leicht überwindbar.

A.3.11 Schwachstellen in WEP und TKIP

Das Ziel mittels WEP Vertraulichkeit, Integrität und Authentizität im WLAN zu sichern, kann eindeutig als nicht erreicht eingestuft werden, denn WEP ist mittlerweile vollständig kompromittiert (siehe Kapitel A.2.3). Lauschangriffe und Angriffe auf Endgeräte und insbesondere auf die Infrastruktur sind bei einem nur mit WEP abgesicherten WLAN sehr leicht möglich.

Wie in Kapitel A.2.4.1 beschrieben, hat auch TKIP Schwachstellen bei der Nutzung von RC4, die unter gewissen Rahmenbedingungen zu einem Lauschangriff auf der Luftschnittstelle genutzt werden können.

A.3.12 Probleme bei der Migration von WEP und TKIP zu IEEE 802.11i bzw. WPA2

In Folge einer Migration muss ein Access Point oft im Kompatibilitätsbetrieb sowohl mit IEEE 802.11i (d.h. WPA2) als auch mit WEP oder TKIP betrieben werden, da einige WLAN-Endgeräte schon auf WPA2 umgestellt sind, andere WLAN-Endgeräte aber nur WEP oder TKIP unterstützen. In diesem Fall kommunizieren zwar prinzipiell alle WPA2-fähigen Endgeräte mit dem Access Point über WPA2, es gibt jedoch einige Einschränkungen: Zunächst werden Multicast- und Broadcast-Nachrichten noch mit WEP verschlüsselt. Weiterhin kann es vorkommen, dass nicht-WPA2-fähige Endgeräte auch IEEE 802.1X nicht unterstützen. Dadurch kann die Authentisierung und der dynamische Schlüsselwechsel umgangen werden.

Insgesamt besteht während einer Migration, die sich über einen längeren Zeitraum hinziehen kann, ein geringeres Sicherheitsniveau, als dies mit IEEE 802.11i möglich wäre.

A.3.13 Schwachstellen bei passwortbasierten Authentisierungsverfahren in WPA, WPA2 bzw. IEEE 802.11i

Werden für die Authentisierung in WPA, WPA2 bzw. IEEE 802.11i passwortbasierte Mechanismen genutzt, wie z.B. Pre-Shared Keys (PSKs) oder PEAP unter Verwendung von EAP-MSCHAPv2, ist grundsätzlich eine Wörterbuchattacke möglich. Die Verwendung eines PSK mit WPA-Personal, bzw. WPA2-Personal gestattet sogar eine Offline-Attacke, bei der es genügt, auf der Luftschnittstelle die ersten zwei Pakete des in Kapitel A.2.4.4 vorgestellten 4-Way-Handshake aufzuzeichnen. Anschließend kann man ohne Verbindung zum WLAN mögliche Passwörter probieren. Dabei wird ausgenutzt, dass im zweiten Paket des 4-Way-Handshake der SSID bereits verschlüsselt übertragen wird. Inzwischen sind hierzu Methoden entwickelt worden, die für allgemein bekannte SSIDs sogenannte Rainbow Tables (d.h. Vorausberechnungen) ermitteln, mit denen die Zeit für die Ermittlung des PSK erheblich verkürzt werden kann. Dabei spielt hierbei natürlich die Komplexität der Passwörter generell eine entscheidende Rolle.

A.3.14 Bedrohung der lokalen Daten

Auf den Endgeräten entstehen durch die Teilnahme am WLAN zusätzliche Bedrohungen für die lokalen Daten. Lokale Datei- bzw. Druckerfreigaben im Betriebssystem erlauben in der Grundeinstellung meist auch über das WLAN Zugriffe auf diese Ressourcen. Ebenso sind bei eingeschaltetem WLAN Angriffe auf den Rechner zu befürchten, die Schwachstellen des verwendeten Betriebssystems ausnutzen. Diese Gefahren bestehen insbesondere auch bei der Nutzung von Hotspots und in Ad-hoc-Netzwerken.

A.3.15 Unkontrollierte Ausbreitung der Funkwellen

Die Funkwellen der WLAN-Komponenten breiten sich auch über räumliche Grenzen des WLAN-Nutzungsbereichs aus. Dabei kann auch in nicht vom WLAN-Betreiber kontrollierten Bereichen ein Empfang möglich sein. Je nach Umgebungsbedingungen und Leistungsfähigkeit der verwendeten Empfangsgeräte (z.B. Richtantennen) besteht eine konkrete Abhörgefahr, sofern keine adäquaten Verschlüsselungsmechanismen eingesetzt werden.

A.3.16 Abhören der WLAN-Kommunikation

Da es sich bei Funk um ein Shared Medium handelt, können die über das WLAN übertragenen Daten leicht aufgezeichnet werden. Dies ist mit frei im Internet erhältlicher Software möglich, welche die WLAN-Karte des Angreifers in den sogenannten Promiscuous Mode schaltet. Aus den aufgezeichneten Daten können auch bei verschlüsselter Datenübertragung zumindest WLAN-Parameter wie SSID, genutzter Funkkanal und eingesetztes Verschlüsselungsverfahren sowie die MAC-Adressen der Kommunikationspartner im WLAN gewonnen werden.

Bei nicht genutzter oder schwacher WLAN-Verschlüsselung können darüber hinaus auch die IP-Adressen und genutzten Ports der Kommunikationspartner sowie gegebenenfalls übertragene Nutzdaten abgehört werden, sofern diese nicht über IP-VPN, SSL oder Verschlüsselung auf Applikationsebene geschützt sind.

A.3.17 Bedrohung der Verfügbarkeit

WLANs übertragen Informationen mittels elektromagnetischer Funkwellen. Strahlen andere elektromagnetische Quellen im gleichen Frequenzspektrum Energie ab, können diese die WLAN-Kommunikation stören und im Extremfall den Betrieb des WLAN verhindern. Dies kann unbeabsichtigt durch andere technische Systeme (z.B. Bluetooth-Geräte, andere WLANs, Mikrowellenöfen, medizinische Geräte, Funk-Überwachungskameras usw.) oder aber durch absichtliches Betreiben einer Störquelle (Jammer) als sogenannter Denial-of-Service-Angriff (DoS-Angriff) erfolgen. Eine solche Störquelle kann sich bei ausreichender Sendeleistung auch außerhalb des Geländes befinden, auf dem das WLAN genutzt wird.

Darüber hinaus sind DoS-Angriffe auch möglich durch wiederholtes Senden bestimmter Steuer- und Management-Signale, z.B. Deauthentication- bzw. Disassociation-Attacken.

Zusammengefasst ist zu betonen, dass in WLAN Angriffe vom Typ DoS nie vermieden werden können, denn ein Störsignal kann wie oben geschildert einfach, effektiv und jederzeit erzeugt werden.

A.3.18 Unerlaubte Mitnutzung des WLAN

Eine WLAN-Installation (insbesondere im SOHO-Bereich), über die ein Internet-Zugang ermöglicht wird, ist der Gefahr der unerlaubten Mitnutzung ausgesetzt, wenn keine hinreichenden Authentisierungsmechanismen für den Zugang zum WLAN implementiert sind. Diese unerlaubte Mitnutzung führt einerseits zur Reduzierung der zur Verfügung stehenden Bandbreite und Erhöhung der Antwortzeiten für autorisierte WLAN-Nutzer sowie andererseits zur unerlaubten und unbezahlten Mitnutzung des Internetzugangs. Bei der Mitnutzung des Internetzugangs ist natürlich auch ein Missbrauch nicht ausgeschlossen, z.B. durch Angriffe auf andere Systeme im Internet, die Verbreitung von Spam-Mails oder das Bereitstellen bzw. Laden von strafrechtlich relevanten Inhalten.

A.3.19 Diebstahl eines Access Point

Access Points stellen einen gewissen Wert dar, der zum Diebstahl verleiten kann.

Dabei ist der monetäre Wert der Access Points beinahe nachrangig: Der Dieb kann auch über den nun dauerhaften und unbeschränkten physikalischen Zugriff unbehindert und unbemerkt Basisinformationen für eine weitere Kompromittierung erlangen, z.B. auf dem Wege des Auslesens eines Shared Secrets zur RADIUS-Authentisierung oder des verwendeten Schlüssels für WEP, WPA-Personal bzw. WPA2-Personal.

A.3.20 Vortäuschung eines gültigen Access Point

Durch Poisoning- und Spoofing-Methoden oder die Man-in-the-Middle-Technik täuscht der Angreifer eine falsche Identität vor bzw. lenkt den Netzwerkverkehr zu seinen eigenen Systemen um und kann so die Kommunikation belauschen und kontrollieren.

A.3.21 Schwachstellen beim administrativen Zugriff auf Access Points

Wird ein Access Point über die Funkschnittstelle über Klartext-Protokolle wie z.B. Telnet, HTTP oder SNMPv1/v2 administriert, können die über das WLAN übertragenen Administrations-Passwörter mitgelesen werden. Mit dieser Information kann ein Angreifer den Access Point umkonfigurieren.

A.3.22 Ungeschützte Übertragung von Management-Paketen

Ein generelles Problem besteht bei der WLAN-Kommunikation darin, dass die Management-Pakete zur Steuerung der Layer-2-Kommunikation ungesichert übertragen werden, d.h. hier fehlt der Schutz der Vertraulichkeit, Integrität und Authentizität. Dadurch ist es beispielsweise möglich, sogenannte Deauthentication-Attacken über frei verfügbare Tools durchzuführen. Diese Attacken können sowohl in Richtung Access Point als auch in Richtung WLAN- Endgerät erfolgen. Aufgrund dieser ungesicherten Management-Pakete besteht die Gefahr von DoS-Angriffen[13].

A.3.23 Ungeschützter LAN-Zugang am Access Point

Der kabelbasierte LAN-Zugang, über den ein Access Point an die Infrastruktur angeschlossen ist, stellt ein besonderes Risiko dar. Wenn ein Access Point sichtbar und ohne physischen Schutz montiert ist (speziell in einem öffentlich zugänglichen Bereich), kann ein Angreifer versuchen, über den LAN-Zugang des Access Point einen Zugriff auf Ressourcen der LAN-Infrastruktur zu erreichen.

Während der Zugang über die Luftschnittstelle mit IEEE 802.11i bzw. WPA2 geeignet abgesichert werden kann, besteht oft kein Schutz auf der Ethernet-Schnittstelle zum LAN.

Sofern in dieser Situation das Distribution System keine separate Infrastruktur ist, die durch eine Sicherheitsschleuse (Firewall oder zumindest Paketfilter) von der LAN-Infrastruktur getrennt ist, hat der Angreifer im schlimmsten Fall einen Zugriff auf die gesamte über das LAN erreichbare Infrastruktur.

Diese Gefährdung besteht insbesondere bei Thin Access Points in einem Controller-basierten WLAN-Design, denn der wesentliche Vorteil dieser Systeme ist ja gerade die Verwendung einer bestehenden LAN-Infrastruktur als Trägernetzwerk für ein WLAN. Zwar kann die Kommunikation zwischen Thin Access Point und WLAN Controller ggf. geschützt werden, dies ist aber nicht das einzige Angriffsziel. Über den Ethernet-Port, an den ein Thin Access Point angeschlossen ist, können eben nicht nur WLAN Controller erreicht werden, sondern oft auch andere Elemente der IT-Infrastruktur.

A.3.24 Erstellung von Bewegungsprofilen

Da die MAC-Adresse eines WLAN-Adapters, welche (sofern sie nicht explizit geändert wurde) die Hardware-Adresse der WLAN-Karte ist, bei jeder Datenübertragung mit versendet wird, ist ein eindeutiger Bezug zwischen MAC-Adresse des Funk-Endgeräts, Ort und Uhrzeit der Datenübertragung herstellbar. Auf diese Weise können Bewegungsprofile über mobile Nutzer in einem Firmen- oder Behörden-WLAN erstellt werden.

In diesem Zusammenhang muss auch die Funktion der Lokalisierung bzw. Ortung von (fremden) WLAN-Endgeräten und Access Points betrachtet werden, die als Bestandteil des WLAN-Managements zunächst zum Schutz des WLAN beiträgt, da fremde, nicht autorisierte WLAN-Geräte nicht nur erkannt werden können, sondern auch ihre Position bestimmt werden kann. Allerdings eignen sich die dabei verwendeten Techniken grundsätzlich auch für die Erstellung von Bewegungsprofilen von Endgeräten im eigenen WLAN, und ihr Einsatz muss daher unter Berücksichtigung dieser Gefährdung mit Bedacht geplant werden.

---

13 Diese Schwachstelle soll durch die kommende Ergänzung IEEE 802.11w beseitigt werden.

A.4 Schutzmaßnahmen

Zur Erhöhung der Sicherheit beim Einsatz von WLAN-Komponenten sind abhängig vom Einsatzszenario und dem Schutzbedarf der Informationen mehrere Maßnahmen erforderlich. Die Maßnahmen sind in drei Kategorien unterteilt:

A. Konfiguration und Administration der Funkkomponenten

B. Zusätzliche technische Maßnahmen

C. Organisatorische Maßnahmen

Maßnahmen, die bei einem hohen Schutzbedarf **zusätzlich** ergriffen werden sollten, sind in Anlehnung an die IT-Grundschutz-Kataloge (siehe [GSK]) im Folgenden mit dem Kürzel „HS“ gekennzeichnet. Diese Maßnahmen können aber durchaus im Einzelfall bereits bei einem normalen Schutzbedarf in Betracht gezogen werden.

Eine detaillierte Betrachtung der Erstellung eines Maßnahmenkatalogs als Bestandteil eines umfassenden WLAN-Sicherheitskonzepts kann dem Teil 2 der Technischen Richtlinie Sicheres WLAN entnommen werden (siehe [TR-S-W2]).

A.4.1 Konfiguration und Administration der Funkkomponenten

Die im Folgenden beschriebenen Maßnahmen betreffen Access Points, WLAN-Endgeräte und die Übertragung auf der Funkstrecke.

A1: Sorgfältige Planung

A1.1 Festlegung eines Frequenzstandards und der Übertragungstechnik

Im Rahmen der WLAN-Planung ist zunächst eine Ist-Aufnahme durchzuführen, welche der von der Behörde bzw. dem Unternehmen betriebenen Systeme in das ISM-Band bei 2,4 GHz sowie in das 5-GHz-Band abstrahlen. Nachdem diese Ist-Aufnahme abgeschlossen wurde, kann in einem Frequenzstandard festgelegt werden, in welchen Einsatzumgebungen solche Systeme erlaubt sind. Insbesondere wird dadurch eine „Eigenstörung“ des WLAN durch andere von der Behörde bzw. dem Unternehmen betriebene Systeme vermieden.

Des Weiteren muss in diesem Frequenzstandard festgelegt werden, in welchen Bereichen (Gebäude, Flure, Hallen, Campus) der Behörde bzw. des Unternehmens die WLAN-Nutzung erlaubt ist und welches WLAN-System nach welchem IEEE-Standard zum Einsatz kommen soll.

A1.2 Untersuchung der Einsatzumgebung auf mögliche Störungen des WLAN auf Funkebene

Sofern Anforderungen an die maximal zulässige Störung der Funkübertragung im WLAN gestellt werden, sollten über WLAN-Messprogramme (ggf. auch mit einem Spektrumanalysator) mögliche Störquellen ermittelt und entsprechende Abhilfemaßnahmen festgelegt werden. Die Ergebnisse sind zu protokollieren.

A1.3 Festlegungen zum Aufbau des Distribution System

Generell ist eine Trennung der Verkehrsflüsse zwischen WLAN-Infrastruktur und kabelbasiertem LAN vorzunehmen.

Dabei ist zunächst die grundsätzliche Entscheidung zu treffen, ob ein Controller-basiertes Design mit Thin Access Points und WLAN Controller durchgeführt werden soll, oder ob ein klassischer WLAN-Aufbau mit autonomen Access Points erfolgt[14].

Weiterhin muss festgelegt werden, ob aus Sicherheitsgründen eine eigene Infrastruktur aufgebaut bzw. geschaltet wird und damit eine physikalische Trennung zur Infrastruktur des internen LAN ermöglicht wird. Andernfalls erfolgt eine logische Trennung zwischen WLAN und LAN durch die Konfiguration von VLAN auf den Access Switches des kabelbasierten LAN bzw. durch den Tunnelmechanismus zwischen Thin Access Points und WLAN Controller. Bei Verwendung einer Controller-basierten WLAN-Lösung sollte zumindest der Kontrollkanal zwischen Thin Access Point und WLAN Controller authentisiert und verschlüsselt werden.

A1.4 Spezifikation der Nutzergruppen des WLAN und Planung der zugehörigen Kommunikationsparameter

Die verschiedenen Nutzergruppen des WLAN und die zugehörigen Sicherheitsanforderungen müssen spezifiziert werden. Dies beinhaltet auch die Festlegung, auf welchen Access Points die den Nutzergruppen zugeordneten SSIDs konfiguriert werden sollen. Beispielsweise würde auf einem Access Point, der einem Automatisierungsbereich zugeordnet ist, kein SSID, der einen Gastzugang identifiziert, und ggf. auch kein SSID für die Bürokommunikation konfiguriert.

Weiterhin müssen für die Nutzergruppen die wesentlichen WLAN-Übertragungsparameter sorgfältig geplant werden. Wenn beispielsweise ein WLAN auch für Sprachkommunikation verwendet werden soll, ist die Konfiguration von WMM zu empfehlen. Dabei kann je nach verwendetem Produkt auch eine Mindestbandbreite für die Sprachübertragung vorgesehen werden. Weiterhin können je nach WLAN-Nutzung spezielle Anforderungen hinsichtlich der Leistung bei einem Handover bestehen, wie es beispielsweise bei diversen Logistik-Anwendungen, fahrerlosen Transportsystemen und insbesondere bei VoIP der Fall ist.

A1.5 Planung der zu verwendenden WLAN-Authentisierungsverfahren und deren Nutzung

Zur Authentisierung sollten nur als allgemein sicher anerkannte Verfahren eingesetzt werden. Zu empfehlen ist bei größeren WLAN die Verwendung von IEEE 802.1X im Rahmen von IEEE 802.11i bzw. WPA2-Enterprise. Als Authentisierungsverfahren kommt insbesondere EAP-TLS in Frage, da hier eine gegenseitige zertifikatsbasierte Authentisierung von Supplicant (WLAN-Endgerät) und Authentication Server durchgeführt wird. Wenn EAP-TLS nicht möglich ist, kann der Einsatz von EAP-FAST in Erwägung gezogen werden. Andere Verfahren, die bei entsprechend geringerem Schutzbedarf verwendet werden können, sind PEAP und EAP-TTLS.

A1.6 Erstellung eines Anforderungskatalogs für die WLAN-Beschaffung

Anhand der Ergebnisse der WLAN-Planung ist ein Anforderungskatalog für die WLAN-Beschaffung zu erstellen (siehe auch Teil 3 der Technischen Richtlinie Sicheres WLAN, [TR-S-W3]). Darin sind auf Basis der laut Schutzbedarfsfeststellung umzusetzenden Sicherheitsmaßnahmen entsprechende Anforderungen an die von den WLAN-Komponenten zu leistenden Sicherheitsmerkmale beschrieben. Neben Anforderungen

14 Der Einsatz eines Controller-basierten Designs gestattet den Aufbau der WLAN-Infrastruktur weitestgehend unabhängig von der Architektur des kabelbasierten LAN. Für den klassischen Aufbau mit autonomen Access Points sind spezielle Rahmenbedingungen zu berücksichtigen (insbesondere hinsichtlich der Layer-3-Strukturierung des Netzes).

an WLAN Controller, Access Points und WLAN-Endgeräte sind darin auch Anforderungen an ein WLAN-Management zu spezifizieren.

A1.7 Planung und Prüfung des Zusammenwirkens aller WLAN-Komponenten und der zugehörigen Infrastruktur

Im Rahmen der Beschaffung sollten Kriterien aufgestellt werden, welche die Kompatibilität und das korrekte Zusammenwirken aller WLAN-Komponenten überprüfen (siehe auch Teil 3 der Technischen Richtlinie Sicheres WLAN, [TR-S-W3]). Bei der Beschaffung einer größeren WLAN-Installation sollten im Rahmen der Ausschreibung entsprechende Teststellungen gefordert werden. Mit Hilfe eines Prüfkatalogs kann die Erfüllung der technischen Anforderungen evaluiert werden.

A1.8 Sichere Migration zu IEEE 802.11i bzw. WPA2

In manchen Fällen muss eine Migration zu IEEE 802.11i bzw. WPA2 für eine bestehende WLAN-Infrastruktur durchgeführt werden. Dabei kommt es vor, dass während der Migration Altgeräte unterstützt werden müssen, die noch nicht für IEEE 802.11i konfiguriert sind. Hier ist (zumindest für die Dauer der Migration) eine geeignete Trennung der verschiedenen Nutzergruppen vorzunehmen, die es gestattet, zwei Sicherheitsmechanismen parallel zu verwenden, ohne dass es zu einer nicht akzeptablen Schwächung des stärkeren Sicherheitsmechanismus kommt.

A2: Schutzmaßnahmen aktivieren

A2.1 Verschlüsselung, Integritätsschutz und Authentisierung auf der Luftschnittstelle

Verschlüsselung und Integritätsschutz mit CCMP (IEEE 802.11i bzw. WPA2) müssen aktiviert werden.

In SOHO-WLAN und bei der Verwendung von WLAN zur LAN-Kopplung können Pre-Shared Keys (WPA2-Personal) eingesetzt werden, da nur eine geringe Anzahl von WLAN-Stationen zu verwalten ist.

In allen anderen WLAN-Installationen sollte WPA2-Enterprise mit Authentisierung und Schlüsselverwaltung über IEEE 802.1X eingesetzt werden. Hier ist dann als Authentisierungsmethode vorzugsweise EAP-TLS, gefolgt von EAP-FAST, mindestens aber EAP-TTLS oder PEAP zu verwenden.

Diese Anforderungen gelten unabhängig von den verwendeten WLAN-Endgeräten und WLAN-Anwendungen.

A2.2 Identifikations- und Passwortvorgaben ändern

- Der Standard-SSID sollte an Access Points und bei allen Endgeräten geändert werden. Dabei sollte der gewählte SSID keine Rückschlüsse auf die Firma bzw. die Behörde und auf das Netzwerk zulassen.
- Das Standard-Passwort zur Konfiguration der Access Points muss geändert werden. Es ist als Mindestanforderung ein komplexes Kennwort zu wählen.

A2.3 SSID Broadcast am Access Point abschalten – falls technisch möglich

In der Default-Konfiguration eines Access Point wird in den periodischen Übertragungen der sogenannten Beacon Frames der SSID übertragen. Viele Hersteller gestatten es, diese Übertragung zu unterdrücken. Nach Möglichkeit sollte diese Einstellung der SSID-Unterdrückung konfiguriert werden. Dies kann allerdings für manche Endgeräte-Systeme zu Beeinträchtigungen in der Netzauswahl führen.

A2.4 Assoziation via Broadcast SSID deaktivieren

Die Assoziation via Broadcast SSID muss am Access Point deaktiviert werden, damit das Endgerät explizit den gewünschten SSID bei der Assoziierung angeben muss.

A2.5 MAC-Adressfilterung

Die Filterung von MAC-Adressen (MAC-Adressauthentisierung) kann am Access Point bzw. WLAN Controller eingeschaltet werden, sofern der Aufwand akzeptabel ist. Bei kleineren WLAN-Installationen (z.B. im SOHO-Bereich) kann die Verwaltung der MAC-Adressen auf dem Access Point bzw. WLAN Controller erfolgen. Bei größeren Installationen ist eine MAC-Adressauthentisierung nur über einen RADIUS-Server praktikabel.

A3: Schlüssel und Zugangspasswörter von hoher Komplexität nutzen

Schlüssel und Zugangspasswörter sollten entsprechend anerkannter Passwortgestaltungsregeln, z.B. gemäß [GSK], so gewählt werden, dass sie einen möglichst wirksamen Schutz gegen Angreifer bieten. Dazu gehört auch der regelmäßige Wechsel.

A4: Pre-Shared Keys (PSKs) regelmäßig wechseln

Wenn ein PSK verwendet wird, sollte dieser regelmäßig gewechselt werden (etwa alle drei bis sechs Monate). Außerdem sollte er möglichst zufällig gewählt oder aus einem Passwort hoher Komplexität mit mindestens 20 Zeichen gebildet werden. Keinesfalls dürfen Passwörter aus bekannten, in Wörterbüchern vorhandenen Zeichenkombinationen bestehen.

A5: Aufstellort und Antennencharakteristik der Access Points optimieren

Aufstellort und Antennencharakteristik der Access Points sollten so gewählt werden, dass möglichst nur das gewünschte Gebiet funktechnisch versorgt wird. Dabei ist zu beachten, dass sich die Funkwellen dreidimensional ausbreiten.

Außerdem sollten die Access Points zugriffssicher (z.B. in Doppelböden, Zwischendecken oder Metallgehäusen) montiert werden, um Manipulationen direkt am Access Point bzw. am Ethernet-Anschluss zum LAN zu verhindern. Dies ist besonders wichtig, wenn keine physikalische Trennung zwischen WLAN Distribution System und dem internen LAN vorgenommen wird (wie es oft bei einem Controller-basierten Design der Fall ist).

Die Außeninstallation von Access Points ist nach Möglichkeit zu vermeiden. Bei einer Antennenmontage im Außenbereich ist auf geeigneten Schutz gegen Blitzschlag und Witterungseinflüsse zu achten.

A6: Sendeleistung an den Access Points optimieren

Die Sendeleistung an den Access Points sollte – falls technisch möglich – reduziert werden, damit nach Möglichkeit nur das gewünschte Gebiet funktechnisch versorgt wird. Hierbei ist zu beachten, dass zur Erzielung der maximalen Datenübertragungsrate eine bestimmte Güte des Signals erforderlich ist.

A7: Regelmäßiges Einspielen von Firmware-Upgrades / Software-Updates auf den WLAN-Komponenten

Die Verfügbarkeit von Firmware-Upgrades, Updates und Patches für die Software der WLAN-Komponenten (insbesondere Access Points und WLAN Controller) sowie zugehörige Gerätetreiber der WLAN-Endgeräte sollte regelmäßig überprüft werden. Neue Firmware- bzw. Software-Versionen oder Patches sollten allerdings erst nach einem angemessenen Test eingespielt werden, um den reibungslosen Betrieb im WLAN nicht zu gefährden. Hierbei ist außerdem zu beachten, dass Upgrades und Updates oft nur greifen, wenn sie auf allen beteiligten WLAN-Komponenten eingespielt werden.

A8: Konfiguration der Access Points nur über sichere Kanäle

Die Konfiguration und Administration der Access Points sollte nur über sichere Kanäle erfolgen, d.h. der administrative Zugriff über die Luftschnittstelle ist, soweit technisch möglich, zu deaktivieren.

Weiterhin sollten unsichere Administrationszugänge wie z.B. Telnet, SSHv1 und HTTP möglichst abgeschaltet werden. Ein administrativer Zugriff muss in jedem Fall über eine verschlüsselte Verbindung erfolgen, z.B. über HTTPS oder SSHv2.

Der physische Zugriff auf die Access Points sollte nur autorisierten Personen möglich sein.

A9: WLAN-Komponenten nur bei Gebrauch einschalten

Bei Nichtbenutzung der WLAN-Komponenten kann in Betracht gezogen werden, deren Funktion zu deaktivieren. Dies gilt gleichermaßen für Access Points und Endgeräte, bei letzteren insbesondere auch für den Ad-Hoc-Modus. Diese Maßnahme ist oft für SOHO-WLAN sinnvoll.

Zwischenfazit

Durch korrekte Konfiguration und Administration der Funkkomponenten des WLAN können viele Angriffe abgewehrt werden, die mit frei verfügbaren Werkzeugen durchführbar sind. Dadurch wird Schutz gegen unberechtigte Anmeldungen an ein WLAN und gegen Mithören des WLAN-Datenverkehrs erreicht. Die Verfügbarkeit des Systems kann mit diesen Maßnahmen gegebenenfalls erhöht werden, das WLAN ist diesbezüglich dennoch leicht angreifbar.

Zum Schutz von sensiblen Daten müssen mindestens Verschlüsselung und Integritätsprüfung mit CCMP (gemäß IEEE 802.11i bzw. WPA2) genutzt werden. Eine Absicherung allein durch WEP reicht unter keinen Umständen aus. Weiterhin muss von TKIP abgeraten werden. Bei größeren WLAN-Installationen ist eine geeignete Authentisierung mit zentraler Schlüsselverwaltung essenziell. Dazu wird IEEE 802.1X verwendet. Bei kleineren WLAN-Installationen im SOHO-Bereich und bei der LAN-Kopplung über WLAN können Pre-Shared Keys eingesetzt werden.

In Behörden- und Firmennetzen mit einer größeren Anzahl von Benutzern sind einige Maßnahmen (z.B. A2.5 und A4) oft nicht im erforderlichen Umfang praktikabel.

A.4.2 Zusätzliche technische Maßnahmen

Zur Erhöhung der Sicherheit können folgende zusätzliche technische Maßnahmen eingesetzt werden.

B1: Verwendung eines VPN zur Absicherung des WLAN – HS

Genauso wie der Remote Access eines Clients über das Internet auf die eigene Infrastruktur mit einem Virtual Private Network (VPN) geeignet abgesichert werden kann, ist es möglich, die Kommunikation über ein WLAN zu schützen. Dies ist allerdings bei Nutzung von WPA2 nur bei hohem Schutzbedarf nötig.

Grundsätzlich kann sowohl ein IP-VPN auf Basis von IPsec als auch ein SSL-VPN genutzt werden. Das Distribution System wird dabei durch ein VPN-Gateway abgeschlossen. Das WLAN bildet das unsichere Transportnetz, über das durch einen entsprechend verschlüsselten Tunnel zwischen Client und VPN-Gateway ein gesicherter Kommunikationskanal etabliert werden kann. Die Kommunikation über das WLAN hinaus mit der weiteren Infrastruktur geschieht ausschließlich über das VPN-Gateway. Der Aufbau des Tunnels muss dabei an eine geeignet starke Authentisierung der Kommunikationspartner geknüpft sein.

B2: Abschottung des drahtgebundenen Firmen-/Behördennetzes durch Firewall und Intrusion Detection System bzw. Intrusion Prevention System – HS

Das drahtgebundene Firmen-/Behördennetz sollte durch eine Firewall gegen die WLAN-Endgeräte (und allgemein gegen Zugriffe auf Access-Point-Ebene) abgeschottet werden. Für diese Abschottung kann das Firewall-System auch durch ein Intrusion Detection System (IDS) bzw. ein Intrusion Prevention System (IPS) ergänzt werden. Durch diese Abschottung können unerlaubte Kommunikationsbeziehungen und Angriffsmuster, wie beispielsweise Port Scans, Buffer Overflows und das Verhalten vieler Würmer und Viren, festgestellt und blockiert werden.

Das Regelwerk der Firewall bzw. die Policy des IDS/IPS müssen in ihrer Schärfe den Schutzanforderungen entsprechend gestaltet werden (beispielsweise darf nur explizit erlaubter Kommunikationsverkehr die Firewall passieren). Für den Einsatz von Firewalls und IDS/IPS müssen insbesondere auch Festlegungen zum Logging und zur Auswertung von Protokolldateien, zur Definition von Sicherheitsvorfällen und zu entsprechenden Reaktionen beim Eintreten eines solchen Sicherheitsvorfalls spezifiziert werden.

Die Abschottung des Firmen-/Behördennetzes ist in folgenden Situationen bereits bei einem normalen Schutzbedarf erforderlich:

- Es werden Geräte im WLAN genutzt, die nicht unter der administrativen Kontrolle des Betreibers der IT-Infrastruktur stehen (z.B. PCs von Gästen oder Geräte von Fremdfirmenmitarbeitern) und daher nicht gemäß A2.1 abgesichert werden können.
- Im Rahmen einer Migration müssen zeitweilig noch Endgeräte-Altlasten im WLAN eingesetzt werden, die nicht die technischen Möglichkeiten für die Umsetzung von A2.1 haben.

B3: Überwachung der Luftschnittstelle des WLAN durch ein Wireless Intrusion Detection System – HS

Mittlerweile sind neben kabelbasierten IDS auch spezielle funkbasierte IDS auf dem Markt verfügbar (sogenannte Wireless IDS), die mit Funksensoren oder mit den produktiv genutzten Access Points das Frequenzspektrum des WLAN überwachen und sicherheitsrelevante Anomalien (z.B. fremde bzw. unbekannte Access Points und Endgeräte) entdecken und melden können. Teilweise wird ein Wireless IDS auch als Komponente eines WLAN-Management-Systems (siehe Maßnahme B5) realisiert.

Bei erhöhtem Schutzbedarf ist der Einsatz eines Wireless IDS (ggf. auch als Ergänzung zu einem kabelbasierten IDS) empfehlenswert.

Hierfür ist eine sorgfältige Planung erforderlich. Bei der Überwachung des WLAN durch Funksensoren sind Anzahl und Aufstellungsort der Funksensoren zu planen. Bei der Verwendung der produktiven Access Points muss beachtet werden, dass die Überwachungsfunktion auf den Access Points zu Leistungseinbußen führen kann. Weiterhin müssen Festlegungen zum Logging, zur Definition von Sicherheitsvorfällen und zur entsprechenden Reaktionen beim Eintreten eines solchen Sicherheitsvorfalls getroffen werden.

B4: Schutz auf Anwendungs- und Server-Ebene – HS

Sicherheitsmaßnahmen auf Anwendungs- und Server-Ebene sind insbesondere erforderlich, wenn im Rahmen einer Migration zeitweilig noch Endgeräte-Altlasten im WLAN eingesetzt werden müssen, die nicht gemäß A2.1 abgesichert werden können. Außerdem kommen die folgenden Maßnahmen zur Absicherung bei einem hohen Schutzbedarf in Frage:

- Auf Anwendungsebene kann eine Authentisierung und eine Ende-zu-Ende-Verschlüsselung vorgenommen werden, sofern diese Funktionen von der Anwendung bzw. dem Client- und dem Server-System unterstützt werden. Die Anforderungen an die Güte der eingesetzten Verfahren unterscheiden sich nicht von der Absicherung der Luftschnittstelle mit IEEE 802.11i oder VPN (siehe A2.1 bzw. B1).

- Eine angemessene Authentisierung und Verschlüsselung der Kommunikation vorausgesetzt kommen hier auch Terminal Server und Portal-Lösungen in Frage.
- Ein weiteres Beispiel ist die Absicherung der Übertragung von VoIP über WLAN. Mechanismen hierzu werden in der Technischen Leitlinie Sichere TK-Anlagen des BSI behandelt (siehe [TLSTK08]), etwa die Ende-zu-Ende-Absicherung der Übertragung von VoIP über WLAN mit dem Secure Real-time Transport Protocol (SRTP).

B5: Einsatz eines zentralen WLAN-Management-Systems

Mit Hilfe eines zentralen WLAN-Management-Systems (gegebenenfalls auch WLAN-Management-Modul zu einem bereits eingesetzten Netzmanagementsystem) sollten die folgenden Funktionen ermöglicht werden:

- Überwachung der Konfiguration von WLAN-Netzelementen (Access Points, WLAN Controller usw.)
- Erkennung und Ortung von Fremdgeräten, insbesondere von fremden (rogue) Access Points und von Störsendern[15]
- Überwachung der Übertragungsqualität auf der Luftschnittstelle
- Überwachung der Verfügbarkeit der Authentisierungs-Server
- gegebenenfalls Wireless IDS zur Erkennung von Sicherheitsvorfällen auf der Luftschnittstelle
- allgemeine Alarm- und Fehlerbehandlung im WLAN mit Schwellwertüberwachung, Auslösung von Maßnahmen, Auswertungen und Statistiken

B6: Absicherung der Endgeräte

Insbesondere bei mobilen Endgeräten, die sich in verschiedene WLANs einbuchen können, sollten weitere lokale Schutzmaßnahmen implementiert werden, wie z.B. Zugriffsschutz, Benutzerauthentisierung, Virenschutz, Personal Firewall, restriktive Datei- und Ressourcen-Freigabe auf Betriebssystemebene, restriktive Browser-Konfiguration, lokale Verschlüsselung usw. Ein WLAN-Endgerät sollte außerdem während der WLAN-Kommunikation keine weitere Netzverbindung aufbauen und auf der WLAN-Verbindung keine Netzwerk-Dienste als Server erbringen.

WLAN-Endgeräte, die Daten mit hohem Schutzbedarf verarbeiten, sollten nicht in unsicheren Umgebungen betrieben werden, d.h. sie sollten nur in WLANs eingesetzt werden, die vertrauenswürdig sind bzw. vollständig unter eigener Kontrolle betrieben werden und einem hohen Schutzniveau genügen.

Diese Maßnahmen gelten generell auch für die Verwendung von PDAs und Smartphones im WLAN: Daten mit erhöhtem Schutzbedarf, die auf dem PDA oder Smartphone abgelegt werden, sollten grundsätzlich verschlüsselt und das Gerät sollte gegen unberechtigten Zugriff geschützt werden. Für eine solche Absicherung der Endgeräte sollte das Gerät beispielsweise automatisch nach einer gewissen Zeitspanne ohne Nutzereingabe gesperrt werden und im Falle eines Smartphones nur einen eingeschränkten Dienstumfang (Annahme von Rufen, Absetzen von Notrufen) zur Verfügung stellen. Zum Entsperren muss der Nutzer sich am Endgerät authentisieren.

Weitere Informationen zur Absicherung auf Ebene der Endgeräte können den IT-Grundschutzkatalogen entnommen werden (siehe [GSK]). Für den erhöhten Schutzbedarf sei außerdem auf die Technische Leitlinie Sichere TK-Anlagen verwiesen (siehe [TLSTK08]).

---

15 Die Ortung von WLAN-Geräten ist inzwischen oft ein Bestandteil eines WLAN-Management-Systems und es gibt auch dedizierte Positionierungssysteme auf WLAN-Basis (siehe Kapitel A.1.5.5). Störsender stellen eine spezielle Bedrohung dar, denn sie sind oft nur durch einen Leistungseinbruch im WLAN detektierbar und können nur schwer – wenn überhaupt – mit WLAN-Mitteln lokalisiert werden, da sie nicht notwendig mit WLAN-Technik arbeiten müssen.

A.4.3 Organisatorische Maßnahmen

Diese nichttechnischen Maßnahmen dienen, in Kombination mit den Maßnahmen A und B, der Anhebung des Sicherheitsniveaus.

C1: Ermittlung des Schutzbedarfs der über das WLAN übertragenen Daten

Für die Ermittlung des Schutzbedarfs hat in einem WLAN-Konzept zunächst eine Erhebung der im WLAN übertragenen oder darüber erreichbaren Daten und Anwendungen zu erfolgen. Als eine Grundlage für die Auswahl und Gestaltung der Sicherheitsmaßnahmen muss dann der Schutzbedarf – etwa unter Einsatz der im BSI-Standard 100-2 beschriebenen Vorgehensweise (siehe [BSI08]) – festgestellt werden.

Dabei sollte (sofern nicht in einem anderen Zusammenhang bereits durchgeführt) auch eine datenschutzspezifische Bewertung der Daten und Anwendungen erfolgen.

C2: Sicherheitsrichtlinien aufstellen

Für den Einsatz von WLAN-Komponenten in Behörden und Unternehmen sollten individuelle Sicherheitsrichtlinien sowohl für Benutzer als auch für Administratoren aufgestellt werden. Diese WLAN-spezifischen Sicherheitsrichtlinien sollten konform zum generellen Sicherheitskonzept der Behörde bzw. des Unternehmens sein und regelmäßig auf Aktualität überprüft und gegebenenfalls angepasst werden. Weiterhin muss das WLAN im Notfallvorsorgekonzept angemessen berücksichtigt werden. Typische Punkte einer WLAN-Sicherheitsrichtlinie findet man z.B. in Teil 2 der Technischen Richtlinie Sicheres WLAN (siehe [TR-S-W2]).

Nutzer eines WLAN sollten für Gefährdungen sowie für Inhalte und Auswirkungen der Richtlinie sensibilisiert werden.

C3: Einhaltung der Sicherheitsrichtlinien überprüfen

Die Einhaltung der Vorgaben sollte ständig kontrolliert werden. Mechanismen zur Überprüfung der Einhaltung sind z.B.:

C3.1 Regelmäßige Kontrollen der Access Points und Endgeräte mittels Protokollanalysator für WLAN und kabelbasiertes LAN

C3.2 Regelmäßige, gegebenenfalls stichprobenartige Auswertung der Protokolldatei (Log) der Access Points und Überprüfung der an einem Access Point angemeldeten Endgeräte

Diese Kontrollen und Auswertungen können durch ein zentrales WLAN-Management-System unterstützt werden.

C4: Gezielte Administratorschulungen

Der verantwortliche Betrieb eines WLAN, insbesondere auch der zugehörigen Sicherheitsmaßnahmen, erfordert den gezielten Aufbau des notwendigen Know-how. Hierfür sollten eine Grundlagenschulung zu den benutzten Mechanismen sowie eine produktspezifische Schulung zu Administrationsaufgaben erfolgen. Danach sollte eine Einweisung zu den Inhalten der WLAN-Sicherheitsrichtlinie erfolgen. Darüber hinaus ist noch eine entsprechende WLAN-spezifische Messtechnik-Schulung sinnvoll.

C5: Schulung der WLAN-Benutzer

Die Nutzer des WLAN sind zu den in der Benutzerrichtlinie aufgeführten Maßnahmen zu schulen. Hierzu gehören auch Hinweise auf die Nutzung komplexer Passwörter.

C6: Sensibilisierung des Objektschutzes zur WLAN-Problematik

Der Objektschutz (z.B. der Werkschutz) sollte dahingehend sensibilisiert werden, dass er darauf achtet, dass sich nicht über längere Zeit unbekannte Personen mit Notebook und gegebenenfalls sogar mit WLAN-Antennen in unmittelbarer Nähe des Liegenschafts- oder Betriebsgeländes aufhalten.

C7: WLAN-spezifische Abnahme

Nach Abschluss der WLAN-Installation sollte anhand des Leistungsverzeichnisses eine Abnahme durchgeführt werden. Dabei sind die speziellen Eigenschaften eines WLAN besonders zu berücksichtigen, z.B. Schwankungen der Empfangsqualität und Mobilität zwischen Access Points. Die Abnahmetests und die zugehörigen Messverfahren (z.B. zur Bewertung der Güte einer WLAN-Ausleuchtung) sollten als Bestandteil der Planungs- bzw. Ausführungsunterlagen festgelegt sein.

C8: Pflege der Dokumentation

Wie für ein LAN ist auch für das gesamte WLAN eine Dokumentation zu führen, in der z.B. die Position der Access Points, Aufbau des Distribution Systems, Firmware- und Software-Stände der WLAN-Komponenten, Konfigurationsdetails, Sicherheitskonfigurationen und eine Historie geführt werden.

Für den WLAN-Einsatz muss die Dokumentation zusätzlich solche bautechnischen Aspekte berücksichtigen, die Einschränkungen der Signalausbreitung auf Funkebene haben können. Diese können Relevanz für die Access-Point-Positionierung haben, sobald ein Bereich durch WLAN-Technik erschlossen werden soll.

C9: Sicherheitsrevision

Folgende Bereiche müssen regelmäßig kontrolliert werden:

C9.1 WLAN-Infrastruktur: Alle Komponenten der WLAN-Infrastruktur sind regelmäßig auf ihre korrekte Konfiguration zu überprüfen. Neben den Access Points zählen hierzu die Komponenten des Distribution System, die WLAN Controller, die Elemente der Sicherheitsinfrastruktur (inklusive Authentication Server) und des Management-Systems.

Zur weitergehenden Verifikation der korrekten Konfiguration sollten zentrale Sicherheitssysteme (wie WLAN Controller, der Authentication Server oder das Koppelelement am Übergangspunkt zwischen Distribution System und LAN) Sicherheits-Scans unterzogen werden.

Insbesondere für Installationen in öffentlich zugänglichen Bereichen sollte eine stichprobenartige Prüfung im Hinblick auf gewaltsame Öffnungsversuche oder Manipulationsversuche (speziell für Access Points) durchgeführt werden.

C9.2 WLAN-Endgeräte: Weiterhin müssen die WLAN-Endgeräte regelmäßig überprüft werden. Bei einer größeren Anzahl sollte dies zumindest stichprobenartig geschehen.

C9.3 WLAN-Sicherheitskonzept: Zusätzlich sollte auch eine regelmäßige Revision des WLAN-Sicherheitskonzepts durchgeführt werden. Insbesondere sollte eine Bewertung erfolgen, ob die ergriffenen Maßnahmen zur Absicherung des WLAN noch dem Stand der Technik entsprechen und ob der zugrunde gelegte Schutzbedarf nach wie vor gültig ist.

Sofern möglich, sollte das Sicherheitskonzept gemäß der BSI IT-Grundschutzmethodik (beispielsweise über das GS-Tool[16]) dokumentiert und gegebenenfalls einer IT-Grund-

[16] Mit der Entwicklung des BSI-Tool IT-Grundschutz (GS-Tool) stellt das BSI eine Software bereit, die den Anwender bei Erstellung, Verwaltung und Fortschreibung von IT-Sicherheitskonzepten entsprechend dem IT-Grundschutz effizient unterstützt.

schutzzertifizierung zugeführt werden. Dadurch ist gewährleistet, dass zumindest alle zwei Jahre – im Rahmen der Re-Zertifizierung – ein umfassendes Audit der WLAN-Infrastruktur durchgeführt wird.

C10: Schutz personenbezogener Daten

Je nach Anwendung eines WLAN muss der Schutz personenbezogener Daten berücksichtigt werden.

C10.1 Wenn personenbezogene Daten bei der Anwendung von WLAN anfallen, muss der Datenschutzbeauftragte in den Prozessen zur Absicherung des WLAN beteiligt werden. Der Datenschutzbeauftragte kann dann zum Schutz der personenbezogenen Daten beispielsweise die WLAN-spezifischen Anforderungen zur Absicherung der WLAN-Übertragung und insbesondere zum Schutz der WLAN-Endgeräte und der dort gespeicherten Daten vor unberechtigtem Zugriff mitgestalten.

Typische Beispiele für WLAN-Anwendungen, bei denen personenbezogene Daten berücksichtigt werden müssen, sind:

- Bei der Nutzung von WLAN im Bereich der Telekommunikation muss beachtet werden, dass hier meist auch sensitive personenbezogene Daten von diesen Systemen verarbeitet und gespeichert werden (z.B. Teilnehmerprofile und Verbindungsdaten).
- Wird im WLAN eine Anwendung zur Ortung von Endgeräten genutzt, besteht oft ein (ggf. indirekter) Bezug zu personenbezogenen Daten. Dies ist beispielsweise der Fall, wenn ein Gerät einer Person zugeordnet ist. Die Positionsdaten werden im WLAN-System erhoben und zwischengespeichert (z.B. im WLAN-Management-System).

C10.2 Ein Nutzer von öffentlichen Hotspots sollte sich versichern, dass der von ihm gewählte Hotspot-Anbieter (Wireless Internet Service Provider, WISP) datenschutzkonform mit den personenbezogenen Daten umgeht.

A.4.4 Beispielszenarien zur Maßnahmenauswahl

Im Folgenden wird für drei typische Größenordnungen von WLAN-Installationen eine Auswahl der oben aufgeführten Sicherheitsmaßnahmen getroffen, die für das entsprechende Szenario einen Schutz für den normalen Schutzbedarf bzw. für einen erhöhten Schutzbedarf bieten. Die aufgeführten Maßnahmen für den hohen Schutzbedarf sind als **zusätzliche Maßnahmen** zu den Basismaßnahmen für den normalen Schutzbedarf zu verstehen.

Betrachtet werden die drei allgemeinen Beispielszenarien

► kleine WLAN-Installation,

► große WLAN-Installation und

► SOHO-WLAN

sowie die Nutzung von Hotspots, die LAN-Kopplung und Mesh-Netze.

Ein normaler Schutzbedarf bedeutet, dass die Schadensauswirkungen begrenzt und überschaubar sind. Bei einem hohen Schutzbedarf können die Schadensauswirkungen beträchtlich sein.

A.4.4.1 Kleine WLAN-Installation

Das Beispielszenario „Kleine WLAN-Installation“ umfasst maximal 10 Access Points, die von ca. 100 WLAN-Endgeräten genutzt werden.

Lösungen für einen normalen Schutzbedarf

Für eine Basislösung sollten die folgenden Schutzmaßnahmen umgesetzt werden:

- A1.1: Festlegung eines Frequenzstandards und der Übertragungstechnik
- A1.2: Untersuchung der Einsatzumgebung auf mögliche Störungen des WLAN auf Funkebene
- A1.3: Festlegungen zum Aufbau des Distribution System

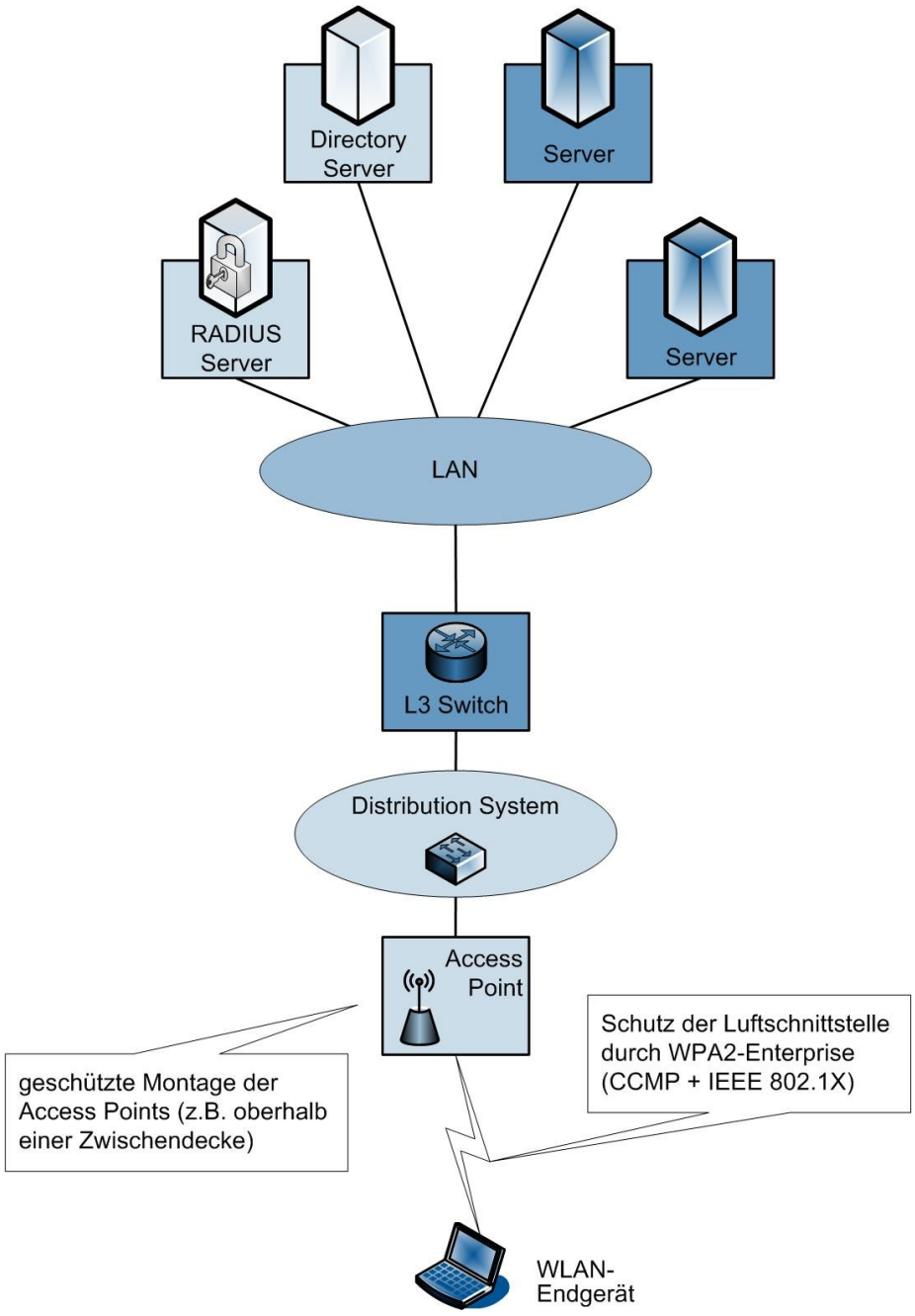
  Aus betrieblichen Gesichtspunkten und zur Realisierung einer klaren Unterscheidung der Infrastruktur des WLAN und der sonstigen IT-Umgebung wird empfohlen, die (maximal 10) Access Points möglichst auf einen eigenen Switch aufzuschalten, der exklusiv für das Distribution System genutzt wird und in einem zentralen Verteilerraum untergebracht sein sollte. Der Switch muss in ein zentrales Netzmanagement integriert werden können.
- A1.5: Planung der zu verwendenden WLAN-Authentisierungsverfahren und deren Nutzung
- A1.6: Erstellung eines Anforderungskatalogs für die WLAN-Beschaffung
- A1.7: Planung und Prüfung des Zusammenwirkens aller WLAN-Komponenten und der zugehörigen Infrastruktur
- A2.1: Für Verschlüsselung und Integritätsschutz sollte WPA2-Enterprise (CCMP und IEEE 802.1X) genutzt werden.

  Die Authentisierung geschieht mit IEEE 802.1X. Dabei können auch die EAP-Methoden PEAP oder EAP-TTLS genutzt werden.
- A2.2: Identifikations- und Passwortvorgaben ändern
- A2.3 / A2.4: SSID Broadcast am Access Point abschalten und Assoziation via Broadcast SSID deaktivieren
- A3: Schlüssel und Zugangspasswörter von hoher Komplexität nutzen
- A5: Aufstellort und Antennencharakteristik des Access Points optimieren
- A6: Sendeleistung an den Access Points optimieren
- A7: Regelmäßiges Einspielen von Firmware-Upgrades / Software-Updates auf den WLAN-Komponenten
- A8: Konfiguration der Access Points nur über sichere Kanäle
- B6: Absicherung der Endgeräte
- C1: Ermittlung des Schutzbedarfs der über das WLAN übertragenen Daten
- C2 / C3: Sicherheitsrichtlinien aufstellen und deren Einhaltung überprüfen
- C4 / C5: Gezielte Administratorschulungen und Schulung der WLAN-Benutzer

- C7: Abnahme
- C8: Pflege der Dokumentation
- C9: Sicherheitsrevision

Diese Basislösung (siehe Abbildung A-17) kann erweitert werden, indem zur Authentisierung anstelle von PEAP oder EAP-TTLS die EAP-Methode EAP-TLS (oder EAP-FAST, falls EAP-TLS nicht möglich ist) genutzt und die Schutzmaßnahme B5 „Einsatz eines zentralen WLAN-Management-Systems“ umgesetzt wird.

Abbildung A-17: Netzplan des Beispielkonzepts für kleine WLAN-Umgebung für normalen Schutzbedarf bei homogener Endgerätesituation



Erweiterung der Lösungen für einen hohen Schutzbedarf

Für den hohen Schutzbedarf werden zwei Szenarien unterschieden:

- In Szenario 1 besteht ein hoher Vertraulichkeits- und Integritätsschutz.
- In Szenario 2 dagegen liegt der hohe Schutzbedarf in den hohen Verfügbarkeitsanforderungen begründet.

Bei Szenario 1 sollte die Basislösung um die Umsetzung der Schutzmaßnahme B1 „Verwendung eines VPN zur Absicherung des WLAN“ mit einer zugehörigen zertifikatsbasierten Authentisierung ergänzt werden. Alternativ ist auch eine Absicherung des WLAN durch den ausschließlichen Einsatz von WPA2-Enterprise zusammen mit der EAP-Methode EAP-TLS zur Authentisierung möglich. Weiterhin ist meist auch der Einsatz von Firewall-Techniken zur Abschottung des kabelbasierten Netzes (Bestandteil der Maßnahme B2) erforderlich. Die Anforderungen an das Firewall-System sind von dem konkreten Einsatzszenario des WLAN abhängig. Eine detailliertere Beschreibung hierzu kann [TR-S-W2] entnommen werden.

In Szenario 2 werden die hohen Verfügbarkeitsanforderungen durch ein Monitoring der Luftschnittstelle z.B. mit einem Wireless IDS (Maßnahme B3) erreicht.

A.4.4.2 Große WLAN-Installation

Dieses Szenario umfasst ca. 100 (oder mehr) Access Points, die von ca. 1000 WLAN-Endgeräten genutzt werden. Es wird auch eine standortübergreifende WLAN-Nutzung betrachtet. Weiterhin soll das WLAN auch für VoIP unter Verwendung von WLAN-IP-Telefonen genutzt werden, und es wird angenommen, dass auch ein Gastzugang unterstützt werden soll.

Lösungen für einen normalen Schutzbedarf

Für eine Basislösung gelten im Allgemeinen die Schutzmaßnahmen für die Basislösung in kleinen WLAN-Installationen. Allerdings müssen zwei Maßnahmen den geänderten Bedingungen angepasst werden (siehe Abbildung A-18):

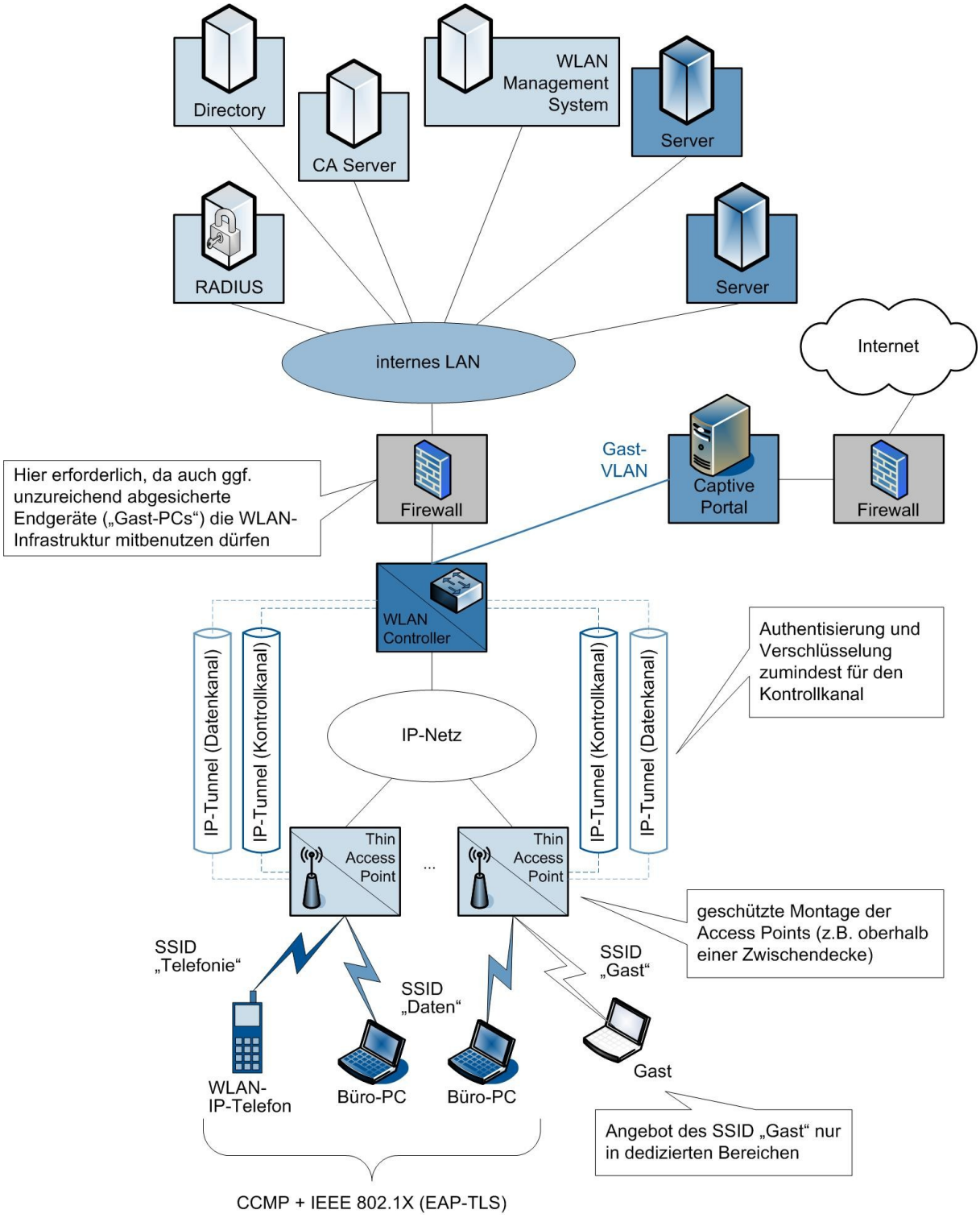
- A1.3: Festlegungen zum Aufbau des Distribution System

  Bei größeren flächendeckenden WLAN-Installationen hat das Controller-basierte WLAN-Design wesentliche Vorteile. Für den normalen Schutzbedarf ist eine physikalische Trennung der Vernetzung von Thin Access Points und WLAN Controller nicht zwingend erforderlich. Bei Bedarf kann ergänzend zur Trennung des WLAN-Verkehrs über den Tunnelmechanismus zwischen Thin Access Points und WLAN Controller eine logische Netztrennung über VLAN – ggf. fortgesetzt auf Layer 3 durch Virtual Routing and Forwarding (VRF) oder ein Multiprotocol Label Switching (MPLS) VPN – vorgenommen werden.

- A2.1: Verschlüsselung, Integritätsschutz und Authentisierung auf der Luftschnittstelle

  Für Verschlüsselung und Integritätsschutz sollte für alle eigenen Geräte (inklusive der WLAN-IP-Telefone) möglichst WPA2-Enterprise (CCMP und IEEE 802.1X) eingesetzt werden, und die Authentisierung nach IEEE 802.1X sollte bevorzugt mit der EAP-Methode EAP-TLS (bzw. wenn dies nicht möglich ist mit EAP-FAST) erfolgen.

Abbildung A-18: Netzplan des Beispielkonzepts für eine große WLAN-Umgebung für drei Nutzergruppen



Außerdem sollten zusätzlich die folgenden Schutzmaßnahmen umgesetzt werden:

- A1.4: Im betrachteten Szenario können beispielsweise die drei Gruppen Büro-PC, IP-Telefon und Gast-Nutzer unterschieden werden. Jeder Nutzergruppe wird ein eigener SSID zugeordnet.

  Auf den Access Points wird WMM zur Priorisierung der Sprachkommunikation aktiviert.

Der SSID für Gast-Nutzer wird ausschließlich in Besprechungsbereichen angeboten. Der WLAN-Verkehr der Gäste wird am WLAN Controller – wie in Abbildung A-6 gezeigt – in ein separates Netz entkoppelt, über das ausschließlich ein Captive Portal erreichbar ist. Weiterhin wird eine Bandbreitenbegrenzung für den Gast-SSID konfiguriert, und es werden ausschließlich personalisierte und zeitlich befristete Gastkonten verwendet.

- B2: Da für Gäste die Nutzung der WLAN-Infrastruktur gestattet wird, ist die strikte Kontrolle des Kommunikationsverkehrs, der über das WLAN auf die interne LAN-Infrastruktur zugreift, erforderlich.
- B5: Einsatz eines zentralen WLAN-Management-Systems
- C6: Sensibilisierung des Objektschutzes zur WLAN-Problematik
- C10.1: Beteiligung des Datenschutzbeauftragten bei der Absicherung des WLAN insbesondere für die Bereiche VoIP und Gastzugang

Diese Basislösung (siehe Abbildung A-18) kann – wie in Abbildung A-16 gezeigt – durch den Einsatz eines Wireless IDS erweitert werden.

Erweiterung der Lösungen für einen hohen Schutzbedarf

Für den hohen Schutzbedarf werden zwei Szenarien unterschieden:

- In Szenario 1 besteht die Anforderung eines hohen Vertraulichkeits- und Integritätsschutzes für die WLAN-Kommunikation.
- In Szenario 2 dagegen liegt der hohe Schutzbedarf in den hohen Verfügbarkeitsanforderungen begründet.

Bei Szenario 1 muss die Basislösung für die Anbindung der PCs um die Umsetzung der Schutzmaßnahme B1 „Verwendung eines VPN zur Absicherung des WLAN“ mit einer zugehörigen zertifikatsbasierten Authentisierung ergänzt werden. Für den weitergehenden Schutz der Sprachkommunikation ist bevorzugt Maßnahme B4 unter Verwendung von SRTP umzusetzen. Wenn dies nicht möglich ist, muss mit Maßnahme B1 auch für die WLAN-IP-Telefone ein VPN verwendet werden.

In Szenario 2 werden die hohen Verfügbarkeitsanforderungen zusätzlich zu den Maßnahmen für den normalen Schutzbedarf durch die Umsetzung der Schutzmaßnahme B3 „Überwachung der Luftschnittstelle des WLAN“ durch ein Wireless Intrusion Detection System, inklusive einer Funktion zur Lokalisierung eines Sicherheitsvorfalls bzw. allgemein einer Störung, erreicht.

Auf einen Gastzugang sollte bei Szenario 2 entweder verzichtet werden, oder durch Verwendung dedizierter Access Points und einer separaten Vernetzung dieser Access Points sollte eine physikalische Trennung gemäß Abbildung A-8 für den Gastzugang erfolgen.

Für die Verbesserung der Verfügbarkeit kann generell die Verwendung des 5-GHz-Bereichs in Betracht gezogen werden, da der größere Frequenzbereich eine robustere Zellplanung mit geringeren Gleichkanalstörungen gestattet und hier – im Gegensatz zu dem Band bei 2,4 GHz – neben WLAN praktisch keine anderen Datenkommunikationssysteme operieren. Im Rahmen der Spezifikation eines Frequenzstandards gemäß Maßnahme A1.1 kann darüber hinaus kritischen Anwendungsbereichen (z.B. VoIP oder Automatisierungsanwendungen in der industriellen Fertigung) ein dedizierter Frequenzbereich zugewiesen werden, den auf dem Gelände des Unternehmens oder der Behörde keine anderen Funkanwendungen nutzen dürfen. Typisch ist hier der Bereich 5,15 bis 5,25 GHz, der ohne Auflagen hinsichtlich DFS (Dynamic Frequency Selection) und TPC (Transmit Power Control) genutzt werden kann.

A.4.4.3 SOHO-WLAN

Dieses Szenario spiegelt die Situation von Heimanwendern oder Freiberuflern wider und umfasst einen Access Point, der von ca. drei WLAN-Endgeräten genutzt wird.

Lösungen für einen normalen Schutzbedarf

Für eine Basislösung sollten die folgenden Schutzmaßnahmen umgesetzt werden:

- A1.1: Festlegung eines Frequenzstandards und der Übertragungstechnik
- A1.2: Untersuchung der Einsatzumgebung auf mögliche Störungen des WLAN auf Funkebene
- A1.5: Planung der zu verwendenden WLAN-Authentisierungsverfahren und deren Nutzung
- A2.1: Für Verschlüsselung und Integritätsschutz sollte möglichst WPA2-Personal (CCMP und PSK) genutzt werden[17]. Wenn dies nicht sinnvoll umsetzbar ist (etwa weil aus organisatorischen Gründen keine komplexe Passphrase oder kein regelmäßiger Wechsel der Passphrase möglich ist) muss zumindest Wi-Fi Protected Setup unter Verwendung von CCMP eingesetzt werden.
- A2.2: Identifikations- und Passwortvorgaben ändern
- A2.3 / A2.4: SSID Broadcast am Access Point abschalten und Assoziation via Broadcast SSID deaktivieren[18]
- A2.5: MAC-Adressfilterung
- A3: Schlüssel und Zugangspasswörter von hoher Komplexität nutzen
- A4: PSK regelmäßig wechseln
- A5: Aufstellort und Antennencharakteristik des Access Points optimieren
- A6: Sendeleistung an den Access Points optimieren
- A7: Regelmäßiges Einspielen von Firmware-Upgrades / Software-Updates auf den WLAN-Komponenten
- A8: Konfiguration der Access Points nur über sichere Kanäle
- A9: WLAN-Komponenten nur bei Gebrauch einschalten
- B6: Absicherung der Endgeräte
- C1: Ermittlung des Schutzbedarfs der über das WLAN übertragenen Daten
- C4 / C5: Gezielte Administratorschulungen und Schulung der WLAN-Benutzer

---

17 Die Verwendung von PSK ist (unter der Voraussetzung einer genügenden Komplexität der zugrunde liegenden Passphrase) akzeptabel, da im SOHO-WLAN nur wenige Stationen beteiligt sind und der Aufwand für eine manuelle und trotzdem effektive Schlüsselverwaltung überschaubar ist.

18 Falls die Endpunkte dies zulassen.

Erweiterung der Lösungen für einen hohen Schutzbedarf

Ein erhöhter Schutzbedarf besteht, wenn über das WLAN besonders zu schützende Daten, wie Patienten- oder Mandantendaten, die gegebenenfalls den Bestimmungen des Bundesdatenschutzgesetzes (BDSG) unterliegen, auf den WLAN-Endgeräten gespeichert und verarbeitet werden.

Bei einem hohen Schutzbedarf muss zusätzlich zu den für einen normalen Schutzbedarf genannten Maßnahmen zumindest WPA2-Personal mit CCMP unter Verwendung von PSK genutzt werden. In diesem Zusammenhang sei auf die strikte Einhaltung der Maßnahmen A3 und A4 hingewiesen.

Ist der Einsatz von WPA2-Personal nicht möglich, kann alternativ auch ein VPN (Schutzmaßnahme B1) zur Absicherung des WLAN eingesetzt werden.

A.4.4.4 Hotspot-Nutzung

Öffentliche Hotspot-Systeme stellen dem Nutzer einen drahtlosen transparenten Internet-Zugang bereit. Im Hinblick auf eine sichere Hotspot-Nutzung sind folgende Grundprinzipien von Hotspot-Systemen relevant:

- Es gibt bis heute keine einheitliche systemübergreifende Authentisierung und Abrechnung für Hotspot-Systeme.
- In der Regel werden keine Verschlüsselungsmechanismen auf der Luftschnittstelle zur Verfügung gestellt.
- Die Anmeldung im Hotspot erfolgt meist an einem Web-Portal über eine Web-Applikation; diese muss für den Schutz der Anmelde-Information sorgen.

Auf Grund der vielfältigen Bedrohungen, denen ein WLAN-Endgerät in einer Hotspot-Umgebung ausgesetzt ist, sind spezielle Konfigurationsvorgaben zur Absicherung des Endgeräts notwendig.

Es ist zu beachten, dass ein Nutzer eines Hotspot-Systems lediglich auf die Konfiguration seines WLAN-Endgeräts Einfluss nehmen kann. Auf die Absicherung der Luftschnittstelle und der Access Points sowie auf die Architektur und Absicherung des Distribution Systems, auf die benötigte Sicherheitsinfrastruktur und das WLAN-Management hingegen hat er keinerlei Einfluss.

Lösungen für einen normalen Schutzbedarf

Für einen normalen Schutzbedarf sollten die folgenden Schutzmaßnahmen umgesetzt werden:

- A7: Regelmäßiges Einspielen von Firmware-Upgrades / Software-Updates (hier Updates und Patches für die Gerätetreiber der WLAN-Endgeräte) nach ausführlichen Tests
- A9: WLAN-Komponenten (hier WLAN-Adapter) nur bei Gebrauch einschalten
- B6: Absicherung der Endgeräte

  Die Verwendung des Hotspot wird möglichst nur für den Aufbau eines VPN-Tunnels gestattet. Dieser Tunnelaufbau sollte möglichst automatisch, unmittelbar nachdem eine Internet-Verbindung über den Hotspot hergestellt ist, erfolgen. Da kein Einfluss auf Sicherheitsmechanismen auf der Luftschnittstelle genommen werden kann, sind Maßnahmen auf Ebene des Endgeräts und auf höheren Netzwerkschichten notwendig, die sich nicht wesentlich von denen für einen mobilen Remote-Access-Client unterscheiden. Grundlage der Absicherung ist die strikte Umsetzung der anwendbaren Maßnahmen der entsprechenden Bausteine der IT-Grundschutz-Kataloge (siehe [GSK]), insbesondere Bausteine B 3.203 „Laptop“ und B 3.208 „Internet-PC“. Hierzu zählen unter anderem:

- Einsatz einer Personal Firewall-Software
- Entfernung von nicht benötigten Stamm-CA-Zertifikaten (Certificate Authority)

  Client-Systeme werden mit einem vorkonfigurierten Satz von Stamm-CA-Zertifikaten ausgestattet. Diese Liste muss auf das notwendige Minimum reduziert werden, um die Angriffsfläche für Man-in-the-Middle-Attacken gegen SSL-Sitzungen zu reduzieren.
- Restriktive Browser-Konfiguration

  Siehe hierzu auch M 5.93 „Sicherheit von WWW-Browsern bei der Nutzung von Internet-PCs“ und M 5.66 „Verwendung von SSL“ der IT-Grundschutz-Kataloge (siehe [GSK]).
- Virenschutz
- Einrichtung einer eingeschränkten Benutzerumgebung
- Zugriffsschutz (komplexe Kennwörter, besonders komplexe Administrator-Kennwörter)
- Scanning und Patching (d.h. Härtung) der WLAN-Endgeräte

► C1: Ermittlung des Schutzbedarfs der über das WLAN übertragenen Daten

► C2 / C3: Sicherheitsrichtlinien (hier Benutzerrichtlinien für die Hotspot-Nutzung) aufstellen und deren Einhaltung überprüfen

In dieser Benutzerrichtlinie werden beispielsweise die folgenden Punkte für die Hotspot-Nutzung geregelt:

- Sensibilisierung zum Umgang mit SSL-Zertifikaten
- Beschreibung, wie eine Plausibilitätsprüfung des Zertifikats erfolgen kann (Fingerprint, Gültigkeitsdauer, Inhaber und Zertifizierungsinstanz des Zertifikates)
- Anweisung, dass WLAN-Adapter auszuschalten sind, wenn sie nicht in Benutzung sind
- Verhaltensweisen bei einer vermuteten Kompromittierung des WLAN- Endgeräts
- Ggf. Verpflichtung des WLAN-Nutzers, den Hotspot-Zugang nur zur Etablierung der RAS-Verbindung (Remote Access Service) zu nutzen

► C4 / C5: Gezielte Administratorschulung und Schulung der WLAN-Benutzer (hier insbesondere hinsichtlich der Hotspot-Nutzung)

Es sollte auch eine regelmäßige Nachschulung der Hotspot-Nutzer erfolgen.

Erweiterung der Lösungen für einen hohen Schutzbedarf

Für WLAN-Endgeräte, die Daten mit hohem Schutzbedarf verarbeiten, werden zwei Alternativen vorgeschlagen, die im Rahmen der Schutzbedarfsfeststellung und einer Risikoanalyse zu bewerten sind:

► Empfohlen wird ein Verbot der Hotspot-Nutzung.

► Abweichend davon muss zumindest eine Einschränkung der Hotspot-Nutzung durch die folgenden Maßnahmen erfolgen, die zusätzlich zum Basisschutz (siehe Maßnahmen für den normalen Schutzbedarf) durchzuführen sind:

- C10: Es wird nur die Nutzung von vertrauenswürdigen Hotspots gestattet, zu deren Betreiber eine entsprechende vertragliche Beziehung besteht. Dabei muss in jedem Fall der Schutz personenbezogener Daten sichergestellt sein.
- Absicherung der Luftschnittstelle

  Es sollten nur Hotspots genutzt werden, die eine Absicherung der Luftschnittstelle mit WPA2 unterstützen (sinngemäße Anwendung von A2.1).

- Die Verwendung des Hotspots wird nur für den Aufbau eines VPN-Tunnels gestattet. Dieser Tunnelaufbau sollte möglichst automatisch, unmittelbar nachdem eine Internet-Verbindung über den Hotspot hergestellt ist, erfolgen. Dies beinhaltet auch die Forderung, dass jeglicher Datenverkehr nach Aufbau des VPN-Tunnels ausschließlich über diesen läuft und beispielsweise kein Internet-Zugang außerhalb des VPN-Tunnels erlaubt ist.
- Restriktivere Einstellung der Regelbasis der Personal Firewall
- Verschlüsselung der Daten auf dem Endgerät
- Erhöhter Zugriffsschutz durch Zweifaktorauthentisierung (Wissen und Besitz) z.B. mit Chipkarten, Token usw.
- Unterbindung bzw. starke Einschränkung der Nutzung von Wechseldatenträgern

A.4.4.5 LAN-Kopplung

Bei einer LAN-Kopplung wird eine WLAN-Übertragung als verbindendes Medium zwischen zwei LANs genutzt. Die Koppelelemente werden als Wireless Bridges bezeichnet und haben, wie auch ein Access Point, auf der einen Seite eine Ethernet-Schnittstelle zur Anbindung an das kabelbasierte LAN und auf der anderen Seite eine WLAN-Schnittstelle.

Bei einer LAN-Kopplung fehlt das dynamische Element mobiler Endgeräte. Die Kommunikation erfolgt statisch zwischen den beteiligten Wireless Bridges.

Bei der LAN-Kopplung werden oft hohe Anforderungen an die Verfügbarkeit gestellt. Die Erwartungshaltung des Nutzers ist eine Verfügbarkeit, die mindestens einer WAN-Verbindung entspricht. Diese Anforderung ist durchaus kritisch zu sehen, da im Außenbereich eine Funkverbindung stets durch die Umwelt oder Störungen beeinflusst wird.

Lösungen für einen normalen Schutzbedarf

Für einen normalen Schutzbedarf sollten die folgenden Schutzmaßnahmen umgesetzt werden:

► A1.1: Festlegung eines Frequenzstandards und der Übertragungstechnik

► A1.2: Untersuchung der Einsatzumgebung auf mögliche Störungen des WLAN auf Funkebene

► A1.5: Planung der zu verwendenden WLAN-Authentisierungsverfahren und deren Nutzung

► A2.1: Für Verschlüsselung und Integritätsschutz WPA2 (CCMP) nutzen

Zur Authentisierung kann die Variante WPA2-Personal mit Pre-Shared Keys zum Einsatz kommen

► A2.2: Identifikations- und Passwortvorgaben ändern

► A2.3 / A2.4: SSID Broadcast am Access Point abschalten und Assoziation via Broadcast SSID deaktivieren

► A3: Schlüssel und Zugangspasswörter von hoher Komplexität nutzen

► A4: Im Fall der Nutzung von Pre-Shared Keys den PSK regelmäßig wechseln

► A5: Aufstellort und Antennencharakteristik der Wireless Bridges optimieren

Die Montage der Wireless Bridges sollte möglichst in einem geschlossenen, geeignet klimatisierten Technikraum bzw. einem entsprechenden Schutzschrank erfolgen. Bei einer Außenmontage einer Wireless Bridge muss die Wireless Bridge entweder eine Außenmontage erlauben, d.h. das

Gehäuse der Wireless Bridge ist geeignet gegen Witterungseinflüsse (Hitze, Kälte, eindringende Feuchtigkeit usw.) geschützt. Andernfalls muss die Wireless Bridge in einen für den Außeneinsatz spezifizierten Schutzschrank montiert werden. Bei der Montage ist weiterhin zu beachten, dass die Wireless Bridge vor elektrischen Entladungen und unberechtigtem Zugriff geeignet geschützt ist. Speziell ist sicherzustellen, dass ein Schutz vor einem unberechtigten Zugriff auf die Kommunikationsschnittstellen (Ethernet, serielle Schnittstelle) besteht.

Bei der Montage einer Außenantenne muss der Schutz vor elektrischen Entladungen berücksichtigt werden. Bei Anbringung von Antennen auf Gebäudedächern muss die Antenne gegen Blitzschlag gesichert werden. Antennen im Außenbereich, die möglicherweise von der Gefahr elektrischer Entladungen betroffen sind, sollten über einen speziellen Überspannungsschutz angeschlossen werden. Außenantennen sind geeignet gegen Schnee-Ablagerung zu schützen. Sie sind entweder windgeschützt anzubringen, oder die Anbringung muss auch bei hohen Windstärken so fest sein, dass sich die Antennenausrichtung nicht verstellt.

- A6: Sendeleistung an den Wireless Bridges optimieren

  Hier müssen in jedem Fall die Vorgaben der Bundesnetzagentur hinsichtlich der maximalen Strahlungsleistung berücksichtigt werden.

- A7: Regelmäßiges Einspielen von Firmware-Upgrades / Software-Updates auf den WLAN-Komponenten (hier für die Wireless Bridges)

- A8: Konfiguration der Wireless Bridges bevorzugt nur über sichere Kanäle

  Diese Maßnahme wird für die LAN-Kopplung bewusst leicht abgeschwächt. Ein administrativer Zugriff auf eine Wireless Bridge sollte bevorzugt über die Ethernet-Schnittstelle bzw. die serielle Schnittstelle von dedizierten Management-Stationen aus erfolgen. Der administrative Zugriff über die Luftschnittstelle sollte auf ein Minimum beschränkt werden und sich dabei möglichst nur auf einen lesenden Zugriff beschränken. Es sind sichere Management-Protokolle zu verwenden. Von der Nutzung Web-basierter Zugriffe wird abgeraten.

- Ggf. B1: Verwendung eines VPN zur Absicherung des WLAN

  Eine Wireless Bridge wird normalerweise möglichst in der Nähe der Außenantenne montiert, da das Hochfrequenzkabel zwischen Wireless Bridge und Antenne je nach verwendetem Kabeltyp das Signal unterschiedlich stark dämpft. In einer solchen Situation kann es vereinzelt vorkommen, dass eine geeignete räumliche Absicherung des Zugangs zur Wireless Bridge nicht vollständig umgesetzt werden kann. In dieser Situation kann bereits bei einem normalen Schutzbedarf der Einsatz eines Site-to-Site IPsec VPN eine Option sein, wobei die beteiligten VPN-Gateways entsprechend gesichert aufgestellt sein müssen und der VPN-Tunnel die unsicheren Bereiche vollständig abdeckt.

- B2: Abschottung des kabelbasierten Firmen-/Behördennetzes

  Die Kopplung zwischen einer Wireless Bridge und dem LAN erfolgt über eine Layer-3-Instanz. Die Wireless Bridges sind Bestandteil eines eigenen IP-Subnetzes (Transportnetz). Sofern die genutzten Dienste sinnvoll begrenzt werden können, ist eine ACL (Access Control List, Layer 3 und höher) auf der Routing-Instanz zu empfehlen.

- Ggf. B3 und B5: Überwachung der Luftschnittstelle des WLAN durch ein Wireless Intrusion Detection System und Einsatz eines zentralen WLAN-Management-Systems

  Werden nur wenige Wireless Bridges im Netzwerk eingesetzt, kann die Verwaltung über die vom Hersteller mitgelieferten Konfigurations-Tools durchgeführt werden.

  Allerdings ist eine effektive und effiziente Überwachung der Wireless Bridges nur über ein zentrales Management möglich. Eine solche kontinuierliche Überwachung der Luftschnittstelle kann bereits bei einem normalen Schutzbedarf in Betracht gezogen werden.

Für einen normalen Schutzbedarf kann prinzipiell auf ein Out-of-Band-Management verzichtet werden. Allerdings ist eine solche Einrichtung für das Management von Wireless Bridges in vielen Fällen technisch sinnvoll.

- C1: Ermittlung des Schutzbedarfs der über das WLAN übertragenen Daten
- C2 / C3: Sicherheitsrichtlinien aufstellen und deren Einhaltung überprüfen (hier keine Benutzerrichtlinie, sondern nur eine Administrationsrichtlinie erforderlich)
- C4: Gezielte Administratorschulungen
- C8: Pflege der Dokumentation
- C9: Sicherheitsrevision

Erweiterung der Lösungen für einen hohen Schutzbedarf

Für den hohen Schutzbedarf wird hier die Schaffung eines hohen Vertraulichkeits- und Integritätsschutzes betrachtet. Hierzu wird das Konzept um ein Site-to-Site-IP-VPN ergänzt. Die Kommunikation zwischen den VPN-Gateways wird über IPsec geschützt. Das VPN-Gateway kann als separate Komponente oder als Modul einer Firewall realisiert sein. Durch den Einsatz einer VPN-Lösung auf IPsec-Basis wird ein vergleichbar hohes Sicherheitsniveau wie bei der Verwendung eines VPN zur Kopplung von Standorten über das Internet erreicht. Die erreichte Schutzklasse der Daten und des LAN hängt primär von der Implementierung des VPN-Gateways ab.

Wenn auch ein hoher Schutzbedarf hinsichtlich der Verfügbarkeit besteht, müssen auch andere Übertragungsalternativen in Betracht gezogen werden. Neben der kabelbasierten Übertragung kann hier auch der Einsatz von Richtfunktechniken in Frage kommen.

A.4.4.6 Mesh-Netze

Für die Absicherung des Mesh-Verkehrs, d.h. für die Kommunikation zwischen den Mesh Access Points (MAPs), gelten grundsätzlich die im Kapitel A.4.4.5 spezifizierten Maßnahmen.

Zu beachten ist allerdings, dass sich Mesh-Netze durch eine größere Dynamik im Sinne wechselnder Übertragungswege im Netz und wechselnder Netzwerkknoten auszeichnen. Ein zentrales Netzmanagement und ein kontinuierliches Monitoring der Luftschnittstelle der beteiligten Stationen sind unabdingbar. In diesem Zusammenhang ist die Authentisierung der MAPs (z.B. durch ein Zertifikat) an einer zentralen Stelle wesentlich. Manche Lösungen erreichen dies durch Realisierung eines Mesh-Netzes über ein Controller-basiertes WLAN-Design. Die MAPs müssen sich dann wie andere Thin Access Points am WLAN Controller authentisieren, um Bestandteil des WLAN zu werden.

Die Absicherung des Access-Verkehrs, d.h. der Kommunikation von WLAN-Endgeräten mit einem MAP, erfolgt mit den in Kapitel A.4.4.1 bzw. A.4.4.2 spezifizierten Maßnahmen.

A.5 Ausblick

WLANs gehören zu den sich am dynamischsten entwickelnden Bereichen der Kommunikationstechnik und man muss sich stets auf Entwicklungen einstellen, die auch Auswirkungen auf die Sicherheit haben. An der kommenden Integration von WLAN und Mobilfunktechnik wird beispielsweise nicht mehr gezweifelt. Die Nutzung von WLANs zur Telekommunikation und sogar ein Handover zwischen GSM- bzw. UMTS-Netzen und WLANs sind inzwischen Realität.

Das Controller-basierte WLAN-Design ist eine weitere Technik, die sich jetzt schon durchgesetzt hat und die sich noch erheblich entwickeln wird. Die hiermit verbundenen Konzepte gewinnen insbesondere im Rahmen der Implementierung von WLANs als natürlichem Bestandteil konvergenter Netze an Bedeutung. WLANs werden vermehrt nicht mehr als separate Spezialnetze gesehen werden, sondern bilden zusammen mit den zugehörigen Sicherheitsmechanismen einen integralen Bestandteil der IT-Infrastruktur. Die Kommunikation über WLAN wird dabei immer stärker auch für kritische Anwendungen sogar als Alternative zur kabelbasierten Endgeräteanbindung gesehen werden. Neben steigenden Anforderungen an die Kapazität werden damit auch die Ansprüche an die Sicherheit wachsen.

A.6 Fazit

Eine Datenübertragung über Funk muss stets durch eine entsprechende Kombination von Mechanismen zur Authentisierung, Verschlüsselung und Integritätsprüfung geeignet abgesichert werden. Der in IEEE 802.11 ursprünglich festgelegte Mechanismus WEP ist hierzu nur mangelhaft geeignet.

Mit der Erweiterung IEEE 802.11i bzw. mit WPA2 stehen inzwischen Bausteine zur Verfügung, die auf der Luftschnittstelle eine adäquate Absicherung eines WLAN hinsichtlich der Sicherheitsziele Vertraulichkeit und Integrität gestatten. Für größere WLANs und generell für WLANs mit höheren Sicherheitsanforderungen ist der Einsatz von IEEE 802.1X in Kombination mit einer angemessen hochwertigen EAP-Methode zur Authentisierung dringend zu empfehlen. Auf der Basis von WPA2 sind inzwischen eine Vielzahl von Produkten von der Wi-Fi Alliance zertifiziert worden. Die Verfügbarkeit ist in WLAN ein grundsätzliches Problem des Übertragungsmediums Funk, da Störungen der Übertragung nicht ausgeschlossen bzw. nicht verhindert werden können. Das Netzmanagement muss daher diese und andere WLAN-spezifischen Eigenheiten berücksichtigen. Dies beinhaltet speziell auch die Erkennung von Fremdstationen (Access Points und Endgeräte) und deren geografische Lokalisierung.

Der hier vorgestellte Maßnahmenkatalog zur Absicherung eines WLAN macht deutlich, dass auch Maßnahmen notwendig sind, die über die Absicherung der Funkübertragung hinausgehen. Die Absicherung eines WLAN erfordert genauso die Betrachtung von Infrastrukturaspekten wie den geeigneten Aufbau des Distribution System und des Übergabepunkts zur LAN-Infrastruktur.

Obwohl mit IEEE 802.11i eine deutliche Verbesserung der WLAN-Absicherung erreicht ist, gibt es noch offene Punkte, wie z.B. die ungesicherte Übertragung von Management Frames auf der MAC-Ebene. Hier ist mit IEEE 802.11w ein entsprechender Standard in Arbeit. Aktuell muss diese Sicherheitslücke aber noch hingenommen werden.

A.7 Literatur und Links

Ausführliche technische Informationen zur Funktionsweise der in WLAN eingesetzten Sicherheitsmechanismen können dem Teil 1 der Technischen Richtlinie Sicheres WLAN (siehe [TR-S-W1]) entnommen werden. Bedrohungsanalyse und Sicherheitsmaßnahmen werden im Teil 2 vertieft (siehe [TR-S-W2]). Der dritte Teil dieser Richtlinie (siehe [TR-S-W3]) spezifiziert Kriterien für die Auswahl von WLAN-Systemen die hierzu gehörenden Prüfkriterien. Für die Nutzung von WLAN im Bereich der Telekommunikation liefert die Technische Leitlinie Sichere TK-Anlagen (siehe [TLSTK08]) einen umfassenden Maßnahmenkatalog und einen zugehörigen Beschaffungsleitfaden. Ferner sind umfangreiche Publikation über das amerikanische National Institute of Standards and Technology (NIST) verfügbar, die sich mit Aufbau, Betrieb und speziell der Absicherung von WLAN befassen, siehe [NIST07] und [NIST08].

Im Folgenden ist weiterhin die Liste der im Text referenzierten Titel aufgeführt. Diese Liste stellt nur eine wertungsfreie Auswahl ohne Anspruch auf Vollständigkeit dar.

[BDKKS09] A. Biryukov, O. Dunkelman, N. Keller, D. Khovratovich, A. Shamir, „Key Recovery Attacks of Practical Complexity on AES Variants With Up To 10 Rounds“, Cryptology ePrint Archive, Report 2009/374, http://eprint.iacr.org/2009/374

[BeTe09] M. Beck, E. Tews, “Practical attacks against WEP and WPA”, Proceedings of the second ACM conference on Wireless network security, Zürich, 2009, http://dl.aircrack-ng.org/breakingwepandwpa.pdf

[BNA03] Bundesnetzagentur, Vfg 89/2003, „Allgemeinzuteilung von Frequenzen im Frequenzbereich 2400,0 – 2483,5 MHz für die Nutzung durch die Allgemeinheit in lokalen Netzwerken; Wireless Local Area Networks (WLAN- Funkanwendungen)“, 2003

[BNA06] Bundesnetzagentur, „Allgemeinzuteilung von Frequenzen in den Bereichen 5150 MHz - 5350 MHz und 5470 MHz - 5725 MHz für Funkanwendungen zur breitbandigen Datenübertragung, WAS/WLAN (Wireless Access Systems including Wireless Local Area Networks)“, Vfg 8 / 2006, http://www.bundesnetzagentur.de/

[BSI08] Bundesamt für Sicherheit in der Informationstechnik, „BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise, Version 2.0“, 2008, verfügbar unter https://www.bsi.bund.de/cae/servlet/contentblob/471452/publicationFile/30748/standard_1002_pdf.pdf

[EC05] Kommission der Europäischen Gemeinschaften, „Entscheidung der Kommission vom 11. Juli 2005 über die harmonisierte Nutzung von Funkfrequenzen in den 5-GHz-Bändern für die Einführung drahtloser Zugangssysteme einschließlich lokaler Funknetze (WAS/Funk-LANs)“, Amtsblatt der Europäischen Union, 19. Juli 2005, verfügbar unter http://ec.europa.eu/information_society/policy/ecomm/radio_spectrum/documents/legislation/index_en.htm

[FMS01] S. Fluhrer, I. Mantin und A. Shamir, „Weaknesses in the Key Scheduling Algorithm of RC4. In Selected Areas in Cryptography“, SAC 2001, Lecture Notes in Computer Science 2259, Springer-Verlag, Seiten 1-24

[GSK] Bundesamt für Sicherheit in der Informationstechnik, „IT-Grundschutz-Kataloge“, verfügbar unter https://www.bsi.bund.de/cln_155/DE/Themen/weitereThemen/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

[IEEE04-1D] IEEE Std 802.1D-2004, „Media Access Control (MAC) Bridges“, 2004, verfügbar unter http://www.ieee.org

[IEEE04-1X] IEEE Std 802.1X-2004, „Port-Based Network Access Control“, 2004, verfügbar unter http://www.ieee.org

[IEEE07] IEEE Std 802.11-2007, „Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications“, 2007, verfügbar unter http://www.ieee.org

[IEEE08-11k] IEEE Std 802.11k-2008, supplement to 802.11-2007, „Amendment 1: Radio Resource Measurement of Wireless LANs“, 2007, verfügbar unter http://www.ieee.org

[IEEE08-11r] IEEE Std 802.11r-2008, supplement to 802.11-2007, „Amendment 2: fast basic service set (bss)“, 2007, verfügbar unter http://www.ieee.org

[KaPa04] V. Kamath, A. Palekar, “Microsoft EAP CHAP Extensions“, IETF, Internet Draft, April 2004, http://www.ietf.org

[NIST07] „Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i“, Recommendations of the National Institute of Standards and Technology, Special Publication 800-97, Februar 2007, http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf

[NIST08] „Guide to Securing Legacy IEEE 802.11 Wireless Networks“, Recommendations of the National Institute of Standards and Technology, Special Publication 800-48 Revision 1, Juli 2008, http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf

[ÖMS08] Bundesamt für Sicherheit in der Informationstechnik, „Öffentliche Mobilfunknetze und ihre Sicherheitsaspekte“, 2008, https://www.bsi.bund.de/cln_155/ContentBSI/Publikationen/Broschueren/oefms/index_htm.html

[RFC2865] RFC 2865, “Remote Authentication Dial In User Service (RADIUS)”, IETF Draft Standard, Juni 2000, http://www.ietf.org/rfc/rfc2865.txt

[RFC3579] RFC 3579, “RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)”, IETF Informational, September 2003, http://www.ietf.org/rfc/rfc3579.txt

[RFC3711] RFC 3711, „The Secure Real-time Transport Protocol (SRTP)“, IETF Proposed Standard, März 2004, http://www.ietf.org/rfc/rfc3711.txt

[RFC3748] RFC 3748, “Extensible Authentication Protocol (EAP)”, IETF Proposed Standard, Juni 2004, http://www.ietf.org/rfc/rfc3748.txt

[RFC4347] RFC 4347, “Datagram Transport Layer Security”, IETF Proposed Standard, April 2006, http://www.ietf.org/rfc/rfc4347.txt

[RFC4851] RFC 4851, “The Flexible Authentication via Secure Tunneling Extensible Authentication Protocol Method (EAP-FAST)”, IETF Informational, Mai 2007, http://www.ietf.org/rfc/rfc4851.txt

[RFC5216] RFC 5216, „The EAP-TLS Authentication Protocol”, IETF Proposed Standard, März 2008, http://www.ietf.org/rfc/rfc5216.txt

[RFC5281] RFC 5281, „Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)”, IETF Informational, August 2008, http://www.ietf.org/rfc/rfc5281.txt

[RFC5415] RFC 5415, “Control And Provisioning of Wireless Access Points (CAP-WAP) Protocol Specification”, IETF Proposed Standard, März 2009, http://www.ietf.org/rfc/rfc5415.txt

[TKG04] „Telekommunikationsgesetz (TKG)“, Bundesgesetzblatt Jahrgang 2004 Teil I Nr. 29, Juni 2004

[TLSTK08] Bundesamt für Sicherheit in der Informationstechnik, „Technische Leitlinie Sichere TK-Anlagen”, 2008; https://www.bsi.bund.de/cln_155/ContentBSI/Publikationen/Broschueren/tkanlagen/TL02103_htm.html

[TR-S-W1] Bundesamt für Sicherheit in der Informationstechnik, „Technische Richtlinie Sicheres WLAN – Teil 1: Darstellung und Bewertung der Sicherheitsmechanismen“, SecuMedia Verlag, 2005

[TR-S-W2] Bundesamt für Sicherheit in der Informationstechnik, „Technische Richtlinie Sicheres WLAN – Teil 2: Vorgaben eines WLAN Sicherheitskonzepts“, SecuMedia Verlag, 2005

[TR-S-W3] Bundesamt für Sicherheit in der Informationstechnik, „Technische Richtlinie Sicheres WLAN – Teil 3: Auswahl und Prüfung von WLAN-Systemen“, SecuMedia Verlag, 2005

[WPA04] Wi-Fi Alliance, „Wi-Fi Protected Access (WPA)“, Version 2.0, April 2003, http://www.wi-fi.org

A.8 Abkürzungen

ACL	Access Control List
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
BDSG	Bundesdatenschutzgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSS	Basic Service Set
CA	Certificate Authority
CAPWAP	Control And Provisioning of Wireless Access Points
CBC-MAC	Cipher Block Chaining Message Authentication Code
CCMP	Counter mode with CBC-MAC Protocol
CHAP	Challenge Handshake Authentication Protocol
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DCF	Distributed Coordination Function
DECT	Digital Enhanced Cordless Telecommunications
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
DS	Distribution System
DSSS	Direct Sequence Spread Spectrum
DTLS	Datagram TLS
EAP	Extensible Authentication Protocol
EAP-FAST	EAP Flexible Authentication via Secure Tunneling
EAP-TLS	EAP Transport Layer Security
EAP-TTLS	EAP Tunneled Transport Layer Security
EAPOL	EAP over LAN
ESS	Extended Service Set
FAST	Flexible Authentication via Secure Tunneling
FCS	Frame Check Sequence
FHSS	Frequency Hopping Spread Spectrum
FMC	Fixed Mobile Convergence
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GTC	Generic Token Card
GTK	Group Temporal Key
HS	Hoher Schutzbedarf

HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IBSS	Independent Basic Service Set
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
ISM	Industrial, Scientific, and Medical
IT	Informationstechnik
IV	Initialisierungsvektor
L3 (Switch)	Layer 3 (Switch)
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Medium Access Control
MAP	Mesh Access Point
MIC	Message Integrity Check
MIMO	Multiple Input Multiple Output
MPLS	Multiprotocol Label Switching
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MSK	Master Session Key
NIST	National Institute of Standards and Technology
OFDM	Orthogonal Frequency Division Multiplexing
PAC	Protected Access Credential
PAP	Password Authentication Protocol
PBX	Private Branch Exchange
PC	Personal Computer
PCF	Point Coordination Function
PDA	Personal Digital Assistant
PEAP	Protected EAP
PHY	Physical Layer (IEEE)
PKI	Public Key Infrastructure
PMK	Pairwise Master Key
PPP	Point to Point Protocol
PSK	Pre-Shared Key
PSTN	Public Switched Telephone Network
PTK	Pairwise Transient Key
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service

RAP	Root Access Point
RAS	Remote Access Service
RC4	Ron's Code 4
RF	Radio Frequency
RFC	Request for Comments (IETF)
RSN	Robust Security Network
SNMP	Simple Network Management Protocol
SOHO	Small Office / Home Office
SRTP	Secure Real-time Transport Protocol
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TPC	Transmit Power Control
TSC	TKIP Sequence Counter
TTLS	Tunneled TLS
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
VLAN	Virtual LAN
VoIP	Voice over IP
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WISP	Wireless Internet Service Provider
WLAN	Wireless LAN
WMM	Wi-Fi Multimedia
WPA	Wi-Fi Protected Access
WZC	Wireless Zero Configuration
XOR	Exklusives Oder (eXclusive OR)

A.9 Glossar

Access Control List (ACL)

Zugriffskontrollliste für die Filterung von zugelassenen IP-/MAC-Adressen

Access Point

Funkfeststation für den Endgeräte-Zugang in ein WLAN

Advanced Encryption Standard (AES)

Symmetrisches Verschlüsselungsverfahren mit einer variablen Schlüssellänge von 128, 192 oder 256 Bit

Assoziation

Anmeldevorgang eines Endgeräts an einem Access Point

Authentisierung

Verifizierung der Identität einer Instanz, z.B. eines Benutzers oder eines Geräts. Zweck ist oft die anschließende Autorisierung für Zugriffe. Ohne Authentisierung ist im Allgemeinen keine sinnvolle Autorisierung möglich.

Certificate Authority (CA)

Siehe Zertifizierungsstelle

Cyclic Redundancy Check (CRC)

Prüfsumme über die zu übertragenden Daten, die in der Nachricht mitgeschickt wird und es dem Empfänger gestattet, Bitfehler, die auf dem Kommunikationskanal entstanden sind, zu erkennen

Denial of Service (DoS)

Ein Angriff vom Typ Denial of Service hat zum Ziel, die Arbeitsfähigkeit des angegriffenen Objekts möglichst stark zu reduzieren. Dies beinhaltet beispielsweise die systematische Überlastung eines Netzknotens durch unsinnigen Verkehr (Dummy Traffic) oder das beabsichtigte Herbeiführen eines Fehlerzustands durch das Einspielen fehlerhafter Nachrichten.

Dictionary-Attacke

Siehe Wörterbuchattacke

Distribution System (DS)

Netzwerk, das Access Points untereinander und mit der weiteren Infrastruktur verbindet. Das DS kann als physikalisch separates LAN oder als VLAN in einer bestehenden LAN-Infrastruktur realisiert werden.

EAP over LAN (EAPOL)

Verfahren zur Verwendung von EAP auf Layer 2 über Lokale Netzwerke (LANs) wie z.B. IEEE 802.3 (Ethernet) oder IEEE 802.11 (WLAN)

EAP-Transport-Layer Security (EAP-TLS)

EAP-Methode, die Zertifikate zur gegenseitigen Authentisierung benutzt

Extensible Authentication Protocol (EAP)

Rahmen (Framework) für die Verwendung von Authentisierungsmethoden. Es wird u.a. für PPP oder auch in Verbindung mit EAPOL unter IEEE 802.1X verwendet.

Funkzelle

Geografischer Bereich um einen Sender (z.B. Access Point) herum, in dem ein genügend guter Empfang besteht. Was als genügend gut zu bezeichnen ist, ist Festlegungssache. Die Empfangsqualität in einem WLAN hängt unter anderem vom verwendeten Übertragungsstandard, von der Qualität der Hochfrequenz-Hardware in den Geräten und von der Charakteristik der Antennen ab. Die Ausdehnung einer Funkzelle wird weiterhin durch den verwendeten Frequenzbereich, die Sendeleistung und insbesondere durch die jeweiligen Umgebungsbedingungen (z.B. Material von Wänden, Türen, Fenstern und Decken) beeinflusst.

Handover

Wechsel von einem (physikalischen) Kommunikationskanal auf einen anderen unter Aufrechterhaltung der Ende-zu-Ende-Kommunikationsbeziehung. Beispiel: Bei einem Telefonat über VoIP over WLAN darf bei einem (mobilitätsbedingten) Wechsel von einer Funkzelle in eine andere das Gespräch nicht signifikant gestört werden oder sogar abreißen.

Hotspot

Öffentlich zugänglicher Internet-Zugang über ein WLAN

Intrusion Detection System (IDS)

Bietet die Möglichkeit unerwünschte Zugriffe, Inhalte und Angriffe zu erkennen. Sobald das IDS einen Verstoß gegen die vereinbarten Regeln erkennt, erfolgen eine Protokollierung und eine Meldung an den Administrator. Dieser kann manuell Gegenmaßnahmen einleiten.

Intrusion Prevention System (IPS)

Ein IPS kann Angriffe nicht nur erkennen, sondern auch eine als Angriff erkannte Kommunikation unterbinden.

ISM-Frequenzband

Lizenzfrei nutzbare Frequenzbänder, die für industrielle, wissenschaftliche und medizinische Zwecke verwendet werden können (ISM = Industrial, Scientific and Medical)

Man in the Middle

Der Angreifer positioniert sich zwischen zwei Kommunikationspartnern und täuscht beiden Parteien vor, der jeweils erwartete eigentliche Partner zu sein. Dabei kann der Man in the Middle den Dialog zwischen den beiden Parteien belauschen oder auch verfälschen. Ziel ist oft die Ermittlung von Passwörtern.

Message Integrity Check (MIC)

Kryptographischer Integritätsschutzmechanismus

Michael

Name des MIC, der bei WPA und TKIP Verwendung findet.

Pre-Shared Key (PSK)

Vorab vereinbarter bzw. verteilter Schlüssel, welcher für eine symmetrische Verschlüsselung genutzt wird

Public Key Infrastructure (PKI)

System zum Erstellen, Verteilen und Prüfen von digitalen Zertifikaten

Remote Authentication Dial-In User Service (RADIUS)

Protokoll für Authentisierung, Autorisierung und Accounting im Bereich Netzzugang

Robust Security Network (RSN)

WLAN, das ausschließlich eine durch die in IEEE 802.11i spezifizierten Sicherheitsmechanismen geschützte Kommunikation erlaubt

Service Set Identifier (SSID)

Bezeichnet den konfigurierbaren Namen eines WLAN. Wird bei der Anmeldeprozedur und optional zyklisch in Beacon Frames (vom Access Point zyklisch übertragene Pakete, die Übertragungsparameter enthalten) übertragen.

Spoofing

Vortäuschen einer in der Regel vertrauenswürdigen Identität (z.B. durch Manipulation von Adressen) mit dem Ziel, Schaden anzurichten oder unerlaubten Zugriff zu erhalten

Temporal Key Integrity Protocol (TKIP)

Im Standard IEEE 802.11i spezifiziertes Protokoll zur Verschlüsselung und zum Integritätsschutz in WLAN; abwärtskompatibel zu WEP

Transport Layer Security (TLS)

Protokoll zur Wahrung der Vertraulichkeit und Integrität einer Datenübertragung zwischen zwei Systemen bzw. Anwendungen; Weiterentwicklung von SSL (Secure Sockets Layer)

Wi-Fi Alliance

Vereinigung von Herstellern von WLAN-Komponenten nach IEEE 802.11

Wi-Fi Protected Access (WPA)

Von der Wi-Fi Alliance veröffentlichter Standard, der auf einem Draft zu IEEE 802.11i basiert und aufwärtskompatibel zu IEEE 802.11i ist; die Folgeversion WPA2 deckt alle zwingenden Anforderungen von IEEE 802.11i ab.

Wired Equivalent Privacy (WEP)

Im Standard IEEE 802.11 spezifiziertes Protokoll zum Schutz von Vertraulichkeit, Integrität und Authentizität im WLAN. Mittlerweile ist WEP vollständig kompromittiert und für die Absicherung eines WLAN allein als ungenügend einzustufen.

Wörterbuchattacke

Eine Wörterbuchattacke (auch als Dictionary-Attacke bezeichnet) wird typischerweise zum Raten eines Passworts oder Schlüssels eingesetzt. Die Annahme für eine Wörterbuchattacke ist, dass Passwörter oder Schlüssel aus einer sinnvollen oder in Wörterbüchern bekannten Zeichenkombination bestehen. In diesem Falle kann das Verfahren schnell zum Erfolg führen.

Zelle

Siehe Funkzelle

Zertifikat

Von einer Zertifizierungsstelle (Certificate Authority, CA) beglaubigter öffentlicher Schlüssel, der einer Person oder einem Objekt zugeordnet ist

Zertifizierungsstelle

Element einer PKI, welches für das Ausstellen von digitalen Zertifikaten zuständig ist

B. Bluetooth

Inhaltsverzeichnis des Abschnitts

B.1 Grundlagen und Funktionalität

Bluetooth ist ein offener Industriestandard (siehe [IEEE05]) für ein lizenzfreies Nahbereichsfunkverfahren zur kabellosen Sprach- und Datenkommunikation zwischen IT-Geräten (Kabelersatz und Ad-hoc-Networking).

Die Entwicklung von Bluetooth geht auf eine Initiative der Bluetooth Special Interest Group (Bluetooth SIG) im Jahre 1998 zurück, der eine große Zahl Hersteller angehört. Die derzeit aktuelle Version der Spezifikation ist 3.0 + HS (siehe [BTSIG09]). Auf der Spezifikation 2.1 + EDR basierende Produkte sind bereits verfügbar, es werden aber auch noch zahlreiche Geräte der Vorgängerversionen 2.0 oder 1.x verwendet und angeboten.

B.1.1 Technische Grundlagen

Bluetooth arbeitet im 2,4-GHz-ISM-Frequenzband auf 79 Kanälen im Frequenzbereich von 2400 bis 2483,5 MHz[1]. Der Kanalabstand beträgt 1 MHz; an den Bandgrenzen wurden 2 bzw. 3,5 MHz freigelassen, damit keine Störungen benachbarter Systeme auftreten.

Die Übertragung der Datenpakete erfolgt zeitschlitzgesteuert (TDD, Time Division Duplex) in Verbindung mit einem Frequenzsprungverfahren (FHSS, Frequency Hopping Spread Spectrum). Dies dient zur Reduzierung der Empfindlichkeit gegenüber Störungen. Die Zeitschlitzlänge beträgt 625 µs, woraus eine Frequenzwechselhäufigkeit von bis zu 1600 pro Sekunde resultiert. Im Allgemeinen findet ein Frequenzsprung nach jedem versendeten Paket statt. Die Sprung-Sequenz ist pseudozufällig, deckt alle 79 Kanäle gleichmäßig in kurzen Zeitabständen ab und wiederholt sich erst nach Ablauf mehrerer Stunden. Geräte ab der Bluetooth-Spezifikation 1.2 verwenden ein adaptives Frequenzsprungverfahren (AFH, Adaptive Frequency-Hopping), das die von der Sprungsequenz abgedeckten Kanäle auf freie, d.h. ungestörte Frequenzen beschränkt. Hierdurch soll ein störungsfreier Parallelbetrieb mit anderen Funkdiensten, die im selben Frequenzbereich operieren, insbesondere WLAN, erreicht werden.

Als Modulationsverfahren wird eine Frequenz- bzw. Phasenmodulation angewandt. Dabei findet der Frequenz- bzw. Phasensprung grundsätzlich einmal pro Mikrosekunde statt; man spricht von einer Symbolrate von 1 MS/s (megasymbols per second). Die resultierende Datenrate ergibt sich aus dem angewendeten Modulationsverfahren, das die Zahl der pro Symbol übertragenen Bits bestimmt. Bluetooth kennt drei verschiedene Verfahren:

- Eine binäre Frequenzmodulation (GFSK, Gaussian Frequency Shift Keying), bei der ein Bit pro Symbol übertragen wird. Die resultierende Datenrate beträgt 1 Mbit/s und wird als „Basic Rate“ bezeichnet. Dieses Verfahren wurde bereits in der Bluetooth-Spezifikation 1.1 (siehe [IEEE05]) veröffentlicht. Alle Bluetooth-Lösungen müssen dieses Verfahren unterstützen.

- Eine vierwertige Phasenmodulation (π/4-DQPSK, Differential Quaternary Phase Shift Keying), bei der zwei Bits pro Symbol übertragen werden. Die resultierende Datenrate, als „Enhanced Data Rate“ bezeichnet, beträgt 2 Mbit/s. Dieses Verfahren ist Teil der Spezifikation Bluetooth Version 2.0 + EDR (siehe [BTSIG04]).

- Eine achtwertige Phasenmodulation (8DPSK, Differential Phase Shift Keying), bei der drei Bits pro Symbol übertragen werden. Die resultierende Datenrate, ebenfalls als „Enhanced Data Rate“ bezeichnet, beträgt 3 Mbit/s. Auch dieses Verfahren ist Teil der Spezifikation Bluetooth Version 2.0 + EDR (siehe [BTSIG04]).

---

1 Diese Angaben gelten für Deutschland und die meisten europäischen Länder.

Eine Kompatibilität von Stationen unterschiedlicher Bluetooth-Spezifikation wird dadurch erreicht, dass die Protokollinformation am Beginn eines jeden Pakets grundsätzlich mit der „Basic Rate“ ausgesendet wird. Erst zur Übertragung der Nutzdaten wird auf eine Variante von EDR umgeschaltet, sofern die Gegenstation dies unterstützt.

Bluetooth nutzt zwei grundsätzlich verschiedene Modi der Datenübertragung:

- Asynchrone verbindungslose Übertragung (ACL, Asynchronous Connectionless Link)

  Datenpakete werden gesendet, sobald ein Freiraum (Slot) besteht. Jedes Paket trägt eine Zieladresse, anhand derer es an den Empfänger vermittelt wird. Das Verfahren gleicht der Übertragung in WLANs.

- Synchrone verbindungsorientierte Übertragung (SCO, Synchronous Connection Oriented)

  Datenpakete werden in einem festen Zeitraster zwischen Stationspaaren ausgetauscht. Das Verfahren entspricht der leitungsvermittelten Übertragung in einem Telefonnetz.

Die erzielbaren Brutto-Datenraten bei ACL betragen maximal 723 kbit/s in der einen und 58 kbit/s in der anderen Richtung (asymmetrisch) bzw. maximal 434 kbit/s in beiden Richtungen (symmetrisch). Mit EDR lässt sich die 3-fache Übertragungsrate erzielen, d.h. maximal 2,2 Mbit/s in der einen und 177 kbit/s in der anderen Richtung (asymmetrisch) bzw. 1,3 Mbit/s in beide Richtungen (symmetrisch).

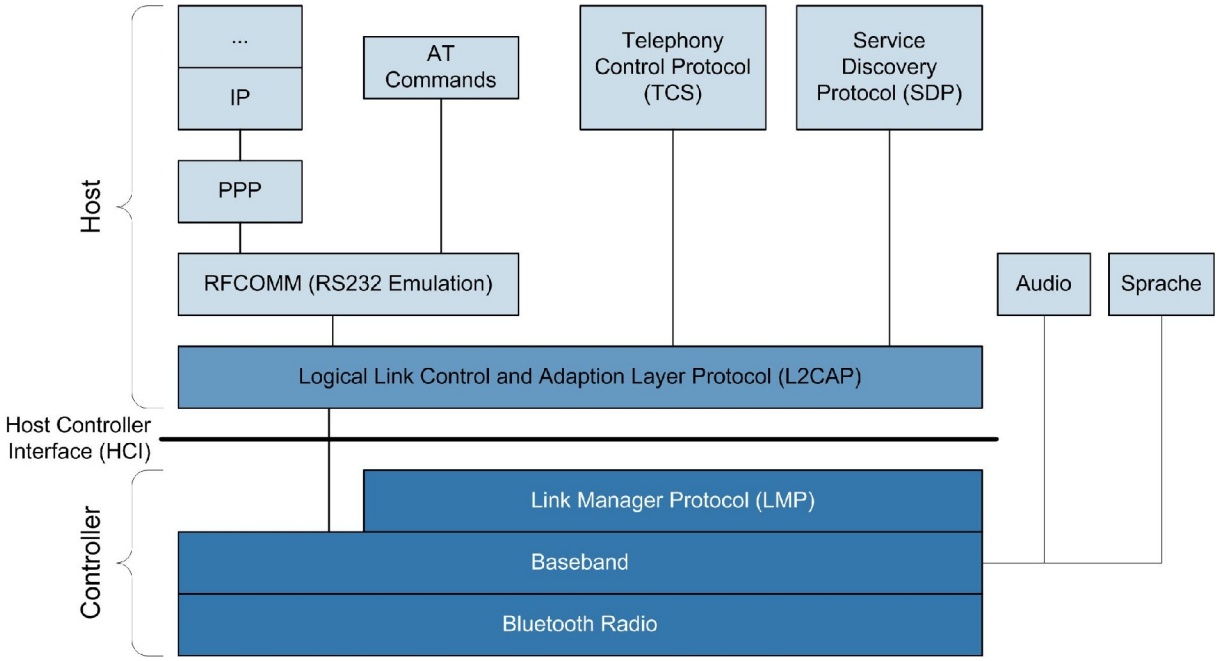
SCO wird für die Übertragung von Sprache eingesetzt. Zu diesem Zweck stehen jeder Station drei Kanäle mit einer Bandbreite von je 64 kbit/s zur Verfügung. Die Kodierung der Sprache erfolgt unter anderem mit logarithmischen PCM-Codecs (Pulse Code Modulation), die auch in der ISDN-Telefonie eingesetzt werden (ITU-T G.711). Ab der Bluetooth-Spezifikation 1.2 stehen synchrone Kanäle mit höherer Bandbreite zur Verfügung, die mit „Extended SCO“ (eSCO) bezeichnet werden. Im Gegensatz zu SCO erlaubt eSCO eine Neuübertragung fehlerhaft empfangener Datenpakte, um die Dienstqualität auch unter ungünstigen Empfangsverhältnissen zu verbessern.

Bluetooth-Stationen werden bezüglich ihrer Sendeleistung klassifiziert. Klasse 1 hat eine maximale Sendeleistung von 100 mW, Geräte mit bis zu 2,5 mW werden in Klasse 2 eingeordnet, solche mit 1 mW in Klasse 3. Die Reichweite variiert von maximal 10 Metern bei 1 mW bis zu ca. 100 Metern bei 100 mW Sendeleistung. Zur Senkung des Stromverbrauchs sind verschiedene Sparmodi (Sniff-, Park- und Hold-Mode) und eine Sendeleistungsregelung (Power Control) spezifiziert.

B.1.2 Protokollarchitektur

Neben den Hardware-nahen Protokollen – Funktechnik und Basisband – definiert die Spezifikation [IEEE05] für das Verbindungsmanagement eine Link-Schicht, die neben Fehlerkorrekturverfahren auch kryptographische Sicherheitsmechanismen bereitstellt. Zusätzlich verfügt sie über eine Host-Controller-Schnittstelle (HCI, Host Controller Interface) sowie das „Logical Link Control and Adaption Layer Protocol“ (L2CAP). Das L2CAP ermöglicht es Bluetooth-Anwendungen, die in Kapitel B.1.1 genannten verbindungsorientierten und verbindungslosen Übertragungsmodi zu initiieren und zu nutzen. Das L2CAP greift über das HCI auf den eigentlichen Bluetooth Controller zu, der über verschiedene Hardware-Schnittstellen angeschlossen sein kann, unter anderem über USB oder serielle Schnittstellen. Eine ausführliche Beschreibung des Bluetooth-Protokoll-Stack findet man in der Literatur (z.B. in [WOLL01]).

Abbildung B-1: Bluetooth-Protokoll-Stack



Um die Interoperabilität unterschiedlicher Geräte sicherzustellen, ohne dass in allen Geräten immer alle existierenden Protokolle implementiert sind, hat die Bluetooth SIG sogenannte Anwendungsprofile definiert. Einige häufig verwandte Profile sind:

- Generic Access Profile (GAP): GAP ist das grundlegende Profil zur herstellerübergreifenden Kommunikation von Bluetooth-Geräten. Das GAP beschreibt die für das Erkennen und den Verbindungsaufbau von Bluetooth-Geräten erforderlichen Prozeduren aus Anwendungssicht. Die Anwendungsprofile setzen die im GAP beschriebenen Prozeduren voraus.

- Serial Port Profile: Serielle Kabelverbindungen (RS-232) zwischen zwei Geräten werden durch Bluetooth ersetzt; das entsprechende Protokoll heißt RFCOMM. Aus der Sicht der Anwendungsprogramme wird durch dieses Profil eine virtuelle serielle Schnittstelle bereitgestellt. Der im Vergleich mit anderen Funktechniken kostengünstige Ersatz serieller Leitungen durch Bluetooth spielt z.B. in der Fertigungsindustrie eine Rolle, wo Leitungen häufig erhöhten Belastungen ausgesetzt sind (ständige Bewegung, Schmutz, usw.).

- Headset Profile und Handsfree Profile: Diese beiden Profile beschreiben Funktionen, die ein Mobiltelefon im Zusammenspiel mit einer Freisprecheinrichtung benötigt. Neben der reinen Übertragung von Sprache in beiden Richtungen spielt beim Handsfree Profile auch die Fernbedienung des Mobiltelefons eine Rolle.

- Advanced Audio Distribution Profile (A2DP): Dieses Profil beschreibt Funktionen zur Übertragung von digitalen Audiodaten in hoher Qualität. Es wird beispielsweise dazu genutzt, hochwertige Stereo-Kopfhörer drahtlos an Abspielgeräte anzubinden.

- Human Interface Device Profile (HID Profile): Dieses Profil beschreibt die Protokolle und Funktionen, die zur drahtlosen Anbindung von Tastaturen, Zeigegeräten (z.B. Mäuse) und Anzeigegeräten an Rechner benötigt werden. Das HID-Profil ersetzt die entsprechenden Funktionen des kabelbasierten Universal System Bus (USB).

- Dialup Network Profile (DUN Profile) und Fax Profile: Diese Profile beschreiben Protokolle und Funktionen zur drahtlosen Anbindung von Modems oder Mobiltelefonen an Rechner mit dem Ziel, darüber Wählverbindungen zur Daten- oder Telefaxübertragung aufzubauen.

- File Transfer, Object Push and Synchronization Profile: Diese Profile werden zum Austausch von Dateien über Bluetooth genutzt. Wichtigste Anwendung ist die Synchronisierung von Kontakten, Terminen, Aufgaben und Mails zwischen tragbaren Geräten (Personal Information Manager, PIM) und Servern. Die Profile basieren auf dem Protokoll OBEX (OBject EXchange).

- Audio/Video Remote Control Profile (AVRCP): Dieses Profil beschreibt Protokolle und Funktionen zur Anbindung von Fernbedienungen an Abspielgeräte.

- SIM Access Profile (SAP): Eine Bluetooth-Station greift auf Daten zu, die in der SIM-Karte einer anderen Station – typischerweise in einem Mobiltelefon – gespeichert sind. Ein typischer Anwendungsfall besteht in einem fest im Fahrzeug eingebauten Autotelefon, das keine eigene SIM-Karte enthält. Stattdessen nimmt es Kontakt zu dem Mobiltelefon des Fahrers auf und meldet sich mit dessen Daten (und auf dessen Kosten) am Mobilfunknetz an.

B.1.3 Verbindungsaufbau und Netztopologien

Damit jedes Bluetooth-Gerät als Kommunikationspartner eindeutig zu identifizieren ist, verfügt es über eine 48 Bit lange öffentlich bekannte und weltweit eindeutige Geräteadresse, die sogenannte Bluetooth Device Address (BD_ADDR).

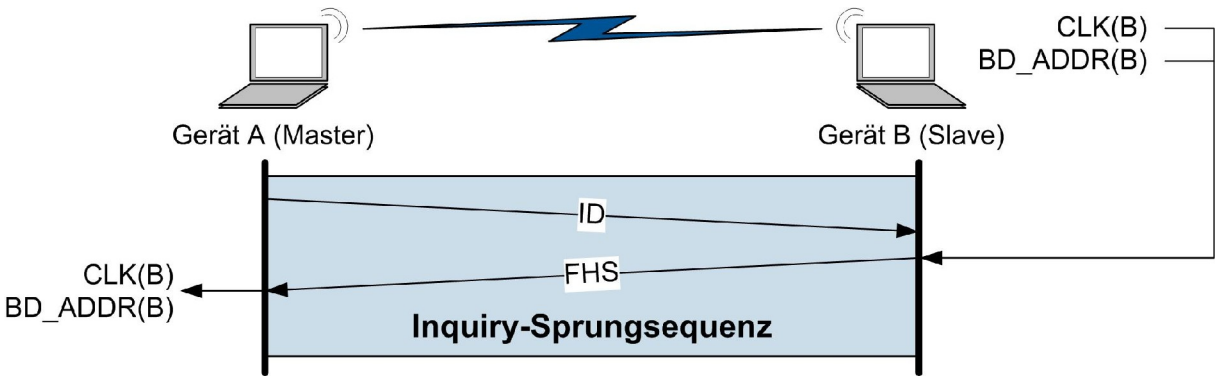
Basis für den Verbindungsaufbau sind die beiden Prozeduren Inquiry und Paging:

- Per Inquiry kann ein Bluetooth-Gerät feststellen, ob sich andere Geräte im Sendebereich befinden. Voraussetzung für das Auffinden eines Geräts mittels Inquiry ist, dass es als erkennbar konfiguriert ist (discoverable). Nach einem Inquiry liegen alle Geräteadressen und Zeittakte („CLK“) der aufgefundenen Geräte vor. Geräte ab der Spezifikation 2.1 + EDR unterstützen ein erweitertes Inquiry, bei dem zusätzlich Gerätename und unterstützte Dienste bekannt gemacht werden.

- Durch eine Paging-Anforderung kann eine Kommunikationsverbindung zu einem per Inquiry gefundenen Gerät aufgebaut werden. Das Gerät, das die Verbindung aufbaut, wird Master genannt, das andere Slave. Während des Paging sendet der Master seine Geräteadresse und seinen Zeittakt an den Slave.

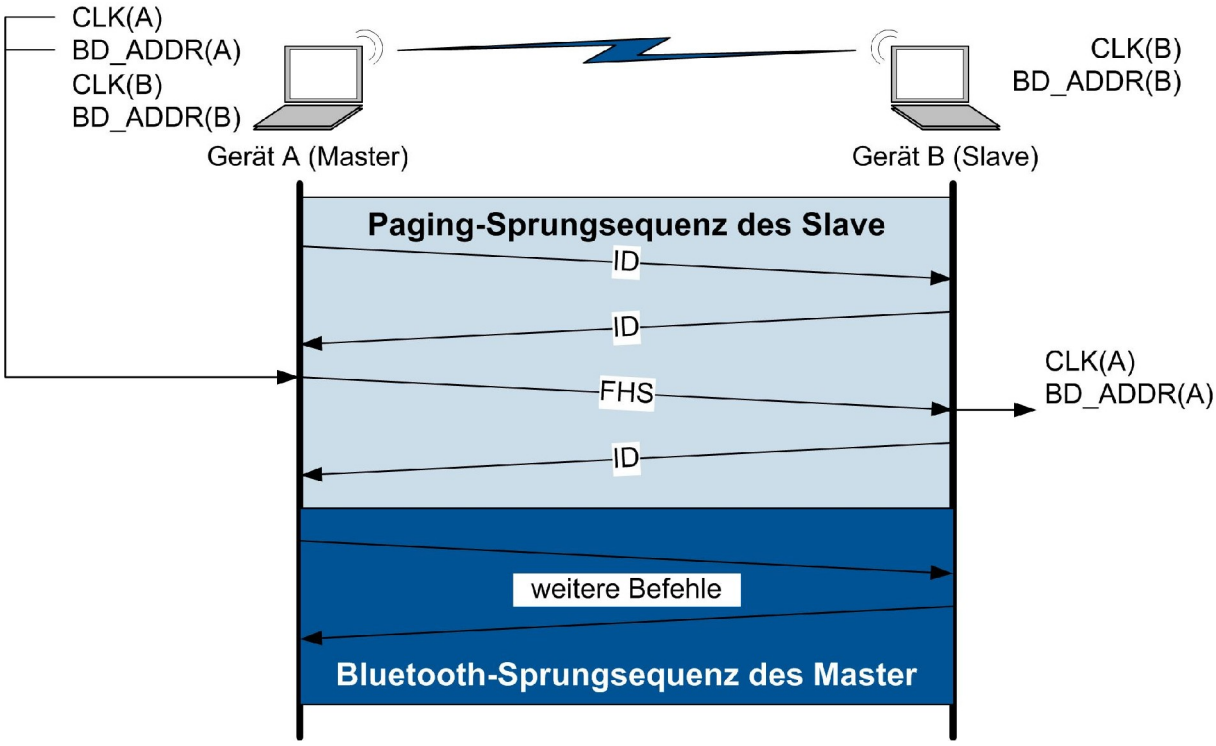
Während Inquiry und Paging verwenden die Geräte vereinfachte Sprungsequenzen mit nur je 32 Frequenzen. Die Periodendauer beträgt ebenfalls 32, sodass jede Frequenz nur pro Sequenz einmal angesprungen wird. Ein Gerät, das auf ein Inquiry wartet, braucht nur diese 32 Frequenzen auf Aktivität zu beobachten. Empfängt es auf einer der Frequenzen ein entsprechendes Paket (ID), kennt es damit bereits die gesamte Sequenz und kann sich darauf synchronisieren. Das Gerät antwortet mit einem Paket (FHS), das sowohl die eigene Geräteadresse (BD_ADDR) als auch den aktuellen Zeittakt (CLK) enthält (siehe Abbildung B-2).

Abbildung B-2: Ablauf des Inquiry (vereinfacht)



Beim Paging kann der Master den Slave gezielt ansprechen, indem er die im Rahmen des Inquiry erhaltene Adresse und Zeittakt verwendet. Er überträgt nun seine Adresse und den Zeittakt an den Slave und benutzt dazu wieder ein FHS-Paket. Damit kann der Slave die wesentlich komplexere Sprungsequenz der eigentlichen Bluetooth-Kommunikation synchron zum Master initiieren (siehe Abbildung B-3). Nach erfolgtem Paging sind somit die physikalischen Voraussetzungen für eine Kommunikation per Bluetooth geschaffen.

Abbildung B-3: Ablauf des Paging (vereinfacht)



Auf das Paging erfolgen in der Regel weitere Schritte als Voraussetzung für eine erfolgreiche Kommunikation. Viele Anwendungsprofile erfordern insbesondere das Herstellen einer paarweisen Geräteverbindung durch Austausch eines sogenannten Link Key (siehe Kapitel B.2.1 und B.2.2). Dieser Vorgang wird im Generic Access Profile (GAP) als Bonding bezeichnet.

Neben einer Punkt-zu-Punkt-Verbindung zwischen zwei Bluetooth-Geräten sieht die Bluetooth-Spezifikation auch Punkt-zu-Mehrpunkt-Verbindungen vor. Bis zu 255 Bluetooth-Geräte (im Sonderfall auch mehr) können in einem sogenannten Piconet als Slaves mit einem Master vernetzt sein. Innerhalb eines Piconet können bis zu 7 Slaves gleichzeitig aktiv mit einem Master kommunizieren. Alle Geräte in einem Piconet folgen der gleichen Channel Hopping Sequence und dem Zeittakt des Masters. Bluetooth sieht sogar die Möglichkeit vor, dass eine Station Teil mehrerer Piconets ist; es entsteht ein sogenanntes Scatternet. Zur Bildung von Scatternets und zum anschließenden Datenaustausch in einem solchen Netz werden jedoch zusätzliche Protokolle benötigt, für die es derzeit nur Ideen, jedoch keine praktischen Implementierungen gibt.

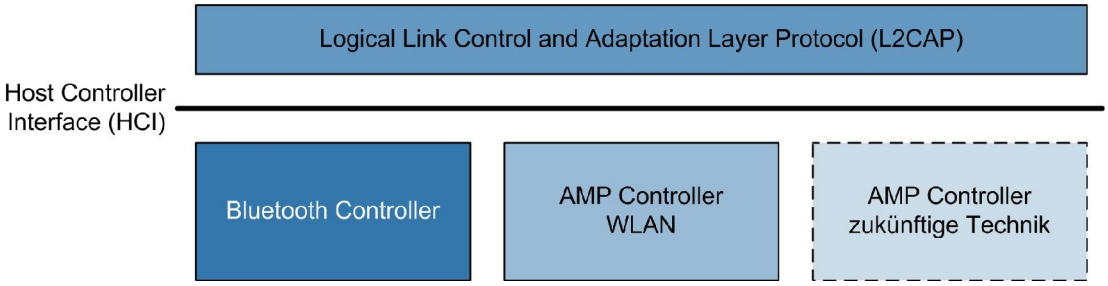
B.1.4 Neue Bluetooth-Varianten

B.1.4.1 Bluetooth über IEEE 802.11 WLAN

In der Spezifikation Bluetooth 3.0 + HS findet sich die Beschreibung einer alternativen Funktechnik, als „Alternate MAC/PHY“ (AMP) bezeichnet. Bluetooth kann unter Nutzung der physikalischen Schnittstelle des WLAN gemäß IEEE 802.11 höhere Datenraten bereitstellen als bisher. Das L2CAP wurde zu diesem Zweck um Funktionen erweitert, die eine Wahl der Funktechnik und des entsprechenden Controllers zulassen. Es gibt sogar Funktionen, die den Wechsel der Funktechnik während einer bestehenden Verbindung erlauben.

Die technologieunabhängige Wahl des Begriffs AMP impliziert, dass es zukünftig weitere Funksysteme für Bluetooth geben kann (siehe auch Kapitel B.1.4.2 und das Kapitel G. UWB).

Abbildung B-4: Wahlweise Verwendung von Bluetooth und alternativen Funksystemen



Kernstück der Spezifikation ist das sogenannte „802.11 Protocol Adaption Layer“ (802.11 PAL). Es stellt das Bindeglied zwischen der Host-Controller-Schnittstelle (HCI) des Bluetooth und der MAC-Schnittstelle des WLAN her. Das 802.11 PAL leistet unter anderem:

- Aufbau physikalischer Verbindungen nach Anforderung durch das HCI. Das 802.11 PAL nutzt dazu die in [IEEE07] beschriebenen Verfahren.
- Datenübertragung mit Hilfe von WLAN-Paketen: Die Bluetooth-Daten werden auf Basis des SNAP in WLAN-Pakete eingebettet. Das 802.11 PAL unterstützt nur den verbindungslosen Modus ACL.
- Vermeiden von Interferenzen zwischen WLAN und Bluetooth im 2.4-GHz-Band. Das PAL sorgt dafür, dass verbindungsorientierter Datenverkehr (SCO), der immer über den Bluetooth Controller abgewickelt wird, nicht gleichzeitig mit verbindungslosen Datenpaketen (ACL) auf dem WLAN Controller gesendet wird.

Es ist erwähnenswert, dass sich die Bluetooth-Spezifikation 3.0 + HS ausschließlich auf den bereits veröffentlichen IEEE-Standard [IEEE07] bezieht. Es werden also WLAN mit Brutto-Datenraten bis 54 Mbit/s unterstützt; die in Arbeit befindliche Ergänzung IEEE 802.11n bleibt unberücksichtigt.

B.1.4.2 Bluetooth über UWB

Seit einigen Jahren gibt es Bestrebungen, Bluetooth auf die Basis schnellerer Übertragungstechniken zu stellen. Das von der WiMedia Alliance vorgestellte UWB-Verfahren (Ultra Wideband) mit Multiband-OFDM stellt eine denkbare Option hierfür dar. In der Tat hat sich die Bluetooth SIG in 2006 positioniert und das genannte Verfahren der WiMedia Alliance ausgewählt. Es soll Datenraten von bis zu 480 Mbit/s ermöglichen. Im März 2009 hat die WiMedia Alliance bekannt gegeben, der Bluetooth

SIG alle UWB-Spezifikationen zu übergeben und danach die Arbeit einzustellen (siehe [WIME09]). Eine entsprechende Bluetooth-Spezifikation liegt zum Zeitpunkt der Veröffentlichung dieses Dokuments noch nicht vor.

B.1.4.3 Ultra Low Power Bluetooth

Die Firma Nokia hat im Rahmen des Standardisierungsprozesses für ZigBee (IEEE 802.15.4) im Jahre 2001 einen eigenen Vorschlag für eine Funktechnik vorgelegt. Im Rahmen von ZigBee wurde diese Technik nicht ausgewählt, jedoch wurde die Technik im Herbst 2006 unter dem Namen Wibree öffentlich vorgestellt. Im Sommer 2007 schloss sich das Wibree-Forum mit der Bluetooth SIG zusammen. Seither propagiert die Bluetooth SIG das Verfahren unter dem Namen Ultra Low Power Bluetooth (ULP Bluetooth).

Ziel von ULP Bluetooth ist es, Geräte mit geringer Stromaufnahme untereinander zu koppeln. Basis sind die für Bluetooth entwickelten Chipsätze. Es erfolgt jedoch eine Erhöhung des Modulationsindex bei gleichzeitig verringerter Symbolrate. Dadurch bleibt die von ULP Bluetooth belegte Bandbreite gleich, es verringert sich jedoch die nutzbare Datenrate. Darüber hinaus führt der höhere Modulationsindex bei gleicher Sendeleistung zu einer verbesserten Reichweite. ULP Bluetooth nutzt diesen Sachverhalt aus, um die Sendeleistung entsprechend zurückzunehmen. Beide Maßnahmen – verringerte Datenrate und kleinere Sendeleistung – führen zu einer Stromersparnis.

Eine Spezifikation von ULP Bluetooth liegt zum Zeitpunkt der Veröffentlichung dieses Dokuments noch nicht vor. Es ist jedoch davon auszugehen, dass ULP Bluetooth nicht als AMP Controller spezifiziert werden wird, sondern als Erweiterung des Bluetooth Radios. Ein entsprechender Hinweis darauf findet sich bereits in der aktuellen Spezifikation 3.0 + HS.

B.2 Sicherheitsmechanismen

B.2.1 Kryptographische Sicherheitsmechanismen

Da Bluetooth ein funkbasiertes Verfahren ist, besteht grundsätzlich die Gefahr, dass "unberechtigte" Bluetooth-fähige Geräte die Bluetooth-Kommunikation mithören bzw. sich aktiv in die Kommunikationsverbindung einschalten. Die in der Bluetooth-Spezifikation vorgesehenen kryptographischen Sicherheitsmechanismen haben die Ausschaltung dieser beiden Bedrohungen zum Ziel. Diese Funktionen sind bereits auf Chipebene implementiert und stehen auf der Link-Schicht einheitlich zur Verfügung.

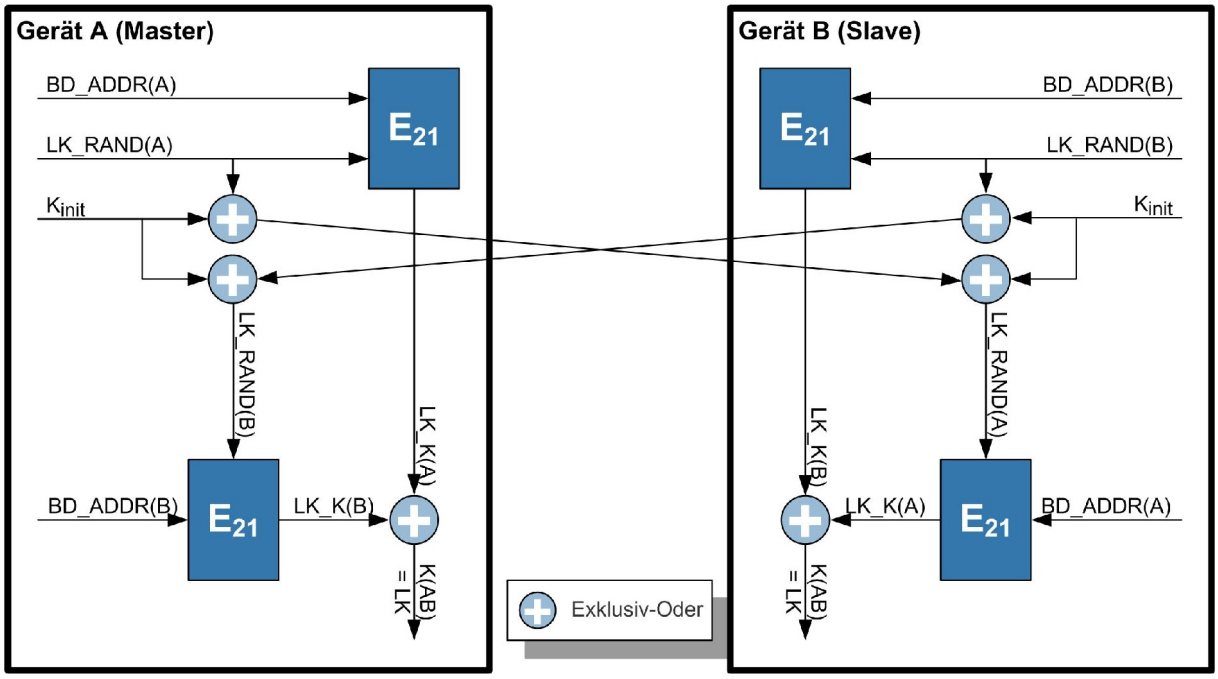
Basis aller eingesetzten kryptographischen Verfahren sind Verbindungsschlüssel (Link Keys), die während der sogenannten Paarung zwischen jeweils zwei Bluetooth-Geräten vereinbart werden.

Paarung (Pairing) und Verbindungsschlüssel

In der Regel wird beim Pairing zweier Bluetooth-Geräte ein nur für die Verbindung dieser beiden Geräte genutzter, 128 Bit langer Kombinationsschlüssel (Combination Key) erzeugt und in jedem Gerät zur zukünftigen Nutzung als Verbindungsschlüssel (Link Key, LK) gespeichert.

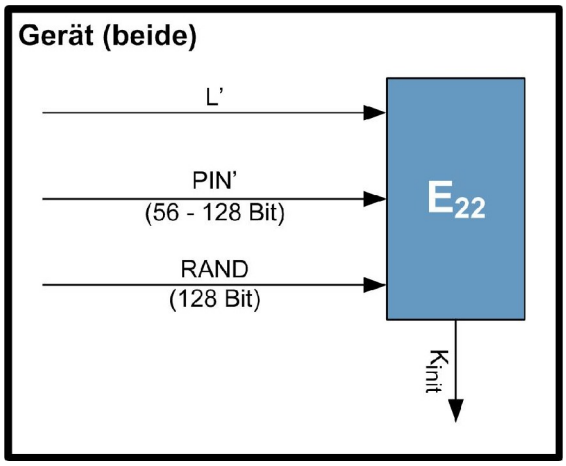
Die Erzeugung des Kombinationsschlüssels K(AB) geht von einem Paar, bestehend aus der Geräteadresse BD_ADDR und einer Zufallszahl LK_RAND, pro Gerät aus. Eine kryptographische Funktion mit der Bezeichnung E_{21} gemäß [IEEE05] wird angewandt, um jedes dieser Paare miteinander zu einem Wert LK_K(A) bzw. LK_K(B) zu kombinieren. Beide LK_K werden in einer Exklusiv-Oder-Funktion miteinander verknüpft und ergeben den Kombinationsschlüssel K(AB) (siehe Abbildung B-5).

Abbildung B-5: Erzeugen des Kombinationsschlüssels



Damit die genannten Verknüpfungen in beiden Geräten erfolgen können, ist die im Gerät erzeugte Zufallszahl LK_RAND auf das jeweils andere Gerät zu übertragen. Für die gesicherte Übertragung der Zufallszahlen wird ein Initialisierungsschlüssel K_{init} verwendet, der sich aus einer weiteren (öffentlichen) Zufallszahl, der Geräteadresse eines Teilnehmers und einer im Allgemeinen konfigurierbaren PIN berechnet. Die Berechnung erfolgt mittels einer kryptographischen Funktion mit der Bezeichnung E_{22} gemäß [IEEE05]. Eingangswerte sind neben der Zufallszahl RAND die mit der Geräteadresse BD_ADDR verlängerte PIN sowie die Länge L' der sich daraus ergebenden PIN' (siehe Abbildung B-6).

Abbildung B-6: Erzeugen des Initialisierungsschlüssels



Die Eingabe einer langen PIN an zwei Geräten durch den Nutzer ist fehleranfällig und kann zudem mit Zeitschranken für den Paarungsablauf in Konflikt kommen. Zur Vermeidung dieses Problems hat bereits die Bluetooth-Spezifikation 2.0 + EDR alternativ einen automatisierten Austausch zwischen den beiden Bluetooth-Geräten vorgeschlagen, z.B. auf Basis des Diffie-Hellmann-Verfahrens. Erst die Spezifikation 2.1 + EDR (siehe [BTSIG07]) führt ein derartiges Verfahren ein, das Secure Simple Pairing (siehe Kapitel B.2.2).

Neben den Kombinationsschlüsseln erlaubt der Standard weitere Möglichkeiten für Link Keys:

- Geräteschlüssel (Unit Keys) können als Link Key genutzt werden. Der Geräteschlüssel wird bei der erstmaligen Verwendung eines Bluetooth-Geräts erzeugt und normalerweise nicht mehr geändert. Die Verwendung von Geräteschlüsseln wird von der Bluetooth-Spezifikation nicht mehr empfohlen, da diese ein Sicherheitsrisiko darstellen.

- Master-Schlüssel (Master Keys) können für die Dauer einer Bluetooth-Sitzung zwischen mehreren Geräten (temporär) vereinbart werden, wenn ein Master mehrere Geräte unter Verwendung desselben Verschlüsselungsschlüssels erreichen will. Master-Schlüssel werden nur bei Punkt-zu-Mehrpunkt-Verbindungen eingesetzt und über die aktuellen Link Keys gesichert vom Master an die Slaves übertragen.

Die Bluetooth-Spezifikation unterscheidet temporäre und semipermanente Verbindungsschlüssel. Temporäre Verbindungsschlüssel sind eine Art Einmal-Schlüssel, d.h. für jede neue Verbindung wird ein neuer Verbindungsschlüssel erzeugt (ein Paarungsvorgang je Verbindung). Semipermanente Verbindungsschlüssel werden dagegen von den beteiligten Bluetooth-Geräten nach Paarungs- und Authentisierungsvorgang in einem nichtflüchtigen Speicher festgehalten. Der Einsatz semipermanenter Verbindungsschlüssel ermöglicht die erneute Verbindung zweier Geräte ohne eine erneute Authentisierung. Der Benutzer braucht dann beim Verbindungsaufbau nicht erneut eine PIN einzugeben. Damit sinkt das Risiko, dass der Verbindungsaufbau abgehört und dabei möglicherweise eine „schwache" PIN erraten werden kann. Hierzu siehe Kapitel B.3.1.3.

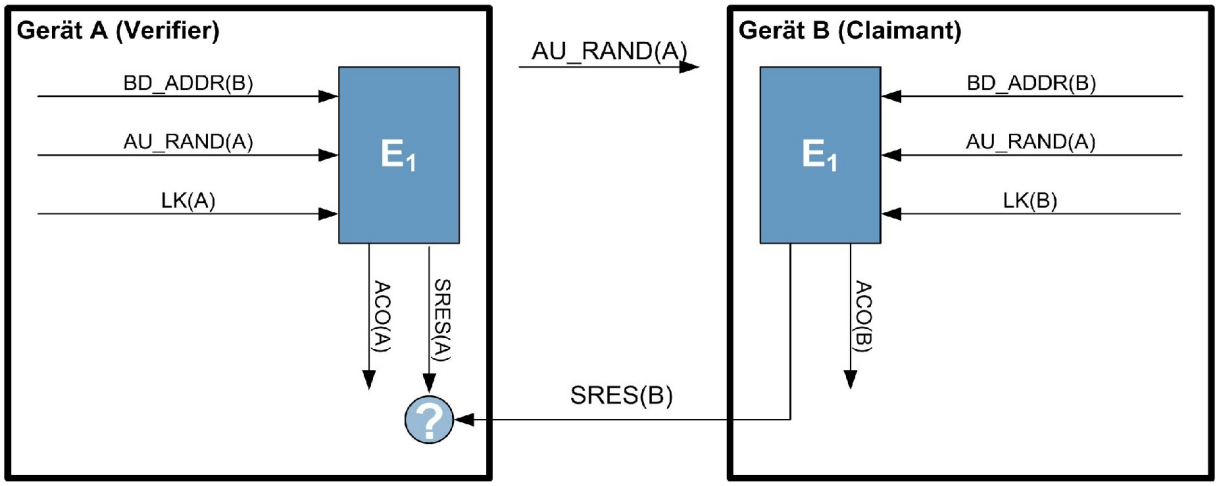
Authentisierung

Zur Authentisierung wird ein Challenge-Response-Verfahren auf Basis eines symmetrischen Chiffrier-Verfahrens verwendet. Es wird grundsätzlich eine einseitige Authentisierung genutzt, d.h. ein Gerät (Claimant) authentisiert sich gegenüber einem anderen Gerät (Verifier). Wollen sich beide Geräte gegenseitig authentisieren, wird die Authentisierung mit vertauschten Rollen wiederholt.

Die Authentisierung läuft wie folgt ab (siehe Abbildung B-7): Der Verifier sendet eine Zufallszahl (AU_RAND) an den Claimant. Dieser beweist, dass er als gemeinsames Geheimnis den Link Key (LK) kennt, indem er unter Benutzung dieses Geheimnisses aus der Zufallszahl und seiner eigenen Geräteadresse (BD_ADDR) eine 32 Bit lange Antwort (SRES) berechnet und zum Verifier zurücksendet. Der Verifier überprüft die Antwort, indem er die gleiche Berechnung durchführt. Sind die Ergebnisse identisch, d.h. LK(A) ist gleich LK(B), ist der Claimant authentisiert.

Gleichzeitig berechnen beide Geräte einen 96 Bit langen sogenannten Authenticated Cipher Offset (ACO), der geheim gehalten wird und bei Bedarf der Erzeugung eines Verschlüsselungsschlüssels dient.

Abbildung B-7: Authentisierung bei Bluetooth (vereinfacht)



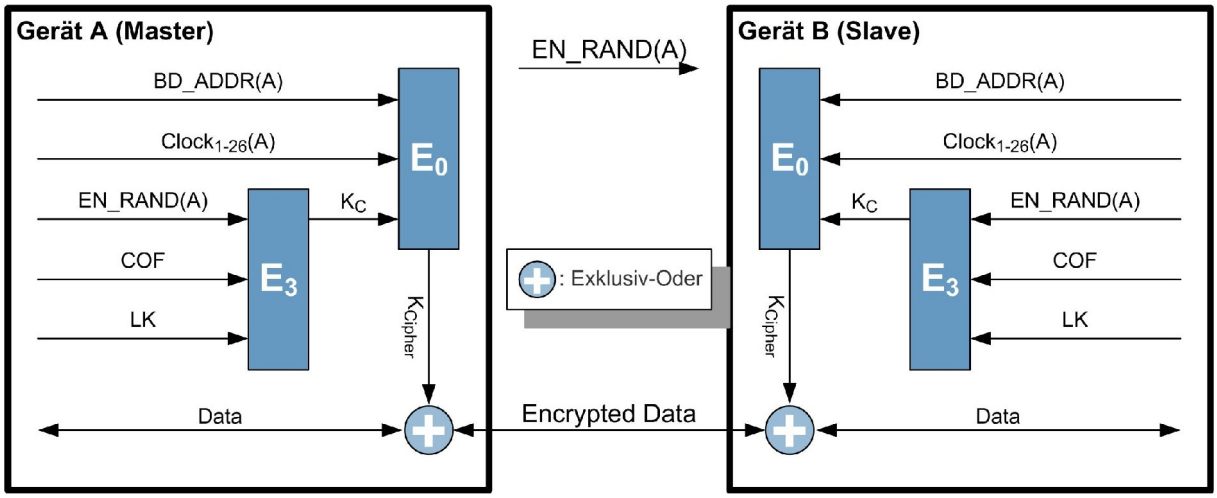
Verschlüsselung

Die Verschlüsselung kann optional verwendet werden, wenn sich mindestens eines der beiden kommunizierenden Geräte gegenüber dem anderen authentisiert hat. Dabei kann die Verschlüsselung sowohl vom Master, als auch vom Slave beantragt werden. Die Verschlüsselung selbst wird jedoch immer vom Master gestartet, nachdem er die notwendigen Parameter mit dem Slave ausgehandelt hat. Dazu einigen sich die beiden Geräte zunächst auf die Länge des zu verwendenden Schlüssels. Anschließend startet der Master die Verschlüsselung, indem er eine Zufallszahl an den Slave sendet. Der Verschlüsselungsschlüssel K_C berechnet sich in der Hash-Funktion E_3 aus dem Link Key (LK), einem Cipher Offset (COF) und einer Zufallszahl EN_RAND, die vor Beginn der verschlüsselten Kommunikation im Klartext übertragen wird und somit den Kommunikationspartnern bekannt ist (siehe Abbildung B-4).

Es stehen für die Verschlüsselung zwei Betriebsarten zur Verfügung: Punkt-zu-Punkt-Verschlüsselung und Punkt-zu-Mehrpunkt-Verschlüsselung. Bei der Punkt-zu-Punkt-Verschlüsselung wird der ACO des Authentisierungsprotokolls (siehe Abbildung B-7) als COF verwendet. Bei der Punkt-zu-Mehrpunkt-Verschlüsselung wird dagegen die Geräteadresse des Master als COF genutzt. Außerdem muss der Link Key durch einen Master-Schlüssel ersetzt werden, bevor die Verschlüsselung gestartet wird.

Eine Punkt-zu-Mehrpunkt-Verschlüsselung wird z.B. in einem Piconetz benötigt, wenn der Master eine Nachricht an mehrere Slaves sendet (Multicast).

Abbildung B-8: Verschlüsselung bei Bluetooth (vereinfacht)



Zum Verschlüsseln wird eine Stromchiffre (im Standard mit E_0 bezeichnet) eingesetzt. Für jedes Datenpaket wird dabei ein neuer Schlüsselstrom (K_{Cipher}) aus der Geräteadresse (BD_ADDR), dem Verschlüsselungsschlüssel (K_C) sowie 26 Bits aus dem Zeittakt des Master ($Clock_{1-26}$) berechnet (siehe Abbildung B-4). Verschlüsselt sind die Daten nur während des Transports per Funk. Vor der Aussendung bzw. nach Empfang liegen die Daten in den beteiligten Geräten unverschlüsselt vor; es handelt sich also nicht um eine Ende-zu-Ende-Verschlüsselung (d.h. Verschlüsselung der Daten von der Eingabe in Endgerät A bis zur Ausgabe bzw. Bearbeitung in Endgerät B).

B.2.2 Secure Simple Pairing (SSP)

Die Bluetooth-Versionen bis einschließlich der Spezifikation 2.0 + EDR weisen verschiedene Schwächen auf, auf die im Kapitel B.3.1 näher eingegangen wird. Ein wesentlicher Kritikpunkt ist die vom Benutzer eingegebene PIN, deren Komplexität ein Sicherheitsmerkmal darstellt. Ein weiterer Kritikpunkt bezieht sich auf die Möglichkeit, mit Hilfe von Man-in-the-Middle-Angriffen die Integrität der Bluetooth-Kommunikation gefährden zu können. Als Antwort auf diese Kritikpunkte hat die Bluetooth SIG in 2007 die Spezifikation 2.1 + EDR veröffentlicht, die als wichtigste Neuerung das Verfahren Secure Simple Pairing (SSP) vorstellt.

SSP etabliert im Rahmen des Verbindungsaufbaus einen sicheren Kanal, über den der Link Key zwischen den Geräten ausgetauscht wird. Zu diesem Zweck erfolgt ein Schlüsselaustausch nach einem Diffie-Hellman-Verfahren mit elliptischen Kurven (Elliptic Curve Diffie-Hellman, ECDH), das für seine geringen Anforderungen an Rechenleistung bekannt ist.

Zur Vermeidung der beim Diffie-Hellman-Schlüsselaustausch prinzipiell bestehenden Gefahr eines Man-in-the-Middle-Angriffs erfolgt eine gegenseitige Authentisierung der Bluetooth-Geräte. Zur Authentisierung bietet SSP vier verschiedene, sogenannte Assoziationsmodelle an:

- Numeric Comparison

  Beide Geräte verfügen über eine Anzeigeeinheit, auf der sich mindestens eine sechsstellige Zahl anzeigen lässt. Sie verfügen darüber hinaus über die Möglichkeit, den Anwender „ja“ oder „nein“ eingeben zu lassen. Als Beispiel mag die Verbindung zwischen einem Mobiltelefon und einem Personal Computer dienen. Auf beiden Geräten wird im Rahmen zur Authentisierung dieselbe

sechsstellige Zahl angezeigt. Der Anwender bestätigt die Gleichheit der Zahlen durch Eingabe von „ja“ auf beiden Geräten.

- Just Works

  Dieses Modell ist für Geräte gedacht, die weder Zahlen anzeigen können noch über eine Eingabemöglichkeit verfügen, wie dies z.B. bei einfachen Ohrhörern der Fall ist. Just Works bietet keinen Schutz gegen Man-in-the-Middle-Angriffe auf die Authentisierung, gleichwohl schützt es ebenso gut vor einem passiven Abhören des Verbindungsvorgangs wie alle anderen Modelle des SSP.

- Out of Band (OOB)

  Dieses Modell basiert darauf, dass vor der eigentlichen Bluetooth-Kopplung über ein anderes Medium ein Kanal zwischen den zu verbindenden Geräten etabliert wird. Über diesen OOB-Kanal können sich die Geräte erkennen, ohne dass ein Bluetooth Inquiry erforderlich wäre. Auf jeden Fall wird der Kanal dazu genutzt, die für die Authentisierung erforderliche Information auszutauschen. Aus der Sicht des Anwenders ähnelt OOB dem Just Works: Es ist keine Benutzer-Interaktion vonnöten. Allerdings ermöglicht der zweite, von Bluetooth unabhängige Kanal das Erkennen von Man-in-the-Middle-Angriffen auf den Diffie-Hellman-Schlüsselaustausch. Eine Voraussetzung dafür ist, dass die für den Kanal verwendete Technik immun gegen solche Angriffe ist. Die Bluetooth SIG hat als OOB-Kanal die Nahfunktechnik NFC (Near Field Communication, siehe Kapitel H. NFC) vorgeschlagen. Voraussetzung für eine erfolgreiche Kopplung unter Zuhilfenahme von NFC ist, dass die beiden zu koppelnden Geräte bis auf wenige Zentimeter angenähert werden.

- Passkey Entry

  Hier verfügt nur ein Gerät über eine Anzeigeeinheit; das andere Gerät besitzt eine Eingabemöglichkeit für Zahlen. Dieses Modell ist beispielsweise dazu geeignet, eine Bluetooth-Tastatur mit einem Personal Computer zu verbinden. Der Anwender liest von dem Gerät mit Anzeigeeinheit eine sechsstellige Zahl ab und gibt sie in das andere Gerät ein. Denkbar ist auch, dass der Anwender einen sechsstelligen Passkey in beide Geräte eingibt, vergleichbar der PIN-Eingabe bei Bluetooth 1.x und 2.0 + EDR.

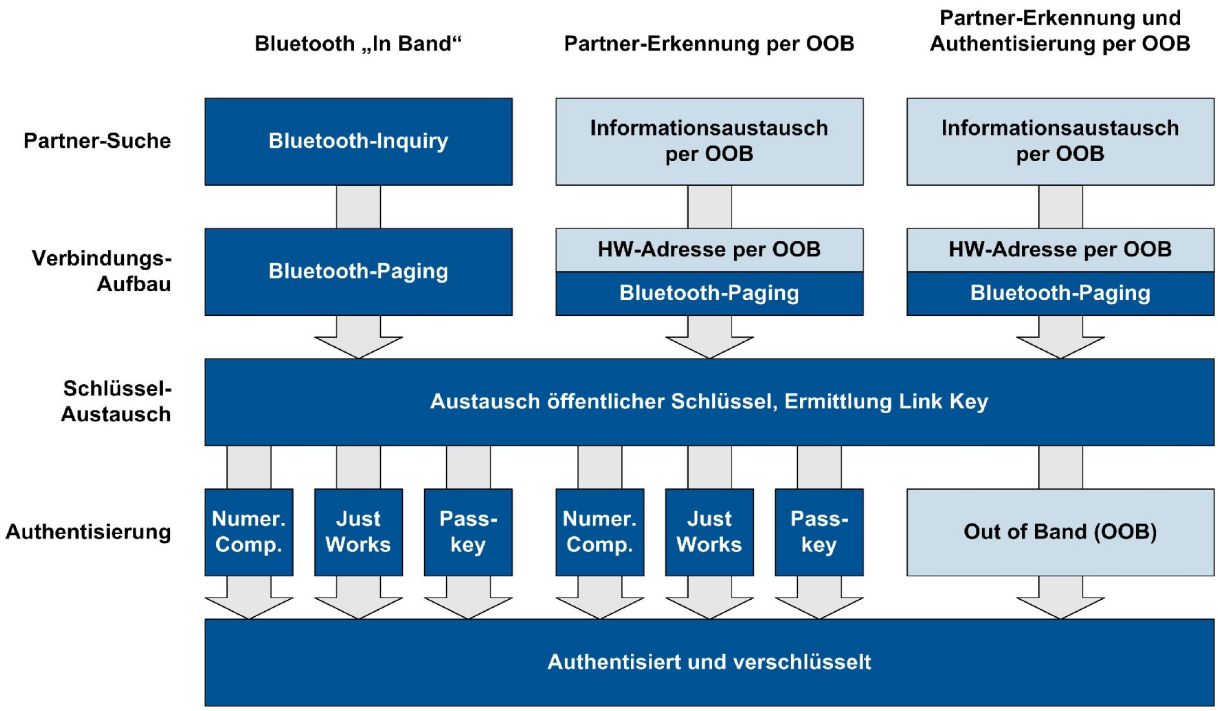
Die Abbildung B-9 stellt die genannten Modelle in einen Zusammenhang mit dem gesamten Verbindungsaufbau. Sofern kein OOB-Kanal zur Verfügung steht, erfolgen Inquiry und Paging auf herkömmliche Weise (siehe Kapitel B.1.3). Dann kann die Authentisierung nur mittels der drei „In Band“-Methoden Numeric Comparison, Just Works oder Passkey Entry erfolgen. Steht der OOB-Kanal zur Verfügung, wird er zunächst dazu genutzt, den Kommunikationspartner zu erkennen; das Bluetooth Inquiry wird durch diesen Vorgang ersetzt. Anschließend kann die Authentisierung mit jedem der vier Assoziationsmodelle erfolgen.

Das eigentliche Secure Simple Pairing umfasst insgesamt die folgenden fünf Phasen:

- Phase 1: Austausch öffentlicher Schlüssel
- Phase 2: Authentisierung 1. Stufe
- Phase 3: Authentisierung 2. Stufe
- Phase 4: Berechnung des Link Key
- Phase 5: Etablieren der Verschlüsselung

Die Phase 2 wird für jedes der vier möglichen Assoziationsmodelle auf eine spezifische Weise durchgeführt. Alle anderen Phasen sind unabhängig vom Modell.

Abbildung B-9: Varianten zum Verbindungsaufbau bei SSP

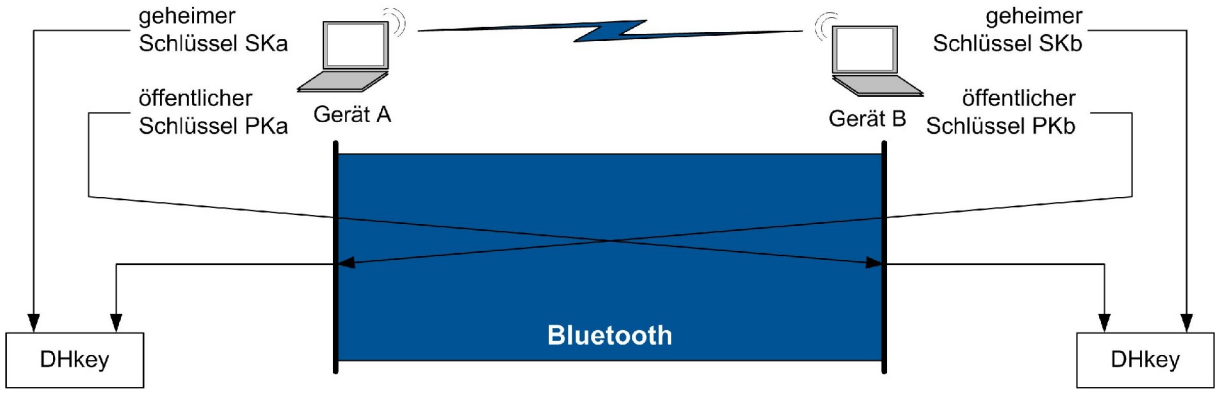


B.2.2.1 Phase 1: Austausch öffentlicher Schlüssel

Jedes Bluetooth-Gerät erzeugt ein Paar DHkey aus öffentlichem und privatem Schlüssel mittels elliptischem Diffie-Hellman-Verfahren (ECDH). Dieser Vorgang braucht grundsätzlich bei jedem Gerät nur einmal zu erfolgen. Die Bluetooth-Spezifikation lässt dem Hersteller die Freiheit, jederzeit ein neues Schlüsselpaar generieren zu lassen.

Beide Geräte übertragen ihren öffentlichen Schlüssel zum Kommunikationspartner. Dafür nutzen sie normalerweise den im Rahmen des Pairing etablierten Bluetooth-Kanal (siehe Abbildung B-10).

Abbildung B-10: Austausch öffentlicher Schlüssel und Berechnung eines Schlüsselpaares (DHkey)



B.2.2.2 Phase 2: Authentisierung 1. Stufe

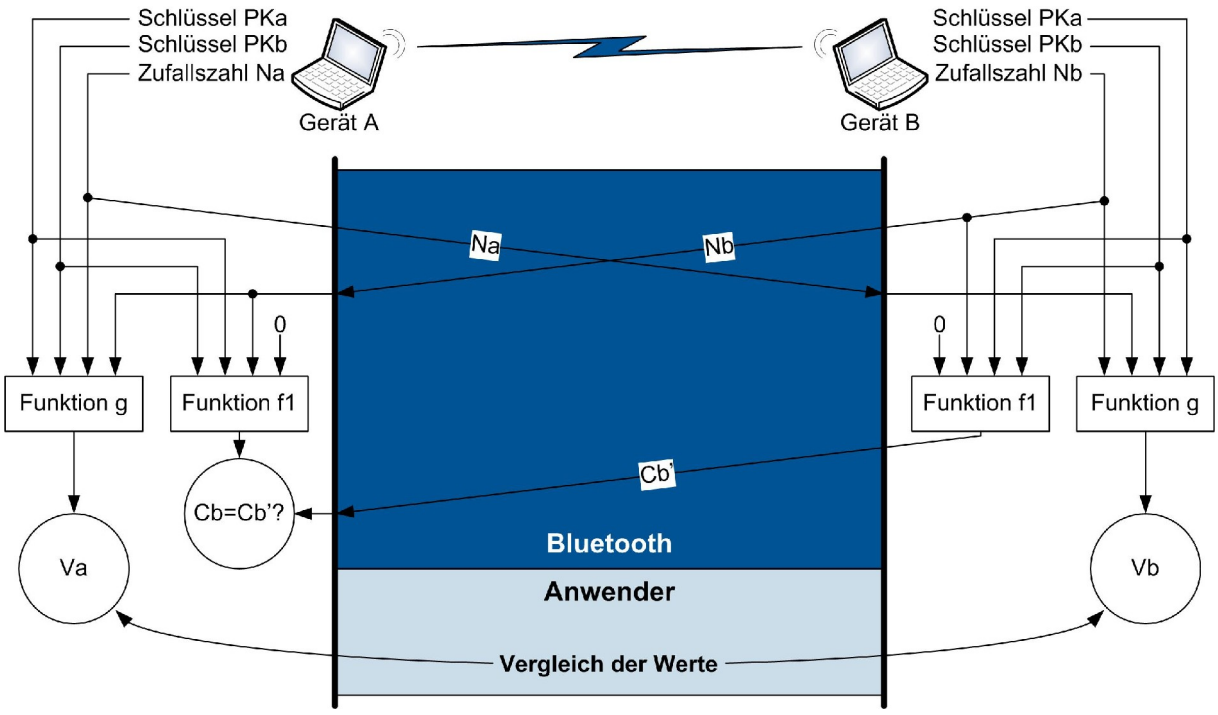
Die Phase 2 stellt sicher, dass die Geräte authentische öffentliche Schlüssel von ihrem Kommunikationspartner erhalten haben. Man-in-the-Middle-Angriffe werden in dieser Phase erkannt. Zu diesem Zweck werden für Numeric Comparison, Passkey Entry und Out of Band jeweils unterschiedliche Protokolle verwendet. Just Works verwendet dasselbe Protokoll wie Numeric Comparison.

Basis für alle Protokolle der Authentisierungsstufe 1 ist eine kryptographische Funktion f1(PKa,PKb,Na,Nb). Die Funktion hat vier Eingabeparameter: PKa und PKb sind die öffentlichen Schlüssel, die in Phase 1 ausgetauscht wurden, Na und Nb sind Zufallszahlen (Nonce), die im Rahmen der Phase 2 erzeugt werden. Das Ergebnis der Funktion f1 wird in der Bluetooth-Spezifikation mit Commitment bezeichnet und als Ca bzw. Cb abgekürzt. Die Authentisierung ist erfolgreich, wenn das in einem Gerät errechnete Commitment mit dem im anderen Gerät errechneten übereinstimmt. Hierzu werden die Commitments zwischen den Geräten ausgetauscht. Die Protokolle unterscheiden sich in der Verwendung der Eingabeparameter der Funktion f1 und in der – neben den Commitments – ausgetauschten Parameter. Beispielhaft werden in den folgenden Absätzen zwei wichtige Protokolle des SSP näher erläutert.

Numeric Comparison

Beide Geräte erzeugen eine Zufallszahl (Na bzw. Nb) und tauschen diese über den Bluetooth-Kanal mit dem Kommunikationspartner aus. Beide Geräte sind darüber hinaus in Besitz beider öffentlicher Schlüssel PKa und PKb. Daraus errechnen beide Geräte je ein Commitment Cb = f1(PKb,PKa,Nb,0). Das Commitment Cb´ (siehe Abbildung B-11) wird von Gerät B an Gerät A übertragen, welches es mit dem selbst berechneten Commitment Cb vergleicht. Fällt der Vergleich positiv aus, präsentiert das Gerät A dem Anwender eine sechsstellige Zahl, die es aus der kryptographischen Funktion g(PKa,PKb,Na,Nb) ermittelt hat. Gerät B führt dieselbe Berechnung durch und präsentiert dem Anwender ebenfalls das Ergebnis. Der Anwender vergleicht die Ergebnisse und bestätigt beiden Geräten deren Übereinstimmung. Abbildung B-11 stellt den Ablauf vereinfacht dar.

Abbildung B-11: Authentisierung mittels Numeric Comparison (vereinfacht)

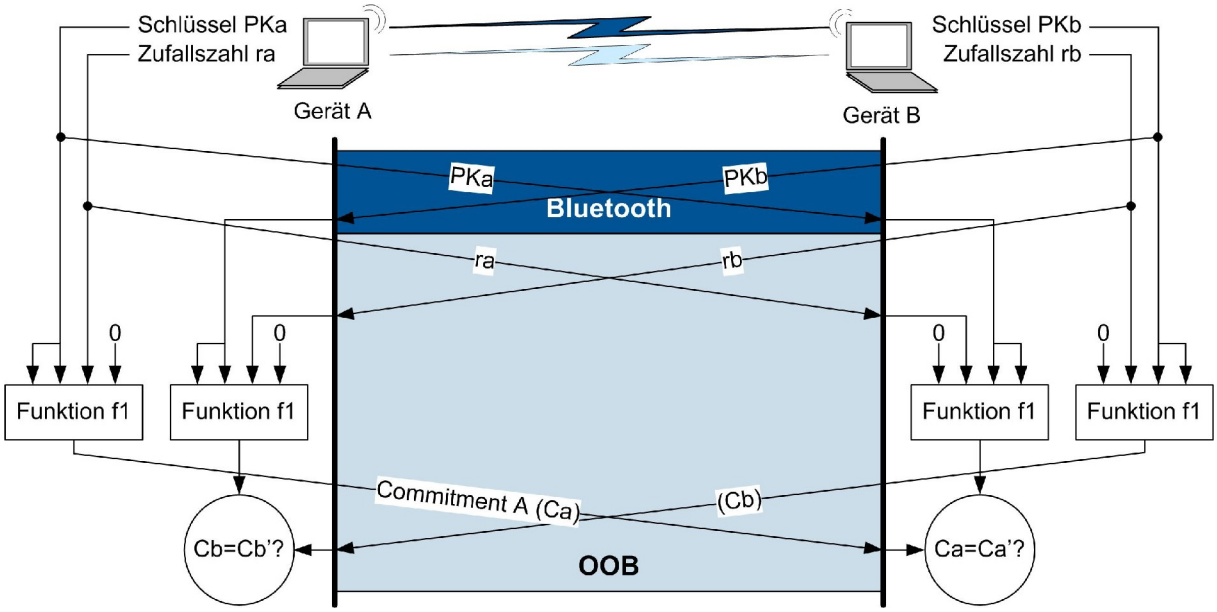


Das Verfahren erscheint bei erster Betrachtung als sicher, weil eine vertrauenswürdige Instanz – der Anwender – über dessen korrekten Abschluss wacht. Typische Anwenderfehler, wie z.B. schwache oder immer gleichbleibende Kennwörter, werden ausgeschlossen, außer „ja“ oder „nein“ wird keine Eingabe vom Anwender erwartet. Es gibt ein Forschungsprojekt mit dem Ziel, die Sicherheit von Numeric Comparison theoretisch herzuleiten (siehe [LIND09]).

Out of Band

Beide Geräte erzeugen eine Zufallszahl (ra bzw. rb) und tauschen diese über den OOB-Kanal mit dem Kommunikationspartner aus. Beide Stationen sind darüber hinaus in Besitz beider öffentlicher Schlüssel PKa und PKb. Daraus errechnen beide Geräte je ein Commitment Ca = f1(PKa,PKa,ra,0) und Cb = f1(PKb,PKb,rb,0). Beide Commitments werden über den OOB-Kanal an den Kommunikationspartner übertragen, der das empfangene Commitment jeweils mit dem selber errechneten vergleicht. Fällt der Vergleich in beiden Fällen positiv aus, gilt der Kommunikationspartner als authentisiert. Abbildung B-12 stellt das Verfahren schematisch dar.

Abbildung B-12: Authentisierung mittels OOB (vereinfacht)



Die Bluetooth-Spezifikation berücksichtigt die Möglichkeit, dass eines der Geräte auf dem OOB-Kanal keine Daten empfangen kann. Dies ist z.B. der Fall, wenn als OOB-Kanal NFC eingesetzt wird und das Gerät nur mit einem passiven NFC-Tag ausgestattet ist. In diesem Fall erfolgt lediglich eine einseitige Authentisierung, in dem das Gerät seine eigene Zufallszahl ra und Commitment Ca aussendet, aber selber keine Prüfung der Werte des Kommunikationspartners vornimmt.

Die Spezifikation berücksichtigt darüber hinaus die Möglichkeit, dass die öffentlichen Schlüssel über den OOB-Kanal ausgetauscht werden. Das ist erforderlich, wenn der Aufbau des Bluetooth-Kanals (das Paging) auf Basis der im OOB-Kanal ausgetauschten Informationen erfolgt. Der Bluetooth-Kanal wird in diesem Fall erst nach Abschluss der Phase 2 etabliert.

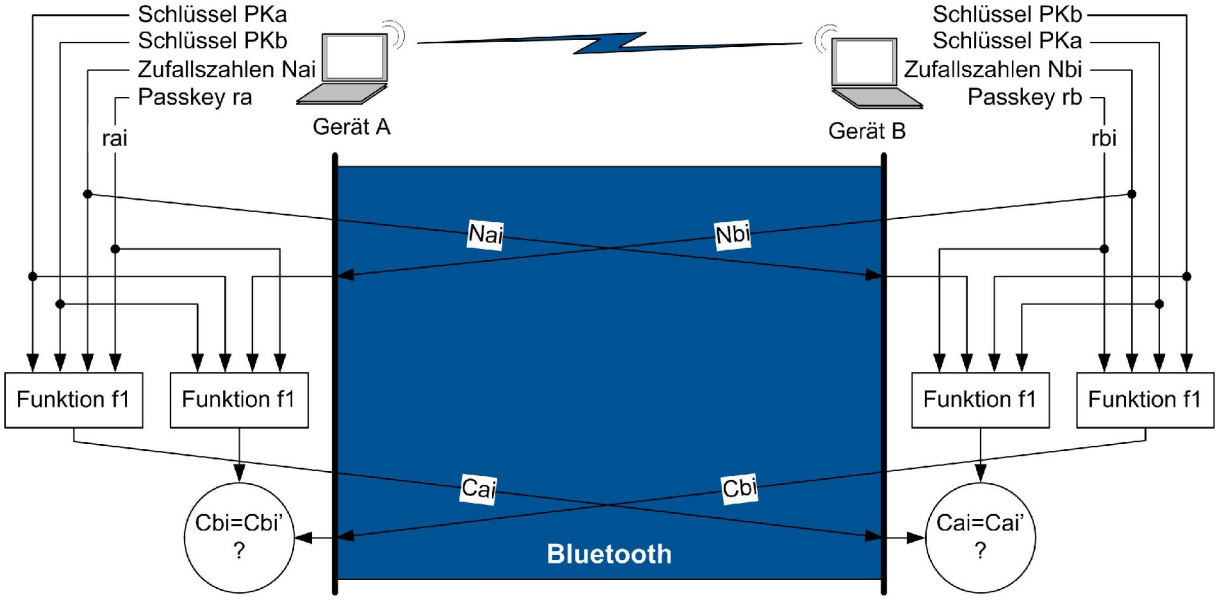
Passkey Entry

Zu Beginn der Phase 2 besitzen beide Kommunikationspartner die öffentlichen Schlüssel PKa und PKb sowie die Passkeys ra und rb. Das Verfahren prüft nun, ob die beiden Passkeys ra und rb identisch sind, dabei ist es unerheblich, ob der Anwender den Passkey an einem Gerät abgelesen hat und am anderen Gerät eingeben konnte oder ob er ihn an beiden Geräten eingegeben hat.

Die Prüfung der Passkeys erfolgt bitweise. Eine sechsstellige Zahl kann maximal den Wert 999999 einnehmen; diese Zahl lässt sich binär mit 20 Bits darstellen. Der in Abbildung B-13 gezeigte Ablauf wird demzufolge insgesamt 20 Mal ausgeführt. Die Variablen rai und rbi bezeichnen dabei die einzelnen Bits des Passkey.

Ein einzelnes Bit des Passkey wird wie folgt geprüft: Beide Geräte erzeugen eine Zufallszahl Nai bzw. Nbi. Die Zufallszahl wird über den bestehenden Bluetooth-Kanal an den Kommunikationspartner übertragen. Außerdem ermittelt jedes Gerät ein Commitment Cai bzw. Cbi über die kryptographische Funktion f1 und überträgt es an den Kommunikationspartner. Der kann anhand der nun vorliegenden Funktion die Rechnung nachvollziehen und das Ergebnis mit dem empfangenen Commitment vergleichen. Beispiel: Gerät A errechnet das Commitment Cai zu f1(PKa,PKb,Nai,rai). Es übermittelt Nai und Cai an Gerät B. Gerät B kann somit die gleiche Rechnung durchführen und das Ergebnis Cai´ mit Cai vergleichen. Waren beide Bits des Passkey gleich, werden auch die Commitments übereinstimmen.

Abbildung B-13: Authentisierung mittels Passkey Entry (Darstellung vereinfacht für ein Bit)



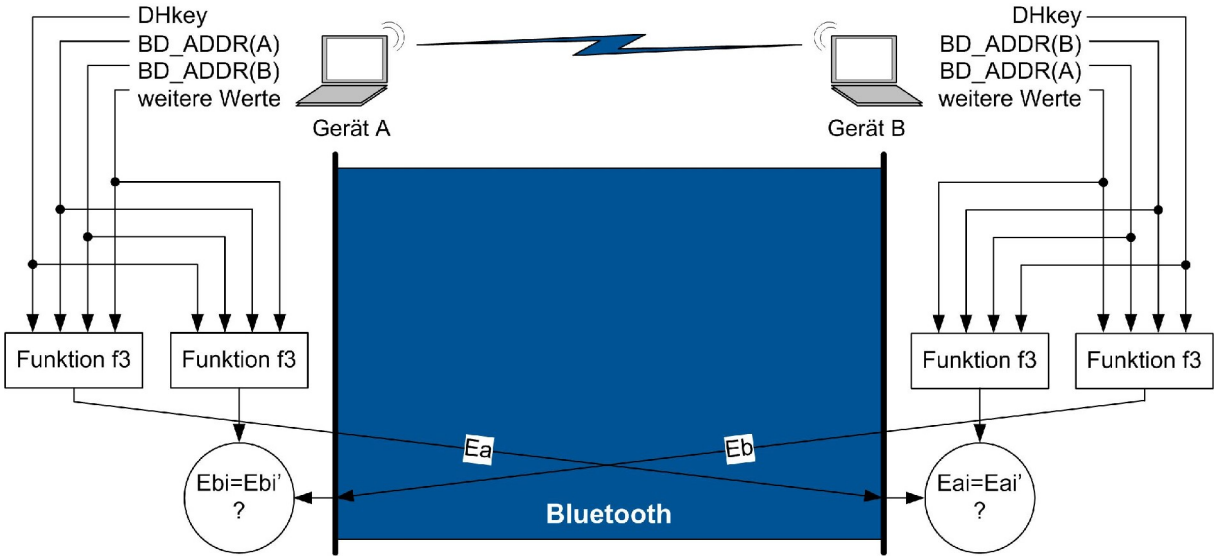
Bereits an dieser Stelle soll darauf hingewiesen werden, dass sich in der Bit-weisen Prüfung des Passkey eine Schwäche des Verfahrens verbirgt. Ein passiver Lauscher ist nämlich in der Lage, die öffentlichen Schlüssel und Zufallszahlen abzuhören. Das ihm unbekannte Bit des Passkey rät er und führt damit die Funktion f1 selber aus. Ist das Ergebnis gleich dem ebenfalls abgehörten Commitment, so hat er das Bit richtig geraten. Fällt der Vergleich negativ aus, so setzt er das komplementäre Bit für den Passkey ein. Ein Angreifer ist auf diese Weise in der Lage, mit geringem Aufwand den für eine erfolgreiche Authentisierung verwendeten Passkey zu ermitteln.

B.2.2.3 Phase 3: Authentisierung 2. Stufe

Diese Stufe dient einer Bestätigung, dass die Authentisierung und damit das Pairing erfolgreich waren. Der aus dem Diffie-Hellman-Verfahren gewonnene symmetrische Schlüssel DHkey, die beiden Geräteadressen BD_ADDR sowie verschiedene in der 1. Stufe verwendete Zufallszahlen („weitere Werte“ in Abbildung B-14), die beiden Kommunikationspartnern gleichermaßen bekannt sind, werden zur Berechnung von Prüfwerten Ea und Eb verwendet. Zu diesem Zweck kommt eine kryptographische Funktion f3 zum Einsatz. Die Prüfwerte werden zwischen den Geräten ausgetauscht und verglichen (siehe Abbildung B-14). Ein erfolgreicher Vergleich auf beiden Seiten ist die Voraussetzung für das Bestehen der Authentisierung.

Diese Phase erfüllt einen wichtigen Zweck im Zusammenhang mit Out of Band. Wenn eines der Geräte nur über ein passives NFC-Tag verfügt, kann es im OOB-Kanal nur Daten senden, aber keine empfangen. Ein solches Gerät erfährt somit nichts über eine eventuell fehlgeschlagene Authentisierung. Dies wird in der Phase 3 nachgeholt, indem die beschriebene beiderseitige Prüfung auf dem Bluetooth-Kanal durchgeführt wird.

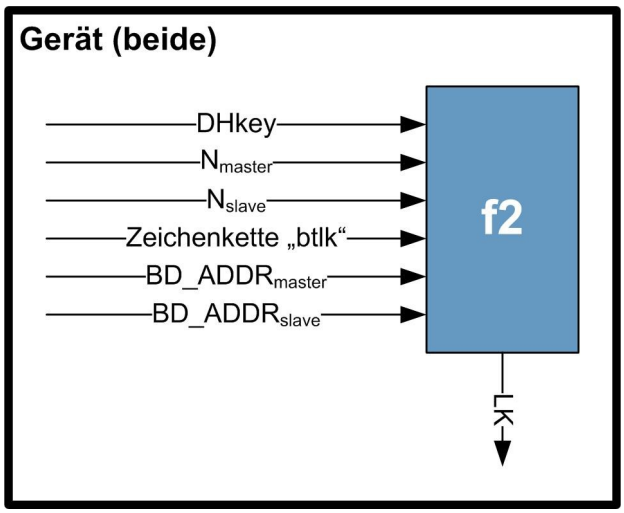
Abbildung B-14: Authentisierung Stufe 2 (vereinfacht)



B.2.2.4 Phase 4: Berechnung des Link Key

Aus den zwischen beiden Geräten ausgetauschten Daten und dem aus dem Diffie-Hellman-Verfahren gewonnenen symmetrischen Schlüssel wird über eine kryptographische Funktion f2 der Link Key ermittelt. In die Funktion fließt ein weiteres, nur für diesen Zweck erzeugtes Paar von Zufallszahlen N_{master}/N_{slave} ein, das sicherstellt, dass immer ein anderer Link Key entsteht, ohne das Diffie-Hellman-Schlüsselpaar bei jedem Verbindungsaufbau neu erzeugen zu müssen. Außerdem fließen die Geräteadressen und eine konstante Zeichenkette in die Berechnung des Link Key ein (siehe Abbildung B-15).

Abbildung B-15: Berechnung des Link Key bei SSP



B.2.2.5 Phase 5: Etablieren der Verschlüsselung

Schließlich ermitteln beide Geräte mit Hilfe des symmetrischen Link Key einen Verschlüsselungsschlüssel K_C, der die Basis für die Verschlüsselung des Datenstroms ist. Das Verfahren entspricht dem bei Bluetooth 1.x und 2.0 + EDR eingesetzten (siehe Kapitel B.2.1, insbesondere Abbildung B-8).

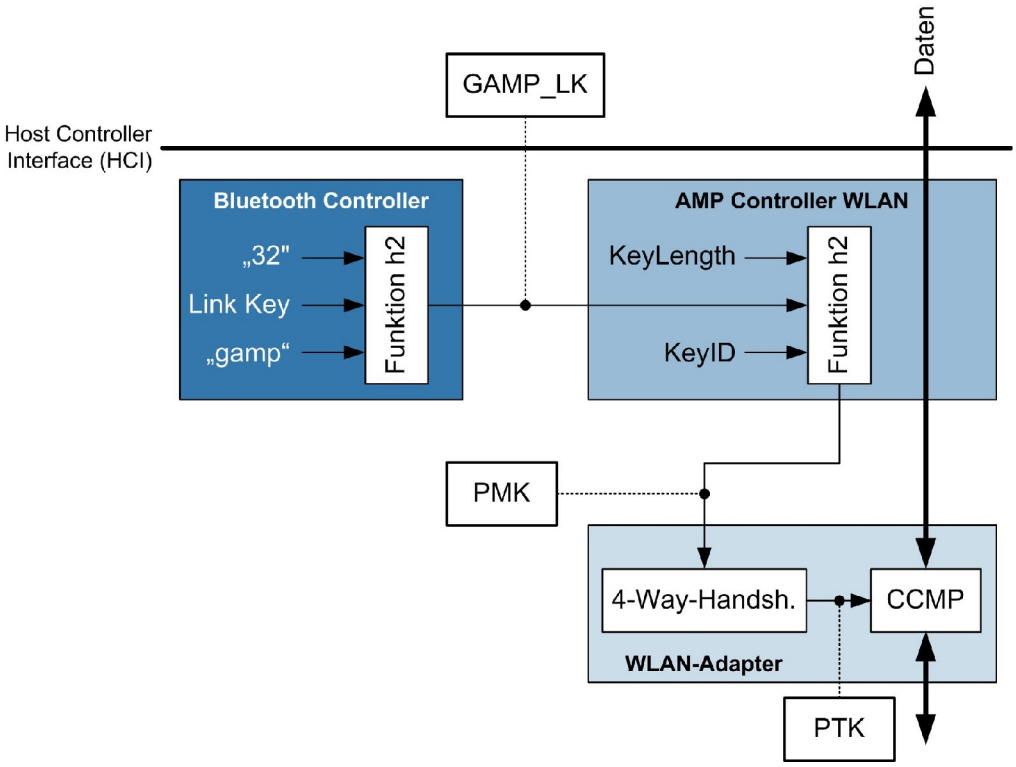
B.2.3 Sicherheit bei alternativen Funktechniken (AMP)

Die bis hierher beschriebenen Sicherheitsmechanismen sind Gegenstand des Link Manager Protocol (LMP) und somit im Bluetooth Controller implementiert (siehe Abbildung B-1). Die Bluetooth-Spezifikation 3.0 + HS enthält daher zusätzliche Sicherheitsmechanismen für AMP.

Sobald Bluetooth-Geräte einen neuen Link Key aushandeln, wird aus diesem Link Key ein eigener Schlüssel für den AMP Controller generiert, der als Generic AMP Link Key (GAMP_LK) bezeichnet wird. Hierzu wird eine kryptographische Funktion h2 verwendet. Dabei handelt es sich um eine Hash-Funktion, in die neben dem Link Key zwei Konstanten[2] einfließen.

Der GAMP_LK wird beim Verbindungsaufbau dazu verwendet, einen Controller-spezifischen Schlüssel zu generieren, der hier als Dedicated AMP Key bezeichnet wird. Die Länge dieses Schlüssels hängt vom tatsächlich verwendeten AMP Controller ab. Bei WLAN wird der Sitzungsschlüssel unmittelbar als Pairwise Master Key (PMK) eingesetzt und ist dementsprechend 256 Bit lang. Er wird, wie im Kapitel A.2.4.4 beschrieben, als Basis für das 4-Way-Handshake zur Ableitung eines Sitzungsschlüssels (Pairwise Transient Key, PTK) verwendet. Anschließend wird jeglicher Datenverkehr über das WLAN mittels CCMP[3] verschlüsselt (siehe Abbildung B-16).

Abbildung B-16: Schlüsselerzeugung bei IEEE 802.11 AMP (vereinfacht)



2 Die als KeyID bezeichnete ASCII-kodierte Zeichenkette „gamp“ und die binär kodierte Zahl 32.

3 Counter Mode with Cipher Block Chaining Message Authentication Code Protocol

Ein regelmäßiges Erneuern des PTK mittels 4-Way-Handshake ist bei IEEE 802.11 AMP nicht vorgesehen. Jedoch wird für jeden Verbindungsaufbau über AMP ein neuer GAMP_LK generiert, auch wenn sich der Link Key in der Zwischenzeit nicht verändert hat. In die Funktion h2 fließt dann neben den genannten Konstanten statt des Link Key der bestehende GAMP_LK ein.

B.2.4 Sicherheitsbetriebsarten

Das Generic Access Profile (GAP) von Bluetooth kennt vier Sicherheitsmodi für Geräte. Die ersten drei beziehen sich auf Geräte bis einschließlich der Bluetooth-Spezifikation 2.0 + EDR (legacy). Der vierte betrifft Geräte ab der Bluetooth-Spezifikation 2.1 + EDR:

- **Sicherheitsmodus 1 (non-secure)**: Das Bluetooth-Gerät initiiert selbst keine speziellen Sicherheitsmechanismen, reagiert aber auf Authentisierungsanfragen anderer Geräte.
- **Sicherheitsmodus 2 (service level enforced security)**: Auswahl und Nutzung von Sicherheitsmechanismen werden abhängig vom Bluetooth-Gerät (trusted oder non-trusted) und vom Dienst auf Anwendungsebene, d.h. abhängig vom Bluetooth-Profil festgelegt. Das Gerät leitet erst dann Sicherheitsprozeduren ein, wenn es eine Aufforderung zum Verbindungsaufbau erhalten hat.
- **Sicherheitsmodus 3 (link level enforced security)**: Es ist generell eine Authentisierung beim Verbindungsaufbau erforderlich; die Verschlüsselung der zu übertragenden Daten ist optional.
- **Sicherheitsmodus 4 (service level enforced security)**: Dieser Modus entspricht im Prinzip dem Sicherheitsmodus 2. Der Dienst auf Anwendungsebene bestimmt, in welcher Art der Link Key mittels Secure Simple Pairing auszutauschen ist. Im Sicherheitsmodus 4 werden drei Attribute unterschieden.
  - Authenticated meint, dass Numeric Comparison, Passkey Entry oder Out-of-Band angewandt wird.
  - Unauthenticated bezieht sich auf Just Works.
  - No Security required fordert keine Sicherheitsmechanismen.

Die Bluetooth-Spezifikation 2.1 + EDR fordert die Verwendung des Sicherheitsmodus 4. Aus Gründen der Rückwärtskompatibilität zu älteren Bluetooth-Geräten kann darüber hinaus der Sicherheitsmodus 2 eingesetzt werden.

Die Auswahl des Sicherheitsmodus obliegt der Anwendung. Beispiel: Die Spezifikation des SIM Access Profile – das Bluetooth-Profil mit den höchsten Sicherheitsanforderungen – fordert grundsätzlich eine Authentisierung und Verschlüsselung. Zu diesem Zweck müssen die Geräte den Sicherheitsmodus 2 oder 3 einsetzen, wenn sie der Bluetooth-Spezifikation 2.0 + EDR oder 1.x entsprechen. Geräte der Spezifikation 2.1 + EDR und 3.0 + HS müssen den Sicherheitsmodus 4 verwenden.

Über diese Sicherheitsmodi hinaus beschreibt das GAP, wie sich das Verhalten von Bluetooth-Geräten beim Verbindungsaufbau steuern lässt:

- **Erkennbarkeit**: Über diesen Modus wird gesteuert, ob das Gerät auf Inquiry antwortet. Neben „non-discoverable mode“ (Gerät antwortet nicht auf Inquiry) und „general discoverable mode“ (Gerät antwortet immer auf Inquiry) ist auch der „limited discoverable mode“ vorgesehen, bei dem das Gerät nur für eine bestimmte Zeitspanne oder infolge bestimmter Gerätezustände erkennbar wird[4].

[4] Der „discoverable mode“ heißt bei aktuellen Bluetooth-Geräten beispielsweise „Bluetooth-Geräte können diesen Computer ermitteln“ oder „Sichtbarkeit des Bluetooth-Geräts“.

- **Möglichkeit des Verbindungsaufbaus**: Dieser Modus steuert die Fähigkeit des Bluetooth-Geräts, auf Verbindungsanfragen mittels Paging zu antworten. Das Gerät ist entweder im „connectable mode“ oder im „non-connectable mode“[5].

- **Möglichkeit einer paarweisen Geräteverbindung**: Hierunter wird die Fähigkeit der Geräte verstanden, sich im Rahmen des Pairing gegenseitig zu authentisieren und einen paarweisen Schlüssel (Link Key) auszutauschen („bondable mode“). Ist ein Gerät dagegen im „non-bondable mode“, lässt sich eine paarweise Verbindung als Basis einer verschlüsselten Kommunikation nicht herstellen. In früheren Bluetooth-Spezifikationen (1.x und 2.0 + EDR) werden diese Modi noch mit dem Begriff „pairable“ belegt.

5 Der „connectable mode“ lässt sich bei aktuellen Bluetooth-Geräten beispielsweise über die Option „Bluetooth-Geräte können eine Verbindung mit diesem Computer herstellen“ steuern. Bei anderen Geräten ist diese Option nicht konfigurierbar, statt dessen muss die Bluetooth-Schnittstelle vollständig aktiviert oder deaktiviert werden.

B.3 Gefährdungen

Zu all den Gefährdungen, denen kabelbasierte Netzwerke ausgesetzt sind (siehe [GSK]), kommen bei der Nutzung von Funknetz-Technik zusätzliche Gefährdungen hinzu, die insbesondere auf den Sicherheitsschwächen der verwendeten Protokolle sowie auf der unkontrollierten Ausbreitung der Funkwellen basieren.

B.3.1 Schwächen im Sicherheitskonzept des Standards

Die in den Bluetooth-Spezifikationen beschriebenen und von Herstellern entsprechend implementierten Sicherheitsmechanismen weisen einige prinzipielle Schwächen auf, die im folgenden benannt werden.

B.3.1.1 Verschlüsselung nicht vorgeschrieben

Unabhängig vom verwendeten Sicherheitsmodus ist die Verschlüsselung der zu übertragenden Daten optional und muss von den Anwendungen explizit beantragt werden.

B.3.1.2 Unsichere Voreinstellungen

Die Voreinstellungen sind von Seiten der Hersteller oft unsicher konfiguriert: Sicherheitsfunktionen wie Authentisierung und Verschlüsselung sind häufig abgeschaltet und PINs auf Standardwerte („0000“, „1234“ usw.) eingestellt. Wenn Geräte keine Eingabemöglichkeit besitzen (z.B. Headsets), ist eine Änderung der voreingestellten Werte gar nicht oder nur schwer möglich.

B.3.1.3 Erraten schwacher PINs bei Bluetooth ohne SSP

Wird bei der Gerätepaarung eine schwache PIN verwendet, kann ein Angreifer die PIN erraten und damit den aus der Paarung resultierenden Verbindungsschlüssel berechnen. Dazu muss der Angreifer nur die Paarung und die folgende Authentisierung abhören. Anhand der Aufzeichnungen der abgehörten Protokolle kann der Angreifer überprüfen, ob die PIN von ihm korrekt geraten wurde.

Die Berechnung einer PIN nach Abhören des Paarungs- und Authentisierungsvorgangs ist keine rein theoretische Gefährdung. Die Autoren von [SHWO05] haben eine Methode beschrieben und auch praktisch implementiert, mit der sich auf die genannte Weise die PIN ermitteln lässt. In [ZOLL06] wird eine entsprechende Software vorgestellt. Die Autoren haben demonstriert, dass sich damit eine 8-stellige numerische PIN innerhalb vom 10 Minuten ermitteln lässt[6]. Inzwischen wurden sogar Implementierungen auf Basis von Spezial-Hardware vorgenommen. Der Autor von [HULT07] hat auf diese Weise eine 8-stellige numerische PIN innerhalb von 10 Sekunden ermittelt. Eine Voraussetzung für die Durchführung dieser Angriffsmethode ist das vollständige Mitschneiden von Paarung und Authentisierung mit einem entsprechenden Werkzeug nebst Software zur Dekodierung der Paketinhalte (z.B. Bluetooth-fähiger Software-Analysator).

Als sicherheitskritisch anzusehen ist, dass die PIN bei Bluetooth ohne SSP als einziger geheimer Parameter in die Erzeugung des Verbindungsschlüssels einfließt. Erfahrungsgemäß lassen sich hier weit verbreitete Nutzer- bzw. Herstellergewohnheiten zu schwachen Sicherheitseinstellungen nur schwer

6 Verwendete Rechner-Hardware: Dual-Core-Prozessor mit einer Taktrate von 2 GHz

durchbrechen. In der Tat gibt es kaum Bluetooth-Geräte, die dem Anwender eine Mindestlänge und Komplexität für die PIN vorgeben. Es bleibt im Allgemeinen dem Anwender überlassen, welche PIN er wählt. Erste zaghafte Ansätze der Hersteller gehen einen dem Secure Simple Pairing entlehnten Weg. Sie geben dem Anwender auf einem der Geräte eine PIN vor, die er auf dem anderen Gerät korrekt eingeben muss. Allerdings begrenzt man dabei im Sinne der Benutzerfreundlichkeit die Länge der PIN. So gibt z.B. die Bluetooth-Implementierung eines modernen Betriebssystems eine 8-stellige numerische PIN vor, deren Sicherheit dem oben beschriebenen Szenario nicht standhält. Ein anderer Hersteller gibt zwar eine 16-stellige numerische PIN vor, die jedoch aus 8 Paaren gleicher Ziffern besteht (z.B. „44770022…“), damit sie vom Anwender fehlerfrei abgetippt werden kann. Im Prinzip ist dieser Ansatz als positiv zu bewerten, die vorgegebene PIN muss jedoch den in Kapitel B.4.3 angegebenen Richtlinien entsprechen. Ist das nicht der Fall, ist das genannte Verfahren als schlecht zu bewerten, da dem Anwender nun nicht die Wahl bleibt, selber eine PIN ausreichender Komplexität einzusetzen.

Die Verwendung von Secure Simple Pairing schützt vor der hier beschriebenen Gefährdung, da in jedem Fall Schlüsselmaterial ausreichender Komplexität übertragen wird (siehe Kapitel B.2.2).

B.3.1.4 Re-Initialisierung semipermanenter Verbindungen bei Bluetooth ohne SSP

Die in Kapitel B.3.1.3 erwähnten Angriffe lassen sich nur unter der Bedingung durchführen, dass der Authentisierungsvorgang abgehört werden kann. Dies wird durch die Verwendung semipermanenter Verbindungsschlüssel erschwert, da nach einmaliger Authentisierung die Verbindungsschlüssel von den Geräten nicht erneut ausgehandelt werden müssen. Allerdings sieht die Bluetooth-Spezifikation [BTSIG04] die Möglichkeit einer erneuten Authentisierung vor, wenn z.B. festgestellt wird, dass der Verbindungsschlüssel in einem der Geräte verloren gegangen ist.

Hierauf lässt sich eine in [SHWO05] beschriebene Angriffsmethode aufbauen: Ein Angreifer streut geschickt im passenden Moment ein entsprechendes Paket in die laufende Kommunikation zweier Geräte ein. Hierdurch wird eine erneute Paarung provoziert, die dann abgehört werden kann.

Ein aufmerksamer Nutzer kann dies bemerken, wenn er ohne ersichtlichen Grund zur erneuten PIN-Eingabe aufgefordert wird. Ein entsprechend sensibilisierter Nutzer kann den Angriff scheitern lassen, indem er die PIN-Eingabe verweigert, kann dann aber vorübergehend seine Geräte nicht wie gewünscht verwenden. Der Angriff wird im Allgemeinen auch scheitern, wenn eine PIN ausreichender Komplexität eingegeben wird (siehe Kapitel B.4.3). Er wird ebenso wenig zum gewünschten Erfolg führen, wenn Secure Simple Pairing verwendet wird (siehe Kapitel B.2.2).

B.3.1.5 Keine verbindliche Vorgabe einer ausreichenden Schlüssellänge

Neben Länge und Komplexität der bei der Authentisierung (bei Bluetooth ohne SSP) verwendeten PIN spielt auch die Länge der für die Verschlüsselung der übertragenen Daten verwendeten Schlüssel eine Rolle für die Sicherheit. Während die Bluetooth-Spezifikation für Schlüssel, die zur Authentisierung benutzt werden, eine Schlüssellänge von 128 Bit fest vorschreibt, kann die Länge des für die Verschlüsselung der weiteren Paketinhalte verwendeten Schlüssels variieren. Beide Geräte handeln im Rahmen des Verbindungsaufbaus die tatsächlich genutzte Schlüssellänge aus. Die Bluetooth-Spezifikation sieht hier eine Spannweite von 8 bis 128 Bit vor, d.h. eine minimale Schlüssellänge von 8 Bit kann verwendet werden, ohne gegen die Spezifikation zu verstoßen.

Dies wiegt umso schwerer, als dass eine Vorgabe der minimalen Schlüssellänge durch den Anwender ausdrücklich ausgeschlossen wird: Die Spezifikation fordert, dass dies eine Werkseinstellung sein soll, die der Nutzer nicht überschreiben kann. Die Güte der erreichbaren Verschlüsselung ist damit allein abhängig von der Herstellerentscheidung. Als Nutzer kann man an dieser Stelle nur durch gezielte Wahl der eingesetzten Geräte Einfluss ausüben, vorausgesetzt, dass entsprechende Herstellerangaben

zur eingestellten minimalen Schlüssellänge verfügbar sind. In allgemein zugänglichen Produktbeschreibungen fehlt eine solche Angabe oft völlig oder es wird nur die maximale Schlüssellänge von 128 Bit angegeben.

B.3.1.6 Ausspähen des Passkey bei SSP möglich

In Kapitel B.2.2.2 wurde das dem Assoziationsmodell Passkey Entry zugrunde liegende Protokoll beschrieben und darauf hingewiesen, dass sich durch Abhören der entsprechenden Kommunikation und sich anschließende wenige Rechenschritte der für eine erfolgreiche Authentisierung verwendete Passkey ermitteln lässt. Diese Tatsache alleine stellt noch keine Sicherheitsgefährdung dar. Erst wenn ein Anwender wiederholt denselben Passkey verwendet, lässt sich diese Schwäche des Standards ausnutzen.

Der Autor von [LIND08] weist in einem Konferenzbeitrag darauf hin, dass die Bluetooth-Spezifikation 2.1 + EDR nicht fordert, dass bei Passkey Entry Einmalpasswörter zu verwenden sind. Er beschreibt denkbare Angriffsszenarien, die für ihren Erfolg voraussetzen, dass der Anwender mehrfach den selben Passkey eingibt.

B.3.1.7 Schwache Integritätssicherung

Zur Integritätssicherung wird ein Cyclic Redundancy Check (CRC, Verfahren zur Erkennung von Übertragungsfehlern anhand einer Prüfsumme) verwendet. Dadurch werden zwar mit hoher Wahrscheinlichkeit zufällige Störungen bei der Übertragung von Datenpaketen erkannt, aber gegen eine absichtliche Manipulation von Datenpaketen bieten CRC-Verfahren keinen Schutz.

B.3.1.8 Qualität des Zufallsgenerators

Zur Zufallserzeugung sehen die Bluetooth-Spezifikationen 1.x und 2.0 + EDR die Verwendung eines sogenannten Pseudozufallszahlen-Generators vor. Es wird jedoch keine Vorgabe für dessen Implementierung gemacht. Es ist daher nicht völlig auszuschließen, dass die verwendeten Zufallszahlen-Generatoren Schwächen aufweisen, die sich für das Überwinden der kryptographischen Verfahren ausnutzen lassen.

In der Bluetooth-Spezifikation ab 2.1 + EDR wird die Verwendung eines Zufallszahlen-Generators gemäß [FIPS1402C] gefordert. Ein entsprechender Algorithmus findet sich demnach in [FIPS1862], Anhang 3.1. Die Prüfung der Implementierung des Zufallszahlen-Generators durch den Hersteller soll gemäß [NIST22R1] erfolgen.

B.3.2 Schwächen der Verschlüsselung

Die von Bluetooth optional verwendete Verschlüsselung weist einige Schwächen auf, die im Folgenden aufgeführt werden.

B.3.2.1 Sicherheit der Stromchiffre E_0

Obwohl E_0 Schlüssellängen von 1 bis 16 Bytes (8 - 128 Bit) akzeptiert, haben Fluhrer und Lucks gezeigt, dass die erreichbare Sicherheit je nach Stärke des Angreifers 73 bzw. 84 Bit nicht übersteigt (siehe [FLUH01]).

B.3.2.2 Verkürzter Initialisierungsvektor

Jedes übertragene Datenpaket wird unter Verwendung eines neuen Initialisierungsvektors verschlüsselt. Dieser errechnet sich unter anderem aus dem Zeittakt des Master. Es wird allerdings das höchstwertige Bit des Zeittaktes "vergessen". Diese Schwäche ist die Voraussetzung dafür, dass sich selbst bei eingesetzter Verschlüsselung Man-in-the-Middle-Angriffe (siehe Kapitel B.3.3) durchführen lassen, da es immer zwei unterschiedliche Offsets in der Sprungsequenz zu einem Initialisierungsvektor gibt. Ein Man-in-the-Middle-Angriff auf eine verschlüsselte Verbindung erlaubt jedoch nur, den Datenstrom zu manipulieren (siehe Kapitel B.3.2.3), nicht jedoch zu entschlüsseln.

B.3.2.3 Manipulation von verschlüsselten Daten

Aufgrund der Eigenschaften von Stromchiffren im Zusammenwirken mit dem zur Integritätssicherung eingesetzten CRC ist es möglich, Änderungen am Chiffrat dergestalt vorzunehmen, dass der Empfänger das Paket nach wie vor als gültig erkennt. So ist es beispielsweise bei Bluetooth ohne SSP im Rahmen eines Man-in-the-Middle-Angriffs möglich, IP-Header gezielt zu manipulieren.

B.3.3 Man-in-the-Middle-Angriffe bei Bluetooth ohne SSP

Ein weiteres Sicherheitsproblem von Bluetooth besteht darin, dass in bestimmten Konfigurationen sogenannte Man-in-the-Middle-Angriffe möglich sind (siehe [KÜGL03]).

Dabei schiebt sich ein Angreifer, der (unberechtigt) Zugriff auf ein Bluetooth-Gerät erhalten will, "mitten zwischen" zwei berechtigte Geräte. Anschließend kommunizieren die beiden Geräte über den Angreifer miteinander, der die Datenpakete abfängt und manipulieren kann. Folgende Szenarien sind denkbar:

- Der Angreifer baut aktiv eine Verbindung zu beiden Geräten auf und gibt dabei vor, jeweils das andere Gerät zu sein. Sofern sich das Gerät des Angreifers gegenüber einem Gerät authentisieren muss, reicht es die Authentisierungsanfrage an das andere Gerät weiter und sendet die Antwort zurück. Anschließend kann der Angreifer mit dem Gerät beliebig interagieren. Als Voraussetzung für die erfolgreiche Durchführung dieses Angriffs müssen beide Geräte connectable sein (siehe Kapitel B.2.4).

- Der Angreifer schaltet sich ein, während die Geräte mittels Pairing eine Verbindung aufbauen. Während des Verbindungsaufbaus müssen sich die Geräte auf die Sprungsequenz synchronisieren. Der Angreifer kann auf diese Synchronisation Einfluss nehmen, sodass beide Geräte zwar die gleiche Sequenz, aber verschiedene Offsets in der Sequenz verwenden.

Man-in-the-Middle-Angriffe werden durch die Verwendung von Secure Simple Pairing in den Modellen Numeric Comparison und Passkey Entry erkannt. Auch das Modell Out of Band ist in der Lage, solche Angriffe zu erkennen, sofern der OOB-Kanal nicht kompromittiert wird. Realisierte Man-in-the-Middle-Angriffe sind zum Zeitpunkt der Veröffentlichung dieser Broschüre nicht bekannt.

B.3.4 Unkontrollierte Ausbreitung der Funkwellen

Die Funkwellen der Bluetooth-Komponenten breiten sich auch über räumliche Grenzen des Bluetooth-Nutzungsbereichs aus. Dabei kann auch in nicht vom Betreiber der Bluetooth-Geräte kontrollierten Bereichen ein Empfang möglich sein. Je nach Umgebungsbedingungen und Leistungsfähigkeit der verwendeten Empfangsgeräte (z.B. Richtantennen) besteht auch hier noch eine konkrete Abhörgefahr, sofern keine adäquaten Verschlüsselungsmechanismen eingesetzt werden.

Inzwischen haben Fachleute vorgeführt, dass sich mit entsprechend modifiziertem Gerät – inkl. Einsatz einer Richtantenne – die Bluetooth-Schnittstelle von Mobiltelefonen auf Entfernungen von nahezu 2 km erfolgreich angreifen lässt (siehe [TRIFORG]).

B.3.5 Bewegungsprofile

Die eindeutigen Bluetooth-Geräteadressen können zum Verfolgen einzelner Geräte missbraucht werden. Auf diese Weise ist es möglich, Bewegungsprofile der Benutzer zu erstellen. Die Geräteadresse wird nicht nur zum Verbindungsaufbau verwendet, die Geräteadresse des Master ist zum Teil (24 der 48 Bit) in jedem Datenpaket enthalten.

Ohne Weiteres gelingt die Erkennung und Verfolgung von Bluetooth-Geräten mittels Inquiry, wenn diese im discoverable mode konfiguriert sind (siehe Kapitel B.2.4). Inzwischen hat man jedoch auch Methoden entwickelt, Bluetooth-Geräte aufzuspüren, wenn sie auf non-discoverable eingestellt sind (siehe [CHLRS07]). Hierzu werden alle möglichen Bluetooth-Adressen durchprobiert. Ähnlich wie bei MAC-Adressen von Ethernet ist auch bei Bluetooth der vordere Teil einer Bluetooth-Adresse nicht willkürlich. Vielmehr beginnt eine solche Adresse generell mit einem herstellerspezifischen Präfix, wobei die entsprechend registrierten Abfolgen offengelegt sind. In Kenntnis der in Frage kommenden Herstellerkennungen kann man einen Angriff erfolgreich durchführen, indem man alle möglichen Kombinationen der verbleibenden hinteren sechs Stellen durchprobiert und die so konstruierten Adressen gezielt anspricht.

B.3.6 Verfügbarkeitsprobleme

Die Verfügbarkeit von Bluetooth kann unter anderem durch folgende Ursachen beeinträchtigt werden:

- Störung durch gezielt eingesetzte Störsender
- Denial-of-Service – Denkbar sind zum Beispiel Angriffe auf die Energiereserven der Geräte durch Verhindern des Ruhe-Modus.
- Störungen durch andere Funk-Anwendungen im gleichen ISM-Band

Prinzipiell verbessert die Einführung des Adaptive Frequency Hopping (AFH) mit Bluetooth 1.2 die Koexistenz von Bluetooth mit anderen Funkdiensten, indem die Nutzung belegter Kanäle vermieden wird. AFH ist jedoch nur während einer bestehenden Verbindung aktiv. Während der Verbindungsaufbauphase (Inquiry, Paging) werden dagegen feste Kanäle verwendet. Während dieser Phase besteht eine höhere Wahrscheinlichkeit der Störung durch andere Anwendungen im gleichen ISM-Band. Außerdem kann Bluetooth in dieser Phase störend auf andere Anwendungen – insbesondere WLAN – einwirken.

B.3.7 Implementierungsschwächen

Mit steigender Verbreitung von Bluetooth steigt auch die Wahrscheinlichkeit, dass Fehler in den Implementierungen der Hersteller auftreten, dass diese bekannt und schließlich für Angriffe ausgenutzt werden. Mittlerweile sind verschiedene Angriffsformen infolge fehlerhafter Implementierungen diskutiert und auch realisiert worden[7].

[7] Z.B. BlueSnarf, BlueBug, Car Whisperer

B.3.7.1 Ungeschützte Dienste

Voraussetzung für den Zugriff auf Dienste in Bluetooth-Geräten ist immer der erfolgreiche Abschluss des Pairing. Teil des Pairing ist generell eine Authentisierung, die in Kapitel B.2.1 bzw. B.2.2 beschrieben wurde. Ohne vorangegangenes Pairing lässt sich jedoch immer Kontakt zum Dienst Service Discovery Protocol (SDP) aufnehmen, der dem Anwender die auf diesem Gerät zur Verbindung bereitstehenden Dienste mitteilt.

In der Vergangenheit wurden jedoch Implementierungen bekannt, bei denen auch andere Dienste ohne vorangegangenes Pairing zugänglich waren. Die Hersteller hatten offensichtlich eine Art Hintertür geöffnet. Diese Dienste wurden jedoch vom SDP nicht bekannt gegeben, waren also für einen normalen Benutzer nicht sichtbar.

Auf Basis dieser Schwachstelle ließen sich unter anderem die folgenden Angriffe erfolgreich durchführen:

- Der Angreifer sendet sogenannte AT-Kommandos an den ungeschützten Dienst RFCOMM eines Mobiltelefons. Die entsprechenden Kommandos sind standardisiert und in [3GPP277] spezifiziert. Es lassen sich unter anderem Anruflisten von einem solchen Telefon kopieren sowie das Telefon vollständig fernsteuern (SMS-Versand oder SMS-Mitlesen, Veränderung der Einstellungen, Nutzung des Telefons als Internet-Zugang, Änderung von Grundeinstellungen wie Rufweiterleitung, Provider-Voreinstellung usw.).

- Der Angreifer nutzt das Profil, das eigentlich für den einfachen Austausch von elektronischen Visitenkarten u.ä. vorgesehen ist (OBEX Push Profile). Dieser Dienst ist auf vielen Geräten nicht über Authentisierung gesichert. Da für Dateien wie Kalender oder Telefonbuch typischerweise Standardnamen verwendet werden, kann der Angreifer sich diese vom angegriffenen Gerät mit einem gezielten Befehl an diesen Dienst herunterladen. Unterstützt ein angegriffenes Bluetooth-Gerät nicht nur den einfachen OBEX-Push-Dienst, sondern einen OBEX-basierenden FTP-Server, so kann ein Angreifer sogar unbefugt schreibenden Zugriff auf OBEX-Basis erhalten.

- Der Angreifer nutzt das Profil für die Anbindung von Eingabegeräten (HID-Profil). Es gibt Geräte, bei denen der entsprechende Dienst standardmäßig aktiviert und nicht über Authentisierung gesichert ist. Der Autor von [MULL07] beschreibt praktische Implementierungen dieses Angriffs.

B.3.7.2 Denial of Service (DoS)

An Mobiltelefonen unterschiedlicher Hersteller wurden in der Vergangenheit fehlerhafte Implementierungen entdeckt, die es einem Angreifer ermöglichten, zeitweise den Bluetooth-Protokoll-Stack oder gar das gesamte Telefon lahm zu legen:

- Der Angreifer bombardiert ein fremdes Bluetooth-Gerät bis zur völligen Überlastung mit L2CAP echo requests.

- Bestimmte Mobiltelefone lassen sich mit einzelnen Bluetooth-Paketen außer Gefecht setzen (siehe [SOBS06]).

B.3.8 Gefährdungen bei Verwendung des SIM Access Profile

Das SIM Access Profile (siehe [BTSIG08]) dient dazu, ein Mobiltelephon die SIM-Karte eines über Bluetooth verbundenen Geräts nutzen zu lassen. Typischerweise handelt es sich um ein fest eingebautes Autotelefon, das sich mit einer SIM-Karte verbindet, die in einem anderen Mobiltelefon eingesetzt ist. Das SIM Access Profile bietet zu diesem Zweck eine transparente Verbindung zwischen Mobilte-

lefon und SIM-Karte. Wird diese Verbindung kompromittiert, lassen sich Angriffe auf die Vertraulichkeit und Integrität der Mobilfunkverbindung durchführen. Der Autor von [HEIN09] hat verschiedene Angriffe erdacht, die auf dem SIM Application Toolkit (STK) basieren, das in vielen SIM-Karten implementiert ist. Als besonders kritisch stuft er die Möglichkeit ein, mit Hilfe des STK den für die Verschlüsselung der Mobilfunkverbindung verwendeten Sitzungsschlüssel per Kurznachricht (SMS) zu versenden und somit auszuspähen.

Die in den voranstehenden Abschnitten beschriebenen Gefährdungen bekommen dadurch eine unerwartete Tragweite. Die Kombination der beiden Techniken Bluetooth und Mobilfunk ermöglicht Angriffsszenarien, die mit jeder Technik für sich genommen nicht möglich wären.

B.3.9 Weitere Sicherheitsaspekte

Folgende Aspekte sind ebenfalls zu bedenken:

- Mobile Geräte sind gegenüber stationären Geräten einem höheren Diebstahlrisiko ausgesetzt.
- Authentisieren muss sich bei Bluetooth nur das Gerät gegenüber einem Kommunikationspartner, in der Regel aber nicht der Benutzer gegenüber dem Gerät. Bei Abhandenkommen mobiler, gepaarter Geräte sind diese also ohne weiteres im Herkunftsbereich durch unbefugte Dritte nutzbar, da die Geräte in der Regel semipermanente Verbindungsschlüssel nutzen.
- Bluetooth-Geräteadressen sind mit geeignetem Equipment prinzipiell manipulierbar.
- Auch in mittels Bluetooth etablierten Ad-hoc-Netzwerken existiert die Gefahr der Verbreitung von Computer-Viren und trojanischen Pferden.
- Das Abhören bzw. Aufzeichnen von Raumgesprächen unter Verwendung von handelsüblichen oder speziell manipulierten Bluetooth-Geräten (z.B. Headset mit 100 mW Sendeleistung) ist grundsätzlich nicht auszuschließen (siehe hierzu auch [ÖMS08]).
- Generell kann man sich nicht vor Dritten sicher fühlen, nur weil zu diesen kein Sichtkontakt besteht (siehe Kapitel B.3.4).

B.4 Schutzmaßnahmen

Im Folgenden wird beschrieben, welche Maßnahmen zum Schutz von Bluetooth-Geräten ergriffen werden können und welche Restrisiken bestehen.

B.4.1 Absicherung von Bluetooth-Geräten

B.4.1.1 Gezielte Produktauswahl

Es sollten grundsätzlich Geräte ausgewählt werden, die der Bluetooth-Spezifikation 2.1 + EDR, 3.0 + HS oder einer nachfolgenden Spezifikation entsprechen. Nach Möglichkeit sind keine Geräte einzusetzen, die mit Geräteschlüsseln arbeiten. Es sind Geräte zu bevorzugen, bei denen die Bluetooth-Schnittstelle im Auslieferungszustand deaktiviert ist und nach Aktivierung auf non-discoverable eingestellt ist. Die Aktivität der Bluetooth-Schnittstelle sollte sich mittels eines gut sichtbaren Symbols jederzeit prüfen lassen. Geräte mit möglichst guter minimaler Schlüssellänge für die Datenverschlüsselung sind zu bevorzugen.

In Umgebungen, bei denen die Gefahr von Interferenzen mit anderen Funkdiensten im 2,4-GHz-Band besteht, sollten Geräte eingesetzt werden, die über AFH hinaus eine Vorgabe der zu verwendenden Kanäle durch einen Administrator erlauben.

B.4.1.2 Einspielen von Sicherheitspatches

Von den Geräteherstellern bereitgestellte Sicherheitspatches bzw. aktuellere Versionen der Firmware sollten nach Test und bei entsprechendem Sicherheitsbedarf eingespielt werden.

B.4.1.3 Allgemeine Konfiguration

Grundsätzlich ist es empfehlenswert, die vom Hersteller voreingestellte Konfiguration zu überprüfen und wenn möglich zu ändern:

- Häufig sind bei Bluetooth-Geräten im Auslieferungszustand viele Dienste aktiviert, damit alle Möglichkeiten der Kommunikation mit anderen Geräten genutzt werden können. Nicht benötigte Dienste sollte der Anwender stets deaktivieren. Nur sporadisch benötigte Dienste sollten bei Bedarf gezielt aktiviert und danach wieder deaktiviert werden.

- Die Bluetooth-Schnittstellen der Geräte sollten bei Nichtbenutzung deaktiviert werden.

- Bluetooth-Geräte sollten möglichst wenig „offen“ konfiguriert werden. Es sind nach Möglichkeit die Betriebsmodi non-discoverable, non-connectable und non-pairable bzw. non-bondable einzustellen.

- Die Sendeleistung von Bluetooth-Geräten sollte so niedrig wie möglich und so hoch wie für die Funktionalität erforderlich gewählt werden. So sollte an z.B. an einem Notebook ein Bluetooth-Gerät Klasse 3 (1 mW) eingesetzt werden, wenn dieses für die Kopplung zu einem Mobiltelefon eingesetzt wird, das sich nur wenige Meter entfernt befindet.

- Falls möglich, sollten voreingestellte PINs sofort geändert werden.

- Authentisierung und Verschlüsselung sind dem Schutzbedarf angemessen zu wählen.
- Für starke Verschlüsselung muss die Schlüssellänge mindestens 64 Bit betragen, und als Verschlüsselungsmodus darf nur Punkt-zu-Punkt-Verschlüsselung akzeptiert werden. Die Schlüssellänge sollte so groß wie möglich gewählt werden. Da sich die Länge des Verschlüsselungsschlüssels vom Benutzer nicht vorgeben lässt, sind nach Möglichkeit nur solche Geräte einzusetzen, die den genannten Anforderungen genügen (siehe Kapitel B.3.1.5).

Darüber hinaus ist es empfehlenswert, Bluetooth-Geräte mit entsprechenden Hilfsmitteln[8] nach versteckten Diensten bzw. offenen Ports zu untersuchen.

B.4.1.4 Stationäre Geräte

Stationäre Geräte, bei denen Bluetooth als Kabelersatz – zum Beispiel zur Verbindung mit immer den gleichen Peripheriegeräten – verwendet wird, sollten mit Authentisierung betrieben werden. Dabei sind Lösungen mit semipermanenten Verbindungsschlüsseln zu bevorzugen. Grundsätzlich sollte Verschlüsselung aktiviert werden. Sofern Geräte den Sicherheitsmodus 2 (siehe Kapitel B.2.4) verwenden, ist darauf zu achten, dass Authentisierung und Verschlüsselung für jeden Dienst separat zu aktivieren ist. Dienste, bei denen dies nicht unterstützt wird, sollten nicht genutzt werden.

B.4.1.5 Mobile Geräte

Bluetooth-Geräte, die mobil verwendet werden und mit fremden Geräten (d.h. Geräten unterschiedlicher Besitzer) kommunizieren, müssen besonders gesichert werden:

- Die Paarung zweier Geräte sollte immer in abhörsicherer Umgebung durchgeführt werden. Dabei ist zu beachten, dass Abhörsicherheit über die Möglichkeit des unbeobachteten Eindringens per Bluetooth von außen zu beurteilen ist. Die Reichweite der eigenen Bluetooth-Geräte alleine ist nicht entscheidend.
- Lösungen mit semipermanenten Verbindungsschlüsseln sind zu bevorzugen.
- Die Paarung sollte nur mit vertrauenswürdigen Geräten erfolgen.
- Bei Verlust/Diebstahl eines mobilen (bzw. stationären) Geräts sollten alle zugehörigen Verbindungsschlüssel in den verbliebenen Geräten gelöscht werden. Dies geschieht im Allgemeinen durch Löschen des entsprechenden Eintrages in der Bluetooth-Geräteliste des verbliebenen Geräts.

B.4.2 Verwendung von Secure Simple Pairing

Wenn beide zu paarenden Geräte mindestens der Bluetooth-Spezifikation 2.1 + EDR entsprechen, sollte Secure Simple Pairing mit den Methoden Numeric Comparison, Passkey Entry oder Out of Band eingesetzt werden (Sicherheitsmodus 4 mit dem Attribut Authenticated, siehe Kapitel B.2.4). Diesbezüglich ist folgendes zu beachten:

- Numeric Comparison zeigt dem Anwender auf beiden Geräten eine 6-stellige Zahl an, deren Übereinstimmung auf beiden Geräten zu bestätigen ist. Dieses Verfahren ist zu bevorzugen, da es ein hohes Maß an Sicherheit bietet.

---

8 Z.B. mittels „BT Audit“

- Passkey Entry gibt es in einer Variante, die dem Anwender auf einem Gerät eine 6-stellige Zahl anzeigt, die er am anderen Gerät eingeben muss. Diese Variante des Passkey Entry wird als sicher angesehen und kann verwendet werden.

- Eine andere Variante des Passkey Entry lässt den Anwender eine selbst gewählte 6-stellige Zahl an beiden Geräten eingeben. Diese Variante ist nur unter der Bedingung als sicher anzusehen, dass bei jedem Vorgang eine andere Zahl gewählt wird. Da dies von einem Benutzer im Allgemeinen nicht gefordert werden kann, wird vom Einsatz dieser Variante des Passkey Entry abgeraten.

- Zur Unterstützung der Methode Out of Band müssen beide zu verbindende Geräte über entsprechende NFC-Chips verfügen. Zur Sicherheit von NFC siehe Kapitel H. NFC.

B.4.3 Hinweise zur Wahl von PINs bei Bluetooth ohne SSP

PINs sollten eine möglichst zufällige Folge aus den verwendbaren Zeichen sein, triviale PINs wie "0000" oder "1234" sind unbedingt zu vermeiden (siehe [GSK]). Für eine ausreichende Sicherheit bei der Paarung zweier Bluetooth-Geräte ist eine ausreichend lange PIN notwendig. Auf einem handelsüblichen PC lassen sich PINs mit bis zu 48 Bit Länge brechen, diese Länge sollten PINs mindestens aufweisen. Empfohlen wird eine Länge von mindestens 64 Bit. Da es bei Bluetooth-Geräten nur möglich ist, PINs in Form von Ziffern bzw. alphanumerischen Zeichen einzugeben, gibt Tabelle B-1 Empfehlungen für die Anzahl der zu verwendenden Zeichen.

Tabelle B-1: Wahl von PINs

Verwendete Zeichen	Min. empfohlene PIN-Länge	Minimale PIN-Länge
0-9 (10 Zeichen)	19 Stellen (= 63 Bit)	15 Stellen (= 50 Bit)
0-9, A-Z (36 Zeichen)	12 Stellen (= 62 Bit)	10 Stellen (= 52 Bit)
0-9, A-Z, a-z (62 Zeichen)	11 Stellen (= 65 Bit)	8 Stellen (= 48 Bit)
(druckbares) ASCII (95 Zeichen)	10 Stellen (= 66 Bit)	8 Stellen (= 53 Bit)

Beispiel zur Erläuterung der Tabelle: Akzeptiert das Gerät nur Ziffern und Großbuchstaben als PIN, sollte in jedem Fall eine PIN von mehr als 10 Stellen verwendet werden; empfohlen werden jedoch PINs mit mindestens 12 Stellen.

Anmerkung zur Tabelle: 19-stellige PINs lassen sich an den meisten Bluetooth-Geräten nicht eingeben. Das höchstmögliche Sicherheitsniveau lässt sich somit nur mittels alphanumerischer PINs erzielen.

Die PIN ist im Normalfall nur bei der ersten Verbindungsaufnahme zwischen Geräten einzugeben (semipermanente Verbindungsschlüssel). Wird bei einem solchen Geräte-Paar zu einem unerwarteten Zeitpunkt vom Benutzer eine PIN-Eingabe verlangt, sollte dieser nach Möglichkeit darauf verzichten, bis er sich in abhörsicherer Umgebung befindet. Eine entsprechende Nutzereinweisung oder -schulung wird empfohlen.

B.4.4 Weitere Schutzmaßnahmen

Über die in Kapitel B.4.1 genannten Maßnahmen hinaus sollten auf Bluetooth-Geräten – falls dies technisch möglich ist – weitere lokale Schutzmaßnahmen implementiert werden. Dazu zählen:

- Zugriffsschutz (materielle Sicherungsmaßnahmen)
- Benutzerauthentisierung
- Virenschutz
- Personal Firewall
- restriktive Datei- und Ressourcenfreigabe auf Betriebssystemebene
- lokale Verschlüsselung

Informationen hierzu findet man in den IT-Grundschutz-Katalogen des BSI (siehe [GSK]). Im Zweifel orientiere man sich am Baustein „Internet-PC“ und wende die zugehörigen Maßnahmen sinngemäß an.

Als Schutzmaßnahme gegen das Abhören von Raumgesprächen ist ein Verbot des Einbringens von Funktechnik in den zu schützenden Raum zu empfehlen (siehe auch [ÖMS08]).

B.4.5 Restrisiko

Unabhängig von den beschriebenen Sicherheitsmaßnahmen sind mit der Verwendung von Bluetooth-Geräten immer folgende Restrisiken verbunden:

- Das Erstellen von Bewegungsprofilen mobiler Geräte (siehe Kapitel B.3.5) kann nicht verhindert werden.
- Die Gefährdung der Verfügbarkeit (siehe Kapitel B.3.6) ist ebenfalls nicht vermeidbar.
- Man-in-the-Middle-Angriffe (siehe Kapitel B.3.3) sind auch bei optimal konfigurierten Geräten der Bluetooth-Spezifikation 2.0 + EDR oder früher theoretisch möglich. Schutz bietet nur der Einsatz von Secure Simple Pairing ab Bluetooth-Spezifikation 2.1 + EDR; die Einsatzrichtlinien in Kapitel B.4.2 sind zu beachten. Schutz lässt sich auch durch zusätzliche Sicherheitsmaßnahmen erreichen, zum Beispiel durch die Verwendung von Sicherheitsdiensten in transportorientierten Schichten des ISO-Referenzmodells (z.B. IPsec) oder direkt auf Anwendungsebene (Ende-zu-Ende-Sicherheit).

B.5 Ausblick

Die Bluetooth-Technik ist etabliert und hält inzwischen auch Einzug in sensible Bereiche wie Automobilelektronik und Fertigungssteuerung. Hierdurch erhalten die aufgezeigten Gefährdungen erhöhte Brisanz, nicht zuletzt auch die Gefahr des Einspielens von Viren nach erfolgreicher, unbefugter Verbindungsaufnahme. Die Entwicklung von Bluetooth 2.1 + EDR mit Secure Simple Pairing (SSP) bietet zusätzliche Sicherheit und ist als positiv zu bewerten. Es steht zu erwarten, dass viele zukünftige Geräte diesen Standard unterstützen werden. Die Verbreitung des auf NFC basierenden SSP-Modells „Out of Band“ bleibt jedoch abzuwarten.

Die Entwicklung von Bluetooth mit noch höheren Bandbreiten steht vor der Tür. Insbesondere die Spezifikation 3.0 + HS (siehe Kapitel B.1.4.1) spiegelt die Anstrengungen der Bluetooth SIG, bald Produkte mit einer schnelleren Technik marktreif vorstellen zu können. Darüber hinaus bietet diese Technik neue Chancen einer Kompatibilität zu WLAN.

B.6 Fazit

Bluetooth ist ein inzwischen weit verbreitetes Verfahren zur drahtlosen Kommunikation zwischen Mobiltelefonen, Personal Computern und Peripheriegeräten. Eine Ausbreitung der Technik in neue Anwendungsfelder wie z.B. die industrielle Fertigung und die Automobilelektronik findet derzeit statt.

Das Sicherheitskonzept von Bluetooth sieht eine gegenseitige Authentisierung der Geräte sowie eine Verschlüsselung des Datenverkehrs vor. Für die Nutzung in Umgebungen mit normalem Schutzbedarf sind die von Bluetooth bereitgestellten kryptographischen Verfahren, insbesondere für die Verschlüsselung, angemessen. Dies gilt auch unter Berücksichtigung der bisher bekannt gewordenen Schwachstellen. Wird höherer Schutzbedarf gefordert, sind zusätzliche Maßnahmen, die über die Möglichkeiten von Bluetooth hinausgehen, zu treffen.

Im Gegensatz dazu ist die Verwendung von PINs als Basis für Authentisierung und Verschlüsselung ein Problem beim praktischen Einsatz von Bluetooth. Typische Gewohnheiten der Nutzer bei der Vergabe von PINs waren in der Vergangenheit häufig Ziele von Angriffen. Hier bietet das neue Secure Simple Pairing Abhilfe. Insbesondere die Methode der Numeric Comparison, bei der vom Benutzer kein Ausdenken eines Kennworts verlangt wird, bietet eine Chance für den sicheren Einsatz von Bluetooth.

Die Absicherung der Kommunikation über Bluetooth lässt sich dennoch technisch nicht erzwingen; sie bleibt auch in Anbetracht der aktuellen Verfahren eine Aufgabe für den Nutzer. Dabei stehen sichere Konfiguration und umsichtiger Umgang mit der Technik im Vordergrund. Hierzu soll die vorliegende Broschüre eine Hilfe sein.

Vom Nutzer nicht zu beeinflussen sind dagegen nachlässige Implementierungen von Bluetooth durch die Hersteller. Zahlreiche in der Vergangenheit veröffentlichte Angriffs-Tools nutzten eben diese Schwächen aus. Hier hilft letztlich nur vollständiges Deaktivieren von Bluetooth – selbstverständlich unter Verzicht auf die Segnungen dieser drahtlosen Technik.

B.7 Literatur und Links

Informationen zum Grundverständnis der Bluetooth-Funktechnik in deutscher Sprache kann man unter anderem [GEIG04] entnehmen, weitere grundlegende deutschsprachige Informationen finden sich in den Büchern [WOLL01] und [MULL01]. Eine genauere Beschreibung der grundlegenden Bluetooth-Sicherheitsarchitektur ist zum Beispiel in [FOX02] enthalten. Interessante Informationen zu Bluetooth findet man unter [JAWE02], [KAOW02] und [LIND08], die aktuelle Spezifikation unter [BTSIG09]. Informationen zu konkreten, als praktikabel nachgewiesenen Angriffsformen finden sich unter [SHWO05] und [ZOLL06].

Es gibt inzwischen zahlreiche Bücher und Publikationen zu Bluetooth. Die Liste der hier aufgeführten Titel und Links stellt nur eine wertungsfreie Auswahl ohne Anspruch auf Vollständigkeit dar.

[3GPP277] 3GPP TS 27.007: AT command set for User Equipment (UE), März 2005, http://www.3gpp.org/ftp/Specs/html-info/27-series.htm,

[BTSIG04] Specification of the Bluetooth System Version 2.0 + EDR, November 2000, http://www.bluetooth.com/Bluetooth/Technology/Building/Specifications/Default.htm

[BTSIG06] Bluetooth SIG selects WiMedia Alliance Ultra-Wideband Technology For High Speed Bluetooth® Applications, Pressemitteilung der Bluetooth SIG, http://www.bluetooth.-com/Bluetooth/Press/SIG/BLUETOOTH_SIG_SELECTS_WIMEDIA_ALLIANCE_ULTRAWIDEBAND_TECHNOLOGY_FOR_HIGH_SPEED_BLUETOOTH_APPLI-CATION.htm, März 2006

[BTSIG07] Specification of the Bluetooth System Version 2.1 + EDR, Juli 2007, http://www.bluetooth.com/Bluetooth/Technology/Building/Specifications/Default.htm

[BTSIG08] SIM Access Profile, Interoperability Specification, Dezember 2008, http://www.bluetooth.com/Bluetooth/Technology/Building/Specifications/Default.htm

[BTSIG09] Specification of the Bluetooth System Version 3.0 + HS, April 2009, http://www.bluetooth.com/Bluetooth/Technology/Building/Specifications/Default.htm

[CHLRS07] D. Cross, J. Hoeckle, M. Lavine, J. Rubin, K. Snow, "Detecting Non-Discoverable Bluetooth Devices", IFIP International Federation for Information Processing, Band 253, Critical Infrastructure Protection, Springer Boston, 2007

[FIPS1402C] Federal Information Processing Standards Publication (FIPS PUB) 140-2, Security Requirements for Cryptographic Modules, Annex C: Approved Random Number Generators for FIPS PUB 140-2, National Institute of Standards and Technology, Oktober 2007, http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexc.pdf

[FIPS1862] Federal Information Processing Standards Publication (FIPS PUB) 186-2, Digital Signature Standard (DSS), Januar 2000

[FLUH01] S. R. Fluhrer und S. Lucks, Analysis of the E_0 Encryption System, Selected Areas in Cryptography - SAC 2001, Lecture Notes in Computer Science 2259, Seiten 38-48, Springer-Verlag, 2001, http://th.informatik.uni-mannheim.de/People/Lucks/papers/e0.ps.gz

[FOX02] D. Fox, Bluetooth Security, Secorvo White Paper 2002, http://www.secorvo.de/whitepapers/secorvo_wp05.pdf,

[GEIG04] J. Geiger, Bluetooth-FAQ, CHIP-online, September 2004, http://www.chip.de/artikel/c1_artikel_12833263.html

[GSK] Bundesamt für Sicherheit in der Informationstechnik, „IT-Grundschutz-Kataloge“, verfügbar unter https://www.bsi.bund.de/cln_155/DE/Themen/weitereThemen/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

[HEIN09] Benedikt Heinz: SIM Application Toolkit basierter Angriff auf mobile Endgeräte durch Hardware-Manipulation an der SIM-Karte, Beitrag zum 11. Deutschen IT-Sicherheitskongress des BSI, Mai 2009

[HULT07] David Hulton, Hacking the Airwaves with FPGAs, Beitrag zu SmooCon 2007 Hacking and Computer Security Conference in Washington D.C., Juli 2007, http://openciphers.sourceforge.net/slides/shmoocon-2007.pdf

[IEEE05] IEEE Std 802.15.1 – 2005, „Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)”, IEEE 802.15.1, 2005, verfügbar unter http://www.ieee.org

[IEEE07] IEEE Std 802.11-2007, „Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications“, 2007, verfügbar unter http://www.ieee.org

[JAWE02] M. Jakobsson und S. Wetzel, Security Weaknesses in Bluetooth. Progress in Cryptography - CT-RSA 2001, Lecture Notes in Computer Science 2020, Seiten 176-191, Springer-Verlag, 2001

[KAOW02] T. Karygiannis und L. Owens, Wireless Network Security, National Institute of Standards and Technology (NIST) Nov. 2002, http://www.csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf

[KÜGL03] D. Kügler, "Man in the Middle" Attacks on Bluetooth, Financial Cryptography '03, Lecture Notes in Computer Science 2742, Seiten 149-161, Springer-Verlag 2003

[LIND08] Andrew Lindell, Bluetooth v2.1 – A New Security Infrastructure and New Vulnerabilities, Black Hat Conference, 2008, http://www.aladdin.com/blog/pdf/AndrewLindell-BlackHat08.ppt

[LIND09] Andrew Lindell: Comparison-Based Key Exchange and the Security of the Numeric Comparison Mode in Bluetooth v2.1, Aladdin Knowledge Systems Ltd., Januar 2009, http://www.cs.biu.ac.il/~lindell/PAPERS/BT-numeric.pdf

[MULL01] N. J. Muller, Bluetooth, MITP-Verlag 2001

[MULL07] Collin A. Mulliner, HID Attack (attacking HID host implementations), Januar 2007, http://mulliner.org/bluetooth/hidattack.php

[NIST22R1] A Statistical Test Suite for Random and pseudo-random Number Generators for Cryptographic Applications, National Institute of Standards and Technology, Special Publication 800-22 Revision 1, August 2008, http://csrc.nist.gov/publications/nistpubs/800-22-rev1/SP800-22rev1.pdf

[NIST121] Guide to Bluetooth Security, Recommendations of the National Institute of Standards and Technology, Special Publication 800-121, September 2008, http://csrc.nist.gov/publications/nistpubs/800-121/SP800-121.pdf

[ÖMS08] Bundesamt für Sicherheit in der Informationstechnik, „Öffentliche Mobilfunknetze und ihre Sicherheitsaspekte“, 2008, https://www.bsi.bund.de/cln_155/ContentBSI/Publikationen/Broschueren/oefms/index_htm.html

[SCHM03] Michael Schmidt: Angriffsmöglichkeiten bei Bluetooth, c’t 11/2003

[SHWO05] Yaniv Shaked and Avishai Wool, Cracking the Bluetooth PIN, Mai 2005, http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/

[SOBS06] Pierre Betouin, Version 0.6 des Bluetooth Stack Smasher, SecuObs.com, Februar 2006, http://www.secuobs.com/news/05022006-bluetooth10.shtml

[TRIFORG] Webseite der Trifinite Group, http://trifinite.org/

[WIME09] WiMedia Alliance: WiMedia Announces New Agreements with Bluetooth SIG and Wireless USB, Pressemitteilung, März 2009

[WOLL01] J. F. Wollert, Das Bluetooth-Handbuch, Franzis Verlag 2001

[ZOLL06] Thierry Zoller, Kevin Finistere, All your Bluetooth is belong to us, Vortrag und Demonstration auf dem 23. Chaos Communication Congress, Dezember 2006, http://www.nruns.com/_downloads/23C3-Berlin-Bluetooth-Hacking-Revisited-Thierry-Zoller.pdf

B.8 Abkürzungen

3GPP	3rd Generation Partnership Project
A2DP	Advanced Audio Distribution Profile
ACL	Asynchronous connection-less
ACO	Authenticated Cipher Offset
AFH	Adaptive Frequency Hopping
AMP	Alternate MAC/PHY
ASCII	American Standard Code for Information Interchange
AT	Attention (Befehlssatz für Modems)
AVRCP	Audio/Video Remote Control Profile
BD_ADDR	Bluetooth Device Address
BSI	Bundesamt für Sicherheit in der Informationstechnik
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
COF	Cipher Offset
CRC	Cyclic Redundancy Check
DPSK	Differential Phase Shift Keying, differenzielle Phasenmodulation
DQPSK	Differential Quad Phase Shift Keying, vierwertige differenzielle Phasenmodulation
DUN	Dial-up Network
ECDH	Elliptic Curve Diffie-Hellman
EDR	Enhanced Data Rate
eSCO	extended SCO
FHSS	Frequency Hopping Spread Spectrum
GAMP_LK	Generic AMP Link Key
GAP	Generic Access Profile
GFSK	Gaussian Frequency Shift Keying
HCI	Host Controller Interface
HID	Human Interface Device
HS	High Speed
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPsec	Internet Protocol Security
ISDN	Integrated Services Digital Network
ISM	Industrial, Scientific, Medical (2,4 GHz-Band)
ISO	International Organization for Standardization
IT	Information Technology
ITU-T	International Telecommunications Union, Telecommunication Standardisation Sector
L2CAP	Logical Link Control and Adaptation Protocol

LAN	Local Area Network
LK	Link Key
LMP	Link Manager Protocol
MAC	Medium Access Control
MB-OFDM	Multiband OFDM
NFC	Near Field Communication
OBEX	OBject EXchange protocol
OFDM	Orthogonal Frequency Division Multiplexing
OOB	Out of Band
PAL	Protocol Adaption Layer
PCM	Pulse Code Modulation
PIM	Personal Information Manager
PIN	Personal Identification Number
PMK	Pairwise Master Key
PPP	Point-to-Point Protocol
PTK	Pairwise Transient Key
RFCOMM	Radio Frequency Communication, Serial Cable Emulation Protocol based on ETSI TS 07.10
RS	Recommended Standard
SAP	SIM Access Profile
SCO	Synchronous Connection-Oriented
SDP	Service Discovery Protocol
SIG	(Bluetooth) Special Interest Group
SIM	Subscriber Identity Module
SMS	Short Message Service
SNAP	Subnetwork Access Protocol
SSP	Secure Simple Pairing
STK	SIM Application Toolkit
TCS	Telephony Control Protocol
TDD	Time Division Duplex
ULP	Ultra Low Power (Bluetooth)
USB	Universal Serial Bus
UWB	Ultra Wide Band
WPAN	Wireless Personal Area Network
WLAN	Wireless Local Area Network

B.9 Glossar

Achtwertige Phasenmodulation (8DPSK, Differential Phase Shift Keying)

Differenzielle Phasenmodulation, bei der drei Bits pro Symbol übertragen werden, mit einer resultierenden Datenrate von 3 Mbit/s

Adaptives Frequenzsprungverfahren (AFH)

Verfahren, das die von der Sprungsequenz abgedeckten Kanäle auf freie, d.h. ungestörte Frequenzen beschränkt

Ad-hoc-Netzwerke

Drahtloses Netz zwischen zwei oder mehr mobilen Endgeräten, das ohne feste Infrastruktur auskommt; insbesondere verwendet bei Bluetooth, um die spontane Koppelung von Mobiltelefonen z.B. mit Headsets zu ermöglichen

Anwendungsprofil

Definition von Untermengen der Bluetooth-Protokolle durch die Bluetooth SIG, um die Interoperabilität unterschiedlicher Geräte sicherzustellen, ohne dass in allen Geräten immer alle existierenden Protokolle implementiert sind, z.B. Serial Port Profile, Headset Profile

Asynchrone verbindungslose Übertragung (Asynchronous Connectionless Link, ACL)

Übertragung, bei der die Datenpakete gesendet werden, sobald ein Freiraum (Slot) besteht; jedes Paket enthält eine Zieladresse, anhand derer es an den Empfänger vermittelt wird

AT-Kommandos

Quasi-Standard für Befehle zum Konfigurieren von Modems und ähnlichen Geräten (AT steht für attention)

Authentisierung

Verifizierung der Identität einer Instanz, z.B. eines Benutzers oder eines Geräts. Zweck ist oft die anschließende Autorisierung für Zugriffe. Ohne Authentisierung ist im Allgemeinen keine sinnvolle Autorisierung möglich.

Binäre Frequenzmodulation (Gaussian Frequency Shift Keying, GFSK)

Zwingend von Bluetooth-Implementierungen unterstützte Frequenzmodulation, bei der ein Bit pro Symbol übertragen wird, mit einer resultierenden Datenrate „Basic Rate“ von 1 Mbit/s

Bluetooth Device Address

48 Bit lange öffentlich bekannte und weltweit eindeutige Geräteadresse

Bluetooth Special Interest Group (Bluetooth SIG)

Interessengemeinschaft zahlreicher Unternehmen, die an der Entwicklung und Verbreitung der Bluetooth-Technologie interessiert sind; 1998 von Ericsson, IBM, Intel, Nokia und Toshiba gegründet; 1999 erweitert durch 3Com, Lucent, Microsoft und Motorola; Eigentümer des Bluetooth-Warenzeichens und Herausgeber der Bluetooth-Spezifikation.

Challenge-Response-Verfahren

Sichere Authentisierung eines Endgeräts bei Kommunikationswunsch auf Basis von Wissen, welches beide Verbindungspartner besitzen (z.B. Passwort)

Channel-Hopping-Sequence

siehe Sprungsequenz

Chiffrat

Verschlüsselte Form der Nachricht

Codec

Es handelt sich um eine Wortkreuzung aus den englischen Begriffen „coder“ und „decoder“. Ein Codec bezeichnet ein Verfahren, mit dem analoge Informationen in digitale Informationen umgewandelt werden.

Cyclic Redundancy Check (CRC)

Der CRC beschreibt eine Prüfsumme über die zu übertragenden Daten, die in der Nachricht mitgeschickt wird und es dem Empfänger gestattet, Bitfehler, die auf dem Kommunikationskanal entstanden sind, zu erkennen.

Denial of Service (DoS)

Ein Angriff vom Typ Denial of Service hat zum Ziel, die Arbeitsfähigkeit des angegriffenen Objekts möglichst stark zu reduzieren. Dies beinhaltet beispielsweise die systematische Überlastung eines Netzknotens durch unsinnigen Verkehr (Dummy Traffic) oder die beabsichtigte Herbeiführung eines Fehlerzustands durch das Einspielen fehlerhafter Nachrichten.

Extended SCO

Synchrone Kanäle mit höherer Bandbreite, die eine Neuübertragung fehlerhaft empfangener Datenpakte erlaubt, um die Dienstqualität auch unter ungünstigen Empfangsverhältnissen zu verbessern

Frequenzmodulation

Modulationsverfahren, bei welchem die Trägerfrequenz durch das zu übertragende Signal beeinflusst wird

Frequenzspreizung

Verfahren in der drahtlosen Datenübertragung, bei dem ein schmalbandiges Signal in ein breitbandiges Signal umgewandelt wird; die Sendeenergie, die zuvor in einem kleinen Frequenzbereich konzentriert war, wird dabei auf einen größeren Frequenzbereich verteilt.

Frequenzsprungverfahren (FHSS)

Frequenzspreizverfahren, bei dem die verfügbare Bandbreite auf viele Kanäle aufgeteilt wird, die nacheinander in einer regelmäßigen zyklischen Sprungsequenz genutzt werden

Geräteschlüssel (Unit Keys)

Intern, bei der ersten Verwendung eines Bluetooth-Geräts erzeugter Schlüssel, der normalerweise nicht mehr geändert wird; kann als Link Key genutzt werden, wenn ein Gerät nicht genügend Speicherplatz für weitere Schlüssel besitzt oder einer großen Gruppe von Nutzern zugänglich sein soll.

Hold-Mode

Stromsparmodus bei Bluetooth-Geräten

Host Controller Interface (HCI)

Schnittstelle zwischen der auf einem Gerät installierten Treibersoftware und dem eigentlichen Bluetooth Controller. Diese Schnittstelle ist standardisiert, sodass Bluetooth Controller und Treiber prinzipiell austauschbar sind. Das HCI entscheidet auch über die Fähigkeiten des Bluetooth

Controller. So kann ein Betriebssystem, das Bluetooth 2.1 + EDR unterstützt, kein Secure Simple Pairing ausführen, wenn ein Bluetooth Controller mit einem „älteren“ HCI eingesetzt wird.

Initialisierungsschlüssel

Für die gesicherte Übertragung der Zufallszahlen für die Bluetooth-Paarung genutzter Schlüssel K_{init}, der sich lokal mittels einer kryptographischen Funktion aus einer öffentlichen Zufallszahl, der Geräteadresse eines Teilnehmers und einer im Allgemeinen konfigurierbaren PIN berechnet

ISM-Frequenzband

Lizenzfrei nutzbare Frequenzbänder, die für industrielle, wissenschaftliche und medizinische Zwecke verwendet werden können (ISM = Industrial, Scientific and Medical)

Just Works

Verfahren, das im Zusammenhang mit SSP bei der Kopplung von Bluetooth-Geräten angewandt wird, und bei dem keine Anwenderaktion erforderlich ist (funktioniert „einfach so“)

Kanalabstand

Frequenzunterschied zwischen zwei benachbarten Kanälen in einem Frequenzband. Innerhalb eines Frequenzbandes sind die Kanäle gleich breit.

Kombinationsschlüssel (Combination Key)

Nur für die Verbindung zweier Geräte genutzter, 128 Bit langer Schlüssel, der in jedem Gerät als Verbindungsschlüssel (Link Key, LK) gespeichert wird und in Abhängigkeit von den Geräteadressen und einer Zufallszahl pro Gerät erzeugt wird.

Kurznachrichtendienst (Short Message Service, SMS)

Ein Dienst, der den Austausch kurzer Textnachrichten erlaubt. Ursprünglich für den GSM-Mobilfunk entwickelt, z.T. jedoch auch im Festnetz nutzbar.

Man in the Middle

Der Angreifer positioniert sich zwischen zwei Kommunikationspartner und täuscht beiden Parteien vor, der jeweils erwartete eigentliche Partner zu sein. Dabei kann der Man in the Middle den Dialog zwischen den beiden Parteien belauschen oder auch verfälschen. Ziel ist oft die Ermittlung von Passwörtern.

Master-Schlüssel (Master Keys)

Temporäre Schlüssel für die Dauer einer Bluetooth-Sitzung, falls ein Master mehrere Geräte unter Verwendung desselben Verschlüsselungsschlüssels erreichen will

Modulationsverfahren

Verfahren bei der drahtlosen Übertragung, mit dem die zu übertragenden Daten mit Signalen hoher Frequenz gemischt – moduliert – werden, da nur diese von einem Sender mit großer Reichweite abgestrahlt werden können.

Numeric Comparison

Verfahren, das im Zusammenhang mit SSP bei der Kopplung von Bluetooth-Geräten angewandt wird, bei dem der Anwender zwei an den Geräten angezeigte Zahlenfolgen vergleicht

Out of Band

Kommunikation von Geräten auf einem zweiten, nicht für den normalen Datenaustausch verwendeten Kanal. Ein derartiges Verfahren wird im Zusammenhang mit SSP bei der Kopplung von Bluetooth-Geräten angewandt, um die Authentizität des Kommunikationspartners ohne Anwenderaktion sicherstellen zu können. Als zweiter Kanal kommt hier eine Nahfunktechnik (NFC) zum Einsatz.

Paarung (Pairing)

Verfahren zu Beginn einer Verbindung zur Kommunikationsabsicherung zweier Bluetooth-fähiger Geräte, insbesondere die Vereinbarung eines Verbindungsschlüssels

Pairwise Master Key, PMK

Geheimer Schlüssel, der im WLAN zur Generierung von Sitzungsschlüsseln verwendet wird

Pairwise Transient Key, PTK

Für eine WLAN-Verbindung verwendeter Sitzungsschlüssel mit begrenzter Gültigkeitsdauer, der beim Verbindungsaufbau mit Hilfe des PMK über ein Challenge-Response-Verfahren erzeugt wird.

Park-Mode

Stromsparmodus bei Bluetooth-Geräten

Passkey Entry

Verfahren, das im Zusammenhang mit SSP bei der Kopplung von Bluetooth-Geräten angewandt wird, bei dem der Anwender gleiche Zahlenfolgen in beide Geräte eingibt

Pulse Code Modulation (PCM)

Verfahren zur Übertragung analoger Signale in binärer Form. Das analoge Signal wird hierbei mit einer bestimmten Frequenz in zeitgleichen Abständen abgetastet und anschließend mit einem Analog-Digital-Wandler in einen Zahlenwert umgewandelt. Der Zahlenwert wird binär codiert und übertragen.

Piconet

Bluetooth-Netzwerk mit maximal acht ad-hoc verbundenen Endgeräten; auch PAN (Personal Area Network) genannt.

Personal Identification Number (PIN)

Konfigurierbare, auf beiden Geräten gleiche Identifikation zur Erzeugung eines Initialisierungsschlüssels

Phasenmodulation

Übertragungsverfahren für analoge oder digitale Signale. Bei der Übertragung von digitalen Signalen wird die Phase einer Sinusschwingung (Träger) durch Phasenverschiebung moduliert.

Scatternet

Gruppe von Piconets, die über gemeinsame Bluetooth-Geräte miteinander verbunden sind

Secure Simple Pairing (SSP)

Ein Verfahren zur Kopplung von Bluetooth-Geräten, das die Nachteile der Verwendung von PINs zu vermeiden sucht

SIM Application Toolkit (STK)

Zusatzfunktionen, die auf SIM-Karten der Mobiltelefonen implementiert sind und die dem SIM erlauben, selbsttätige Aktionen der Endgeräte zu initiieren

Sniff-Mode

Stromsparmodus bei Bluetooth-Geräten

Sprungsequenz

Regelmäßige Abfolge der Kanäle in einem Frequenzsprungverfahren

Stromchiffre

Symmetrische, kontinuierliche und verzögerungsfreie Ver- oder Entschlüsselung eines Datenstroms, bei der die Daten Bit für Bit bzw. Zeichen für Zeichen ver- oder entschlüsselt werden

Subnetwork Access Protocol (SNAP)

Das SNAP stellt ein Paketformat zur Verfügung, das es erlaubt,von IEEE nicht spezifizierte Protokolle und Datenformate in Netzen gemäß IEEE 802 zu übertragen. Prominentestes Beispiel ist die Übertragung von IP-Paketen, die auf einem alten Ethernet-Paketaufbau basieren, in WLAN. Auch das Versenden von Bluetooth-Daten in WLAN erfordert den Einsatz von SNAP.

Synchrone verbindungsorientierte Übertragung (SCO)

Übertragungsmodus, bei dem Datenpakete in einem festen Zeitraster zwischen Stationspaaren ausgetauscht werden; es entspricht der leitungsvermittelten Übertragung in einem Telefonnetz

Time Division Duplex (TDD)

Zeitversetzte, in kurze Sequenzen aufgeteilte Übertragung der Daten, bei der Sende- und Empfangskanal die gleiche Frequenz nutzen, jedoch zeitlich voneinander getrennt sind. Die Informationen werden mit Hilfe eines festgelegten Zeitgebers in kurzen Sequenzen zeitversetzt übertragen. Das Umschalten zwischen Sende- und Empfangsmodus geschieht so schnell, dass dem Nutzer die kurzzeitige Unterbrechung des Kanals nicht auffällt.

Verbindungsschlüssel (Link Key, LK)

Ein nur für die Verbindung zweier Geräte genutzter 128 Bit langer Kombinationsschlüssel (Combination Key), Geräteschlüssel (Unit Key) oder Master-Schlüssel (Master Key)

Vierwertige Phasenmodulation (Differential Quad Phase Shift Keying, π/4-DQPSK)

Differenzielle Phasenmodulation, bei der zwei Bits pro Symbol übertragen werden, mit einer resultierenden Datenrate von 2 Mbit/s

C. DECT

Inhaltsverzeichnis des Abschnitts

C.1 Grundlagen und Funktionalität

DECT war ursprünglich die Abkürzung für „Digital European Cordless Telephone“ und wurde Ende der 80er-Jahre als europaweit einheitlicher Standard konzipiert, der die bis dahin vorhandenen verschiedenen schnurlosen Telefonsysteme (Cordless Telephone, CT), z.B. CT1, CT1+, CT2, ersetzen sollte. Seit dem 31. Dezember 2008 ist die Betriebserlaubnis für Systeme nach den Standards CT1+ und CT2 erloschen. Für CT1 gilt dies bereits seit dem 1. Januar 1998. Heute steht DECT für „Digital Enhanced Cordless Telecommunications“, einen 1992 verabschiedeten Standard des European Telecommunications Standards Institute (ETSI) [EN300175]. In den USA und in Kanada wird diese Technik unter dem Begriff „DECT 6.0“ in einem anderen Frequenzspektrum vermarktet.

Der DECT-Standard spezifiziert ein vollständig digitales Mobilfunknetz zur Übertragung von Sprache und Daten, das sich im Vergleich zu analogen Schnurlostelefon-Standards durch eine hohe Sprachqualität und Optionen für eine höhere Abhörsicherheit auszeichnet. Seit Ende 2006 steht mit CAT-iq eine Erweiterung des DECT-Standards zur Verfügung, die unter anderem eine verbesserte Sprachqualität, die Vereinigung von DECT und dem Internet sowie eine verbesserte Interoperabilität beinhaltet.

Als typische Einsatzorte von DECT sind in erster Linie Bürogebäude und Firmengelände sowie Heimbereiche zu nennen. Eine Verwendung als WLL-Technik (Wireless Local Loop) zur Überbrückung der letzten Meile zwischen einem Netzbetreiber und Kunden ist ebenfalls möglich, hat sich aber nicht durchsetzen können. Dagegen steht heute in sehr vielen Haushalten und Büroumgebungen ein DECT-Telefon. Hinzu kommen Systeme, in denen DECT zur Funkübertragung genutzt wird, wie beispielsweise Alarmanlagen, Kreditkarten- bzw. EC-Bezahlsysteme, Verkehrsleitsysteme oder Anwendungen im Bereich der Heimelektronik.

Im Folgenden werden Architektur, Protokolle und Sicherheitsmechanismen von DECT und dem darauf aufbauenden CAT-iq vorgestellt, mögliche Sicherheitslücken untersucht und entsprechende Sicherheitsmaßnahmen empfohlen.

C.1.1 Architektur

Mit DECT-Systemen können komplette schnurlose Nebenstellenanlagen aufgebaut werden. Neben den normalen Telekommunikationsverbindungen über einen Amtsanschluss an ein öffentliches Telefonnetz (Public Switched Telephone Network, PSTN) können dann interne Kommunikationsverbindungen zwischen mehreren mobilen Endgeräten gebührenfrei über die DECT-Basisstation aufgebaut werden.

Bei einem schnurlosen Telefon für den Heimbereich, der am häufigsten anzutreffenden DECT-Anwendung, besteht das DECT-System aus einer Feststation, dem sogenannten Fixed Part (FP), und einem oder mehreren Mobilstationen, den sogenannten Portable Parts (PP).

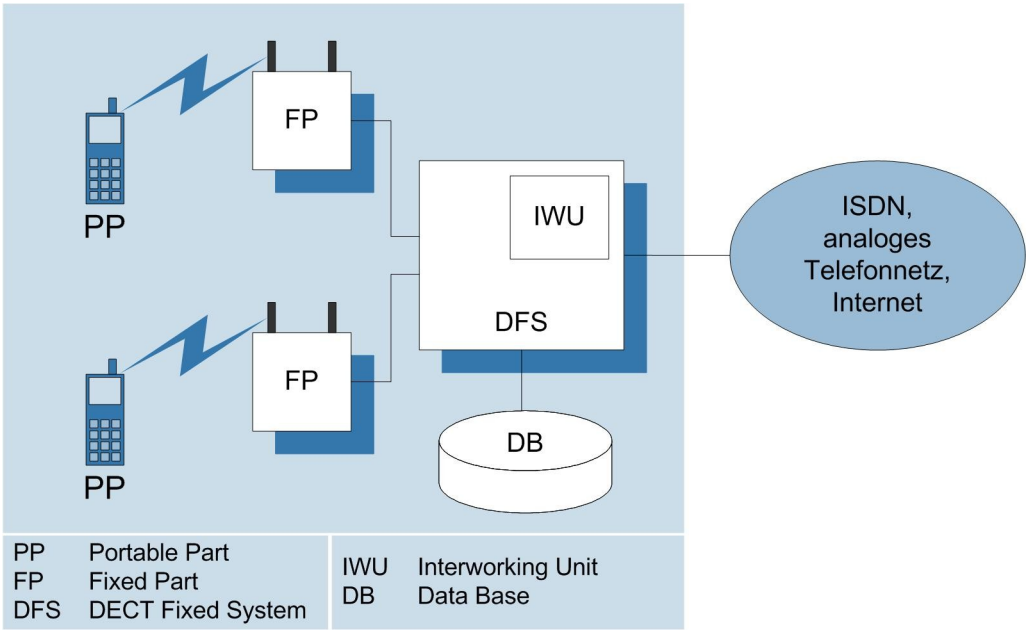
Eine noch einfachere Systemkonfiguration ist der Direkt-Modus, bei dem zwei DECT-Endgeräte (PP) direkt miteinander kommunizieren. Im Direkt-Modus lässt sich z.B. fern von jeder DECT-Infrastruktur eine Datenfunkverbindung zwischen zwei mit Datenfunkmodulen ausgestatteten Laptops oder eine Walkie-Talkie-Verbindung zwischen zwei Sprachtelefonie-PPs realisieren.

DECT ist multizellenfähig und unterstützt Verfahren wie Roaming[1] und Handover[2]. Bei Mehrzellen-Systemen besteht ein DECT-Netz aus mehreren FPs, die an eine zentrale Vermittlungskomponente (DECT Fixed System, DFS) angeschlossen sind. Der abgedeckte Bereich kann durch überlappende Funkzellen flächendeckend versorgt werden. Das DFS verfügt hierzu über eine Datenbank zur Nutzer- bzw. Endgeräte-Verwaltung. Für den Anschluss an ein externes Telefonnetz gibt es im DFS eine sogenannte Interworking Unit (IWU), die für die Anpassung der DECT-spezifischen Protokolle an die Protokolle des analogen Telefonnetzes bzw. des ISDN (Integrated Services Digital Network) sorgt. Das DFS ist an eine Telekommunikationsanlage (TK-Anlage) angeschlossen (siehe Abbildung C-1) oder als Modul einer TK-Anlage realisiert. Zur Versorgung eines größeren Areals können mehrere DFSs und ggf. auch TK-Anlagen eingesetzt und zu einem größeren Netz verbunden werden.

In einem kleinen DECT-System bestehend aus einem einzelnen FP (wie im Heimbereich üblich) werden die Funktionen des DFS im FP realisiert.

Zur Erweiterung eines DECT-Systems können auch sogenannte Wireless Relay Stations (WRS), auch Relais oder Repeater genannt, eingesetzt werden. Repeater sind sowohl in Indoor- als auch Outdoor-Ausführungen erhältlich und können die Reichweite eines DECT-Systems bis zu ca. 1 km (Indoor) respektive ca. 15 km (Outdoor) erhöhen. Die Kommunikation zwischen FP und PP erfolgt über die Luftschnittstelle, wobei auch eine Kaskade von Repeater möglich ist (siehe Abbildung C-2). Die Nutzung eines Repeater setzt die Aktivierung des Repeater-Modus des FP voraus. Damit verbunden ist in der Regel eine automatische Deaktivierung der Verschlüsselung!

Abbildung C-1: Vereinfachter Aufbau eines DECT-Systems



Mit einem PP bleibt ein Teilnehmer im gesamten Abdeckungsbereich des DECT-Netzes (z.B. einem Gebäude oder sogar auf einem größeren Gelände) unter seiner gewohnten Rufnummer erreichbar.

Damit ein problemloses Zusammenspiel von PPs verschiedener Hersteller gewährleistet ist, gibt es das Generic Access Profile (GAP), das in [EN300444] spezifiziert ist und Minimalanforderungen für Fernsprechdienste festlegt. Sogenannte Interworking Profiles definieren die Schnittstellen zu anderen Netzen (z.B. ISDN). Weiterhin können auch schnurlose Datennetze mit entsprechenden Geräten auf

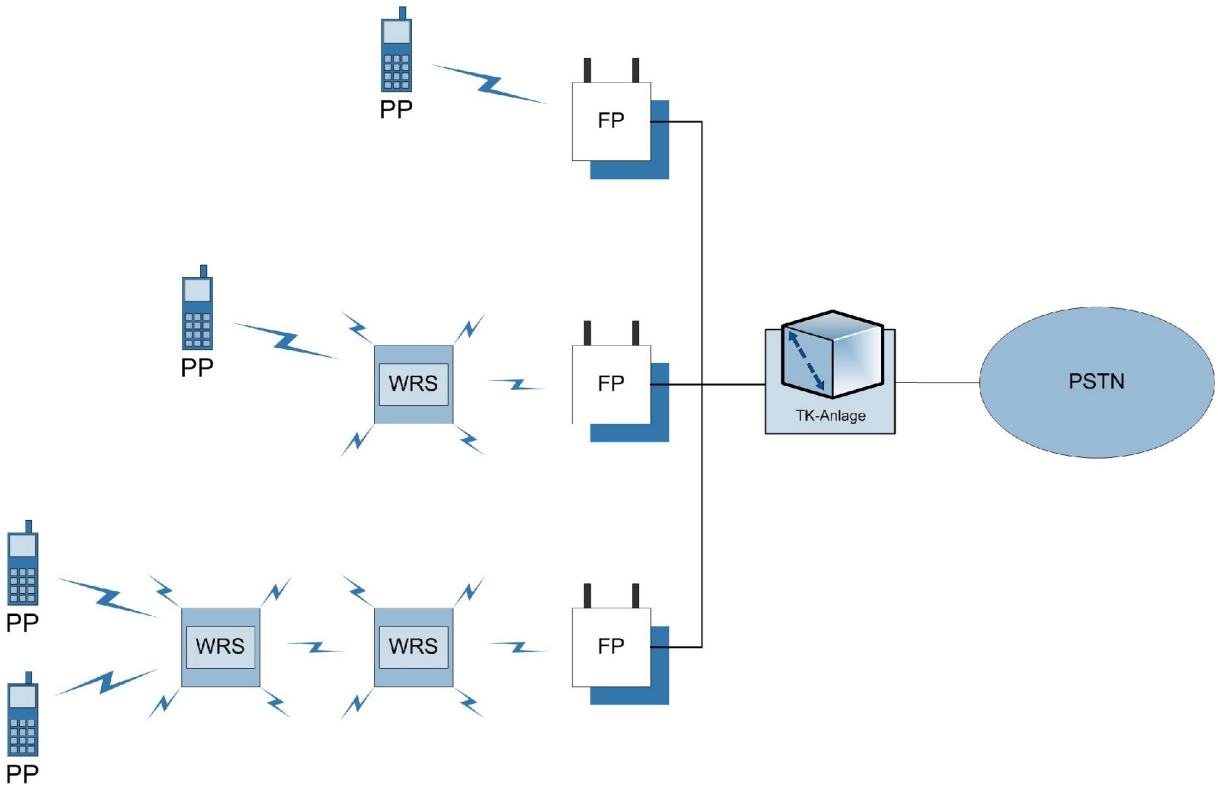
1 Wechsel eines PP zwischen verschiedenen DECT-Netzen

2 Wechsel eines PP zwischen zwei benachbarten Funkzellen (d.h. den durch FPs versorgten Bereichen) unter Aufrechterhaltung der Ende-zu-Ende-Verbindung

DECT-Basis aufgebaut werden. In sogenannten Application Profiles sind Kommunikationsdienste für spezielle Anwendungen spezifiziert.

Der DECT Packet Radio Service (DPRS, [EN301649]) und das DECT Multimedia Access Profile (DMAP, [EN301650]) ermöglichen beispielsweise eine Datenkommunikation mit höheren Datenraten (vergleichbar z.B. mit denen von Bluetooth). Mit einem Datenfunkmodul als PP lässt sich damit über einen entsprechend ausgestatteten FP beispielsweise auch ein drahtloser DECT-basierter Internet-Zugang realisieren. Ebenso ist die Kommunikation mit weiteren Datenfunkmodulen möglich. Auf diese Weise ist ein Datenaustausch zwischen PCs über DECT-Datenfunkverbindungen ebenfalls realisierbar.

Abbildung C-2: DECT-Aufbau mit Repeater und Integration einer TK-Anlage

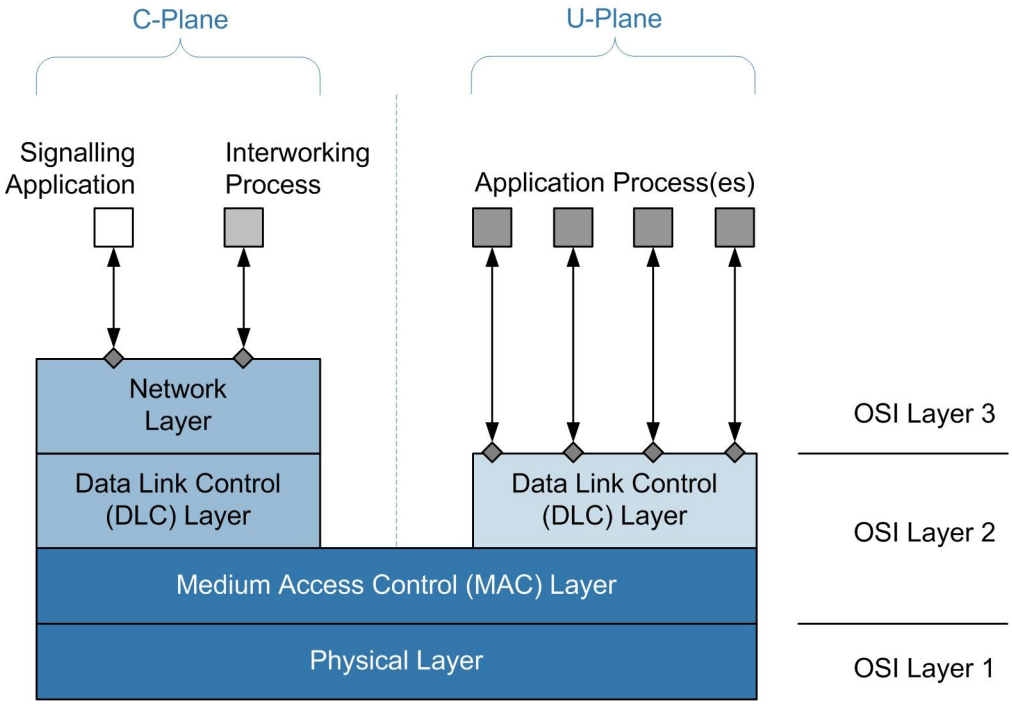


C.1.2 Funkschnittstelle

Die Übertragung auf der Funkschnittstelle geschieht ähnlich zu anderen Telekommunikationssystemen (z.B. ISDN) über zwei getrennte Protokoll-Stacks: einen für die Übertragung der Nutzer- bzw. Applikationsdaten (z.B. Sprache) und einen für die hierzu nötigen Signalisierungsdaten. Der Protokoll-Stack für die Nutzerdaten wird als U-Plane bezeichnet, der für die Signalisierungsdaten als C-Plane[3]. Beide Protokoll-Stacks setzen auf einer gemeinsamen Kanalzugriffsebene (Medium Access Control, MAC) auf. Die Signalisierungsdaten beinhalten für den Austausch von Applikationsdaten Kontrollinformationen für Aufbau, Aufrechterhaltung und Abbau einer Verbindung. Abbildung C-3 zeigt die vereinfachte Protokollarchitektur im Überblick (siehe auch [EN300175]).

3 U = User, C = Control

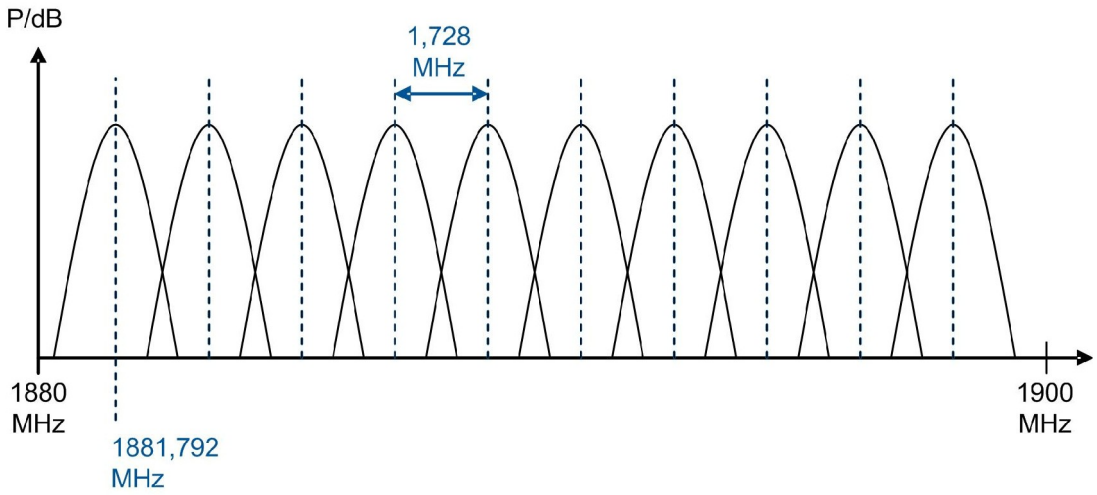
Abbildung C-3: : Protokolle auf der Luftschnittstelle (vereinfacht)



C.1.2.1 Physikalische Übertragung und Kanalzugriff

DECT arbeitet in Europa im explizit reservierten Frequenzband zwischen 1880 MHz und 1900 MHz. Es stehen 10 Trägerfrequenzen im Abstand von 1,728 MHz (Frequency Division Multiplex, FDM), wie in Abbildung C-4 gezeigt, zur Verfügung[4].

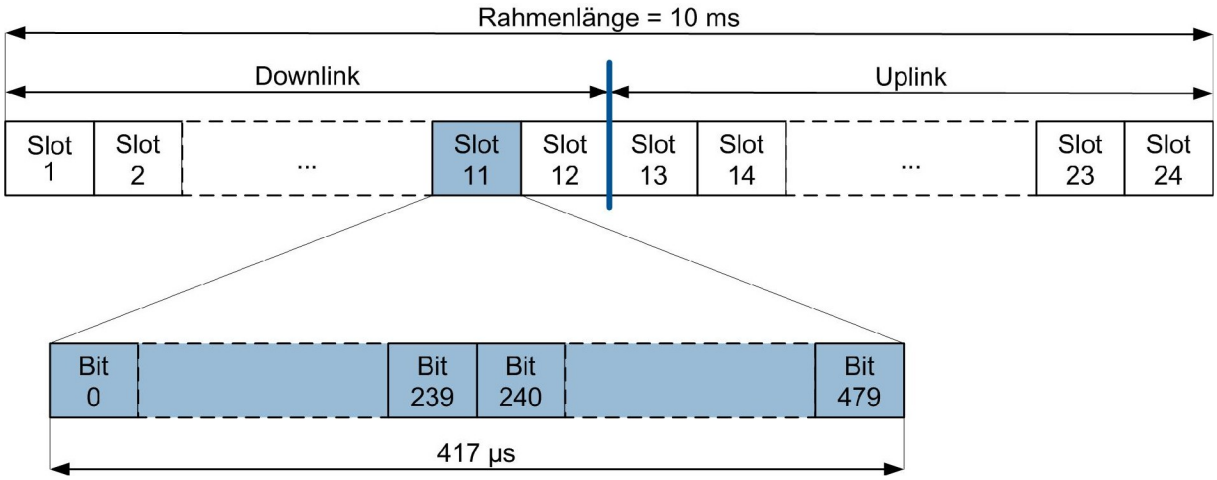
Abbildung C-4: Trägerfrequenzen



[4] Die Trägerfrequenzen f berechnen sich wie folgt: $f = (1881{,}792 + k*1{,}728)$ MHz, für $k = 0, ..., 9$

Jeder Träger ist durch Zeitschlitze (Slots) in 24 Kanäle eingeteilt (Time Division Multiple Access, TDMA). Ein solcher aus 24 Slots bestehender Rahmen (Frame) ist 10 ms lang und wiederholt sich periodisch alle 10 ms. Der Duplexbetrieb erfolgt mittels Time Division Duplex (TDD). Dabei werden die ersten 12 Slots eines Rahmens im Downlink, d.h. in der Übertragungsrichtung vom FP zu den PPs, verwendet. Die zweiten 12 Slots bilden den Uplink, d.h. die Übertragungsrichtung von den PPs zum FP. Somit ergeben sich pro Träger 12 Duplexkanäle; auf den 10 Trägerfrequenzen stehen also insgesamt 120 Duplexkanäle zur Verfügung (siehe Abbildung C-5). Ein für den DECT-Nutzer aufgebauter bidirektionaler Kommunikationskanal zwischen FP und PP belegt immer zwei Slots[5]. Neben dem hier beschriebenen Slot, dem sogenannten Full Slot, existieren weitere Slot-Formate (z.B. Half Slot, Double Slot) die sich in der Länge und damit auch der Übertragungsrate unterscheiden. Insbesondere bei CAT-iq ist ein neues variables Slot-Format (Long Slot) anzutreffen.

Abbildung C-5: Zeitmultiplex

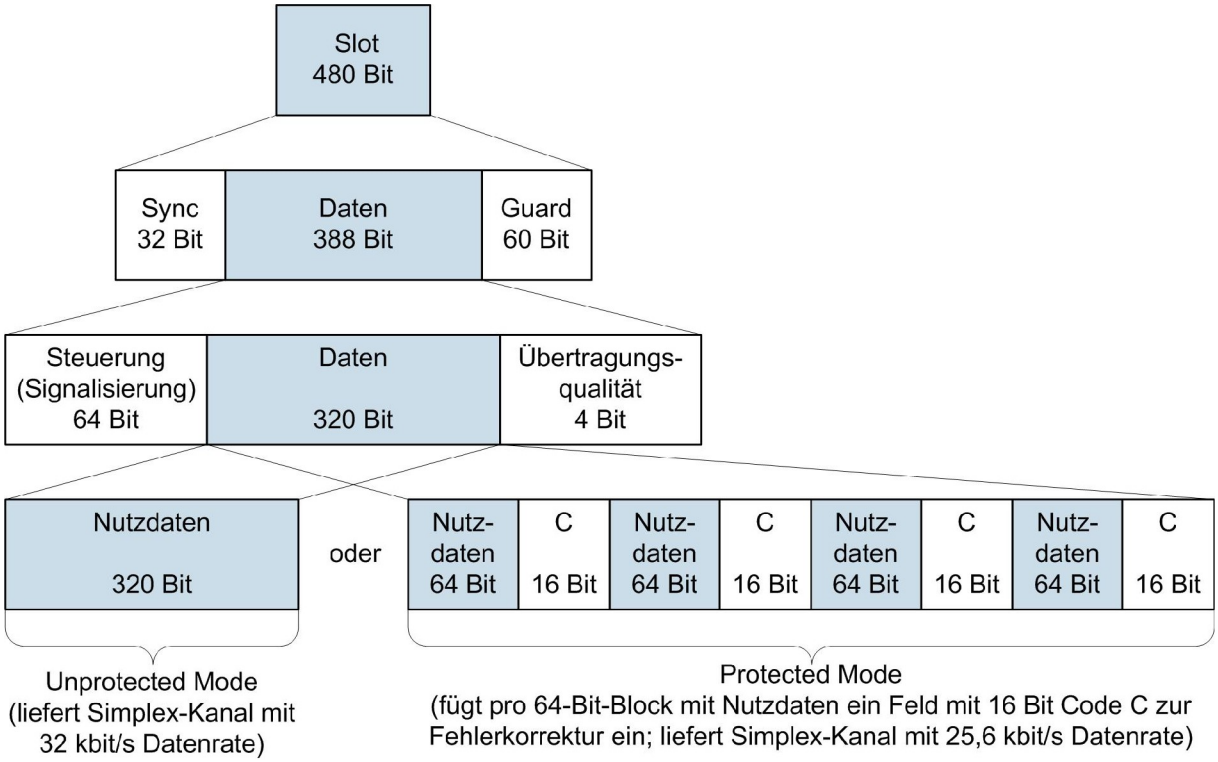


Zur Modulation wird bei DECT GMSK (Gaussian Minimum Shift Keying) verwendet. Mit dieser Modulationsart erreicht man hier eine maximale modulierte Gesamtbitrate von 1152 kbit/s auf jeder Trägerfrequenz. Jedes physikalische Datenpaket transportiert sowohl Signalisierungs- als auch Nutzdaten. Die Nutzdatenrate liegt bei maximal 32 kbit/s pro Kanal (Unprotected Mode). Um die Datenübertragung gegen Bitfehler zu schützen, können die Nutzdaten in Gruppen zu je 80 Bit aufgeteilt werden. Davon werden dann 64 Bit zur Datenübertragung und 16 Bit zur Fehlerkorrektur verwendet (Protected Mode). In diesem Fall sind pro Kanal effektiv 25,6 kbit/s möglich (siehe Abbildung C-6). Im DECT-Standard sind verschiedene Übertragungsmodi spezifiziert, mit denen sich eine Vielzahl elementarer Kanäle (sogenannte MAC-Bearer) aufbauen lassen, die sich bezüglich der Datenraten und Fehlerschutzmechanismen unterscheiden. MAC-Bearer lassen sich zum Erreichen höherer Datenraten auch kombinieren.

Die maximale Sendeleistung beträgt 250 mW (bei mittlerer Sendeleistung von 10 mW), womit sich abhängig von den Funkausbreitungsbedingungen eine Reichweite (maximale Entfernung zwischen Basis- und Mobilstation) von bis zu 300 m im Freien und bis zu 50 m in Gebäuden ergibt. Mit Hilfe von Richtantennen lässt sich die Reichweite auf bis zu 5 km erhöhen, solche Lösungen sind z.B. für stationäre WLL-Systeme praktikabel.

5 Bei der Verwendung einer WRS muss berücksichtigt werden, dass sich eine WRS einem FP gegenüber als PP verhält. Eine WRS sendet dann die so empfangenen Pakete in einem anderen Zeitschlitzpaar an einen PP weiter. Für jedes über eine WRS geführte Gespräch müssen somit insgesamt vier Zeitschlitze belegt werden.

Abbildung C-6: Format der Daten in einem Slot



In diesem Zusammenhang existieren seit einigen Jahren Produkte, welche mit speziellen Funktionen zur Strahlungsreduzierung werben. Der Schwerpunkt liegt hierbei auf einer vorsorglichen Reduzierung der Strahlung unter gesundheitlichen Aspekten, wie es beispielsweise das Bundesamt für Strahlenschutz (BfS) fordert[6]. Weiterhin können diese Funktionen dazu beitragen, die Ausbreitung der Funkwellen und somit auch die Wahrscheinlichkeit reduzieren, erkannt und belauscht zu werden.

Begriffe wie ECO-DECT, Low Radiation (LR), (Voll-)ECO-Modus oder ECO-Modus-Plus werden hierbei genannt, wobei generell zwischen verschiedenen Funktionalitäten unterschieden werden muss:

- Abschaltung des Bakensignals der Basisstation: Hierbei wird das regelmäßige Bakensignal[7] deaktiviert und es kommt zu einer vollständigen Reduzierung der Sendeleistung im Standby-Betrieb. Diese Funktion muss sowohl von der Basisstation als auch von der Mobilstation unterstützt werden, gilt jedoch auch für mehrere angemeldete Mobilstationen und auch außerhalb der Ladestationen. Basis- und Mobilstation wiederum müssen hierbei kontinuierlich die Zeitschlitze eines vorher festgelegten Kanals auf Aktivität scannen. Das kontinuierliche Scannen verbraucht, im Vergleich zum Betrieb mit Bakensignal, mehr Akku-Kapazität, sodass die Standby-Zeit der Mobilstation in der Regel geringer ausfällt als bei einem Betrieb mit Bakensignal. Diese Funktionalität wird z.T. auch unter dem Begriff ECO-Modus-Plus (bzw. ECO Mode Plus) oder Voll-ECO-Modus geführt.

- Reduzierung der Sendeleistung der Basisstation: Hierbei findet eine automatische Reduzierung (z.T. auf unter 1%) der Sendeleistung der Basisstation statt, sofern sich die Mobilstation in der Ladevorrichtung der Basisstation befindet. Für separate Ladestationen (vorwiegend bei IP-kompatiblen Basisstationen) gilt dies in der Regel nicht. Weiterhin tritt dies generell nur in Kraft, wenn keine zusätzlichen Mobilstationen an der Basisstation angemeldet sind. Es gibt Hersteller, welche zusätzlich die Möglichkeit bieten, die Sendeleistung der Basisstation manuell um bis zu

6 http://www.bfs.de/de/elektro/Strahlungsarme_Dect_Schnurlostelefone.html

7 Ein Bakensignal wird von einer Basisstation als regelmäßige Anwesenheitsmeldung ausgesendet.

80% zu reduzieren. Hiervon sind entsprechend alle Mobilstationen betroffen. Die Reichweite der Basistation wird in diesem Fall um ca. die Hälfte reduziert, auf 150 m im Freien und 25 m in Gebäuden. Sowohl die automatische Reduzierung der Sendeleistung für eine Mobilstation (in der Ladevorrichtung der Basisstation) als auch die manuelle Reduzierung der Sendeleistung der Basisstation sind häufig unter dem Begriff ECO-Modus (bzw. ECO Mode) anzutreffen.

- Bedarfsgerechte Anpassung der Sendeleistung der Mobilstation: Die bedarfsgerechte Regelung der Sendeleistung betrifft hierbei allein die Mobilstation. Der Reduktionsfaktor kann je nach Entfernung (i.d.R. kleiner als 25 m) zwischen 60% und 90% liegen. Grundsätzlich gilt diese Anpassung der Sendeleistung nur für den Standby-Betrieb, d.h. nicht während eines Gespräches.

Viele Hersteller vereinen diese Funktionen oder Teile davon unter einem gemeinsamen Begriff wie beispielsweise ECO-DECT oder Low Radiation (LR) DECT. Energiesparende Netzteile oder umweltverträgliche Materialien können weitere Kriterien für diese Bezeichnung sein.

Die Begrifflichkeiten sind nicht standardisiert, sodass es hier zu Unterschieden zwischen Herstellern kommen kann. Auch innerhalb der Produktlinie eines Herstellers können sich hinter einem „ECO-Begriff“ unterschiedliche Merkmale verbergen, sodass im Zweifel der Hersteller konsultiert werden sollte. Mit CAT-iq soll dieser Zustand behoben werden, indem eine standardisierte Funktion zur Reduzierung der Sendeleistung der Basisstation in die CAT-iq-Spezifikation aufgenommen werden soll. Derzeit wird diese Funktion unter dem Namen Adapted Power Control geführt.

C.1.2.2 Höhere Protokollschichten

Oberhalb der MAC-Schicht ist in der DECT-Protokollarchitektur (siehe Abbildung C-3) eine Sicherungsschicht (Data Link Control, DLC) vorgesehen, die die Aufgabe hat, Daten aus höheren Schichten aufzubereiten, sodass sie mit der jeweils geforderten Qualität (Bitfehlerrate, Verzögerung usw.) über die MAC-Bearer übertragen werden können. Oberhalb der DLC-Schicht liegt die Netzwerk-Schicht, welche für Verbindungsaufbau- und -abbau sowie für das Mobilitäts-Management zuständig ist; darüber liegen die Anwendungsschichten.

C.1.2.3 Übertragung der Nutzdaten

Die Übertragung der Nutzdaten erfolgt bei DECT mit einer Datenrate von 32 kbit/s (Unprotected Mode) respektive 25,6 kbit/s (Protected Mode) pro Kanal, wie in Kapitel C.1.2.1 dargestellt.

Zur Erzielung höherer Datenraten können mehrere Kanäle gebündelt werden. Die Duplexverbindungen können auch asymmetrisch ausgelegt sein, sodass für Hin- und Rückrichtung unterschiedliche Datenraten möglich sind. Durch DMAP [EN301650] wird der DECT-Standard diesbezüglich um zusätzliche Möglichkeiten erweitert.

Sprachdaten werden in DECT mittels Adaptive Differential Pulse Code Modulation (ADPCM) kodiert und mit einer Datenrate von 32 kbit/s übertragen.

C.1.3 Verbindungsaufbau

Jeder FP[8] sendet auf einem Kanal regelmäßig Bakensignale in Form der 40 Bit langen RFPI (Radio Fixed Part Identity) aus. Die in der Funkzelle befindlichen PPs können diese RFPI dekodieren und können so die in ihrer Reichweite befindlichen FPs identifizieren. In den PPs sind Informationen über

[8] Streng genommen ist es der sogenannte Radio Fixed Part (RFP), der diese Funktion ausführt. Eine detailgenaue Aufschlüsselung des DECT-Systemaufbaus würde jedoch den Rahmen dieser Broschüre sprengen.

die jeweiligen Zugriffsrechte, sogenannte PARKs (Portable Access Rights Keys), abgespeichert. Die Zugriffsrechte werden während einer Subscription (siehe Kapitel C.2.6) vereinbart.

Nach Einschalten synchronisiert sich ein PP auf die in der Umgebung vorhandenen FPs auf, misst die jeweiligen Empfangspegel und dekodiert die Systeminformationen. Mit diesen Informationen wählt der PP aus den FPs, zu denen er Zugriffsrechte hat, den FP mit dem stärksten Empfangspegel aus und geht in Bereitschaft, in der ausgewählten Zelle Paging-Meldungen[9] zu empfangen und eine Verbindung aufzubauen. Bei Veränderung der Empfangsbedingungen findet erneut eine Zellauswahl statt.

Beim Einbuchen eines PP in einer Funkzelle erhält der PP vom FP eine eindeutige temporäre Kennung, die 20 Bit lange TPUI (Temporary User Identity). Mit dieser TPUI wird der PP bei einem ankommenden Anruf ausgerufen (Paging).

Ein Verbindungswunsch wird sowohl durch abgehende Anrufe als auch durch die Bereitschaft, einen eingehenden Anruf anzunehmen, ausgelöst. Eingehende Anrufe werden zuvor mittels Funkruf vom FP signalisiert. Für einen Verbindungsaufbau muss der PP geeignete Funkkanäle auswählen. Hierfür führt er auf allen verfügbaren Kanälen Empfangspegelmessungen durch und wählt die empfangsstärksten aus. Während einer laufenden Verbindung führt der PP weiterhin Pegelmessungen durch, um aus allen zur Verfügung stehenden Kanälen stets den nicht belegten mit der geringsten Störung auswählen zu können (dynamisches Kanalwahlverfahren). Die Entscheidung über den zu verwendenden Kanal trifft stets der PP. Das gleiche gilt übrigens auch für die Entscheidung über einen Handover bei Mehrzellenbetrieb. Der FP passt sich der vom PP gewählten Frequenz und dem gewählten Zeitschlitz an, weshalb für die Feststationen keine Frequenzplanung erforderlich ist.

C.1.4 Konvergenz von DECT und IP

Im Rahmen der Konvergenz von Sprache und Daten auf Basis einer einheitlichen paketvermittelnden Infrastruktur (Next Generation Network, NGN) und der weiter fortschreitenden Nutzung von Voice over IP (VoIP) ist generell die Frage von Interesse, wie drahtlose Techniken diesem Integrations- und Vereinheitlichungsprozess folgen können. Die Nutzung von Voice over WLAN (VoWLAN), also die Übertragung von VoIP über WLAN, oder die Nutzung von Mobilfunktechnik können heute bereits Alternativen zu DECT darstellen.

Mit CAT-iq steht eine Erweiterung des DECT-Standards zur Verfügung, die u.a. die Vereinigung von DECT und Breitband-Techniken zum Ziel hat.

C.1.5 CAT-iq (New Generation DECT)

CAT-iq (Cordless Advanced Technology – internet and quality) wurde Ende 2006 der Öffentlichkeit vorgestellt und ist neben DECT und DECT 6.0 eine weitere Entwicklung des Industrieverbandes DECT-Forum in Kooperation mit dem ETSI sowie der Home Gateway Initiative (HGI). Die Ziele von CAT-iq liegen insbesondere in einer verbesserten Sprachqualität, der Verknüpfung von Internet und Schnurlostelefonie sowie der Interoperabilität. Dazu zählen beispielsweise:

- Nutzung von Internet-Telefonie und Breitband-Codecs

[9] Wenn in einem Mobilfunknetz ein Ruf zu einem mobilen Teilnehmer vermittelt werden soll, muss das Mobilfunknetz zunächst die Funkzelle ermitteln, in der sich der Teilnehmer aktuell aufhält. Hierzu schickt das Mobilfunknetz in den Funkzellen, in denen es den Teilnehmer vermutet, spezielle Nachrichten aus, die den Teilnehmer auffordern sich zu melden. Erst wenn dies geschehen ist, kann der Ruf zum Teilnehmer durchgestellt werden. Dieser Prozess des Teilnehmerausrufs mit der Bitte sich zu melden wird allgemein als Paging bezeichnet.

- Nutzung von Internet-Applikationen, z.B. E-Mail, Instant Messaging, RSS-Feeds (Really Simple Syndication)
- Streaming von Audio-Daten (z.B. Internet-Radio)

Die Zielgruppe von CAT-iq sind primär Heimanwender und kleine Büroumgebungen.

CAT-iq basiert auf dem DECT-Standard und wird durch das ETSI unter der Bezeichnung „New Generation DECT (NG DECT)“ standardisiert. Aufgrund der gemeinsamen Basis „DECT“ ist CAT-iq abwärtskompatibel zu DECT (GAP) und nutzt daher das gleiche Frequenzspektrum, d.h. in Europa den Bereich 1880 bis 1900 MHz. Die zusätzlichen Funktionen stehen nur CAT-iq-kompatiblen Endgeräten zur Verfügung. Die Kompatibilität soll anhand von spezifizierten Testfällen des ETSI im Rahmen des Zertifizierungsprogramms „CAT-iq“ des DECT-Forums gewährleistet werden.

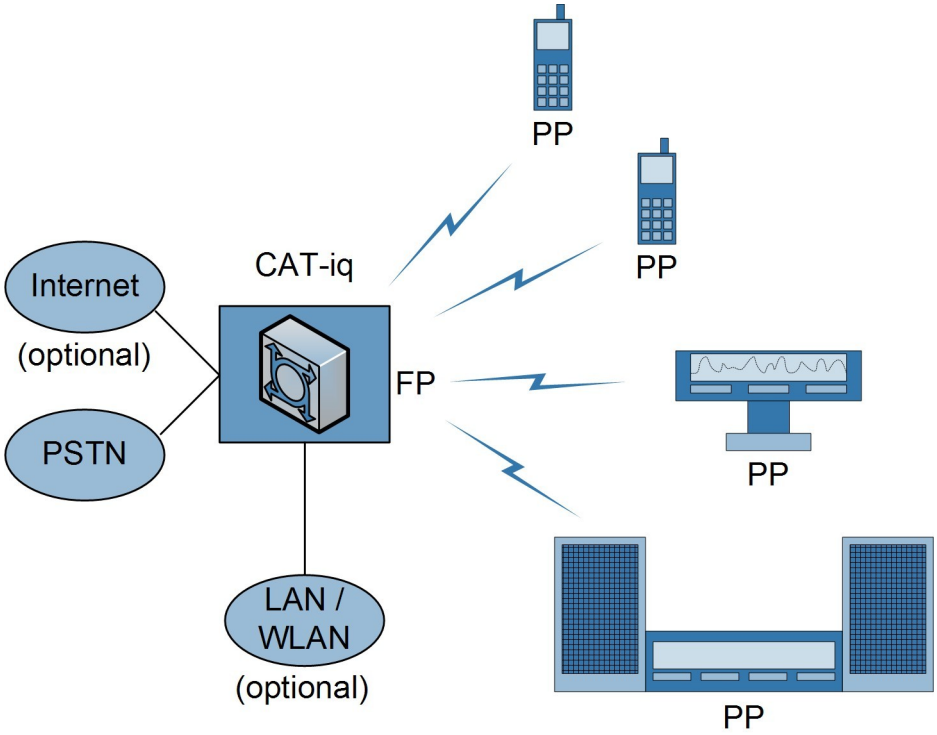
Einen Überblick der relevanten Standards findet man in [TR102570], während die jeweiligen CAT-iq-Funktionen in den Dokumenten ETSI TR 102 527 Teil 1 – 4 definiert sind; aktuell sind nur Teil 1 [TR1025271] und Teil 2 [TR1025272] verabschiedet, Teil 3 und 4 befinden sich noch im Draft-Status. Weiterhin wurden die bestehenden DECT-Standards angepasst und um CAT-iq-relevante Teile ergänzt. Eine Verabschiedung der aktualisierten ETSI-Serie EN 300 175 ist für Ende 2009 geplant.

Da CAT-iq auf dem DECT-Standard basiert, werden in den nachfolgenden Kapiteln nur die grundlegenden Änderungen zwischen DECT und CAT-iq vorgestellt. Sicherheitsmechanismen, mögliche Gefährdungen und Sicherheitsmaßnahmen werden gemeinsam in den Kapiteln C.2, C.3 und C.4 thematisiert.

C.1.5.1 Architektur

Die prinzipielle Architektur von CAT-iq entspricht der von DECT, d.h. ein CAT-iq-System besteht weiterhin aus einer Feststation, dem Fixed Part (FP), und einem oder mehreren Mobilstationen, den sogenannten Portable Parts (PP). Aufgrund der Abwärtskompatibilität können bestehende DECT-Mobilstationen weiterhin an einem CAT-iq-System betrieben werden. Dies bezieht sich auf Mobilstationen, welche GAP (siehe [EN300444]) unterstützen. Die Nutzung der CAT-iq-Funktionen erfordert jedoch neue Komponenten, die sich von bisherigen teilweise unterscheiden.

Abbildung C-7: Übersicht eines CAT-iq-Szenarios



Der FP eines CAT-iq-Systems ist häufig integriert in ein generisches Gateway bzw. einen Router, der auch für für die Internet-, PSTN-, LAN- und WLAN-Anbindung zuständig sein kann (siehe Abbildung C-7). Bei den CAT-iq-Mobilstationen sind neben Telefonen neue Produkte im Bereich der Unterhaltungselektronik möglich, wie z.B. Internet-Radios bzw. generell Multimedia-Systeme. Auch Systeme aus dem Bereich der Haustechnik wie Lichtsteuerung, Gegensprechanlage oder Alarmanlage können per CAT-iq betrieben werden.

Die Zuordnung der für den Betrieb erforderlichen Funktionen auf die jeweilige Gerätekategorie erfolgt über unterschiedliche CAT-iq-Profile bzw. Versionen. Derzeit sind für CAT-iq die folgenden Versionen vorgesehen:

- CAT-iq 1.0 „HD Sound“

  Diese Version ermöglicht eine verbesserte Sprachqualität im Vergleich zu DECT durch die Verwendung von Breitband-Codecs. Weitere Inhalte dieser Version sind die Kompatibilität zu GAP-Mobilstationen und grundlegende Telefonie-Leistungsmerkmale wie z.B. die Rufnummernanzeige (CLIP). CAT-iq 1.0 wird z.T. auch noch mit vb-Profil[10] bezeichnet. Produkte nach CAT-iq 1.0 sind bereits verfügbar.

- CAT-iq 2.0 „Multi-Line“

  Aufbauend auf CAT-iq 1.0 werden in dieser Version zusätzliche Leistungsmerkmale, Verbesserungen der Sprachqualität und zusätzliche Funktionen wie z.B. „Easy Pairing“ bereitgestellt. CAT-iq 2.0 wird z.T. auch noch mit ve-Profil[11] bezeichnet. Eine überarbeitete Version CAT-iq 2.1 soll je nach Marktsituation geringfügige Anpassungen enthalten, z.B. Funktionen zur Steuerung eines Anrufbeantworters. Derzeit befinden sich Produkte nach CAT-iq 2.0 in der Entwicklung.

10 "vb" steht für "Wideband voice with Basic interoperability".

11 "ve" steht für "Wideband voice with Extended interoperability".

- CAT-iq 3.0 „Internet Ready“

  Diese Version beinhaltet die Unterstützung für den Transport von IP-Paketen auf Basis von DPRS (siehe [EN301649]) und wird beispielsweise für Geräte benötigt, die einen direkten Zugang zum Internet erfordern. Hierzu gehören beispielsweise CAT-iq-kompatible Internet-Radios.

  Des Weiteren soll diese Version die Konfiguration und den Betrieb der Produkte vereinfachen. Hierfür sind einfache Datendienste, Software-Updates über die Luftschnittstelle (Software Update Over The Air, SUOTA) und HTTP-basierte Anwendungen definiert. CAT-iq 3.0 ist noch nicht verabschiedet, sodass mit Produkten frühestens 2010 gerechnet werden kann.

- CAT-iq 4.0 „Intelligent Networking“

  Für diese Version sind derzeit Funktionen wie Plug & Play, QoS für Streaming Media oder die Unterstützung von Instant Messaging vorgesehen. Laut Zeitplan wird der Standardisierungsprozess von CAT-iq 4.0 frühestens Mitte 2010 beginnen.

Weitere Funktionen sind geplant. Dazu zählen beispielsweise:

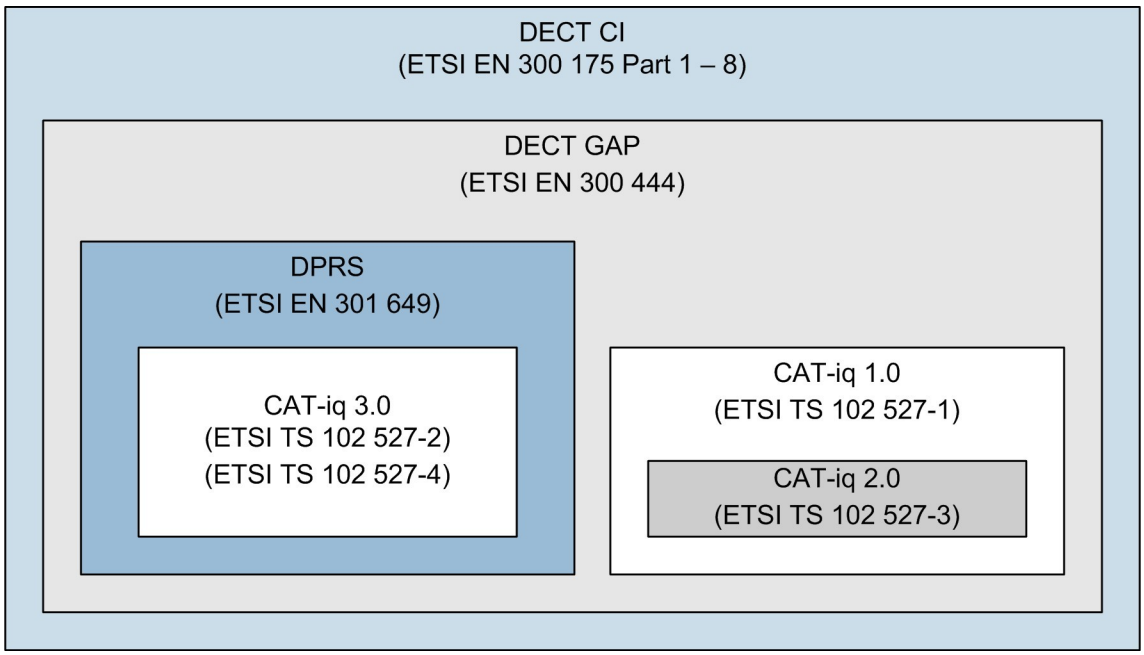
- „Home Control“: Diese Funktion ist für Geräte der Haustechnik vorgesehen; Beispiele sind die Licht- oder Rollladensteuerung.

- „Adapted Power Control“: Zur Minimierung der Strahlenbelastung, wie es u.a. seitens des Bundesamtes für Strahlenschutz gefordert wird, existierten bisher proprietäre Verfahren (siehe auch Kapitel C.1.2.1). Die Implementierung einer bedarfsgerechten Regelung der Sendeleistung eines FP soll innerhalb von CAT-iq standardisiert werden.

Die Zuordnung der Versionen zu den jeweiligen ETSI-Standards ist in Abbildung C-8 illustriert.

Während das ETSI im Rahmen der NG-DECT-Standards die verbindlichen und optionalen Funktionen auswählt, sind diese im Detail in den jeweiligen aktualisierten DECT-Standards [EN300175] einschließlich GAP [EN300444] und DPRS [EN301649] definiert. Im Rahmen der CAT-iq-Zertifizierung werden die definierten Testfälle dann überprüft.

Abbildung C-8: Einordnung der CAT-iq-Versionen in die DECT-Standards von ETSI



C.1.5.2 Funkschnittstelle

C.1.5.2.1 Physikalische Übertragung und Kanalzugriff

Basierend auf den Erläuterungen aus Kapitel C.1.2.1 stehen auch bei CAT-iq zehn Trägerfrequenzen zur Verfügung, welche per TDM (Time Division Multiplex) in Zeitschlitze (Slots) unterteilt sind. Als Modulationsverfahren ist aus Gründen der Abwärtskompatibilität GMSK vorgeschrieben, wobei weitere Modulationsverfahren optional implementiert werden können. Die angegebenen Übertragungswerte gelten nur bei Nutzung von GMSK, wobei ein Symbol einem Bit entspricht.

Die bei DECT üblichen 24 Zeitschlitze voller Länge (Full Slots) werden bei CAT-iq um eine weitere verbindliche Kategorie ergänzt. Diese sogenannten Long Slots gehören zur Kategorie variabler Slot-Längen mit einer Nutzdatenübertragung von 640 Bits[12]. Long Slots werden bei CAT-iq beispielsweise für die Übertragung von Gesprächsdaten mit dem Sprach-Codec G.722 verwendet. Die Nutzdatenrate pro Kanal ist im Vergleich zu DECT von 32 kbit/s auf 64 kbit/s erhöht worden, um den Anforderungen der neuen Sprach-Codecs gerecht zu werden.

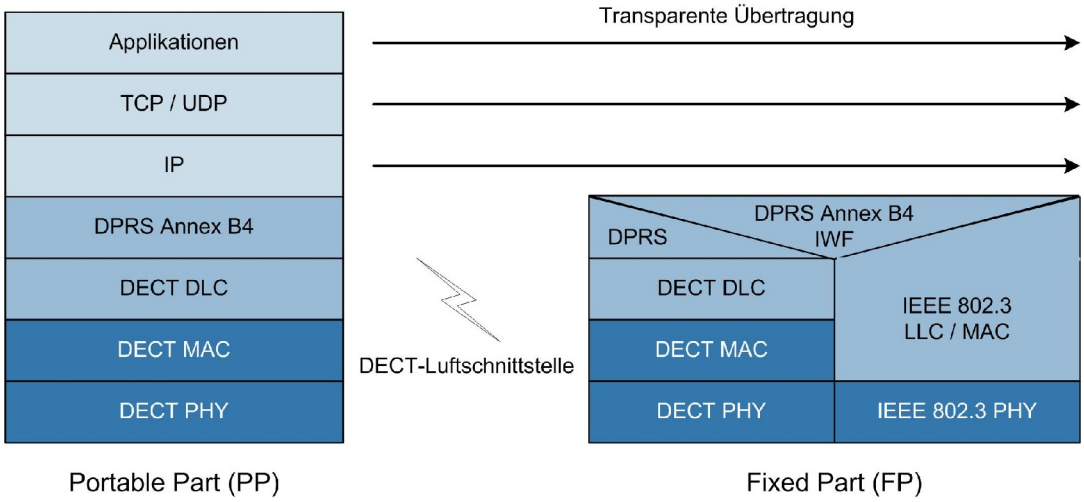
C.1.5.2.2 IP-Transport über DECT

Ein Schwerpunkt von CAT-iq liegt in der Integration von DECT und IP. Der hierfür nötige Transport von Paketen der IP-Version 4 (IPv4) und IP-Version 6 (IPv6) erfolgt in CAT-iq-Systemen auf Basis von DPRS innerhalb des Protokoll-Stack für Nutzerdaten (U-Plane, siehe auch Kapitel C.1.2). Eine transparente Übertragung von IP-Paketen ist sowohl für den FP als auch den PP eines CAT-iq-Systems verpflichtend. Dabei wird zwischen zwei Konfigurationen unterschieden:

Konfiguration 1: IEEE 802.3 over DECT

In dieser Konfiguration werden Ethernet-Frames (bis auf Präambel und Prüfsumme) per DECT transportiert (Abbildung C-9). Die Interworking Functions (IWF) regeln hierbei die Zusammenarbeit zwischen DECT- und Ethernet-Stack, wobei der Fixed Part in dieser Konfiguration als Switch agiert. Diese Konfiguration ist für PP und FP eines CAT-iq-Systems verpflichtend. Details sind in [TR1025272] respektive in [EN301649], Annex B.4 beschrieben.

Abbildung C-9: Protokoll-Stack (U-Plane/Nutzerebene) und Kommunikation bei IEEE 802.3 over DECT

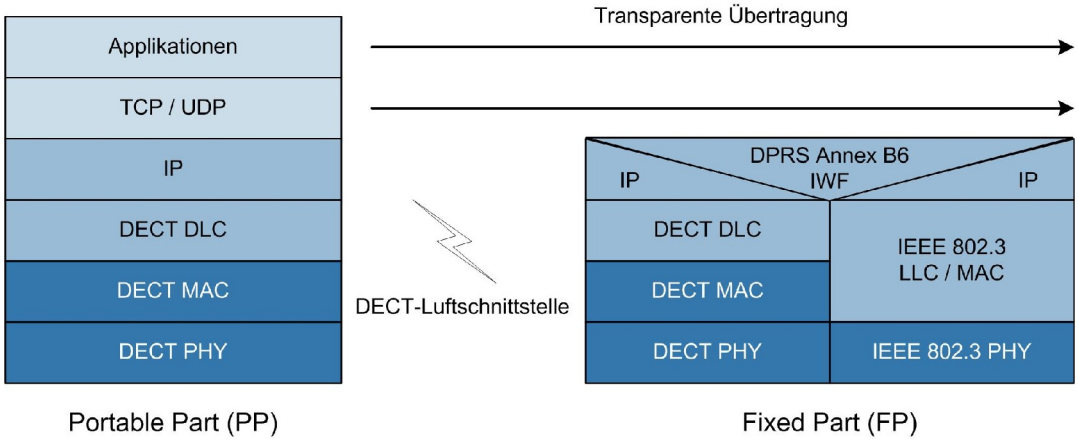


12 Optional sind auch 672 Bits definiert.

Konfiguration 2: IP over DECT

In dieser Konfiguration werden IP-Pakete direkt per DECT transportiert (siehe Abbildung C-10). Der Fixed Part agiert in dieser Konfiguration als Router. Diese Konfiguration ist für PP und FP eines CAT-iq-Systems optional. Details sind in [TR1025272] respektive in [EN301649] Annex B.6 beschrieben.

Abbildung C-10: Protokoll-Stack (U-Plane/Nutzerebene) und Kommunikation bei IP over DECT



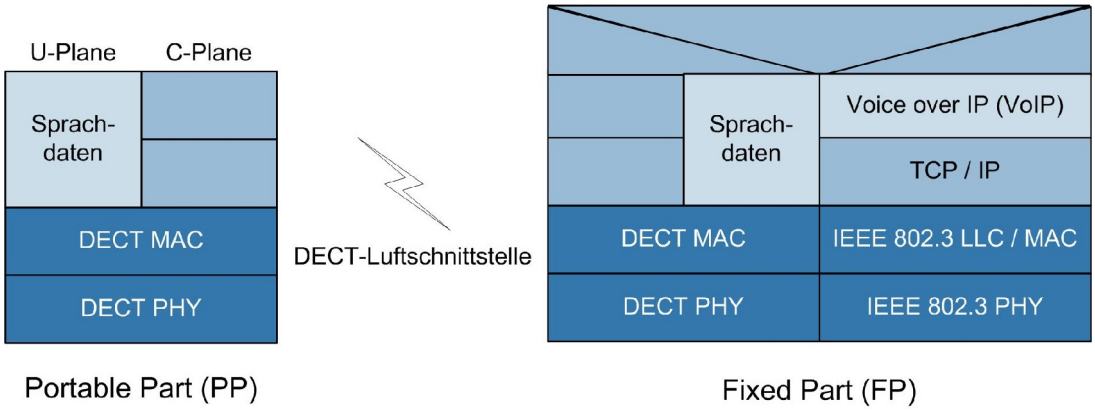
Aufgrund der Kompatibilität zu den IEEE-802.3-Systemen werden auch DHCP (Dynamic Host Configuration Protocol) und ARP (Address Resolution Protocol) durch PP und FP unterstützt.

Je nach Anforderung der jeweiligen CAT-iq-Komponente stehen für die Datenübertragung unterschiedliche Übertragungsraten zur Verfügung. Diese werden allgemein in drei Kategorien unterteilt:

- Kategorie 1: symmetrische Datenrate von 51,2 kbit/s (ein Kanal, Long Slot)
- Kategorie 2: symmetrische und asymmetrische Datenrate bis zu 563,2 kbit/s (mehrere Kanäle, Long Slot)
- Kategorie 3: symmetrische und asymmetrische Datenrate bis zu 844,8 kbit/s (mehrere Kanäle, Double Slot)

Sprachdaten werden aus Gründen des geringeren Overhead und der damit verbundenen geringeren Verzögerung bei CAT-iq nicht über IP übertragen, d.h. zwischen FP und PP findet auf der DECT-Luftschnittstelle keine Nutzung von VoIP statt (siehe Abbildung C-11).

Abbildung C-11: Protokoll-Stack (vereinfacht) für den Transport der Sprachdaten bei CAT-iq



Eventuell vorhandene erweiterte Funktionen des FP, wie beispielsweise ein WLAN- oder Internet-Zugang, sind hiervon unberührt. Generell kann der FP als Router oder Switch in einem solchen Szenario fungieren.

C.1.5.2.3 Sprachübertragung

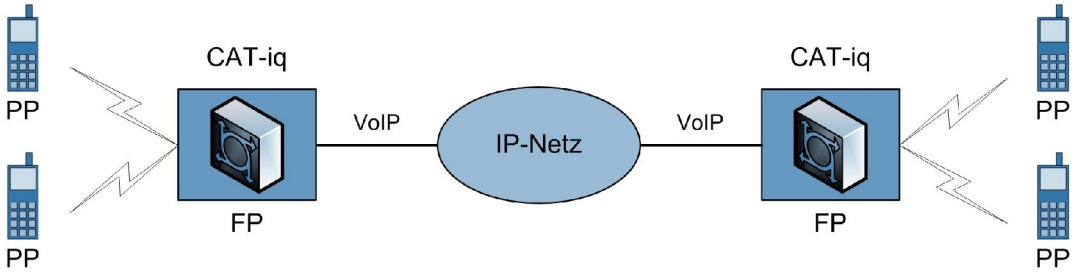
Ein signifikante Änderung bezüglich der Telefonie zwischen DECT GAP und CAT-iq betrifft die Qualität und den Kommunikationsfluss der Sprachdaten. Während die Sprachkodierung bei DECT mittels ADPCM (G.726) und 32 kbit/s erfolgt, setzt CAT-iq auf den Breitband-Codec G.722 bei 64 kbit/s. D.h. anstatt der klassischen Bandbreite von 300 bis 3400 Hz bei G.726 wird die Sprache bei G.722 zwischen 50 und 7000 Hz abgetastet. Die Nutzung der Breitband-Codecs wird von den Herstellern auch als „HD-Telefonie“ bezeichnet. Weitere Sprach-Codecs wie G.711, G.729 oder MPEG-4 ER AAC-LD[13] sind bei CAT-iq 1.0 optional.

Diese Breitband-Codecs können jedoch nur zur Anwendung kommen, wenn beide Kommunikationspartner sowie dazwischenliegende Infrastrukturkomponenten diese Codecs ebenfalls unterstützen. Werden diese nicht unterstützt, wird über einen Codec-Auswahlmechanismus, der in CAT-iq definiert ist, ein alternativer Codec gewählt (z.B. ADPCM).

Die CAT-iq-Funktionalität ist häufig nur eine Teilkomponente eines Kombigeräts. Weitere mögliche Funktionen sind insbesondere der Internet-Zugang sowie integrierte TK-Anlagen für kleinere Heim- oder Büroumgebungen einschließlich PSTN-Zugang. Neben dem PSTN-Zugang für analoge oder digitale Telefone ist auch die Internet-Telefonie häufig ein Bestandteil des Funktionsumfangs. Die Anbindung der Komponenten einschließlich des VoIP-Kommunikationspfades in einem solchen Szenario ist exemplarisch in Abbildung C-12 dargestellt. Hierbei wird die Sprache auf der DECT-Luftschnittstelle weiterhin TDM-basiert übertragen, während die Übertragung zwischen FP und dem VoIP-Dienstanbieter (Internet Telephony Service Provider, ITSP) mittels IP erfolgt. Diese VoIP-Verbindung zwischen FP und ITSP auf Basis des Signalisierungsprotokolls SIP (Session Initiation Protocol) wird als SIP-Trunk bzw. allgemein als IP-Anlagenanschluss bezeichnet und ist detailliert in der „Technischen Leitlinie Sichere TK-Anlagen“ des BSI (siehe [TLSTK08]) beschrieben.

13 ER = Error Resilient, AAC = Advanced Audio Coding, LD = Low Delay

Abbildung C-12: Kommunikationsfluss eines Gesprächs bei Nutzung der Internet-Telefonie

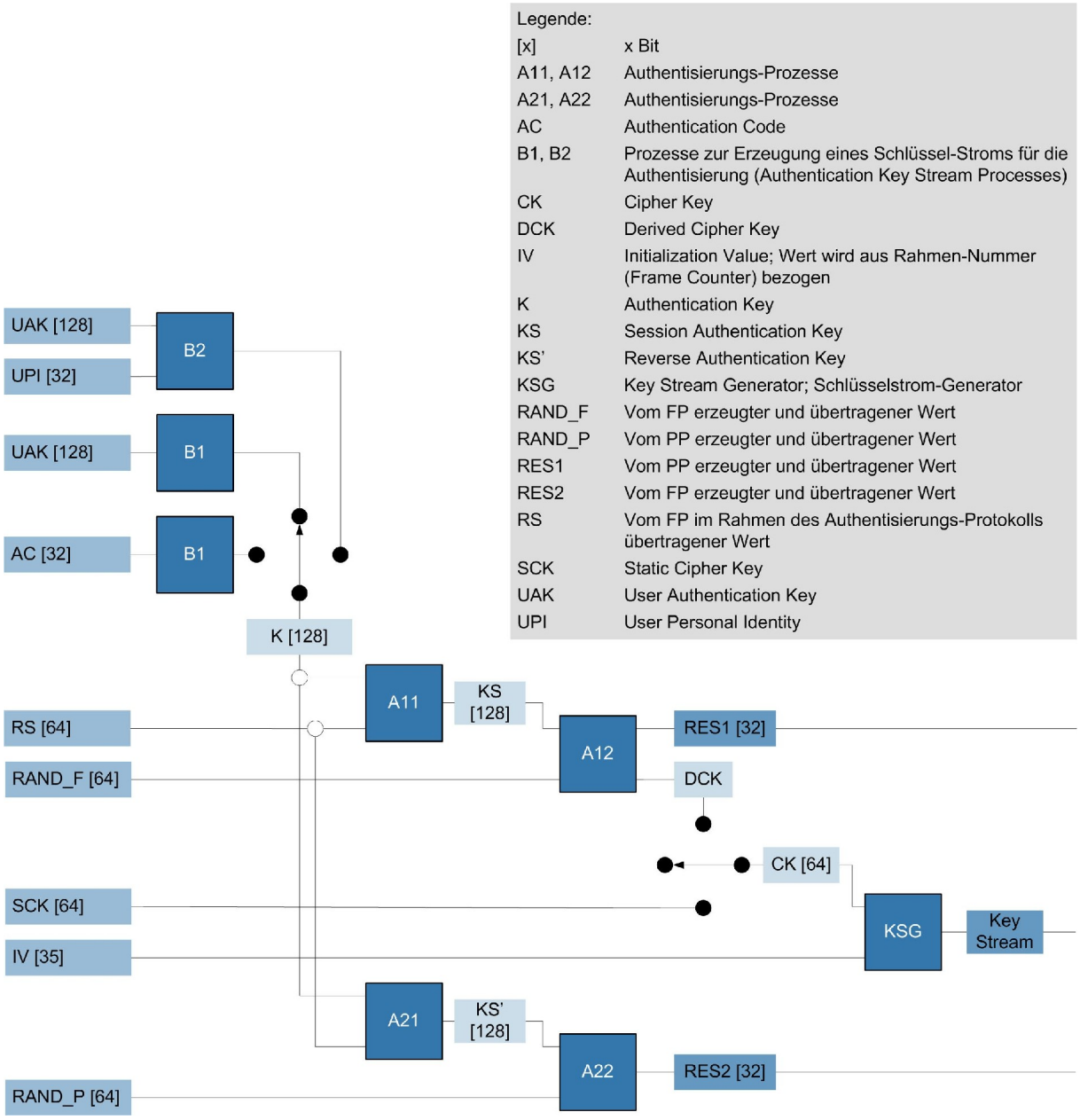


Die VoIP-Kommunikation ist hierbei nicht beschränkt auf das Internet, sondern kann generell auf Basis einer beliebigen IP-Infrastruktur erfolgen.

C.2 Sicherheitsmechanismen

Da DECT ein funkbasiertes Verfahren ist, besteht grundsätzlich die Gefahr, dass „unberechtigte“ DECT-fähige Geräte die DECT-Kommunikation mithören bzw. sich aktiv in die Kommunikationsverbindung einschalten. Neben nicht-kryptographischen Verfahren zum Schutz gegen Übertragungsfehler sieht die Spezifikation kryptographische Authentisierungs- und Verschlüsselungsalgorithmen vor. Die für die kryptographische Sicherheit verantwortlichen Parameter und Algorithmen sind in Abbildung C-13 aufgeführt.

Abbildung C-13: Kryptographische Sicherheitsmechanismen bei DECT (siehe [EN300175])



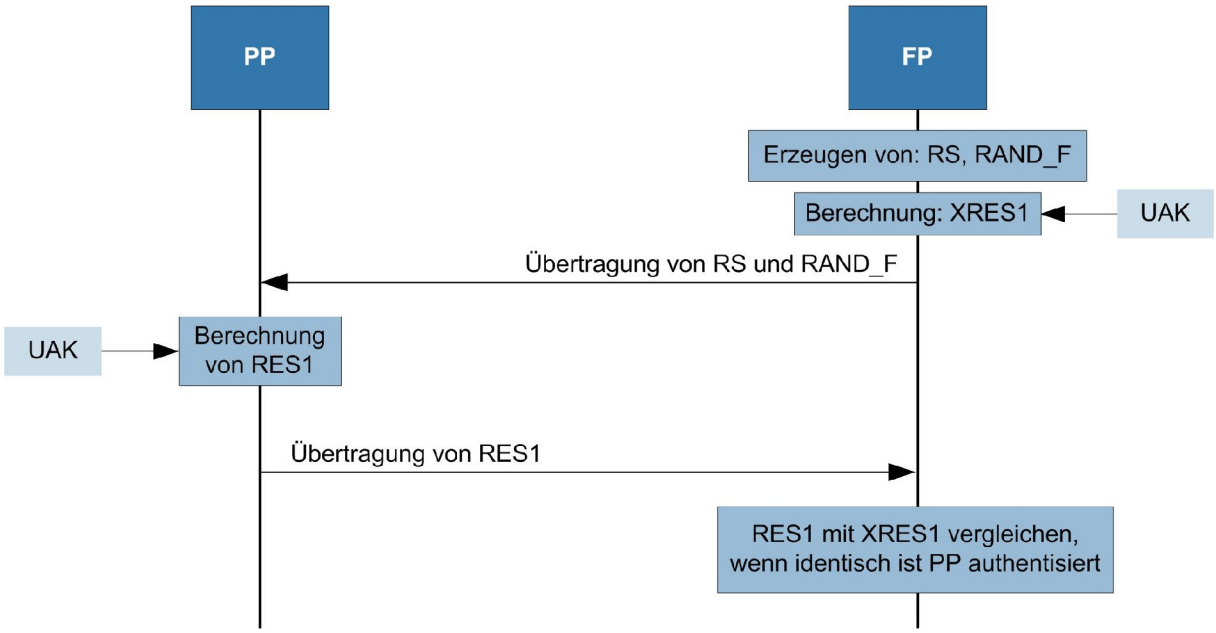
Dargestellt sind sowohl mögliche Eingangsparameter und deren Bitanzahl, wie z.B. UAK (User Authentication Key) und UPI (User Personal Identity) mit 128 Bit respektive 32 Bit, der zugehörige Pro-

zess (B2) sowie das Ergebnis (ausgefüllter Kreis). Sind verschiedene Varianten der Ergebnisbildung möglich, wie z.B. bei der Bildung des Authentication Key K mittels UAK und UPI, UAK oder allein basierend auf AC, ist dies durch ein Schaltersymbol illustriert, wobei der Pfeil in Richtung Quelle zeigt. In der Spezifikation sind viele Optionen beschrieben, die ein Hersteller von DECT-Systemen bei der Implementierung von Sicherheitsmechanismen verwenden kann. Die folgenden Beschreibungen beziehen sich auf die im Wesentlichen anzutreffenden Sicherheitsmechanismen gemäß GAP (siehe [EN300444]). Die beschriebenen Mechanismen gelten ebenso für CAT-iq, sofern nicht explizit anders erwähnt.

C.2.1 Authentisierung der Mobilstation

Jeder PP muss sich vor einem Verbindungsaufbau authentisieren. Hierdurch sollen unberechtigte Netzzugriffe verhindert werden. Die Authentisierung basiert auf einem sogenannten Challenge-Response-Verfahren, wie in Abbildung C-14 gezeigt.

Abbildung C-14: Authentisierung der Mobilstation bei DECT (vereinfacht)



Aus den vom FP gesendeten 64 Bit-Zufallszahlen RAND_F und RS (Challenge) wird im PP unter Verwendung des Langzeitgeheimnisses UAK[14] und dem Wert RS unter Zuhilfenahme des Prozesses A11 ein Zwischenschlüssel KS erzeugt. Der Prozess A12 verwendet diesen Wert KS sowie die vom FP gelieferte Zufallszahl RAND_F und erzeugt daraus die Antwort RES1 (32 Bit) für den FP sowie den 64 Bit langen Chiffrier-Schlüssel DCK (siehe Kapitel C.2.4), welcher für den DECT-Verschlüsselungsalgorithmus DSCA (DECT Standard Cipher Algorithm) verwendet werden kann. Der Wert RES1 wird über die Luftschnittstelle zum FP übertragen[15]. Stimmen die RES1-Werte, d.h. der gesendete Wert RES1 und der erwartete Wert XRES1 des FP, überein, gilt der PP als authentisiert. Dies ist vereinfacht in Abbildung C-14 dargestellt, weitere Details sind Abbildung C-13 zu entnehmen.

---

14 Genauer gesagt erfolgt dies unter Verwendung des Authentication Key (K). Dieser kann von UAK und UPI, vom AC oder allein vom UAK abgeleitet werden. Da jedoch in der Regel nur der UAK zur Ableitung von K dient, wird nachfolgend auf eine weitergehende Unterteilung verzichtet und allein der UAK dargestellt.

15 Die Prozesse B1 und B2, die in Abbildung C-13 gezeigt sind, dienen der Bereitstellung der Eingangsparameter für den Prozess A11.

Der DECT-Authentisierungsalgorithmus (DECT Standard Authentication Algorithm, DSAA) bestehend aus den Prozessen A11, A12, A21 und A22 ist nicht in den öffentlich zugänglichen ETSI-Standards enthalten. Der DSAA wurde jedoch rekonstruiert und gilt als vollständig kompromittiert (siehe auch [DECTSEC] bzw. [LSTWW09]).

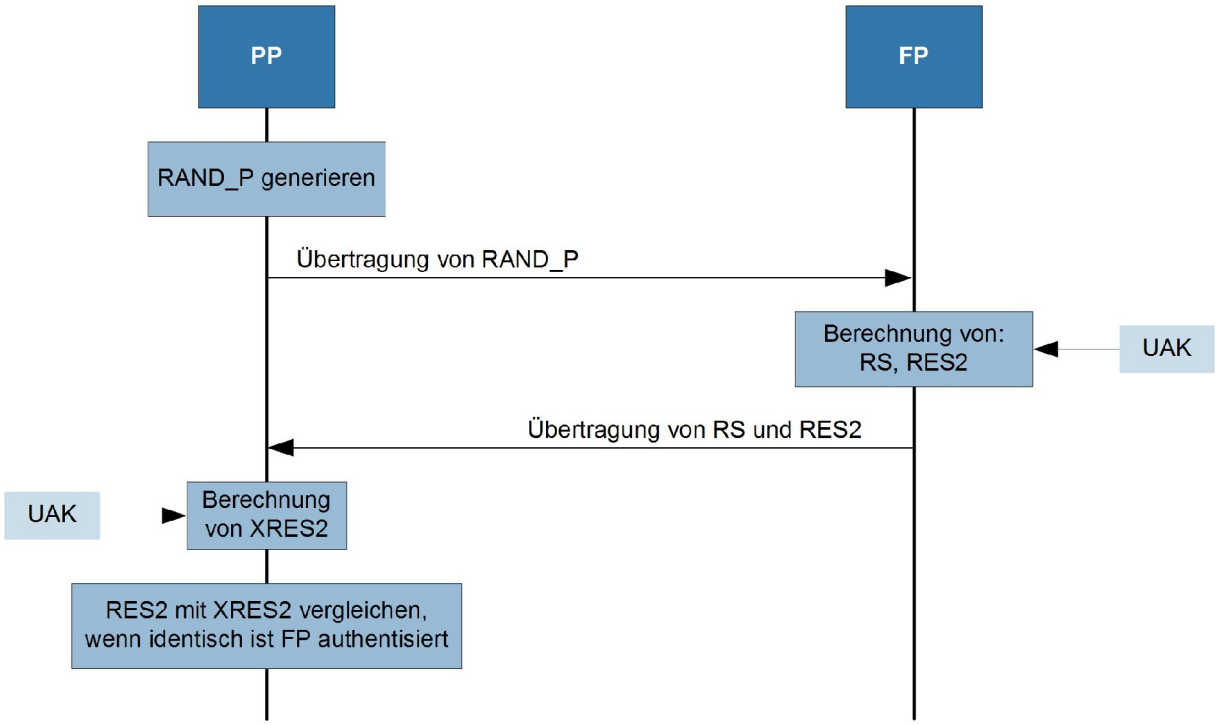
Das Langzeitgeheimnis UAK (User Authentication Key) muss in beiden Geräten (Mobil- und Feststation) gespeichert sein (siehe Kapitel C.2.6).

C.2.2 Authentisierung der Feststation

Die Authentisierung des FPs gegenüber dem PP zum Schutz der Mobilstation vor Verbindungen über unberechtigte Feststationen ist optional. Der Ablauf ist im Prinzip ähnlich wie bei der Authentisierung der Mobilstation, jedoch sind die Aufgaben von PP und FP vertauscht. Zuerst generiert der PP einen 64 Bit langen Wert RAND_P und sendet diesen an den FP. Der FP wiederum generiert den Wert RS (64 Bit) und erzeugt mit dem Prozess A21 unter Verwendung des UAK und dem Wert RS einen 128 Bit langen Zwischenschlüssel KS. Im Anschluss generiert der Prozess A22 aus den Werten KS und RAND_P die Antwort RES2 (32 Bit). Die Werte RES2 und KS werden zum PP gesendet, der die gleiche Berechnung durchführt. Stimmen der gesendete Wert RES2 und der berechnete Wert XRES2 überein, ist der FP authentisiert (siehe auch [EN300175] Teil 7). Dieser Ablauf ist vereinfacht in Abbildung C-15 dargestellt.

Die Authentisierung der Feststation dient insbesondere nicht der Generierung von Schlüsselmaterial für die optionale Verschlüsselung. Dies erfolgt nur über die Authentisierung des PP oder der Verwendung eines statischen Schlüssels (Static Cipher Key, SCK).

Abbildung C-15: Authentisierung der Feststation bei DECT (vereinfacht)



C.2.3 Gegenseitige Authentisierung

DECT sieht verschiedene Varianten der gegenseitigen Authentisierung vor. Generell wird hierbei zwischen einem direkten Mechanismus und verschiedenen indirekten Mechanismen unterschieden. Der direkte Mechanismus besteht aus der Authentisierung des PP und anschließender Authentisierung des FP wie zuvor beschrieben. Die indirekten Verfahren basieren auf dem Einsatz von Verschlüsselung und ggf. einer einseitigen Authentisierung. Letztere können insbesondere aufgrund des optionalen Charakters der Verschlüsselung als ungeeignet für eine gegenseitige Authentisierung angesehen werden, da der alleinige Einsatz von Verschlüsselung nicht genügt, um den wahren Absender bzw. Eigentümer des Schlüssels zu identifizieren. Hieraus resultiert ein möglicher Replay-Angriff, indem Authentisierungsanfragen gestellt werden und bereits aufgezeichneter verschlüsselter Datenverkehr wiederholt gesendet wird (siehe [LSTWW09]). Details zur Authentisierung und den verschiedenen Verfahren werden in [EN300175] Teil 7 beschrieben.

C.2.4 Verschlüsselung

Optional werden die Nutzdaten auf der Funkschnittstelle zum Schutz der Vertraulichkeit verschlüsselt übertragen. Die Verschlüsselung erfolgt auf Basis einer Stromchiffrierung, deren Schlüsselstrom (Key Stream) vom Schlüsselstromgenerator mit Hilfe des 64 Bit langen Chiffrier-Schlüssels CK (Cipher Key) und eines von der aktuellen Frame-Nummer abgeleiteten Initialisierungsvektors IV erzeugt wird. Der Schlüsselstrom sollte sich dabei in einem statistischen Sinne wie eine zufällige Bitfolge verhalten. Da der Schlüsselstrom jedoch systematisch erzeugt wird, spricht man auch von einem pseudozufälligen Bitstrom. Der Schlüssel CK kann ein statischer Chiffrier-Schlüssel (Static Cipher Key, SCK) sein, oder er ist der beim Verbindungsaufbau abgeleitete Chiffrier-Schlüssel (Derived Cipher Key, DCK).

Der Schlüsselstrom wird mit den Klardaten bitweise XOR-verknüpft (XOR = exklusives Oder). Auf diese Weise wird der Klartext quasi in dem pseudozufälligen Schlüsselstrom versteckt. Sofern der Schlüsselstrom sich statistisch mit genügender Qualität wie ein echter Zufall verhält, kann nur unter Kenntnis des Schlüsselstroms der Klartext wieder ausgefiltert werden. Dies geschieht auf der Empfängerseite einfach dadurch, dass der Empfänger seinerseits den Schlüsselstrom aus CK und IV erzeugt und die empfangenen verschlüsselten Daten bitweise mit dem Schlüsselstrom XOR-verknüpft. Das Ergebnis sind die Klardaten.

Der verwendete Stromchiffrierer ist der sogenannte DECT Standard Cipher (DSC). Dieser Algorithmus ist nicht veröffentlicht, jedoch bereits teilweise rekonstruiert und insbesondere für den erhöhten Schutzbedarf aus Sicht der IT-Sicherheit nicht geeignet. Als kritisch zu bewerten ist zusätzlich, dass die Nutzung der Verschlüsselung optional ist und in der Regel nicht erzwungen werden kann.

C.2.5 Authentisierung des Benutzers

Veränderungen wichtiger Einstellungen an DECT-Geräten erfordern in der Regel die Eingabe einer typischerweise 4- bis 8-stelligen Geheimnummer, der persönlichen Identifikationsnummer (PIN). Beispielsweise ist die PIN-Eingabe erforderlich, wenn an einem DECT-Telefon Nummernsperren o.Ä. eingegeben werden sollen. Die PIN ist in der Regel änderbar, indem im entsprechenden Menü zuerst die aktuell gültige PIN eingegeben wird und dann die PIN, die zukünftig gültig sein soll.

C.2.6 Subscription

Als Subscription bezeichnet man die Anmeldung eines PP bei einem FP mit der Folge, dass dem PP fortan die Dienste des FP (und des damit verbundenen DECT-Netzwerks) zur Verfügung stehen. Die ursprünglich spezifizierte Subscription von DECT (siehe Kapitel C.2.6.1) wurde für CAT-iq erweitert (siehe Kapitel C.2.6.2).

C.2.6.1 Subscription bei DECT

Auch bei der Subscription ist in der Regel die Eingabe einer PIN (siehe Kapitel C.2.5) erforderlich. Bei den meisten DECT-Telefonen für den Heimgebrauch wird die PIN im FP gespeichert und muss bei der Anmeldung eines PP auf diesem PP eingegeben werden, nachdem der FP durch Knopfdruck in einen Zustand versetzt wurde, der für eine begrenzte Zeit Anmeldungen neuer PPs zulässt. Während eines solchen Subscription-Prozesses wird für den PP ein Zugriffsrecht zum FP vereinbart und es wird bei FP und PP das Langzeitgeheimnis UAK für das Geräte-Paar (FP, PP) erzeugt. Dabei muss in beiden Geräten die gleiche PIN vorhanden sein, denn die PIN wird zur Generierung des Authentication Code (AC) verwendet, welcher wiederum in die Berechnung des neuen UAK einfließt[16]. Der UAK wird fortan bei jedem Verbindungsaufbau für die Authentisierung benutzt.

Zusätzlich dient der UAK der Generierung des Schlüsselmaterials für den DSC. Auch wenn in den DECT-Standards weitere Mechanismen zur Ableitung des Schlüsselmaterials vorgesehen sind, kommt hierfür in der Regel nur der UAK zum Einsatz. Geräte, die dem Generic Access Profile (GAP, siehe [EN300444]) genügen, unterstützen eine sogenannte On-Air-Subscription. Dabei wird die für die Subscription benötigte Zufallszahl RS über die Luftschnittstelle übertragen.

C.2.6.2 Subscription bei CAT-iq

Neben den Subscription-Verfahren wie in Kapitel C.2.6.1 beschrieben, sieht CAT-iq 2.0 zusätzlich die beiden folgenden Methoden der On-Air-Subscription vor:

- Easy PIN code registration
- Easy Pairing

Die beiden Methoden müssen bei CAT-iq 2.0 durch den PP unterstützt werden. Bei der Methode „Easy PIN code registration“ sucht der PP den FP mit der besten Signalstärke und aktiviertem Subscription-Modus. Dieser Subscription-Modus wird in der Regel durch Drücken einer bestimmten Taste aktiviert. Aus Sicherheitsgründen kann nur ein einziges Gerät je Anmeldevorgang registriert werden. Der PP wird dann aufgefordert, die PIN einzugeben. Nach Eingabe der PIN wird diese als Authentication Code genutzt. Stimmt dieser mit den Angaben des FP überein, ist der PP erfolgreich registriert und beide Geräte verfügen über den UAK.

Easy Pairing basiert auf dem gleichen Prozedere, jedoch unter der Annahme, dass die PIN der Voreinstellung „0000“ entspricht. Eine manuelle Eingabe der PIN entfällt. Dies soll die Anmeldung von Mobilstationen erleichtern. Um die Gefährdung eines versehentlichen Anmeldens am falschen FP zu verringern, sieht CAT-iq 2.0 weitere Mechanismen vor. Zu diesen gehört das Broadcasting des Gerätenamens des FP sowie eine Rückmeldung (z.B. in Form einer Displayanzeige an PP und FP und/oder Audiosignalen) für den Nutzer.

Easy Pairing ist das voreingestellte Verfahren bei Mobilstationen nach CAT-iq 2.0. Ist der Subscription-Vorgang mittels Easy Pairing nicht erfolgreich, wird auf Easy PIN code registration gewechselt.

[16] Der neue UAK entspricht dem bei der Authentisierung mit Verwendung von AC entstehenden KS´ in Abbildung C-13.

C.3 Gefährdungen

Neben den Gefährdungen, denen kabelbasierte Netzwerke ausgesetzt sind (siehe [GSK]), ergeben sich bei der Nutzung von Funknetz-Technik zusätzliche Gefährdungen, die insbesondere auf den Sicherheitsschwächen der verwendeten Protokolle sowie auf der unkontrollierten Ausbreitung der Funkwellen basieren.

C.3.1 Unkontrollierte Ausbreitung der Funkwellen

Der Funkverkehr von DECT-Verbindungen kann mit Hilfe von DECT-Protokollanalysatoren passiv empfangen und aufgezeichnet werden. Alle Schichten des DECT-Protokoll-Stack können offline betrachtet bzw. analysiert werden. Das Extrahieren und Mitlesen der übertragenen Nutzdaten ist bei fehlender Verschlüsselung möglich. Durch den Einsatz einer Antenne mit starker Richtcharakteristik und geeigneter Elektronik zur Verstärkung eines empfangenen DECT-Signals kann ein solcher Lauschangriff auch noch in einer gegenüber der Reichweite normaler DECT-Geräte größeren Entfernung durchgeführt werden. Der Aufwand für das Aufzeichnen von unverschlüsselten Gesprächen ist seit Ende 2008 nochmals verringert worden, indem bestimmte PCMCIA-Karten als Protokollanalysatoren mit entsprechender Software, die im Internet frei verfügbar ist, verwendet werden können.

Wünschenswert ist daher eine dynamische Anpassung der Sendeleistung der DECT-Geräte auf ein akzeptables Minimum, um den skizzierten Lauschangriff zumindest zu erschweren. Eine Sendeleistungsregelung ist allerdings optional und wird nicht von jedem DECT-Gerät unterstützt.

Dies ist insbesondere bei der Nutzung von DECT bzw. CAT-iq in sensitiven Bereichen als äußerst kritisch zu bewerten. Hierzu zählen beispielsweise Alarmanlagen, Kreditkarten- bzw. EC-Bezahlsysteme, Verkehrsleitsysteme oder Anwendungen im Bereich der Heimelektronik.

C.3.2 Schwächen im Sicherheitskonzept

C.3.2.1 Gegenseitige Authentisierung und Subscription

In der Praxis authentisiert sich nur der PP gegenüber dem FP, die Authentisierung des FP findet in der Regel nur bei der Subscription statt. Die nicht durchgeführte gegenseitige Authentisierung (Mutual Authentication) macht DECT anfällig für Spoofing-Angriffe, indem die DECT-Kommunikation zwischen PP und FP mit einem angreifenden FP mit gefälschten Identität (Radio Fixed Part Identity, RFPI) gestört wird. Sofern der PP sich aufgrund einer ausreichenden Signalstärke am falschen FP anmeldet, wird der Angreifer-FP jegliche Authentisierung akzeptieren und die Verschlüsselung unterbinden. Dies ermöglicht das Aufzeichnen und Umleiten jeglicher ausgehender Gespräche des PP.

Der Authentisierungsalgorithmus benutzt ein 128 Bit langes Geheimnis, den UAK. Dieser Algorithmus (siehe Kapitel C.1.2) wird seitens der ETSI bzw. des DECT-Forums nicht der Allgemeinheit zugänglich gemacht, wurde jedoch im Jahr 2008 rekonstruiert und ist seitdem im Internet veröffentlicht. Der Authentisierungsalgorithmus DSAA ist als schwach einzustufen und stellt im Idealfall eine symmetrische Schlüsselstärke von 64 Bit bereit.

In der Implementierung des Schlüsselmanagements haben die Hersteller einige Freiheiten. Es ist in der Regel möglich, einen PP an einen FP neu anzumelden, auch wenn diese noch kein gemeinsames Geheimnis UAK besitzen (Subscription). Im GAP und damit auch bei CAT-iq ist die Anmeldung über die Luftschnittstelle vorgesehen. Dabei werden ausschließlich der AC (32 Bit) und die Zufallszahl RS

(64 Bit) benutzt, um den UAK zu erzeugen, sodass die kryptographische Stärke (Entropie) des UAK auf maximal 96 Bit beschränkt ist. In diesem Zusammenhang muss bei der On-Air-Subscription berücksichtigt werden, dass die Zufallszahlen RAND_F und RS im Klartext über die Luftschnittstelle übertragen werden. Der UAK wird in der Regel im nichtflüchtigen Speicher abgelegt und es besteht grundsätzlich die Gefährdung des unerlaubten Auslesens. Dies kann beispielsweise missbraucht werden, um Mobilstationen bzw. Identitäten zu klonen und alle damit verbundenen Funktionen und Leistungsmerkmale zu Ungunsten des Eigentümers zu nutzen. Optional kann der UAK auch auf einer externen Komponente, einem sogenannten DAM (DECT Authentication Module) abgelegt werden. Dies ist vergleichbar mit der SIM-Karte im Mobilfunkbereich. Die Verwendung von DAMs ist in der Praxis jedoch unüblich.

Die Qualität des implementierten Zufallsgenerators, der zur Erzeugung von RS dient, wirkt sich zusätzlich entscheidend auf die Entropie des UAK aus (siehe auch Kapitel C.3.4).

C.3.2.2 Verschlüsselung und Integritätsprüfung

In der Produktwerbung findet man gelegentlich die Behauptung, dass allein die Verwendung des digitalen DECT-Standards Abhörsicherheit garantiert. Für einen qualifizierten Angreifer stellt die digitale Übertragung allein jedoch kein Hindernis dar, wenn die Verschlüsselung in den DECT-Geräten nicht implementiert ist. Genau das ist aber bei vielen DECT-Geräten der Fall und diese Schwachstelle kann leicht ausgenutzt werden. Entsprechende Geräte zum Aufzeichnen der über die DECT-Luftschnittstelle übertragenen Protokoll- und Nutzdaten (Protokollanalysatoren) sind auf dem Markt ebenso verfügbar wie komplette Systeme zum Abhören unverschlüsselter DECT-Sprach-Telefonate. Wird an einem FP, der Verschlüsselung unterstützt, ein PP eingesetzt, der diese Funktion nicht bietet, wird typischerweise der PP nicht abgewiesen, sondern die Kommunikation findet automatisch unverschlüsselt statt. Daher muss der Anwender hier darauf achten, dass alle eingesetzten Geräte (auch die PPs) eine Verschlüsselung unterstützen. Insbesondere die auf dem Markt erhältlichen DECT-Repeater funktionieren in der Regel nur bei deaktivierter Verschlüsselung, auch wenn dies vom Standard her nicht erforderlich ist. Vom Repeater-Einsatz ist aus diesem Grund abzuraten!

Ist die Verschlüsselung aktiviert, so wird für die Verschlüsselung ein 64 Bit langer Chiffrier-Schlüssel CK benutzt. Diese Schlüssellänge wird von Experten allenfalls für ein geringes Sicherheitsniveau als ausreichend angesehen. Der verwendete Verschlüsselungsalgorithmus DSC (DECT Standard Cipher) ist nur Mitgliedern des DECT-Forums bei Unterzeichnung eines NDA zugänglich, wurde jedoch bereits teilweise rekonstruiert (siehe [LSTWW09]). Es ist davon auszugehen, dass eine vollständige Rekonstruktion zeitnah erfolgt.

Da es sich bei DSC um eine Stromchiffrierung handelt, muss beachtet werden, dass bei Verwendung derartiger Chiffren sich der Schlüsselstrom nicht innerhalb kurzer Zeiträume wiederholen darf. Falls dies geschieht, entspricht die XOR-Summe der jeweiligen Chiffrate der XOR-Summe der zugehörigen Klartexte, da sich die identischen Bitströme der Schlüsselströme gegenseitig aufheben (dies wird auch als „In-die-Tiefe-Lesen“ bezeichnet). Je nach Redundanz der benutzten Klartexte erlaubt dies deren Rekonstruktion. Bei einem ausreichend großen Schlüsselraum und einem kryptographisch starken Schlüsselstromgenerator besteht hier keine Gefahr. Der DECT-Standard erlaubt jedoch die Nutzung eines statischen Chiffrier-Schlüssels SCK. Da der SCK permanent beibehalten wird, hängt die Variation der Schlüsselströme ausschließlich vom Initialisierungsvektor IV ab. Die effektive Länge des IV beträgt 28 Bit. Da der IV im Wesentlichen der Frame-Nummer entspricht, die infolge des kontinuierlichen Sendens des FP alle 10 ms um 1 erhöht wird, sind nach ca. 1 Monat alle möglichen IV durchlaufen, sodass dann bei Nutzung des SCK identische Bitströme zum Verschlüsseln der Klartexte auftauchen.

Das „In-die-Tiefe-Lesen“ ist unter Umständen auch direkt möglich, wenn eine Kanalbündelung zum Erzielen höherer Datenraten so implementiert ist, dass auf allen Kanälen identische Initialisierungsvektoren verwendet werden und somit die Schlüsselströme identisch sind. Dies gilt unabhängig davon, ob dabei der statische Schlüssel SCK oder der abgeleitete Schlüssel DCK verwendet wird.

Es gibt in DECT keine kryptographische Absicherung der Integrität der übertragenen Daten. Werden von einem Angreifer gezielt Bits in den Chiffratdaten gestört, so werden genau diese Bits in den Klardaten gestört. Auf diese Weise kann ein Angreifer gezielt Nachrichten manipulieren, wenn er gewisse Kenntnisse über den Nachrichtenaufbau hat.

C.3.3 Unsichere Voreinstellungen

Voreinstellungen sind von Seiten des Herstellers oft unsicher konfiguriert: PINs sind beispielsweise häufig auf „0000“ eingestellt. Derart ungeschützte PPs könnten z.B. bei fremden FPs angemeldet werden, wenn der Angreifer kurzzeitig Zugang zum PP hat. Analog können an entsprechend ungeschützten FPs neue PPs unberechtigt angemeldet werden. Bei FPs einiger Hersteller genügt es, einen Knopf zu drücken, um die Bereitschaft für die Anmeldung neuer PPs herzustellen.

CAT-iq 2.0 sieht beispielsweise einen „Easy Pair“-Modus vor, der genau auf einer solchen Voreinstellung der PIN basiert (siehe auch Kapitel C.2.6.2) und die Sicherheit zugunsten der Benutzerfreundlichkeit weiter verringert.

C.3.4 Implementierungsfehler

Wie in Kapitel C.3.2.1 aufgeführt, hängt die kryptographische Stärke des UAK beim Anmelden eines PP signifikant von der Qualität des implementierten Pseudozufallszahlengenerators (Pseudo-Random Number Generator, PRNG) ab. Allein die PIN und eine Zufallszahl werden zur Bildung des UAK herangezogen.

Der PRNG sollte im Idealfall eine Entropie von 64 Bit bereitstellen. Untersuchungen haben jedoch gezeigt, dass je nach Implementierung deutlich weniger (z.B. nur 22 Bit) Entropie durch den PRNG erzeugt werden. Anfällige PRNGs können mit einem geringen Aufwand identifiziert werden. Auf diese Weise ermittelte UAKs bedeuten eine vollständige Kompromittierung des DECT-Systems (z.B. Aufzeichnen von verschlüsselten Gesprächen, Nutzung fremder FPs usw.).

C.3.5 IP-fähige FPs

Insbesondere bei CAT-iq-kompatiblen FPs sind eine Ethernet-Schnittstelle und die Nutzung der TCP/IP-Protokollfamilie obligatorisch. In der Konsequenz bedeutet dies, dass hierfür relevante Angriffe wie beispielsweise ARP- und/oder IP-Spoofing oder Angriffe vom Typ DoS (Denial of Service) zu berücksichtigen sind.

Die folgenden Punkte sollten hierbei berücksichtigt werden:

- Die Administration erfolgt in der Regel über unverschlüsselte Protokolle wie z.B. HTTP.
- Durch die Nutzung von IP ist für den Zugriff auf die Administrationsschnittstellen kein direkter lokaler Anschluss nötig, im Gegensatz zu beispielsweise einem direkten Konsolenanschluss. Dies ermöglicht bei fehlender Absicherung der IP-basierten Kommunikation auch einen Fernzugriff durch nicht autorisierte Personen.
- Im Unterschied zu nicht IP-fähigen DECT FPs ist die Wahrscheinlichkeit für Software-Fehler aufgrund der multiplen Schnittstellen und der Entwicklung neuer Funktionen bei IP-fähigen FPs, insbesondere CAT-iq-Systemen, höher einzustufen.

Weitere Informationen hierzu können den IT-Grundschutz-Katalogen (siehe [GSK]) entnommen werden. Als Grundlage des auszuwählenden IT-Systems kann hierfür der Baustein für „Router und Switches“ betrachtet werden.

C.3.5.1 IP-Anlagenanschluss

Basierend auf einer IP-fähigen Basisstation besteht gerade bei CAT-iq-Systemen die Möglichkeit einer PSTN-Anbindung über das Internet. Anstatt die Telefonie TDM-basiert über einen Analog- oder ISDN-Anschluss zu führen, erfolgt diese IP-basiert zwischen dem FP und der Gegenstelle des VoIP-Anbieters. Hierbei wird die Signalisierung mittels SIP realisiert, sodass in diesem Zusammenhang anstatt IP-Anlagenanschluss auch häufig der Begriff SIP Trunk genutzt wird. Die eigentliche Übertragung der Sprachdaten erfolgt über RTP (Real-Time Transport Protocol).

Abgesehen von einer expliziten Konfiguration eines VoIP-Anbieters auf dem FP besteht eine mögliche Gefährdung darin, dass ein vom Hersteller betriebener VoIP-Server bereits voreingestellt ist. Dies ermöglicht dann beispielsweise, dass Teilnehmer mit Produkten dieses Herstellers über das Internet kostenlos telefonieren können. Generell besteht hierbei aber die Gefahr des Abhörens von Gesprächen sowie von unerwünschten Anrufen über das Internet, sogenanntem SPIT (Spam over Internet Telephony).

Die Protokolle für die Signalisierung und die Sprachdaten werden dabei in der Regel unverschlüsselt übertragen. Eine detaillierte Beschreibung sowohl des IP-Anlagenanschlusses als auch der zugehörigen Gefährdungen ist der „Technischen Leitlinie Sichere TK-Anlagen“ des BSI (siehe [TLSTK08]) zu entnehmen.

C.3.5.2 Ungesicherte Nutzung IP-basierter Dienste

Mit der Einführung von Mobilstationen nach dem CAT-iq-Standard ist die Nutzung von IP-basierten Anwendungen explizit vorgesehen. Die Kommunikation findet in der Regel über das Internet statt. Zu diesen Diensten zählen beispielsweise:

- Telefonbuch

  Die Mobilstation greift via IP auf ein Online-Telefonbuch zu. Neben der herkömmlichen Rufnummernsuche kann dies auch für die Rufnummernauflösung von noch unbekannten ankommenden Rufnummern eingesetzt werden, sodass der Name des Anrufenden angezeigt wird, unabhängig davon, ob dieser im lokalen Telefonbuch eingetragen ist.

- E-Mail

  Eine mögliche Funktion ist die Anzeige von E-Mails direkt auf der Mobilstation. Hierzu ist auf Seite der Mobilstation mindestens die Konfiguration des Mailservers sowie Benutzername und Passwort erforderlich. Häufig kommt hierbei das Protokoll POP3 für den Mailabruf zum Einsatz. Die zur Verfügung stehenden Sicherheitsmechanismen sind oft nicht mit denen eines vollwertigen E-Mail-Clients vergleichbar. Insbesondere die Übertragung von Benutzername und Passwort im Klartext ist als kritisch einzustufen.

- Instant Messaging / Präsenzdienste

  Eine weitere Anwendung beinhaltet die Anzeige des Präsenzstatus anderer Teilnehmer sowie den Austausch von Kurznachrichten. Hierbei kommt häufig das Protokoll XMPP (Extensible Messaging and Presence Protocol, Jabber) zum Einsatz. Auch hier stellt die Übertragung von Benutzername und Passwort im Klartext eine Gefährdung dar. Hinzu kommen gegebenenfalls zu berücksichtigende Aspekte des Datenschutzes.

- Weitere Dienste

  Weitere Dienste sind beispielsweise RSS-Feeds zur Anzeige von Nachrichten oder Internet-Radios. Generell sind jegliche Zusatzdienste und deren spezifische Gefährdungen zu berücksichtigen, speziell webbasierte Anwendungen. Schwerpunkte betreffen die oft unverschlüsselte Kommunikation, das Einbringen schadenstiftender Software oder Angriffe vom Typ DoS.

Abgesehen von den hier aufgeführten „IP over DECT“-basierten Diensten sind auch Dienste über andere Schnittstellen der Mobilstation zu berücksichtigen, beispielsweise über Bluetooth. An dieser Stelle wird auf die weiteren Kapitel dieses Dokuments verwiesen.

C.3.6 Gefährdungen durch Kombigeräte

Sofern der FP eines DECT- bzw. CAT-iq-Systems nur eine Teilfunktion eines Geräts darstellt, beispielsweise eines Kombigeräts, ist jede Schnittstelle zunächst für sich zu betrachten und geeignet abzusichern. Weitergehend muss aber berücksichtigt werden, dass übergreifende Effekte entstehen können, die über eine Sicherheitslücke auf einer Schnittstelle einen Angriff auf einer anderen Schnittstelle ermöglichen. Der Worst Case besteht in der vollständigen Kompromittierung des Geräts und damit dem Zugriff auf den gesamten Kommunikationsfluss.

Mögliche Komponenten und Schnittstellen eines solchen Systems sind beispielsweise eine integrierte TK-Anlage (ISDN oder VoIP), Druck- und Fileserver, LAN/WLAN- oder Mobilfunk-Zugänge. Die Basis besteht hierbei oft aus einem NAT-fähigen Router mit Paketfilter für den Internet-Zugang. Für diese Aspekte wird auf die weiteren Publikationen des BSI verwiesen, namentlich die IT-Grundschutz-Kataloge (siehe [GSK]) sowie die "Technische Leitlinie Sichere TK-Anlagen" (siehe [TLST-K08]).

C.3.7 Weitere Gefährdungen

Folgende Aspekte sind ebenfalls zu bedenken:

- Die Verfügbarkeit einer DECT-Infrastruktur kann durch Nutzung eines gezielt eingesetzten Störsenders beeinträchtigt werden. Durch das reservierte DECT-Frequenzband sind jedoch zufällige Störungen durch legal betriebene, mit anderen Funkstandards arbeitende Geräte ausgeschlossen.

- Handelsübliche oder speziell manipulierte DECT-Geräte können auch zum Abhören von Raumgesprächen oder zur missbräuchlichen Datenübertragung verwendet werden (siehe hierzu auch [BSI03] und [ÖMS08]). Das Abhören von Raumgesprächen ist insbesondere mit solchen Geräten möglich, die eine sogenannte Babyfon-Funktion unterstützen.

- Mit Hilfe von Protokollanalysatoren kann überwacht werden, ob und wie oft über einen bestimmten FP – verschlüsselt oder unverschlüsselt – telefoniert wird, somit können ggf. Kommunikationsprofile erstellt werden (siehe [BSI03] und [ÖMS08] zum Thema Kommunikationsprofile).

- Sofern die Mobilstationen auch über Möglichkeiten des SMS/MMS-Empfangs (Short Message Service / Multimedia Messaging Service) sowie der Over the Air-Konfiguration verfügen, sind diese Aspekte ebenfalls zu berücksichtigen. Weitere Informationen zu diesen Themen sind der Veröffentlichung „Öffentliche Mobilfunknetze und ihre Sicherheitsaspekte“ des BSI zu entnehmen (siehe [ÖMS08]).

C.4 Schutzmaßnahmen

Nachfolgend werden entsprechende Maßnahmen beschrieben, um die aufgeführten Gefährdungen zu minimieren oder auszuschließen.

C.4.1 Nutzung von alternativen Techniken

Aufgrund der dargestellten Gefährdungen und der als schwach einzustufenden Sicherheitsmechanismen bei DECT und CAT-iq kann eine Maßnahme in der Vermeidung dieser Techniken für die vertrauliche Kommunikation bestehen. Dies bezieht sich nicht nur auf die Telefonie, sondern jegliche Dienste und Anwendungen, die auf Basis von DECT genutzt werden und keine weiterreichenden Sicherheitsmechanismen besitzen.

In diesem Fall sollte eine Evaluierung alternativer Techniken erfolgen, beispielsweise Voice over WLAN (VoWLAN) oder Mobilfunk. Dabei muss allerdings der erhöhte Stromverbrauch von WLAN-Geräten berücksichtigt werden.

C.4.2 Gezielte Produktauswahl

Bei der Beschaffung von DECT-Geräten sollte als Mindestkriterium eine Verschlüsselung gelten. Zusätzlich sollte die Authentisierung beidseitig zwischen FP und PP unterstützt werden. Es ist durch gezielte Produktauswahl darauf zu achten, dass eine Verschlüsselung nicht nur vom PP unterstützt wird, sondern auch von den FPs, da die Übertragung sonst unverschlüsselt erfolgt (siehe Kapitel C.3.2.2). Hier kann der Benutzer meist nicht aktiv eingreifen und eine Konfiguration wählen, die einen PP, der keine Verschlüsselung unterstützt, abweist. Wünschenswert wäre in diesem Zusammenhang eine Anzeige auf dem PP, ob eine verschlüsselte Verbindung genutzt wird, sowie eine Konfigurationsoption zum Erzwingen einer verschlüsselten Verbindung. Auch die Authentisierung des FPs durch den PP ist eine optionale Funktion des Standards und sollte explizit angefragt werden.

Sofern die Verschlüsselung und gegenseitige Authentisierung nicht in den Produktunterlagen aufgeführt ist, sollte eine Anfrage an den Hersteller gestellt werden. Je nach Anforderung kann eine Überprüfung durch entsprechendes Messequipment eine sinnvolle Maßnahme darstellen.

Für den erhöhten Schutzbedarf ist von der Nutzung von DECT abzuraten, sofern die Sicherheit nur auf den bisherigen DECT-Mechanismen DSAA und DSC basiert. Mögliche Alternativen schnurloser Telefonie bestehen in der Verwendung von VoWLAN oder Mobilfunksystemen.

C.4.3 Gesicherte Montage bzw. Aufstellung eines FP

Um die Anmeldung fremder PPs an einem FP zu vermeiden, sind materielle Sicherungsmaßnahmen zu empfehlen, die den unautorisierten Zugriff auf einen FP verhindern.

Die gesicherte Montage eines FP ist weiterhin bei der Verwendung eines FP mit Ethernet-Anschluss (siehe Kapitel C.1.4) sehr wichtig, da ein Zugriff auf den Ethernet-Anschluss einen Angriff auf die gesamte LAN-Infrastruktur gestattet, an die der FP angeschlossen ist.

C.4.4 Überprüfung und Anpassung von Voreinstellungen

Grundsätzlich ist es empfehlenswert, die vom Hersteller voreingestellten, oft unsicheren Konfigurationen zu überprüfen und – wenn nötig und möglich – zu ändern. Insbesondere die PINs sollten nicht-trivial und mit größtmöglicher Länge gewählt werden. Dies verhindert ebenfalls den bei CAT-iq vorgesehenen Easy Pair-Modus. Für diesen Punkt empfiehlt es sich generell, die Produktunterlagen nach sicherheitsrelevanten Einstellungen zu prüfen.

Sofern eine Verschlüsselung erzwungen werden kann, sollte dies unbedingt aktiviert werden.

C.4.5 Erzwingung von Verschlüsselung

Sofern das Produkt (FP oder PP) die Verschlüsselung durch eine entsprechende Konfigurationsoption erzwingen kann, sollte dies aktiviert werden. Gegebenenfalls kann der Hersteller konsultiert werden, ob eine solche Funktion vorgesehen ist bzw. durch ein Firmware-Upgrade ermöglicht werden kann.

C.4.6 Erzwingung einer gegenseitigen Authentisierung

Es sollte überprüft werden, ob der FP eine Authentisierung des PP durchführt und erzwingen kann. Dies gilt ebenso für den PP, der eine Authentisierung des FP unterstützen und erzwingen sollte. In der Praxis wird dies in den seltensten Fällen in den Produktunterlagen aufgeführt und auch die Konstellation von FP und PP ist hier entscheidend. Gewissheit bringt im Regelfall nur eine Aufzeichnung des Authentisierungsvorgangs mit einem Protokollanalysator.

C.4.7 Deaktivierung von nicht benötigen Diensten und Schnittstellen

Nicht genutzte Dienste und Schnittstellen sowohl des FP als auch des PP sollten deaktiviert werden. Dies beinhaltet beispielsweise eine Bluetooth-Funktionalität oder SMS/MMS-Dienste des PP. Auch hier sollten die Produktunterlagen konsultiert werden.

C.4.8 Durchführung von Subscription in sicherer Umgebung

Die On-Air-Subscription von PPs an die FPs sollte in einer gesicherten Umgebung vorgenommen werden, die einem Angreifer einen Lauschangriff zur Ermittlung der Subscription-Parameter möglichst nicht gestattet.

C.4.9 Aktivierung der bedarfsgerechten Regelung der Sendeleistung

Um die Ausbreitung der Funkwellen zu minimieren, sollte die bedarfsgerechte Regelung der Sendeleitung genutzt werden. Aufgrund der zum Teil unterschiedlich definierten Begriffe ECO-Modus, ECO-Modus-Plus und Low Radiation (LR) sollte im Zweifel der Hersteller konsultiert werden. Einige dieser Funktionen gelten nur unter bestimmten Bedingungen (z.B. nur eine Mobilstation, welche sich in der Ladevorrichtung der Basisstation befinden muss). CAT-iq sieht für die bedarfsgerechte Regelung der Sendeleistung der Basisstation die Funktion „Adapted Power Control“ vor.

Weitere Details hierzu sind in Kapitel C.1.2.1 dargestellt.

C.4.10 Verzicht auf DECT-Repeater

Aufgrund der in der Regel erforderlichen – manuellen oder automatischen – Deaktivierung der Verschlüsselung beim Einsatz von DECT-Repeater sollte auf deren Nutzung verzichtet werden. Wenn möglich sollten stattdessen zusätzliche FPs genutzt werden.

C.4.11 Absicherung IP-fähiger FPs

Die Absicherung von IP-fähigen FPs sollte mindestens aus der Maßnahme C.4.5 bestehen. Weitere Maßnahmen können je nach Funktionsumfang auf Basis der IT-Grundschutz-Kataloge für die IT-Systeme Router und Switches bzw. Sicherheits-Gateways (Firewalls) ergänzt werden. Zusätzlich sollten die Produktunterlagen auf mögliche Sicherheitsmaßnahmen bzw. Empfehlungen geprüft werden.

Insbesondere bei der Kopplung mit einer IP-basierten Infrastruktur sollte die DECT/CAT-iq-Infrastruktur als unsicheres Medium angesehen und entsprechend restriktiv behandelt werden. Entsprechende Mittel hierzu sind beispielsweise Firewall-Systeme. Weitere Details zu dieser Thematik finden sich in Kapitel A. Funk-LAN (WLAN, IEEE 802.11).

Häufig anzutreffende Maßnahmen beinhalten weiterhin:

- Aktivierung von Verschlüsselung für die Administration des FP (z.B. Nutzung von HTTPS)
- Deaktivierung einer Fernwartung. Die Administration sollte möglichst nur über eine Schnittstelle erfolgen (z.B. LAN). Wenn eine Fernwartung nicht zwingend erforderlich ist, sollte keine Kopplung an bestehende IP-Netze erfolgen.
- Der FP sollte in den Prozess der Software-Pflege eingebunden werden.

C.4.11.1 Absicherung des IP-Anlagenanschlusses

Für die Absicherung des IP-Anlagenanschlusses wird auf die „Technische Leitlinie Sichere TK-Anlagen“ des BSI verwiesen (siehe [TLSTK08]).

Häufig bieten IP-basierte FPs nicht den Funktionsumfang von dedizierten TK-Systemen zur Anbindung an einen IP-Anlagenanschluss. Hier kann der Verzicht auf den IP-Anlagenanschluss eine mögliche Maßnahme darstellen.

C.4.11.2 Absicherung IP-basierter Dienste

Die Absicherung IP-basierter Dienste baut primär auf der Maßnahme C.4.5 auf. Für jeden der verbliebenen Dienste (siehe auch Gefährdung C.3.5.1) existiert eine Vielzahl an applikationsspezifischen Sicherheitsmaßnahmen. Im Rahmen dieses Dokumentes kann auf diese nicht im Detail eingegangen werden. Hier wird auf die Publikationen des BSI sowie die empfohlenen Sicherheitsmechanismen der jeweiligen Dienste verwiesen, z.B. Nutzung von SSL/TLS (Secure Sockets Layer / Transport Layer Security) für E-Mail und Instant Messaging.

C.4.12 Absicherung von Kombigeräten

Nach Möglichkeit sollte auf den Einsatz von Kombigeräten verzichtet werden. Stattdessen sollten die gewünschten Funktionen separat ausgelegt werden, beispielsweise WLAN Access Point, DECT FP usw.

Sollten Kombigeräte dennoch zum Einsatz kommen, muss jede Schnittstelle und Funktion einzeln betrachtet werden. Die Gefährdung durch übergreifende Effekte wird dadurch verringert. Für spezifische Maßnahmen zu einzelnen Schnittstellen und Funktionen wird auf die jeweiligen Kapitel dieses Dokuments sowie die Publikationen des BSI verwiesen.

C.4.13 Weitere Schutzmaßnahmen

Über die bereits genannten Maßnahmen hinaus sollten insbesondere bei der Nutzung von DECT oder CAT-iq für die Datenübertragung in Abhängigkeit des individuellen Schutzbedarfs weitere Schutzmaßnahmen implementiert werden, wie z.B.

- Nutzung von Sicherheitsmechanismen auf höheren Schichten, z.B. auf IP-Ebene
- Benutzerauthentisierung
- Virenschutz
- Personal Firewall
- restriktive Datei- und Ressourcen-Freigabe auf Betriebssystemebene
- Einsatz von zusätzlicher Verschlüsselung und Integritätsschutz, unabhängig von den DECT-Mechanismen greifend, z.B. VPN-Tunnel

Wenn möglich, sollte eine Ende-zu-Ende-Verschlüsselung zwischen den kommunizierenden Teilnehmern genutzt werden.

Informationen hierzu findet man in den IT-Grundschutz-Katalogen des BSI (siehe [GSK]).

C.5 Ausblick

Es ist eine Zunahme von Kombigeräten festzustellen, die neben DECT auch weitere Schnittstellen wie z.B. Ethernet, WLAN, Mobilfunk oder Bluetooth besitzen. Insbesondere sind hier CAT-iq-Geräte zu nennen. Neben der generellen Zusammenlegung von Schnittstellen und Funktionen innerhalb eines Geräts ist insbesondere die Verbindung von DECT und Internet-Diensten (z.B. E-Mail, RSS-Feeds, Instant Messaging oder Internet-Radio) als äußerst kritisch zu betrachten, da insbesondere die Sicherheitsmechanismen auf DECT-Ebene nicht verbessert wurden.

Auch die Nutzung eines Kombigeräts für den IP-basierten PSTN-Zugang über einen IP-Anlagenanschluss nimmt zu. Die Anbindung an das PSTN erfolgt hierbei nicht länger über ISDN, sondern IP-basiert über das Internet. Die Sprachdaten werden per VoIP in der Regel unverschlüsselt übertragen, bei gleichzeitig höherem Gefährdungspotenzial. Die hierfür genutzten Kombigeräte und die VoIP-Dienstleister bieten in der Regel keine oder nur minimale Sicherheitsmechanismen an. In diesem Bereich ist eine Verbesserung erforderlich. Dennoch könnten diese Geräte Sicherheitsmechanismen auf Basis von IP oder höher nutzen, da der Transport von IP explizit in CAT-iq vorgesehen ist. Dies würde die Nutzung von als sicher geltenden Algorithmen ermöglichen und damit eine deutliche Aufwertung der Sicherheit bei DECT bedeuten.

C.6 Fazit

DECT bietet insgesamt einen höheren Sicherheitsstandard als analoge Schnurlos-Standards, bei denen bereits ein Funkscanner zum Abhören der Telefonate ausreicht. Allerdings gibt es auf dem Markt auch zahlreiche Geräte, bei denen die DECT-Verschlüsselung überhaupt nicht implementiert ist. Über einfach zu erwerbendes Equipment sowie im Internet verfügbare Anleitungen und Software lassen sich unverschlüsselte DECT-Gespräche heutzutage relativ einfach abhören. Spezialequipment und tiefer gehende Kenntnisse von DECT sind hierfür nicht erforderlich.

Mittlerweile sind Inhalte der durch ETSI nicht allgemein zugänglichen Algorithmen DSAA und DSC öffentlich bekannt geworden und verdeutlichen die nur geringe Sicherheit dieser Mechanismen. Insbesondere für als kritisch einzustufende Anwendungen kann daher nur dringend von DECT abgeraten werden, sofern keine weitergehenden Mechanismen zum Einsatz kommen. Hier sollten die Alternativen Voice over WLAN (VoWLAN) oder Mobilfunk in Betracht gezogen werden.

Dies gilt umso deutlicher bei der Nutzung von CAT-iq, da hier zusätzliche Schnittstellen und Funktionen implementiert sind, ohne die Sicherheit zu erhöhen. Dies führt im Vergleich zu DECT zu einem geringeren Sicherheitsniveau. An dieser Stelle ist eine Verbesserung der Sicherheit bei CAT-iq seitens des DECT-Forums erforderlich. Die Nutzung von IP als generischem Träger ermöglicht weiterhin die Absicherung auf höheren Ebenen, z.B. mittels SSL/TLS.

C.7 Literatur und Links

Ausführliche Informationen zur DECT-Spezifikation in deutscher Sprache kann man u.a. dem Buch [Wa01] entnehmen. Es gibt zahlreiche Bücher und Publikationen zum Thema DECT. Die Liste der hier aufgeführten Titel und Links stellt nur eine wertungsfreie Auswahl ohne Anspruch auf Vollständigkeit dar.

Informationen zu DECT und CAT-iq enthalten die Internet-Seiten [DECTWE], [DECTFO] und [CATIQ].

Informationen und Analysen zur Sicherheit bei DECT, insbesondere zu den Algorithmen DSAA und DSC finden sich unter [DECTSEC] sowie [LSTWW09]. Eine Diskussion verschiedener Schwächen im Sicherheitskonzept von DECT findet man auch in der Spezifikation [EN300175].

[BSI03] „GSM-Mobilfunk, Gefährdungen und Sicherheitsmaßnahmen“, BSI, 2003, https://www.bsi.bund.de/cln_155/ContentBSI/Publikationen/Broschueren/oefms/index_htm.html

[CATIQ] Offizielle CAT-iq-Seite http://www.CAT-iq.org

[DECTFO] DECT-Forum http://www.dect.ch

[DECTSEC] deDECTed https://dedected.org

[DECTWE] DECT-web http://www.dectweb.com

[EN300175] ETSI EN 300 175-1, 300 175-2 bis 300 175-8, „Digital Enhanced Cordless Telecommunications (DECT), Common Interface (CI), Part 1 bis Part 8”, verfügbar unter http://www.etsi-org/

[EN300444] ETSI EN 300 444, „Generic Access Profile (GAP)“, verfügbar unter http://www.etsi-org/

[EN301649] ETSI EN 301 649, „DECT Packet Radio Service (DPRS)“, verfügbar unter http://www.etsi-org/

[EN301650] ETSI EN 301 650, „DECT Multimedia Access Profile (DMAP)“, verfügbar unter http://www.etsi-org/

[GSK] Bundesamt für Sicherheit in der Informationstechnik, „IT-Grundschutz-Kataloge“, verfügbar unter https://www.bsi.bund.de/cln_155/DE/Themen/weitereThemen/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

[LSTWW09] S. Lucks, A. Schuler, E. Tews, R-P. Weinmann, M. Wenzel, „Attacks on the DECT authentication mechanisms“, RSA Conference, 2009

[MENG09] Alexandra Mengele, „Security of Digital Enhanced Cordless Telecommunication (DECT) devices for residential use“, TU Darmstadt, 2009

[ÖMS08] Bundesamt für Sicherheit in der Informationstechnik, „Öffentliche Mobilfunknetze und ihre Sicherheitsaspekte“, 2008, https://www.bsi.bund.de/cln_155/ContentBSI/Publikationen/Broschueren/oefms/index_htm.html

[TLSTK08] „Technische Leitlinie Sichere TK-Anlagen“, BSI, 2008, https://www.bsi.bund.de/cln_155/ContentBSI/Publikationen/Broschueren/tkanlagen/TL02103_htm.html

[TR1025271] ETSI TR 102 527-1, „New Generation DECT; Part 1: Wideband speech”, verfügbar unter http://www.etsi-org/

[TR1025272] ETSI TR 102 527-2, „New Generation DECT; Part 2: Support of transparent IP packet data“, verfügbar unter http://www.etsi-org/

[TR102570] ETSI TR 102 570, „New Generation DECT; Overview and Requirements“, verfügbar unter http://www.etsi-org/

C.8 Abkürzungen

AC	Authentication Code
ADPCM	Adaptive Differential Pulse Code Modulation
ARP	Address Resolution Protocol
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAT-iq	Cordless Advanced Technology – internet and quality
CI	Common Interface (DECT)
CK	Cipher Key
CLIP	Calling Line Identification Presentation
CT	Cordless Telephone
C-Plane	Control Plane
DAM	DECT Authentication Module
DB	Data Base
DCK	Derived Cipher Key
DECT	Digital Enhanced Cordless Telecommunications
DFS	DECT Fixed System
DHCP	Dynamic Host Configuration Protocol
DLC	Data Link Control
DMAP	DECT Multimedia Access Profile
DoS	Denial of Service
DPRS	DECT Packet Radio Service
DSAA	DECT Standard Authentication Algorithm
DSC	DECT Standard Cipher
DSCA	DECT Standard Cipher Algorithm
EC	Electronic Cash
EN	European Norm (ETSI)
ETSI	European Telecommunications Standards Institute
FDM	Frequency Division Multiplex, Frequenzmultiplex
FP	Fixed Part, DECT-Feststation
GAP	Generic Access Profile
GMSK	Gaussian Minimum Shift Keying
HGI	Home Gateway Initiative
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPv4	Internet Protocol Version 4

IPv6	Internet Protocol Version 6
ISDN	Integrated Services Digital Network
IT	Information Technology
ITSP	Internet Telephony Service Provider
IV	Initialisierungsvektor
IWF	Interworking Functions
IWU	Interworking Unit
LAN	Local Area Network
LLC	Logical Link Control
LR	Low Radiation
MAC	Medium Access Control
MMS	Multimedia Messaging Service
NAT	Network Address Translation
NDA	Non-Disclosure Agreement
NG DECT	Next Generation DECT
NGN	Next Generation Network
OSI	Open System Interconnection
PARK	Portable Access Rights Key
PCMCIA	Personal Computer Memory Card International Association
PHY	Physical Layer (IEEE)
PIN	Personal Identification Number
PP	Portable Part, DECT-Mobilstation
PRNG	Pseudo-Random Number Generator
PSTN	Public Switched Telephone Network
POP3	Post Office Protocol Version 3
RARP	Reverse Address Resolution Protocol
RFP	Radio Fixed Part
RFPI	Radio Fixed Part Identity
RSS	Really Simple Syndication (für Version 2.0)
RTP	Real-Time Transport Protocol
SCK	Static Cipher Key
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMS	Short Message Service
SPIT	Spam over Internet Telephony
SSL	Secure Sockets Layer
SUOTA	Software Update Over The Air
TCP	Transmission Control Protocol
TDD	Time Division Duplex, Zeitduplex
TDM	Time Division Multiplex, Zeitmultiplex

TDMA	Time Division Multiple Access
TK	Telekommunikation
TLS	Transport Layer Security
TPUI	Temporary User Identity
TR	Technical Report (ETSI)
TS	Technical Specification (ETSI)
UAK	User Authentication Key
UDP	User Datagram Protocol
UPI	User Personal Identity
U-Plane	User Plane
VoIP	Voice over IP
VoWLAN	Voice over WLAN
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WLL	Wireless Local Loop
WRS	Wireless Relay Station, DECT-Repeater
XMPP	Extensible Messaging and Presence Protocol
XOR	Exklusives Oder

C.9 Glossar

Authentisierung

Verifizierung der Identität einer Instanz, z.B. eines Benutzers oder eines Geräts. Zweck ist oft die anschließende Autorisierung für Zugriffe. Ohne Authentisierung ist im Allgemeinen keine sinnvolle Autorisierung möglich.

Audio-Codec

Siehe Sprach-Codec

Codec

Es handelt sich um eine Wortkreuzung aus den englischen Begriffen „coder“ und „decoder“. Ein Codec bezeichnet ein Verfahren, mit dem analoge Informationen in digitale Informationen umgewandelt werden.

Chiffrier-Schlüssel (Cipher Key, CK)

Dient zusammen mit einem Initialisierungsvektor zur Erzeugung eines Schlüsselstroms, mit dem der Klartext über ein XOR verknüpft und verschlüsselt wird.

Downlink

Frequenz-Zeit-Kanal, in dem der FP zum PP sendet.

Fixed Part (FP)

DECT-Feststation, die als Basisstation die Funkverbindung mit dem Portable Part und mit der Festnetzseite unterhält.

Paging

Ausrufen eines Teilnehmers in einem Teil des Mobilfunknetzes, verbunden mit der Bitte, dass sich das Gerät des Teilnehmers meldet.

Persönliche Identifikationsnummer (PIN)

4- bis 8-stellige Geheimnummer, die zur Authentisierung des Benutzers dient.

Portable Part (PP)

DECT-Mobilstation

Sprach-Codec

Ein Sprach-Codec kodiert und dekodiert Sprachinformationen nach einem bestimmten Verfahren, wobei sowohl das sendende als auch das empfangende Gerät den gleichen Kodierungsstandard für die Sprachübertragung unterstützen müssen. Zusätzlich wird eine Datenkompression des digitalen Signals vorgenommen.

Subscription

Anmeldung eines PP bei einem FP

User Authentication Key (UAK)

Langzeitgeheimnis für die Authentisierung

Uplink

Frequenz-Zeit-Kanal, den der PP zum Senden an den FP verwendet.

D. WiMAX, IEEE 802.16

Inhaltsverzeichnis des Abschnitts

D.1 Grundlagen und Funktionalität

WiMAX (Worldwide Interoperability for Microwave Access) ist ein Industriestandard, der auf den Standards der Serien IEEE 802.16 und ETSI HIPERMAN (High Performance Radio MAN[1]) basiert. Inhalt dieser Standards ist die Spezifikation eines drahtlosen Breitband-MAN. Das WiMAX-Forum ist verantwortlich für die WiMAX-Spezifikationen und unterstützt die Entwicklung von standardkonformen und interoperablen Produkten. Die Rolle des WiMAX-Forums ist vergleichbar mit der Rolle der Wi-Fi Alliance im WLAN-Bereich.

Der Standard IEEE 802.16 hat in der ersten veröffentlichten Version von 2001 unter dem Titel „Air Interface for Fixed Broadband Wireless Access System" lediglich eine Kommunikation zwischen ortsfesten Stationen beschrieben. Die Kommunikation erfolgt dabei zwischen einer zentralen Base Station (BS) und mehreren stationären Subscriber Stations (SS). Ursprünglich wurde im Jahr 2001 diese Funkschnittstelle für Frequenzen zwischen 10 GHz und 66 GHz festgelegt. Problem dieses Frequenzbereichs ist es allerdings, dass eine Sichtverbindung (Line-of-Sight, LOS) zwischen Sender und Empfänger bestehen muss. Die Verbindung soll unter Idealbedingungen eine Datenrate von 70 Mbit/s und Reichweiten von bis zu 50 km erreichen können. Es bestand jedoch ein größeres Interesse, den Frequenzbereich zwischen 2 GHz und 11 GHz für eine drahtlose MAN-Technik zu etablieren, da damit keine Sichtverbindung mehr erforderlich ist. Der daraus entstandene Standard ist IEEE 802.16-2004 und wird auch Fixed WiMAX genannt, da auch in diesem Standard nur ortsfeste Subscriber Stations beschrieben werden. Nachfolgend bezieht sich die Bezeichnung IEEE 802.16 auf den Standard IEEE 802.16-2004 (siehe [IEEE04]).

Die Erweiterung um die direkte Unterstützung mobiler Endgeräte ist in der Ergänzung IEEE 802.16e-2005 spezifiziert und im Februar 2006 veröffentlicht worden. Nachfolgend bezieht sich die Bezeichnung IEEE 802.16e auf den Standard IEEE 802.16e-2005 (siehe [IEEE05]). Dieser Standard wird auch als Mobile WiMAX bezeichnet. Mobile WiMAX ist für Geschwindigkeiten von bis zu 125 km/h ausgelegt.

Mittlerweile ist IEEE 802.16e in den Standard IMT-2000 (International Mobile Telecommunication) für 3G-Mobilfunknetze der ITU aufgenommen worden. Intensiviert wird das Thema Mobilfunk mit dem derzeit in Entwicklung befindlichen Standard IEEE 802.16m. Das Ziel hierbei ist eine Aufnahme in den Standard IMT-Advanced für Mobilfunknetze der vierten Generation (4G). IEEE 802.16m wird in diesem Dokument nicht weiter betrachtet.

Mitte 2009 wurde der Standard IEEE 802.16-2009 veröffentlicht, welcher neben Ergänzungen und Korrekturen insbesondere 802.16-2004 und IEEE 802.16e-2005 in einem Dokument zusammenfasst.

Im Folgenden werden die beiden aktuellen Standards IEEE 802.16 und IEEE 802.16e kurz vorgestellt. In den weiteren Kapiteln werden dann die spezifizierten Sicherheitsfunktionen beschrieben, mögliche Gefahren analysiert und entsprechende Gegenmaßnahmen empfohlen.

D.1.1 Fixed WiMAX (IEEE 802.16)

Fixed WiMAX nach dem Standard IEEE 802.16 dient primär zur Überbrückung der sogenannten letzten Meile zum Teilnehmeranschluss und ist daher zunächst für Netzbetreiber von Interesse. Der Schwerpunkt liegt hier insbesondere in der Versorgung von Regionen ohne kabelgebundenen Breitbandanschluss (z.B. auf Basis von DSL, Digital Subscriber Line). Auch die Anbindung von DSL-Vermittlungsstellen (Digital Subscriber Line Access Multiplexer, DSLAM) per Fixed WiMAX ist eine

1 MAN = Metropolitan Area Network

mögliche Option. Weiterhin kann Fixed WiMAX eine Alternative für Richtfunkstrecken sein, die beispielsweise zur Ankopplung von Mobilfunk-Netzelementen verwendet werden. Für Unternehmen ist WiMAX als Redundanz zu bestehenden Netzanbindungen (z.B. Internet) interessant. Für Unternehmen, die grundstücksübergreifend verschiedene Gelände in einem Radius von mehreren Kilometern vernetzen müssen, kann WiMAX eine Alternative zur Anbindung über ein öffentliches Netz sein. Außerdem kann WiMAX prinzipiell auch in Backbone-Netzen und als WLAN Distribution System eingesetzt werden. WiMAX ermöglicht die Nutzung von flexiblen Bandbreiten und QoS für die angeschlossenen Geräte.

D.1.1.1 Architektur

Fixed WiMAX unterscheidet zwei Kommunikationsformen:

- Point-to-Multipoint-Modus (siehe Abbildung D-1)
- Mesh-Modus (siehe Abbildung D-2)

Abbildung D-1: Point-to-Multipoint-Modus (Beispiel)

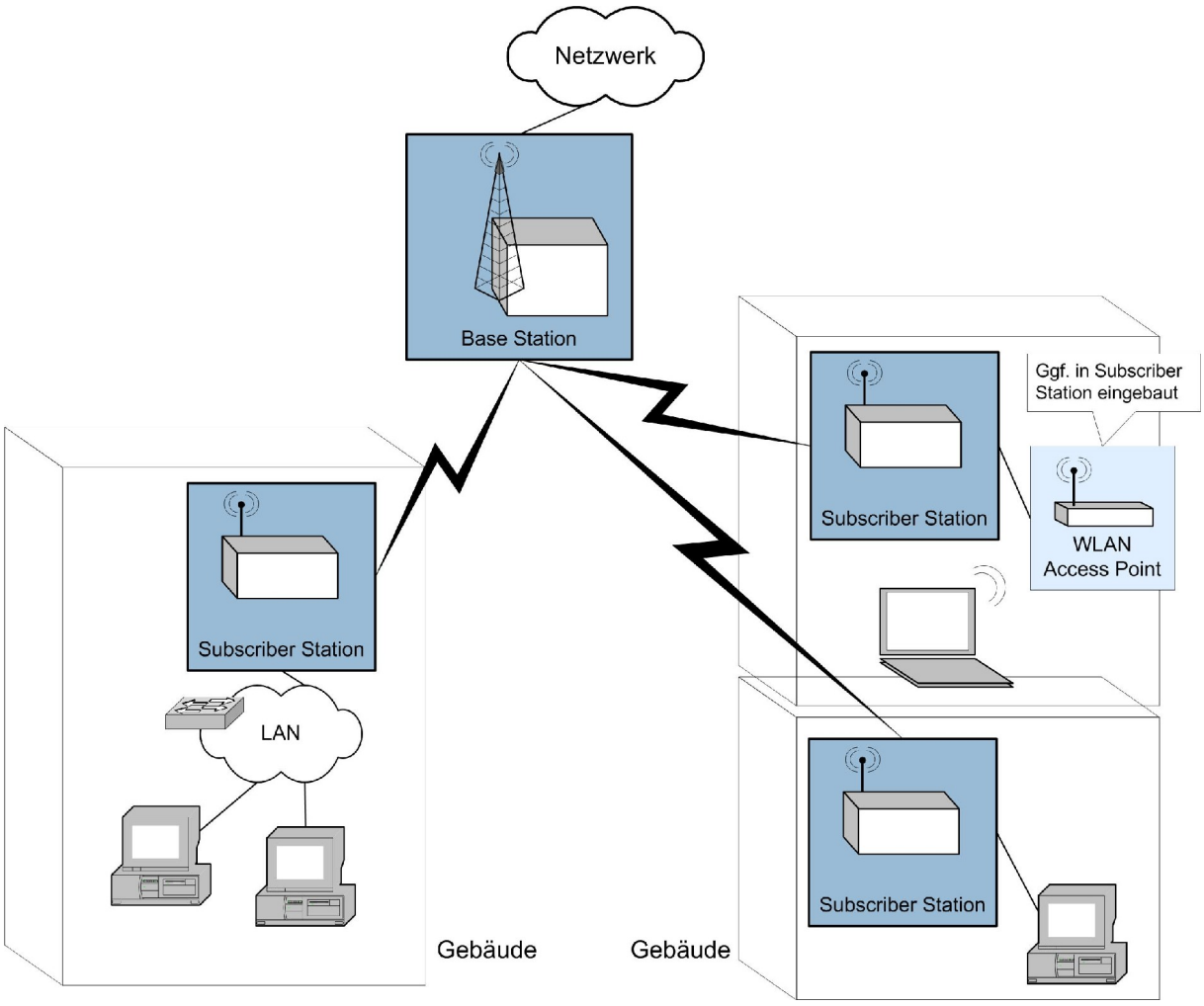
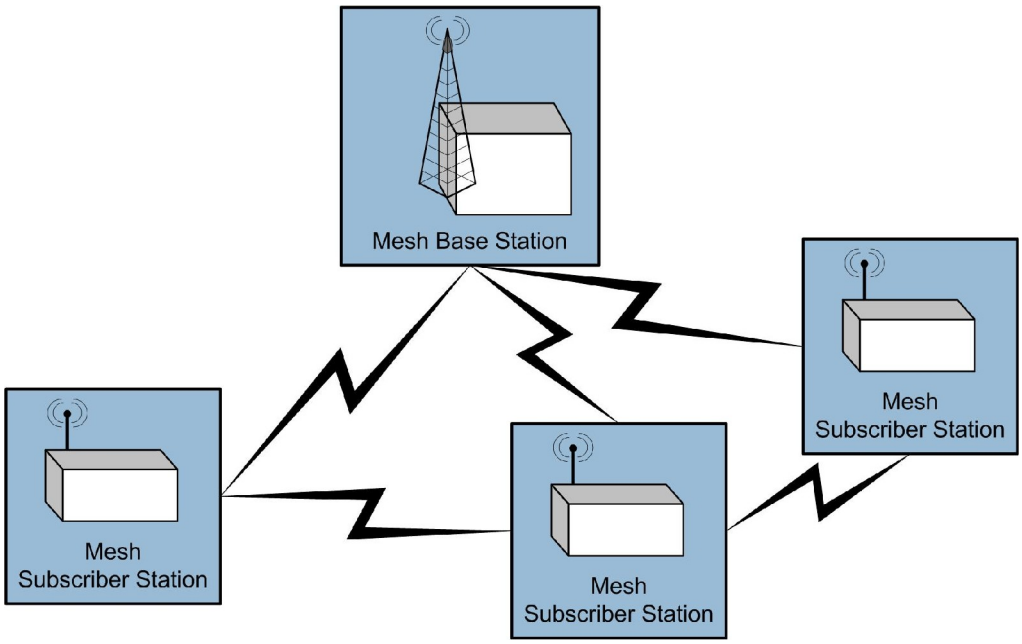


Abbildung D-2: Mesh-Modus (Beispiel)



Im Point-to-Multipoint-Modus sendet die Base Station (Basisstation) über eine Sektorenantenne die Daten an alle Subscriber Stations in diesem Sektor[2]. Die Subscriber Stations übernehmen nur die Pakete, die für ihre Verbindung gültig sind. Auch Multicast (z.B. Video) oder Broadcast-Verbindungen sind möglich. Die Kommunikation erfolgt immer zwischen der Base Station und den Subscriber Stations. Eine direkte Kommunikation zwischen verschiedenen Subscriber Stations ist nicht erlaubt. Dies ist dagegen im Mesh-Modus möglich. Eine Subscriber Station im Mesh-Modus wird auch Mesh Subscriber Station genannt. Die Mesh Base Station ist diejenige Station, die eine direkte Verbindung zu Stationen außerhalb des Funknetzes hat. Die Kommunikation zu diesem externen Netz kann entweder direkt von den Mesh Subscriber Stations zur Mesh Base Station erfolgen oder über mehrere Mesh Subscriber Stations geroutet werden. Auch eine direkte Kommunikation zwischen den Mesh Subscriber Stations ist möglich, ohne dass diese eine Verbindung zum externen Netz oder der Mesh Base Station haben.

Der IEEE-Standard 802.16 spezifiziert die physikalische Übertragung (Physical Layer) und den Kanalzugriff (Medium Access Control, MAC) zwischen Base Station und Subscriber Stations bzw. zwischen Subscriber Stations.

D.1.1.2 Physikalische Übertragung

Der Standard spezifiziert verschiedene physikalische Übertragungsverfahren, die sich primär in der Nutzung der Frequenzbänder und der verwendeten Modulationsverfahren unterscheiden:

- WirelessMAN-SC

  WirelessMAN-SC ist für die Nutzung von Frequenzen zwischen 10 GHz und 66 GHz spezifiziert worden. Dabei sollen unter Idealbedingungen (Sichtverbindung zwischen Sender und Empfänger, Line-of-Sight, LOS[3]) Datenraten von 70 Mbit/s und Reichweiten von bis zu 50 km erreicht werden können.

---

2 Die Subscriber Station bildet den Teilnehmeranschluss mit einer WiMAX-Luftschnittstelle auf der einen Seite und beispielsweise einem oder mehreren Ethernet-Anschlüssen oder einem integrierten WLAN Access Point auf der anderen Seite.

- WirelessMAN-SCa

  Dieses Übertragungsverfahren ist von WirelessMAN-SC abgeleitet und für die Nutzung von Frequenzen unter 11 GHz ausgelegt. Damit sind dann auch NLOS-Verbindungen (Non-LOS-Verbindungen) möglich.

- WirelessMAN-OFDM

  Die Spezifikationen für WirelessMAN-OFDM beschreiben die Nutzung von Frequenzen unter 11 GHz. Auch hier sind NLOS-Verbindungen möglich. Als Modulationsverfahren kommt OFDM (Orthogonal Frequency Division Multiplexing) zum Einsatz.

- WirelessMAN-OFDMA

  Diese Variante basiert ähnlich zu WirelessMAN-OFDM auf OFDM und ist für Frequenzen unter 11 GHz und NLOS-Verbindungen geeignet. Darüber hinaus wird ein Mehrfachzugriff mit orthogonalen Unterträgern spezifiziert, d.h. die Aufteilung des Mediums auf mehrere Nutzer wird bei OFDMA durch die physikalische Übertragung (in Ergänzung zum MAC-Protokoll) unterstützt.

- WirelessHUMAN

  WirelessHUMAN sieht die Nutzung des 5-GHz-Bereichs vor. Das Kanalraster wurde aus Interferenzgründen an die Frequenzen von WLAN nach IEEE 802.11a angepasst. Die sonstigen Spezifikationen basieren entweder auf WirelessMAN-SCa oder WirelessMAN-OFDM oder WirelessMAN-OFDMA.

In Deutschland regelt die Bundesnetzagentur die Vergabe der Frequenzen für WiMAX-Netze im Rahmen des sogenannten Broadband Wireless Access (BWA). Im Dezember 2006 wurde ein Teil der Frequenzen im Bereich 3600 MHz bis 3800 MHz versteigert [BNA06]. Die Bieter haben sich damit verpflichtet, in den jeweiligen Regionen eine Versorgung von 15% bis Ende 2009 und 25% bis Ende 2011 zu gewährleisten. Noch verfügbare Frequenzen in diesem Bereich sollen im Jahr 2009 standortspezifisch vergeben werden[4]. Die Vergabe nach Standort und nicht nach Region wurde gewählt, um Interferenzen mit bestehenden Funkeinrichtungen, speziell der Satellitenkommunikation zu vermeiden.

Weiterhin plant die Bundesnetzagentur weitere Frequenzen für die Breitbandversorgung, u.a. mittels WiMAX, zur Verfügung zu stellen. Hierzu zählt beispielsweise der Bereich um 2,6 GHz. Auch der Bereich um 5,8 GHz (Broadband Fixed Wireless Access, BFWA) kann für WiMAX genutzt werden. Allerdings ist der Bereich bereits einem Primärnutzer zugeteilt, sodass keine exklusive Nutzung des Frequenzspektrums möglich ist. Weitere Details bezüglich BFWA finden sich in Kapitel E. Richtfunktechniken.

D.1.1.3 MAC Layer

Der MAC Layer ist im WiMAX-Standard in drei Sublayer aufgeteilt (siehe Abbildung D-3):

- Der Service Specific Convergence Sublayer (CS) dient der Anpassung an verschiedene Netzwerkprotokolle, um beispielsweise eine Kompatibilität sowohl zu ATM-Netzen als auch zu IP-Netzen zu gewährleisten.

- Der Common Part Sublayer (CPS) enthält die Kernfunktionen des MAC Layer wie Verbindungsaufbau, Bandbreiteneinteilung und Verbindungshaltung.

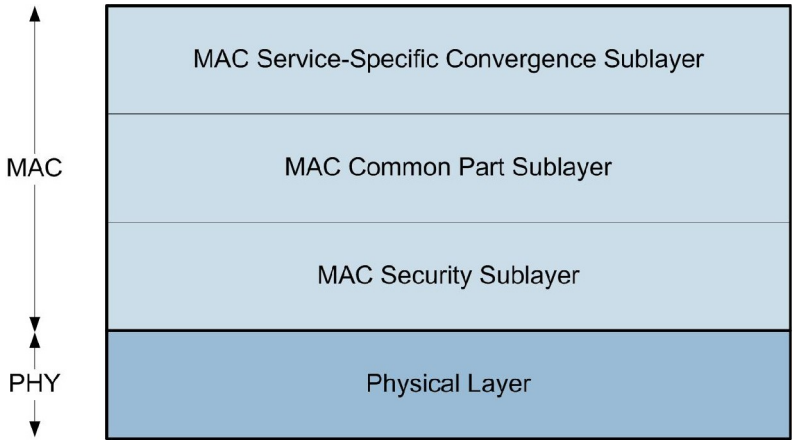
---

3 Sichtverbindung bedeutet hier stets eine funktechnische (nicht optische) Sichtverbindung. Dabei muss ein spezielles Ellipsoid mit einer gewissen Ausdehnung zwischen Sender und Empfänger weitestgehend frei von Hindernissen sein. Dies ist die sogenannte Fresnel-Zone.

4 http://www.bundesnetzagentur.de/enid/Frequenzordnung/Broadband_Wireless_Access__BWA__2qc.html

► Die Sicherheitsfunktionen bilden den Security Sublayer. Diese werden im Kapitel D.2.1 beschrieben.

Abbildung D-3: Struktur des MAC-Layer



Eine wichtige Aufgabe des MAC Common Part Sublayer (MAC CPS) ist der Netzeintritt der Subscriber Station. Eine eindeutige 48 Bit lange MAC-Adresse dient hierbei als Identifizierungsmerkmal für die Luftschnittstelle der Subscriber Station. Der Netzeintritt im Point-to-Multipoint-Modus kann in folgende Phasen unterteilt werden:

A. Auffinden einer Base Station (Scan) und Synchronisation: Nach einem Signalverlust oder während des erstmaligen Netzeintritts wird nach einer Base Station gesucht und der Downlink (Richtung Base Station zu Subscriber Station) hergestellt.

B. Einholen der Sendeparameter: Nachdem der Downlink hergestellt ist, wird der Uplink (Richtung Subscriber Station zu Base Station) hergestellt.

C. Ranging: Zu den physikalischen Parametern, die während des sogenannten Ranging justiert werden können, gehören beispielsweise die Sendeleistung oder das Timing der Zeitschlitze. Weiterhin werden die Management-Verbindungen aufgebaut. Diese werden unter anderem für die weiteren Schritte des Netzeintritts benötigt.

D. Aushandlung grundlegender Fähigkeiten: Neben der Übertragung der aktuellen Sendeleistung werden in dieser Phase die maximale Sendeleistung, Modulationsverfahren oder Duplex-Einstellungen ausgehandelt.

E. Authentisierung und Schlüsselaustausch: Die Subscriber Station authentisiert sich in dieser Phase gegenüber der Base Station, kryptographische Verfahren werden ausgehandelt und das Schlüsselmaterial ausgetauscht.

F. Registrierung: In der Phase erfolgt die Autorisierung der Subscriber Station. Verläuft diese erfolgreich, wird der Subscriber Station der Netzzugang gewährt.

G. Herstellen der IP-Konnektivität

H. Synchronisation von Datum und Uhrzeit

I. Übertragung der Konfiguration: Subscriber Stations erhalten in dieser Phase von einem TFTP-Server ihre Konfiguration (gilt für zentral administrierte Subscriber Stations).

Im Rahmen des Netzeintritts werden unterschiedliche Typen von Verbindungen aufgebaut. Generell wird zwischen Management- und Transport-Verbindungen unterschieden. Während Management-Ver-

bindungen bzw. darüber übertragene Nachrichten die eigentliche Verbindung ermöglichen und aufrechterhalten, werden die eigentlichen Nutzdaten (z.B. Web-Kommunikation oder E-Mails) über die Transport-Verbindungen übertragen.

Bei den Management-Verbindungen wird aufgrund verschiedener QoS-Anforderungen zwischen drei Typen unterschieden:

- Basic Connection: Die Basic Connection wird für die Übertragung von kurzen, zeitkritischen MAC-Management-Nachrichten genutzt und in der Phase C. des Netzeintritts aufgebaut.
- Primary Management Connection: Die Primary Connection wird für die Übertragung von längeren, weniger zeitkritischen MAC-Management-Nachrichten genutzt und ebenfalls in der Phase C. des Netzeintritts aufgebaut.
- Secondary Management Connection: Für zeitlich unkritischen IP-basierten Management-Verkehr (z.B. DHCP, TFTP, SNMP) wird die Secondary Management Connection in der Phase F. des Netzeintritts aufgebaut (gilt für zentral administrierte Subscriber Stations).

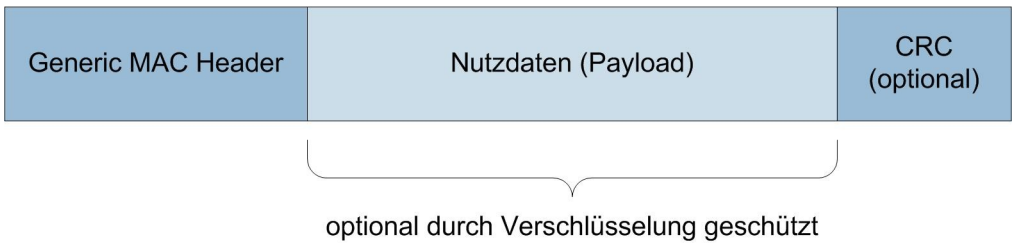
Jede Verbindung zwischen einer Subscriber Station und einer Base Station wird durch einen 16 Bit langen Connection Identifier (CID) bestimmt. Weiterhin arbeiten alle Verbindungen innerhalb des MAC Layer verbindungsorientiert, um eine Zuordnung zwischen Diensten und QoS-Parametern zu Subscriber Stations zu ermöglichen.

Über die Basic Connection sowie die Primary Management Connection werden MAC-Management-Nachrichten übertragen. Diese werden beispielsweise für folgende Aufgaben eingesetzt:

- Ranging
- Austausch der Fähigkeiten
- Registrierung
- Multicast

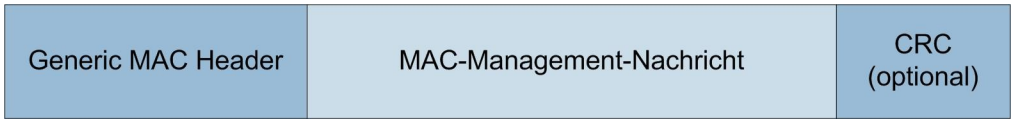
Der allgemeine Aufbau einer Dateneinheit des MAC Layer ist in Abbildung D-4 dargestellt. Optional können die Nutzdaten verschlüsselt werden. Der Generic MAC Header, welcher beispielsweise die MAC-Adresse beinhaltet, wird immer unverschlüsselt übertragen.

Abbildung D-4: Aufbau einer MAC Protocol Data Unit (MAC PDU)



MAC-Management-Nachrichten wiederum werden in Form von Nutzdaten transportiert, wie in Abbildung D-5 illustriert. Je nach physikalischem Übertragungsverfahren ist die Prüfsumme in Form der CRC zwingend. MAC-Management-Nachrichten werden generell unverschlüsselt übertragen, um laut Spezifikation den einwandfreien Betrieb zu gewährleisten.

Abbildung D-5: Aufbau einer MAC Protocol Data Unit mit MAC-Management-Nachricht



Zum Teil werden MAC-Management-Nachrichten, z.B. für den Schlüsselaustausch oder die Registrierung, einer Integritätsprüfung unterzogen. Dies erfolgt mittels eines Message Authentication Code basierend auf einer kryptographischen Hash-Funktion (Keyed-Hash Message Authentication Code, HMAC). Fixed WiMAX nutzt für den HMAC das Verfahren SHA-1 (Secure Hash Algorithm). Alle anderen Datenübertragungen, z.B. Verkehr über die Transport-Verbindungen, sind nicht in die Integritätsprüfung miteinbezogen und somit nicht vor Manipulationen geschützt.

D.1.2 Mobile WiMAX (IEEE 802.16e)

Die als Mobile WiMAX bezeichnete Erweiterung IEEE 802.16e des WiMAX-Standards erlaubt die direkte Anbindung von mobilen Endgeräten. Im Unterschied zu Fixed WiMAX soll Mobile WiMAX ausschließlich Frequenzen in Bereichen unter 11 GHz nutzen.

Die Ergänzung IEEE 802.16e spezifiziert (wie auch der Basisstandard IEEE 802.16) die Protokollebenen zur physikalischen Übertragung und für den Kanalzugriff. Basierend auf IEEE 802.16e hat das WiMAX-Forum ein sogenanntes Profil für Mobile WiMAX spezifiziert, das neben einer Auswahl aus den verschiedenen in IEEE 802.16e spezifizierten Übertragungsmöglichkeiten auch Konzepte für den Aufbau von Mobile-WiMAX-Netzen festlegt (siehe [WiMAX]).

Um den Anforderungen mobiler Endgeräte gerecht zu werden, wurden zusätzliche Funktionen in den Standard aufgenommen. Dazu gehören beispielsweise:

- Handover – die Möglichkeit der Bewegung eines Endgeräts zwischen den Abdeckungsbereichen verschiedener Base Stations unter Aufrechterhaltung der Ende-zu-Ende-Kommunikation, d.h. ohne signifikante Einbußen hinsichtlich der Qualität

- Sleep Mode – ein besonders energiesparender Betriebszustand

Weiterhin wurden für die Unterstützung mobiler Endgeräte Anpassungen im gesamten Protokoll-Stack des Basis-Standards IEEE 802.16 gemacht. Insbesondere wurden einige Sicherheitsfunktionen speziell für mobile Geräte spezifiziert bzw. adaptiert. Diese Funktionen werden in Kapitel D.2.2 vorgestellt.

D.1.2.1 Architektur

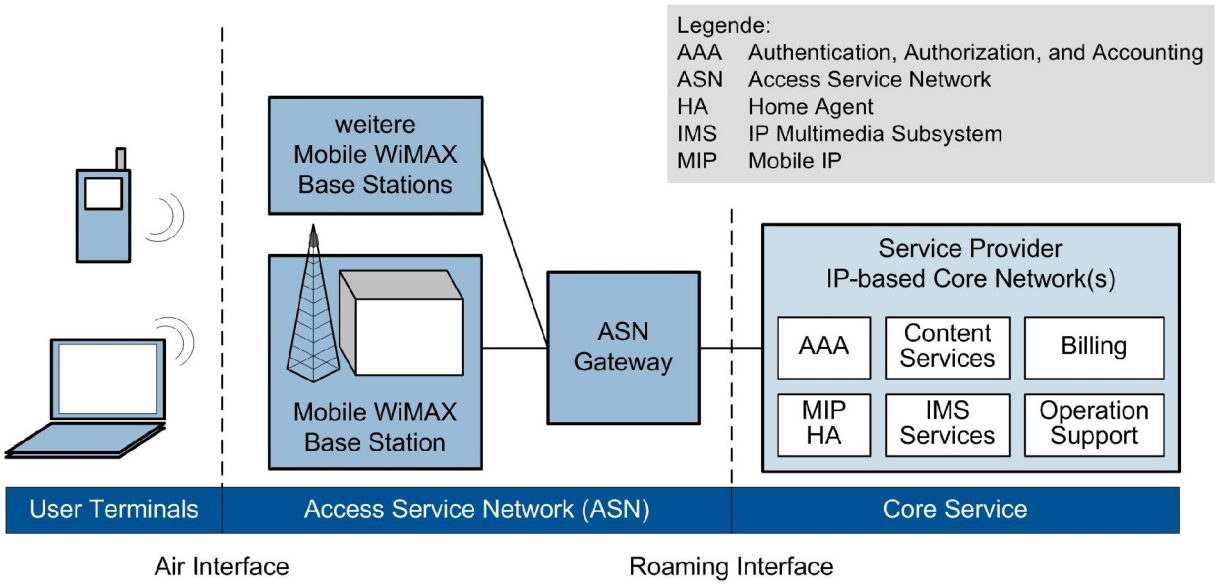
Da Mobile WiMAX eine Ergänzung von Fixed WiMAX darstellt, entspricht die Architektur prinzipiell der von Fixed WiMAX, wie in Kapitel D.1.1.1 erläutert. Dies beinhaltet primär Subscriber Stations und Base Stations.

Aufgrund der zusätzlichen Mobilität der Teilnehmer sind jedoch auch Änderungen an der Architektur erforderlich. Generell werden die Endgeräte laut WiMAX-Spezifikation als User Terminals bezeichnet. Diese beinhalten sowohl stationäre Subscriber Stations, wie in Fixed WiMAX beschrieben, als auch mobile Subscriber Stations. Mobile Subscriber Stations werden in IEEE-802.16e auch als Mobile Stations (MS) bezeichnet.

Für Mobile WiMAX ist neben der Luftschnittstelle (Air Interface) ein Roaming Interface als Referenzpunkt definiert, über das die Anbindung der WiMAX-Infrastruktur an die IP-Infrastruktur eines Netzbetreibers geschieht. Über diese Schnittstelle kann sich ein mobiler Teilnehmer sich am Netz an-

melden, die Informationen für eine Authentisierung werden bereitgestellt und über Mobile IP wird dem Endgerät die Möglichkeit gegeben sich uneingeschränkt auch IP-Netz-übergreifend zu bewegen. Weiterhin werden über das Roaming Interface auch Funktionen zur Abrechnung der Dienstnutzung angestoßen. Abbildung D-6 zeigt die vom WiMAX-Forum spezifizierte Architektur im Überblick.

Abbildung D-6: Architektur Mobile WiMAX (vereinfacht)



D.1.2.2 Physikalische Übertragung

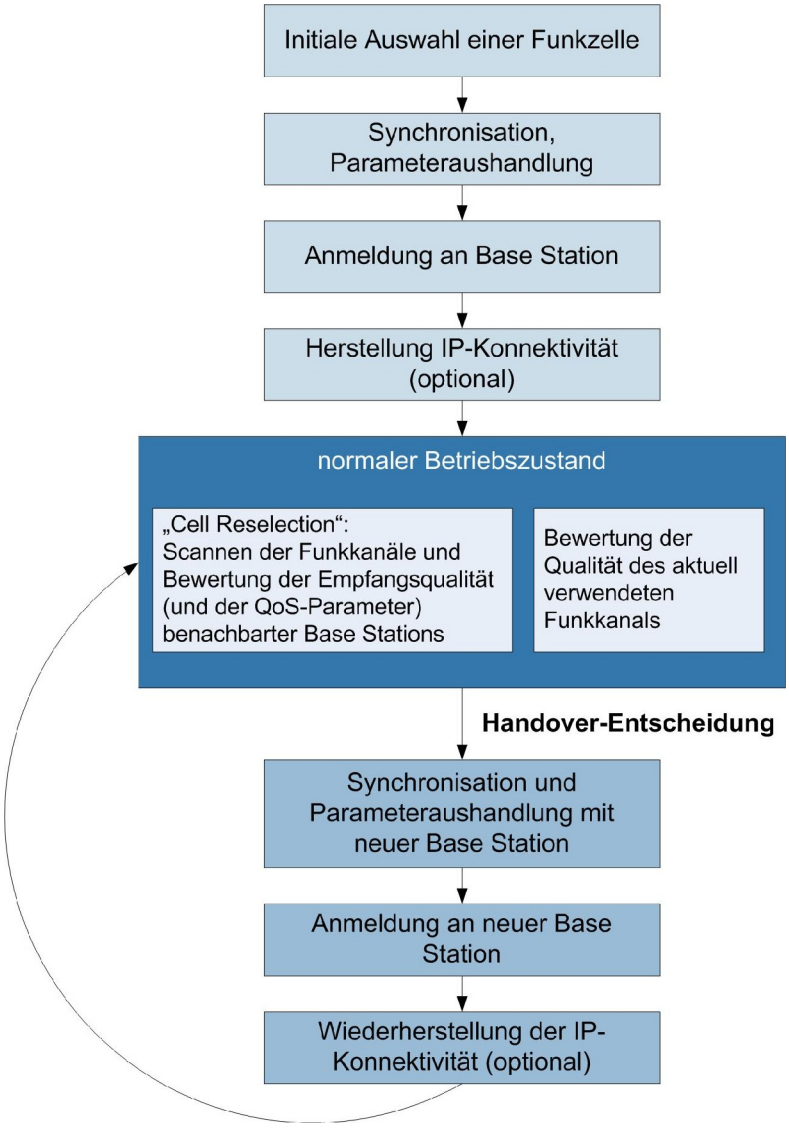
In IEEE 802.16e sind folgende der in IEEE 802.16 spezifizierten physikalischen Übertragungsverfahren für die direkte Anbindung mobiler Endgeräte vorgesehen: WirelessMAN-SCa, WirelessMAN-OFDM und WirelessMAN-OFDMA (siehe Kapitel D.1.1.2). Das Mobile-WiMAX-Profil des WiMAX-Forums konzentriert sich zunächst auf WirelessMAN-OFDMA. Damit ist Mobile WiMAX zunächst auf lizenzierte Bänder festgelegt.

D.1.2.3 MAC Layer

Der MAC Layer bei Mobile WiMAX entspricht grundsätzlich dem von Fixed WiMAX, wie in Kapitel D.1.1.3 beschrieben. Änderungen beziehen sich hauptsächlich auf neue Nachrichten-Typen, z.B. MAC-Management-Nachrichten. Diese adressieren Anforderungen mobiler Subscriber Stations wie z.B. Stromspar- und Handover-Mechanismen sowie Korrekturen hinsichtlich der Sicherheit. Letzteres betrifft speziell das aktualisierte Protokoll für das Schlüssel-Management (siehe Kapitel D.2.2.2).

Die wesentlichen Elemente zur Unterstützung mobiler Endgeräte, die auf dem MAC Layer realisiert werden, sind eine Funktion zur dynamischen An- und Abmeldung von mobilen Endgeräten an einer Base Station und eine Handover-Funktion. Die Handover-Funktion muss dabei einen Wechsel zwischen benachbarten, von Base Stations aufgespannten Funkzellen ermöglichen, ohne dass die Ende-zu-Ende-Kommunikation signifikante Einbußen erfährt. Dabei müssen die ausgehandelten Dienstgüte- und Sicherheitseinstellung einer Verbindung bei einem Handover beibehalten werden. Je nach Anwendung (z.B. Voice over IP) muss ein Handover außerdem sehr schnell ablaufen, damit der Handover nicht spürbar ist. Mobile WiMAX legt hierzu spezifische Protokollmechanismen fest, wie in Abbildung D-7 gezeigt wird.

Abbildung D-7: Ablauf von Anmeldung und Handover der mobilen Endgeräte



Die neu hinzugekommenen MAC-Management-Nachrichten werden ebenfalls zum Teil durch eine Integritätsprüfung vor Manipulationen geschützt. Neben HMAC steht als weiteres Verfahren für die Integritätsprüfung von MAC-Management-Nachrichten ein Blockchiffre-basierter Message Authentication Code (Cipher-based Message Authentication Code, CMAC) zur Verfügung. Als Blockchiffre wird Advanced Encryption Standard (AES) verwendet. Die Verwendung des CMAC setzt jedoch die Nutzung des aktualisierten Schlüssel-Management-Protokolls voraus.

Eine weitere wesentliche Neuerung ist die Integritätsprüfung der Nutzdaten mittels CCM-Modus (Counter with CBC-MAC). Dieser Blockchiffre-Modus erlaubt neben der Verschlüsselung auch eine Integritätsprüfung der Daten. CCM ist spezifiziert für Blockchiffren mit einer Blockgröße von 128 Bit. Als Blockchiffre kommt AES zum Einsatz.

MAC-Management-Nachrichten werden auch bei Mobile WiMAX unverschlüsselt übertragen.

Eine genaue Beschreibung der Sicherheitsmechanismen bei Mobile WiMAX ist in Kapitel D.2.2 enthalten.

D.2 Sicherheitsmechanismen

In den beiden folgenden Kapiteln werden die Sicherheitsmechanismen für Fixed WiMAX (siehe Kapitel D.2.1) nach IEEE 802.16 sowie Mobile WiMAX (siehe Kapitel D.2.2) nach IEEE 802.16e beschrieben.

D.2.1 Fixed WiMAX (IEEE 802.16)

Die MAC-Schicht der WiMAX-Spezifikation ist dreigeteilt. Den untersten, direkt auf die physikalische Schicht aufsetzenden Teil bildet der Security Sublayer. Der Security Sublayer stellt Sicherheitsmechanismen wie Authentisierung, sicheren Schlüsselaustausch und Verschlüsselung zur Verfügung.

Für diese Aufgabe sind zwei Protokolle spezifiziert:

- Das Encapsulation Protocol ermöglicht die Verschlüsselung der Datenpakete zwischen der Base Station und den Subscriber Stations. Hierfür werden sogenannte Cryptographic Suites (d.h. im allgemeinen Paare von Mechanismen zur Datenverschlüsselung und Integritätsprüfung, siehe Tabelle D-1) und die Regeln für die Anwendung dieser Algorithmen auf die Datenpakete definiert.

- Das Key Management Protocol stellt einen Mechanismus für die sichere Verteilung von Schlüsselmaterial von der Base Station zu den Subscriber Stations bereit. Hierfür wird das PKM-Protokoll (Privacy Key Management) genutzt (siehe Kapitel D.2.1.2).

D.2.1.1 Security Associations und Schlüsselmaterial bei Fixed WiMAX

Sämtliche Verbindungen und Datenübertragungen zwischen einer Base Station und ihren Subscriber Stations werden sogenannten Security Associations (SAs) zugeordnet. Eine SA ist ein Satz von Sicherheitsinformationen, die eine Base Station und eine Subscriber Station teilen, das heißt, alle zugeordneten Verbindungen werden entsprechend den in der SA genannten Sicherheitsmechanismen gesichert. Jede SA hat eine eindeutige Identifikation, den sogenannten SAID (SA Identifier).

Während der Initialisierungsphase muss jede Subscriber Station eine primäre SA initiieren. Diese enthält mindestens die zwischen Base Station und Subscriber Station genutzte Cryptographic Suite der Subscriber Station und ggf. darüber hinaus Schlüsselmaterial und Initialisierungsvektoren.

Das Schlüsselmaterial für jede SA wird von der Base Station verwaltet und mit Hilfe des Key-Management-Protokolls (siehe Kapitel D.2.1.2) mit den Subscriber Stations synchronisiert. Der Aufbau einer SA und die Verwendung der verschiedenen Schlüsseltypen wird in Abbildung D-8 gezeigt. Folgende Schlüsseltypen werden unterschieden:

- Authorization Key (AK)

  Der AK wird der Subscriber Station während der Authentisierung von der Base Station über ein Public-Key-Verfahren zugeteilt und ist eine bestimmte Zeitspanne gültig. Die Subscriber Station muss vor Ablauf der Gültigkeitsdauer einen neuen AK anfordern, wenn sie weiterhin mit der Base Station kommunizieren möchte. Jede Subscriber Station verfügt für alle ihre SAs nur über einen einzigen AK (bzw. während der Übergangsphase von einem bald ablaufenden zu einem neuen AK temporär über zwei AKs).

  Vom Authorization Key werden der Key Encryption Key (KEK) und die Message Authentication Keys abgeleitet.

- Traffic Encryption Key (TEK)

  Mit dem TEK wird der Datenverkehr zwischen einer Subscriber Station und der Base Station verschlüsselt. Eine Subscriber Station muss für jede SA einen TEK führen und ist dafür verantwortlich, vor dessen Gültigkeitsablauf einen neuen TEK bei der Base Station anzufordern, der dann mit dem Key Encryption Key verschlüsselt übertragen wird. Anhand einer 2 Bit langen TEK-Sequenznummer werden die verschiedenen Generationen des TEK-Schlüsselmaterials unterschieden. Dies ermöglicht maximal vier Generationen pro SA.

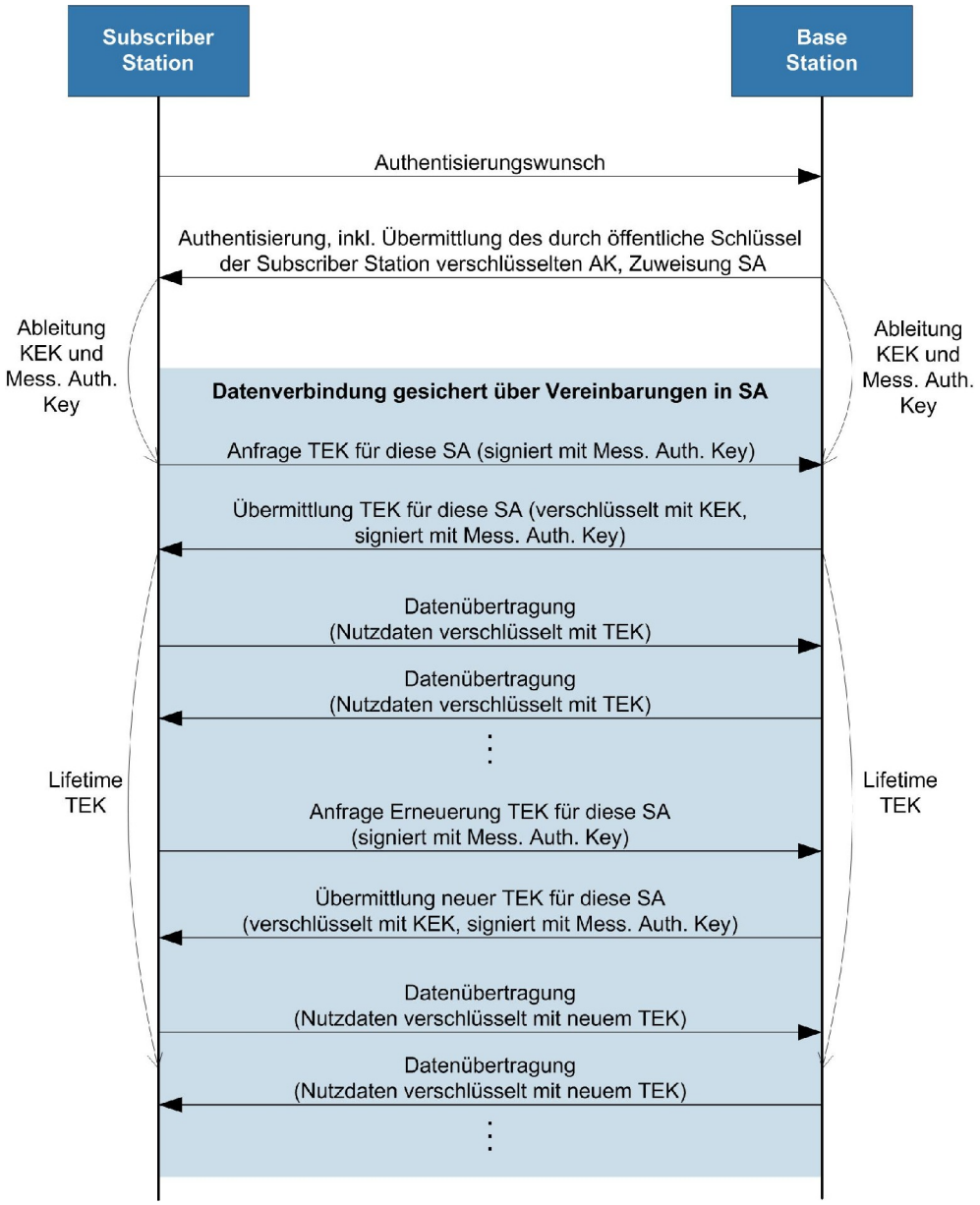
- Key Encryption Key (KEK)

  Der KEK wird vom AK abgeleitet und zur Verschlüsselung der TEKs während der Übertragung von der Base Station zur Subscriber Station verwendet.

- Message Authentication Keys

  Mit den Message Authentication Keys werden Management-Nachrichten, z.B. zur Anforderung und Verteilung von TEKs, zwischen Base Station und Subscriber Stations signiert und verifiziert.

Abbildung D-8: Verwendung von Schlüsseln in Fixed WiMAX



D.2.1.2 Privacy Key Management Protocol (PKM-Protokoll) bei Fixed WiMAX

Jede Subscriber Station verfügt über ein vom Hersteller ausgegebenes und installiertes digitales X.509-Zertifikat mit zugehörigem privatem Schlüssel und über das zugehörige X.509-Zertifikat des Herstellers.

Eine Subscriber Station beginnt den Authentisierungsprozess, welcher in Abbildung D-9 im Überblick dargestellt ist, mit einer Authentication Information Message, in der sie der Base Station das Zertifikat des Herstellers übermittelt. Direkt danach sendet sie einen Authorization Request an die Base Station, der die folgenden Informationen enthält:

- das Zertifikat der Subscriber Station
- eine Liste von Cryptographic Suite IDs, die von der Subscriber Station unterstützt werden (siehe Kapitel D.2.1.3)
- den Connection Identifier der Subscriber Station

Die Base Station prüft die Zertifikate und stellt fest, ob die Subscriber Station autorisiert ist, das WiMAX-basierte Netzwerk zu nutzen. Ist dies der Fall, erhält die Subscriber Station von der Base Station einen Authorization Reply mit den folgenden Informationen:

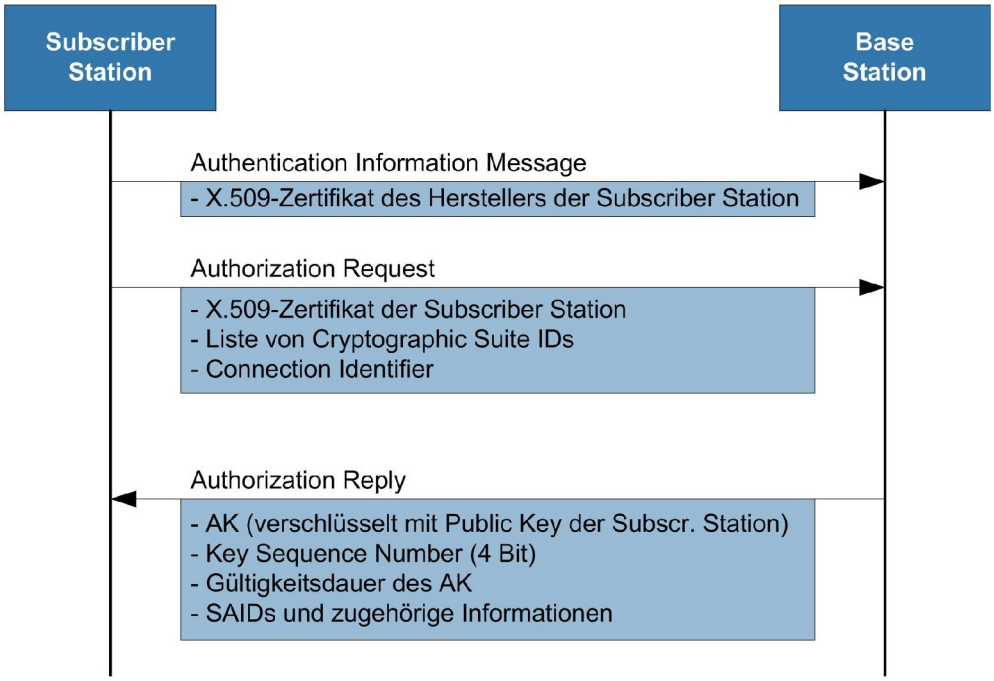
- einen Authorization Key (AK), der mit dem im Zertifikat übermittelten Public Key der Subscriber Station verschlüsselt wurde (siehe Abbildung D-8)
- eine 4 Bit lange Key Sequence Number, durch die die einzelnen Schlüsselgenerationen unterschieden werden
- die Gültigkeitsdauer des AK
- die SAIDs und Informationen der primären und ggf. weiterer statischer SAs (Auswahl einer Cryptographic Suite und ggf. Traffic Encryption Keys und deren Gültigkeitsdauer)

Von dem AK werden sowohl von der Base Station als auch von der Subscriber Station nach einem vorgegebenen Algorithmus Key Encryption Key (KEK) und Message Authentication Keys abgeleitet, welche die weitere Anforderung und Übermittlung von Traffic Encryption Keys (TEK) absichern.

Sollen die Daten im WiMAX-basierten Netz verschlüsselt werden, muss die Subscriber Station immer vor Ablauf der Gültigkeitsdauer des verwendeten TEK einen neuen TEK anfordern. In der Point-to-Multipoint-Architektur startet sie dazu für jede ihrer SAs eine TEK State Machine, die für das regelmäßige Senden von Key Request Messages zuständig ist und somit das Schlüsselmaterial aktuell hält. Die Key Request Messages werden mit Message Authentication Keys signiert und der TEK wird mit dem Key Encryption Key verschlüsselt übermittelt.

In der Mesh-Architektur hingegen startet die Subscriber Station für jede Nachbarstation eine TEK State Machine, die regelmäßig Key Request Messages für TEKs für alle SAs sendet. Die Nachbarstationen übermitteln den aktuellen TEK der Base Station, der in dem Fall mit dem Public Key der Subscriber Station verschlüsselt wird.

Abbildung D-9: Authentisierung in Fixed WiMAX



D.2.1.3 Encapsulation Protocol bei Fixed WiMAX

Über das Encapsulation Protocol werden sogenannte Cryptographic Suites festgelegt, welche die Fähigkeiten der Subscriber Station zur Verschlüsselung und Integritätsprüfung spezifizieren. Jede Cryptographic Suite hat eine eindeutige Identifikation. Eine Liste dieser Identifikationen wird bei der Authentisierung der Subscriber Station an die Base Station übermittelt, die dann die erlaubten SAs ermitteln kann. Wie Tabelle D-1 zeigt, ist eine kryptographische Integritätsprüfung bei Fixed WiMAX nicht vorgesehen.

Für die Datenverschlüsselung können die folgenden Verschlüsselungsalgorithmen verwendet werden:

- keine Verschlüsselung
- Data Encryption Standard (DES) im CBC-Modus (Cipher Block Chaining) mit 56-Bit-Schlüssel
- Advanced Encryption Standard (AES) im CCM-Modus[5] (Counter with CBC with Message Authentication Code) mit 128-Bit-Schlüssel

Wenn eine Verschlüsselung erfolgen soll, wird grundsätzlich nur der Nutzdatenteil (Payload) der MAC PDU (Protocol Data Unit) verschlüsselt (siehe Abbildung D-4). Der Generic MAC Header und die optionale CRC werden nicht verschlüsselt. Außerdem werden alle MAC-Management-Nachrichten unverschlüsselt übertragen (siehe auch Kapitel D.1.1.3).

5 CCM = Counter with CBC-MAC, CBC-MAC = CBC with Message Authentication Code; CCM ist eine generische Methode für die Verschlüsselung und Integritätsprüfung von Daten, die für die Verwendung einer 128-Bit-Blockchiffrierung (z.B. AES) spezifiziert ist. In Kapitel A. Funk-LAN (WLAN, IEEE 802.11) ist diese Methode kurz beschrieben. Die Funktion der Integritätsprüfung wird in Fixed WiMAX allerdings nicht genutzt.

Der Traffic Encryption Key kann bei seiner Übermittlung an die Subscriber Station mit den folgenden Verschlüsselungsalgorithmen verschlüsselt werden:

- 3DES im EDE-Modus[6] (Encrypt-Decrypt-Encrypt) mit 128-Bit-Schlüssel
- RSA[7] mit 1024-Bit-Schlüssel
- AES im ECB-Modus (Electronic Code Book) mit 128-Bit-Schlüssel

Tabelle D-1: Cryptographic Suites für Fixed WiMAX

Cryptographic Suite ID	Beschreibung		
	Datenverschlüsselung	Integritätsprüfung	TEK-Verschlüsselung
0x000001	keine	keine	3DES im EDE-Modus mit 128-Bit-Schlüssel
0x010001	DES im CBC-Modus mit 56-Bit-Schlüssel	keine	3DES im EDE-Modus mit 128-Bit-Schlüssel
0x000002	keine	keine	RSA mit 1024-Bit-Schlüssel
0x010002	DES im CBC-Modus mit 56-Bit-Schlüssel	keine	RSA mit 1024-Bit-Schlüssel
0x020003	AES im CCM-Modus mit 128-Bit-Schlüssel	keine	AES im ECB-Modus mit 128-Bit-Schlüssel
alle anderen Werte	Reserviert		

D.2.2 Mobile WiMAX (IEEE802.16e)

Auch in der Mobile-WiMAX-Spezifikation ist die MAC-Schicht dreigeteilt (siehe Kapitel D.1.2.3 bzw. Kapitel D.1.1.3). Hier heißt der für die Sicherheitsaufgaben zuständige Sublayer allerdings nicht mehr Security Sublayer, sondern Privacy Sublayer.

Das Sublayer umfasst ebenfalls die beiden Protokolle Encapsulation Protocol und Key Management Protocol, letzteres allerdings in zwei Versionen:

- PKMv1 ist vergleichbar mit PKM bei Fixed WiMAX.
- PKMv2 bietet erweiterte Funktionen wie z.B. eine neue Schlüsselhierarchie, AES-CMAC, AES Key Wrap und Multicast-/Broadcast-Service.

Die Authentisierung ist bei Mobile WiMAX nicht nur über Zertifikate, wie in Fixed WiMAX, sondern auch über das Extensible Authentication Protocol (EAP) möglich[8].

6 Bei 3DES (Triple DES) im EDE-Modus werden drei DES-Chriffrierer hintereinander geschaltet, wobei der mittlere DES-Chriffrierer invers eingebaut ist.

7 RSA ist ein Public-Key-Verfahren (d.h. basierend auf einem asymmetrischen Verschlüsselungsalgorithmus), der nach seinen Erfindern R. Rivest, A. Shamir und L. Adleman benannt ist.

D.2.2.1 Security Associations und Schlüsselmaterial bei Mobile WiMAX

Das Konzept der Security Associations (SAs) wurde vom Fixed-WiMAX-Standard übernommen. Allerdings gibt es im Mobile-WiMAX-Standard noch weitere SAs. Unterschieden werden:

- SAs für den Unicast-Verkehr, wie bereits in Kapitel D.2.1.1 beschriebenen
- Group Security Association (GSA) für Multicast-Gruppen

  Multicast/Broadcast-Service Group Security Association (MBS-GSA), für den Multicast-/Broadcast-Service

Für die beiden unterschiedlichen Authentisierungsverfahren gibt es bei Mobile WiMAX ein eigenes Schlüsselmaterial, aus dem der Authorization Key (AK) jeweils abgeleitet werden kann:

- Pre-Primary Authorization Key (Pre-PAK)

  Der Pre-PAK wird bei der zertifikatsbasierten RSA-Authentisierung an die Mobile Station übermittelt (verschlüsselt mit dem Public Key der Mobile Station). Aus dem Pre-PAK wird dann der Primary Authorization Key abgeleitet.
- Primary Authorization Key (PAK)

  Der PAK wird aus dem Pre-PAK abgeleitet und dient seinerseits zur Ableitung des Authorization Keys.
- Master Session Key (MSK)

  Der MSK wird bei der Authentisierung über EAP generiert. Aus ihm wird der Pairwise Master Key abgeleitet.
- Pairwise Master Key (PMK)

  Der PMK wird aus dem MSK abgeleitet und dient seinerseits zur Ableitung des Authorization Keys.
- Authorization Key (AK)

  Der AK wird vom PAK oder PMK abgeleitet und hat dieselbe Funktion wie bei Fixed WiMAX (siehe Kapitel D.2.1.1).

Für die weiteren SAs, die in Mobile WiMAX spezifiziert sind, gibt es folgende Schlüssel:

- Group Key Encryption Key (GKEK)

  Der GKEK wird zufällig von der Base Station generiert und der Mobile Station mit dem KEK verschlüsselt übermittelt. Der GKEK dient zur Verschlüsselung der Group Traffic Encryption Keys bei der Übermittlung von der Base Station zu den Mobile Stations.
- Group Traffic Encryption Key (GTEK)

  Der GTEK für Multicast-Verkehr entspricht dem TEK, der für Unicast-Verkehr genutzt wird.
- MBS Traffic Key (MTK)

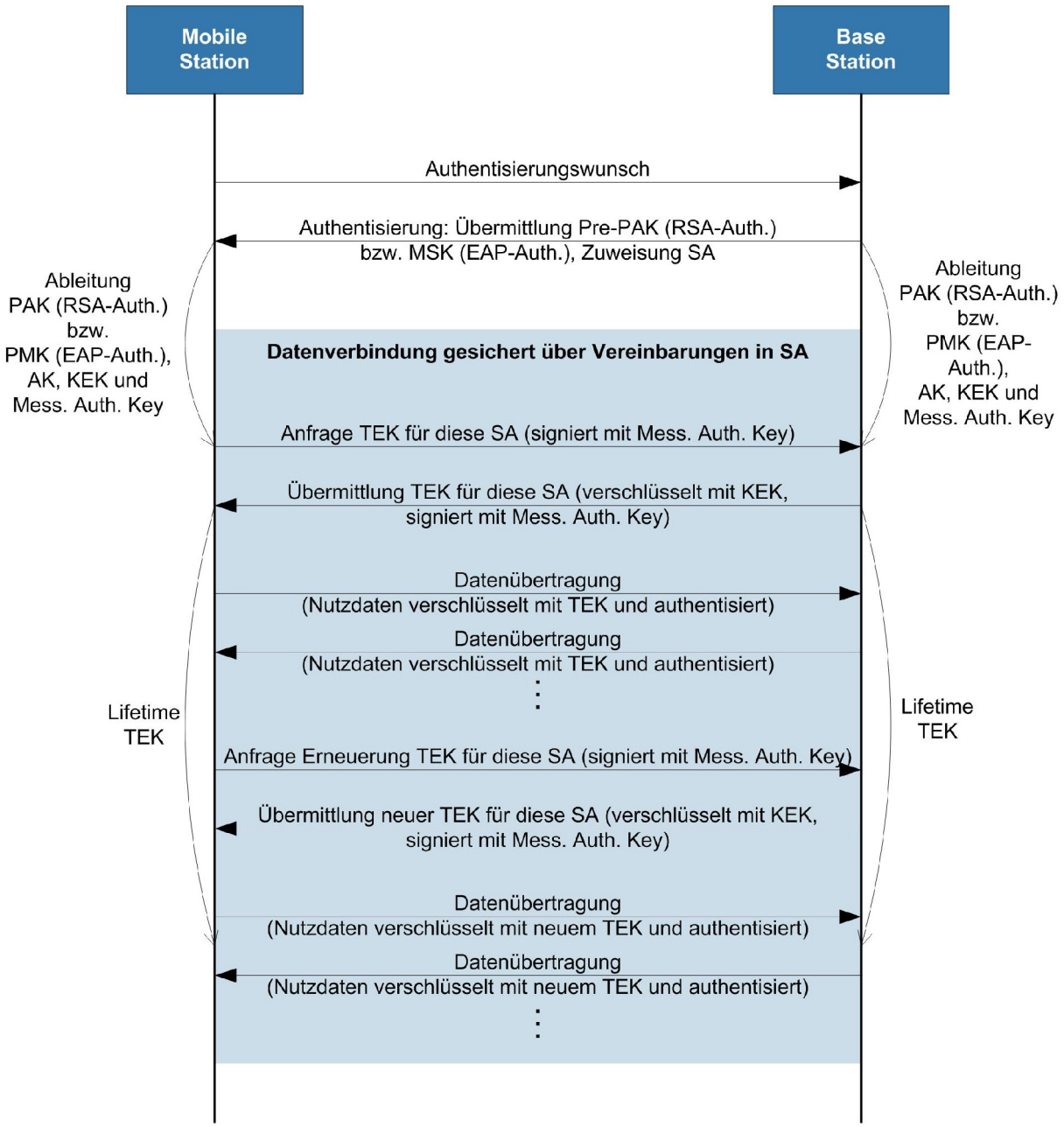
---

8 EAP ist ein Authentisierungs-Framework, d.h. EAP spezifiziert eine generische Schnittstelle, die von verschiedensten Authentisierungsmethoden, sogenannten EAP-Methoden, genutzt werden kann. Eine Beschreibung einiger besonders wichtiger Authentisierungsmethoden kann Kapitel A. Funk-LAN (WLAN, IEEE 802.11) entnommen werden.

Der MTK wird aus einem im Mobile-WiMAX-Standard nicht spezifizierten MBS Authorization Key (MAK) abgeleitet. Generierung und Übermittlung dieses MAK muss auf höheren Schichten geschehen. Mit dem MTK wird der MBS-Verkehr verschlüsselt.

Die übrigen in Kapitel D.2.1.1 beschriebenen Schlüssel (TEK, KEK und Message Authentication Keys) werden identisch auch in Mobile WiMAX genutzt. Abbildung D-10 zeigt den Aufbau einer SA und die Verwendung der verschiedenen Schlüsseltypen.

Abbildung D-10: Verwendung von Schlüsseln in Mobile WiMAX



D.2.2.2 Key Management Protocol bei Mobile WiMAX

Wie schon erwähnt, gibt es bei Mobile WiMAX zwei Versionen des Privacy Key Management Protocol: das mit PKM bei Fixed WiMAX vergleichbare PKMv1 sowie das PKMv2 mit erweiterten Funktionen wie z.B. einer neuen Schlüsselhierarchie, AES-CMAC, AES Key Wrap und Multicast-/Broadcast-Service (siehe auch Kapitel D.2.2.1).

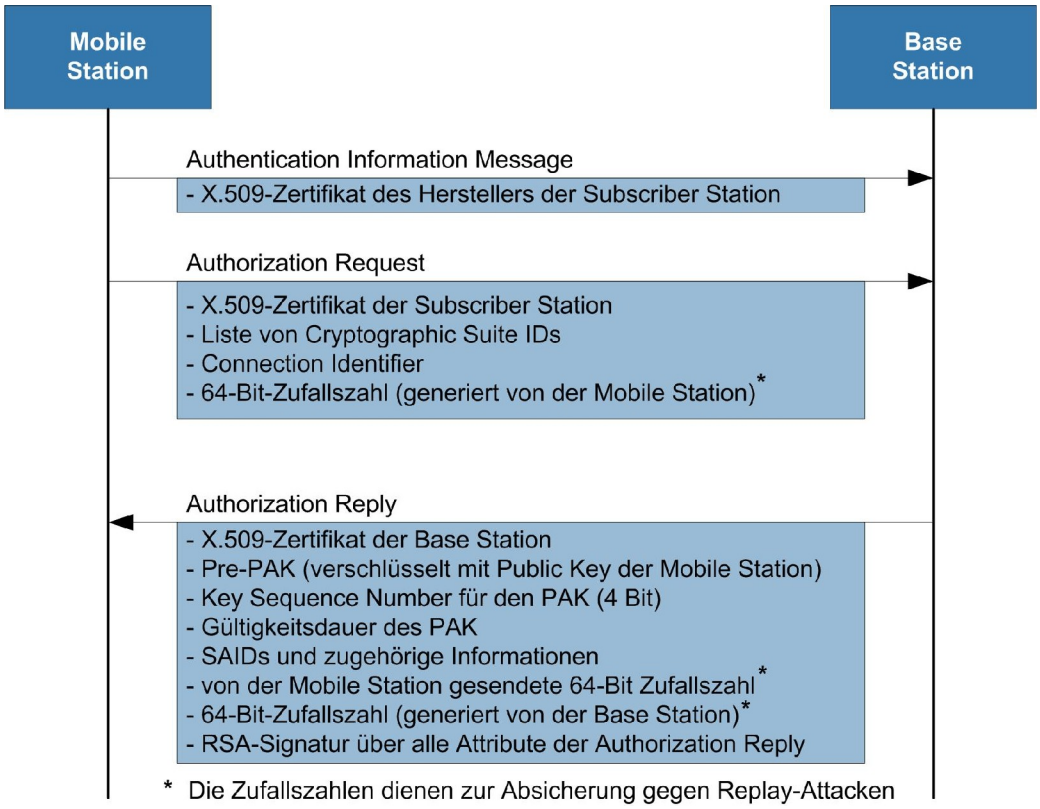
Die Authentisierung ist bei Mobile WiMAX über zwei verschiedene Methoden möglich:

- RSA-Authentisierung über X.509-Zertifikate wie bei Fixed WiMAX

  Die RSA-Authentisierung läuft wie bei Fixed WiMAX ab (siehe Kapitel D.2.1.2). Allerdings ist in PKMv2 auch eine gegenseitige Authentisierung möglich, in dem die Base Station in ihrer Authorization Reply ihr Zertifikat an die Mobile Station sendet (siehe Abbildung D-11).

  Die RSA-Authentisierung muss in PKMv1 unterstützt werden (nur einseitige Authentisierung möglich) und ist in PKMv2 optional.

Abbildung D-11: Gegenseitige Authentisierung in Mobile WiMAX mit PKMv2



- Authentisierung über das Extensible Authentication Protocol (EAP, siehe [RFC3748])

  Bei der Authentisierung über EAP kann die EAP-Methode vom WiMAX-Netzbetreiber frei gewählt werden. Der genaue Vorgang der Authentisierung und die EAP-Methode werden im Mobile-WiMAX-Standard nicht spezifiziert, die EAP-Methode sollte aber die Pflichtkriterien des RFC 4017, Abschnitt 2.2 (siehe [RFC4017]) erfüllen:

  - Generierung von symmetrischem Schlüsselmaterial
  - Generierung von Schlüsselmaterial mit einer effektiven Schlüssellänge von 128 Bit

- Für EAP-Methoden, welche eine Ableitung von Schlüsseln unterstützen, müssen der exportierte Master Session Key (MSK) sowie der Extended Master Session Key (EMSK) mindestens 512 Bit lang sein
- Unterstützung einer gegenseitigen Authentisierung
- Widerstandsfähigkeit gegen Dictionary-Attacken
- Schutz gegen Man-in-the-Middle-Attacken
- Gesicherte Verhandlung von Folgeschlüsseln

Die EAP-Authentisierung ist in beiden PKM-Versionen optional.

Im Mobile-WiMAX-Standard ist eine Pre-Authentication möglich, um ein schnelleres Handover von einer Base Station zu einer benachbarten Base Station zu ermöglichen. Diese Pre-Authentication wird im Mobile-WiMAX-Standard allerdings nicht genauer spezifiziert.

D.2.2.3 Encapsulation Protocol bei Mobile WiMAX

Die Aufgabe des Encapsulation-Protokolls ist die gleiche wie bei Fixed WiMAX. Allerdings sind bei Mobile WiMAX weitere Verschlüsselungsmethoden erlaubt und auch eine Integritätsprüfung für die Nutzdatenübertragung ist möglich. Eine Liste der zugelassenen Cryptographic Suites findet sich in Tabelle D-2.

Für die Datenverschlüsselung sind die folgenden Varianten zugelassen:

- ► Keine Verschlüsselung
- ► DES im CBC-Modus mit 56-Bit-Schlüssel
- ► AES im CCM-Modus mit 128-Bit-Schlüssel
- ► AES im CBC-Modus mit 128-Bit-Schlüssel
- ► AES im CTR-Modus mit 128-Bit-Schlüssel für Multicast /Broadcast Services mit 8 Bit Rollover Counter

Auch hier wird grundsätzlich nur die MAC PDU Payload verschlüsselt. Der Generic MAC Header und die optionale CRC werden nicht verschlüsselt. Außerdem müssen alle MAC-Management-Nachrichten unverschlüsselt übertragen werden (siehe auch Kapitel D.1.2.3).

Die Integritätsprüfung der Nutzdaten ist im CCM-Modus mittels AES und 128-Bit-Schlüssel möglich.

Der Traffic Encryption Key / Group Traffic Encryption Key / MBS Traffic Encryption Key kann bei seiner Übermittlung an die Mobile Station mit den folgenden Verschlüsselungsalgorithmen verschlüsselt werden:

- ► 3DES im EDE-Modus mit 128-Bit-Schlüssel
- ► RSA mit 1024-Bit-Schlüssel
- ► AES im ECB-Modus mit 128-Bit-Schlüssel
- ► AES Key Wrap mit 128-Bit-Schlüssel

Tabelle D-2: Cryptographic Suites für Mobile WiMAX

Cryptographic Suite ID	Beschreibung		
	Datenverschlüsselung	**Integritätsprüfung**	**TEK-Verschlüsselung**
0x000001	keine	keine	3DES im EDE-Modus mit 128-Bit-Schlüssel
0x010001	DES im CBC-Modus mit 56-Bit-Schlüssel	keine	3DES im EDE-Modus mit 128-Bit-Schlüssel
0x000002	keine	keine	RSA mit 1024-Bit-Schlüssel
0x010002	DES im CBC-Modus mit 56-Bit-Schlüssel	keine	RSA mit 1024-Bit-Schlüssel
0x020103	AES im CCM-Modus mit 128-Bit-Schlüssel	AES im CCM-Modus mit 128-Bit-Schlüssel	AES im ECB-Modus mit 128-Bit-Schlüssel
0x020104	AES im CCM-Modus mit 128-Bit-Schlüssel	AES im CCM-Modus mit 128-Bit-Schlüssel	AES Key Wrap mit 128-Bit-Schlüssel
0x030003	AES im CBC-Modus mit 128-Bit-Schlüssel	keine	AES im ECB-Modus mit 128-Bit-Schlüssel
0x800003	AES im CTR-Modus mit 128-Bit-Schlüssel für Multicast / Broadcast Services mit 8 Bit Rollover Counter	keine	AES im ECB-Modus mit 128-Bit-Schlüssel
0x800004	AES im CTR-Modus mit 128-Bit-Schlüssel für Multicast / Broadcast Services mit 8 Bit Rollover Counter	keine	AES Key Wrap mit 128-Bit-Schlüssel
alle anderen Werte	reserviert		

D.3 Gefährdungen

Dieses Kapitel beschreibt typische Gefährdungen, denen ein WiMAX-basiertes Netz ausgesetzt sein kann. Sofern nicht explizit erwähnt, gelten die Gefährdungen sowohl für Fixed WiMAX als auch für Mobile WiMAX. Da bisher nur eine punktuelle Versorgung durch WiMAX-Netze realisiert wurde und oft noch ein Testbetrieb erfolgt, gibt es nur wenig praktische Erfahrungen mit diesen Systemen. Eine detaillierte Analyse der Bedrohungen findet sich beispielsweise in [BARB05].

D.3.1 Ausfall durch höhere Gewalt

Wie im kabelgebundenen LAN kann es auch in WiMAX-basierten Netzen durch Überspannungen zum Ausfall von Komponenten kommen. Außerdem sind Außeninstallationen (z.B. Antennen) durch Blitz und Witterungseinflüsse gefährdet.

D.3.2 Unkontrollierte Ausbreitung der Funkwellen

Die Funkwellen der WiMAX-Komponenten breiten sich auch über räumliche Grenzen des WiMAX-Nutzungsbereichs aus. Dabei kann auch in nicht vom WiMAX-Betreiber kontrollierten Bereichen ein Empfang möglich sein. Je nach Umgebungsbedingungen und Leistungsfähigkeit der verwendeten Empfangsgeräte (z.B. Richtantennen) besteht auch hier noch eine konkrete Abhörgefahr, sofern keine adäquaten Verschlüsselungsmechanismen eingesetzt werden.

D.3.3 Bedrohung der Verfügbarkeit

WiMAX-Netze übertragen Informationen mittels elektromagnetischer Funkwellen. Strahlen andere elektromagnetische Quellen im gleichen Frequenzspektrum Energie ab, können diese die WiMAX-Kommunikation stören und im Extremfall den Betrieb des WiMAX-Netzes verhindern. Dies kann unbeabsichtigt durch andere technische Systeme oder aber durch absichtliches Betreiben einer Störquelle (Jammer) als sogenannter Denial-of-Service-Angriff (DoS-Angriff) erfolgen. Eine solche Störquelle kann sich bei ausreichender Sendeleistung auch außerhalb des Bereiches befinden, in dem das WiMAX-Netz genutzt wird.

D.3.4 Physischer Zugangsschutz

Base Station und Subscriber Station müssen vor Fremdzugriff geschützt werden. Während die Base Station in der Regel durch den Netzanbieter angebracht und abgesichert wird, besteht für die Subscriber Station eine höhere Gefährdung eines unautorisierten Zugriffs. Insbesondere wenn die Subscriber Station mehrere Teilnehmer oder Wohnungseinheiten versorgt, stellt dies eine Gefährdung dar.

Speziell der für das RSA-Verfahren benötigte private Schlüssel muss vor Zugriff geschützt werden. Ein auf diese Weise durchgeführter Identitätsdiebstahl kann für weitere Angriffe missbraucht werden.

D.3.5 Schwächen im Sicherheitskonzept

Nachfolgend werden Schwächen im Sicherheitskonzept von Fixed WiMAX und Mobile WiMAX dargestellt, sowie hieraus resultierende Gefährdungen.

D.3.5.1 Nur teilweise Authentisierung von MAC-Management-Nachrichten

Die Integrität von MAC-Management-Nachrichten kann bei Fixed WiMAX per HMAC und bei Mobile WiMAX bei Verwendung von PKMv2 wahlweise auch mittels CMAC geprüft werden. Manipulationen können auf diese Weise entdeckt werden. Sowohl bei Fixed WiMAX als auch bei Mobile WiMAX werden MAC-Management-Nachrichten jedoch zum Teil ohne Integritätsschutz übertragen. Details hierzu finden sich beispielsweise in [HAN08] und [DEIN07].

Dies ermöglicht verschiedene Typen von Angriffen:

- Denial of Service (DoS)

  Ein DoS-Angriff kann sowohl auf die SS als auch die Base Station zielen und den Dienst einschränken (z.B. Verringern der Sendestärke der Subscriber Station) oder vollständig unterbinden. Für Mobile WiMAX bestehen hier zusätzliche Gefährdungen durch das absichtliche Setzen des Sleep-Modus oder das Verhindern eines Handovers.

- Man in the Middle (MITM)

  Weiterhin besteht eine Gefährdung durch gefälschte MAC-Management-Nachrichten im Rahmen der Verbindungsaushandlung von SS und BS. Ein Angreifer kann beispielsweise die Kommunikation zwischen Subscriber Station und Base Station stören und schwächere Sicherheitsparameter an die Base Station übermitteln, als durch die legitime Subscriber Station theoretisch möglich wären. Dies könnte in der Konsequenz zu einer Klartextübertragung führen.

D.3.5.2 Zum Teil nur Authentisierung der Subscriber Station

Sowohl bei Fixed WiMAX als auch bei der RSA-basierten Authentisierung von Mobile WiMAX, wenn PKMv1 genutzt wird, erfolgt nur eine einseitige Authentisierung. Dies bedeutet, dass sich zwar die Subscriber Station gegenüber der Base Station authentisieren muss, aber keine Authentisierung der Base Station gegenüber der Subscriber Station stattfindet.

Die Subscriber Station hat also keine Möglichkeit, die Authentizität der Base Station zu überprüfen und kann somit eine falsche Base Station nicht erkennen. Dies ermöglicht einen Angriff vom Typ Man in the Middle (MITM). Bei diesem Angriff übernimmt eine falsche Base Station die Rolle einer richtigen Base Station und kann dann sämtlichen über sie laufenden Datenverkehr abgreifen. Wenn sie den Datenverkehr als MITM gleichzeitig auch an den Adressaten weiterleitet, können die Subscriber Stations den Angriff nicht bemerken. Da die Base Station auch für die Generierung des Authorization Key zuständig ist, ist sie potenziell auch noch in der Lage, den abgegriffenen Datenverkehr zu entschlüsseln.

D.3.5.3 Unsichere Erzeugung des Authorization Key (Fixed WiMAX)

Die Erzeugung des Authorization Key (AK), von dem weitere Schlüssel wie der KEK abgeleitet werden, ist bei Fixed WiMAX (PKMv1) nur abhängig von der BS. Es werden z.B. keine Zufallszahlen der Subscriber Station berücksichtigt. Da der KEK auch für die Verschlüsselung des TEK genutzt werden kann (z.B. bei Verwendung von AES oder 3DES) ist dieser als besonders sensitiv anzusehen, da bei Bekanntwerden des TEK ein Entschlüsseln der Nutzdaten möglich ist.

Bei Mobile WiMAX wurde dies durch ein mehrstufiges Verfahren behoben, indem u.a. Zufallszahlen der Subscriber Station in die Erzeugung des AK einfließen.

D.3.5.4 Ungeeignete Verfahren für Authentisierung und Verschlüsselung

Der WiMAX-Standard bietet die Möglichkeit, auf eine Verschlüsselung der Datenkommunikation zu verzichten bzw. nicht ausreichend sichere Verfahren zu wählen. Insbesondere für die verschlüsselte Nutzdatenübertragung ist DES mit 56 Bit Schlüssellänge ungeeignet. Weitere kritische Punkte sind der vorhersagbare Initialisierungsvektor für die Blockchiffrierung mittels DES, der fehlende Replay-Schutz sowie die nicht vorhandene Integritätsprüfung der optional verschlüsselten Nutzdaten.

Für Mobile WiMAX muss zusätzlich berücksichtigt werden, dass bei der optionalen Verwendung von EAP der Netzanbieter Freiheiten bei der Wahl der EAP-Methode hat. Speziell passwortbasierte Methoden (z.B. im Rahmen von EAP-TTLS[9]) sind potenziell durch Wörterbuchattacken angreifbar, was bei der Verwendung von schwachen Passwörtern eine Gefährdung darstellen kann. Hier ist der Netzanbieter für die Stärke der Absicherung verantwortlich.

D.3.5.5 Fehlender Schutz vor Replay-Angriffen (Fixed WiMAX)

In Fixed WiMAX werden die MAC-Management-Nachrichten zwar teilweise einer Integritätsprüfung unterzogen, diese gewährleistet aber keinen Schutz gegen sogenannte Replay-Attacken aufgrund fehlender zeitabhängiger Informationen (z.B. Paketnummern). Hierbei werden die MAC-Management-Nachrichten abgefangen und zu einem späteren Zeitpunkt wieder an den Empfänger gesendet. Dies wird auch oft im Zusammenhang mit Man-in-the-Middle-Attacken benutzt.

Diese Tatsache ermöglicht eine weitere Möglichkeit für Replay-Attacken durch die nur zwei Bit lange Key Sequence Number des TEK (siehe Kapitel D.2.1.1). Hierdurch können abgefangene TEK-Nachrichten regelmäßig wieder eingespielt werden und der TEK wechselt immer zwischen den gleichen vier Werten, was einem Angreifer eine größere Möglichkeit zur Entschlüsselung des Datenverkehrs bietet.

D.3.5.6 Keine Integritätsprüfung der Nutzdaten

Im Fixed-WiMAX-Standard ist keine kryptographische Integritätsprüfung für die Nutzdatenübertragung vorgesehen. Es kann also nicht unmittelbar festgestellt werden, ob die übermittelten Daten zwischen Sender und Empfänger manipuliert wurden. In Mobile WiMAX ist hierfür der CCM-Modus mittels AES als zusätzliche Cryptographic Suite vorgesehen. Bestehende Cryptographic Suites wie „keine Verschlüsselung“ oder „Nutzung von DES“ stehen jedoch ebenfalls zur Verfügung, sodass auch schwach abgesicherte Konfigurationen möglich sind (siehe auch Tabelle D-1).

D.3.5.7 Shared Keys im Multicast-/Broadcast-Betrieb (Mobile WiMAX)

Im Zusammenhang mit Mobile WiMAX ist auch der Multicast- und Broadcast-Betrieb vorgesehen. Der hierfür vorgesehene symmetrische Schlüssel (Group Traffic Encryption Key, GTEK) für die Verschlüsselung und Integritätsprüfung muss allen Teilnehmern bekannt sein und birgt die Gefahr, dass Nachrichten manipuliert werden oder ein Teilnehmer selbst generiertes Schlüsselmaterial in Umlauf bringt. Dies würde auch Angriffe vom Typ DoS ermöglichen, da Broadcast-/Multicast-Verkehr der ursprünglichen Base Station nicht länger entschlüsselt werden könnte (siehe auch [DEIN07]).

---

9 TTLS = Tunneled Transport Layer Security

D.3.5.8 Klartextübertragung von Management-Nachrichten

Sowohl bei Fixed WiMAX als auch bei Mobile WiMAX werden sämtliche MAC-Management-Nachrichten unverschlüsselt übertragen. Dadurch können MAC-Management-Nachrichten sehr leicht abgehört werden. Aus den abgefangenen MAC-Management-Nachrichten kann ein Angreifer Informationen über den Aufbau des Netzes erhalten oder dies in Kombination mit nicht authentisierten Nachrichten für Angriffe verwenden (siehe auch Kapitel D.3.5.1).

Die MAC-Management-Nachrichten werden innerhalb der MAC PDU übertragen (siehe Abbildung D-4). Die zusätzlichen Anteile einer MAC PDU wie Generic MAC Header (respektive Bandwidth Request Header) und CRC werden immer im Klartext übertragen.

D.3.6 Vertrauen in PKI

Bei der Verwendung des RSA-Verfahrens zur Authentisierung ist der Hersteller in der Pflicht, entsprechende Zertifikate für die Subscriber Stations entweder vor Auslieferung zu installieren oder dynamisch zu generieren. Insbesondere wenn die Zertifikate vorinstalliert wurden, muss dem Hersteller vertraut werden, dass diese sicher generiert wurden und keine zwei Geräte identisches Schlüsselmaterial besitzen. In Kooperation mit Zertifizierungsstellen stellt das WiMAX-Forum eine PKI bereit, über die Zertifikate für Sub-CAs (Certifcate Authority), Server und Clients angefordert werden können[10].

D.3.7 Erstellung von Bewegungsprofilen (Mobile WiMAX)

Mit Mobile WiMAX können sich Anwender frei bewegen. Da jedes WiMAX-Gerät eine eindeutige MAC-Adresse besitzt, kann so ein Bezug zwischen MAC-Adresse, Ort und Uhrzeit der Datenübertragung hergestellt werden. Auf diese Weise können Bewegungsprofile über mobile Nutzer in einem WiMAX-Netz erstellt werden.

10 Siehe auch http://www.wimaxforum.org/resources/pki

D.4 Schutzmaßnahmen

Nachfolgend werden entsprechende Maßnahmen beschrieben, um die aufgeführten Gefährdungen zu minimieren oder auszuschließen.

D.4.1 Absicherung der Datenkommunikation

WiMAX-Netze sollten grundsätzlich mit Verschlüsselung und Integritätsschutz betrieben werden. Die Geräte sollten immer die höchstmögliche Verschlüsselungsmethode nutzen. Für Fixed WiMAX ist für die Datenverschlüsselung beispielsweise die Verwendung von AES im CCM-Modus mit 128-Bit-Schlüssel zu empfehlen.

Wird WiMAX als Ersatz für z.B. DSL auf der letzten Meile eingesetzt, gelten für den Nutzer die entsprechenden Empfehlungen der IT-Grundschutz-Kataloge des BSI für die Absicherung eines Internet-Zugangs (siehe [GSK]). Wird WiMAX als Backbone-Technik bzw. zur LAN-Kopplung eingesetzt und werden Daten mit einem normalen oder sogar hohen Schutzbedarf übertragen, wird die Nutzung einer VPN-Lösung mit adäquater Verschlüsselung und Authentisierung empfohlen.

Weitere Schutzmaßnahmen gelten für den Anschluss eines Endgeräts an eine Subscriber Station. Dies beinhaltet insbesondere die geeignete Trennung des lokalen Systems von dem Funknetz durch den Einsatz von Firewall-Techniken (ggf. ergänzt durch ein Intrusion Detection System (IDS) oder ein Intrusion Prevention System (IPS)) und den Einsatz eines Virenschutzes für die lokal angeschlossenen Systeme.

Es gibt Subscriber Stations, die für den Anschluss von Endgeräten einen integrierten WLAN Access Point haben. Die Gefährdungslage und der empfohlene Maßnahmenkatalog entsprechen hier den Ausführungen in Kapitel A. Funk-LAN (WLAN, IEEE 802.11). Analoges gilt für Bluetooth (siehe Kapitel B. Bluetooth) oder DECT (siehe Kapitel C. DECT).

D.4.2 Absicherung der Netzelemente

Netzelemente eines WiMAX-Systems sind geeignet zu härten, damit ein erfolgreicher Angriff über die Luftschnittstelle möglichst unwahrscheinlich ist. Der Endkunde hat hierbei bestenfalls Einfluss auf die Subscriber Stations, während Base Stations und die dahinter liegende Infrastruktur in der Verantwortung des Providers liegen. Denn wenn WiMAX den Massenmarkt erreicht, besteht gerade bei den Subscriber Stations die Gefahr, dass Voreinstellungen unsicher sind bzw. der Nutzer Fehleinstellungen vornehmen kann (z.B. die Abschaltung der Verschlüsselung).

D.4.3 Absicherung der Clients bei Mobile WiMAX

Bei mobilen Clients, die sich direkt in ein Mobile-WiMAX-Netz einbuchen, sollten weitere lokale Schutzmaßnahmen implementiert werden, wie z.B. Zugriffsschutz, Benutzerauthentisierung, Virenschutz, Personal Firewall, restriktive Datei- und Ressourcenfreigabe auf Betriebssystemebene, restriktive Browser-Konfiguration, lokale Verschlüsselung (siehe [GSK]).

D.4.4 Restrisiko

Unabhängig von den beschriebenen Sicherheitsmaßnahmen sind mit der Verwendung von WiMAX-Systemen immer folgende Restrisiken verbunden:

- Das Erstellen von Bewegungsprofilen mobiler Geräte (siehe Kapitel D.3.7) kann nicht verhindert werden.
- Die Bedrohung der Verfügbarkeit ist nicht vermeidbar.

D.5 Ausblick

Mittlerweile existieren zertifizierte Produkte für Fixed WiMAX und Mobile WiMAX. Jedoch sind WiMAX-Systeme in Deutschland noch nicht weit verbreitet. In Zukunft können im Rahmen der Breitbandinitiative zur Versorgung von ländlichen Regionen weitere Systeme hinzukommen. Ähnliches gilt für die nomadische Nutzung von Mobile WiMAX. Als Gründe führen Netzanbieter die nicht zu erwartende Rentabilität sowie Konkurrenz aus dem Bereich der Mobilfunk- oder Satelliten-Technik auf. Im Mobilfunk hat sich UMTS/HSDPA/HSUPA als 3G-Technik behauptet, ein Wechsel auf Mobile WiMAX zeichnet sich derzeit nicht ab. Inwiefern sich IEEE 802.16m im Zusammenhang mit der nächsten Mobilfunkgeneration (4G) durchsetzen wird, bleibt abzuwarten. Derzeit ist insbesondere Long Term Evolution (LTE) als Nachfolger von UMTS eine Alternative zu WiMAX.

D.6 Fazit

WiMAX spezifiziert die OSI-Ebenen 1 (Physical Layer) und 2 (MAC Layer) eines drahtlosen Breitbandzugangs im MAN-Bereich. Die Sicherheitsmechanismen konzentrieren sich daher auf die reine Absicherung der Funkübertragung. Übergeordnete Aspekte wie Teilnehmerauthentisierung oder die Kriterien für die Auswahl einer Cryptographic Suite wurden bewusst in den Standards ausgeklammert. Dabei ist anzumerken, dass die Sicherheitsmechanismen bei Mobile WiMAX als deutlich sicherer anzusehen sind als bei Fixed WiMAX. Dies beinhaltet insbesondere eine gegenseitige Authentisierung, EAP als generisches Authentisierungsverfahren, den CCM-Modus auf Basis von AES für die Verschlüsselung und Integritätsprüfung der Nutzdaten sowie weitere Detailverbesserungen. Jedoch ist zunächst der Netzbetreiber durch Implementierung geeigneter Mechanismen bzw. Einsatz geeigneter Produkte gefordert, eine angemessen sichere Infrastruktur zu schaffen. Der Nutzer hat bei der Absicherung der Systeme einen nur sehr beschränkten Einfluss.

Der Nutzer, der letztendlich über WiMAX kommuniziert, sollte im Einzelfall prüfen, ob das angebotene Sicherheitsniveau auch zum Schutzbedarf der über WiMAX transportierten (bzw. erreichbaren) Daten passt. Ist dies nicht der Fall, muss er selbst zusätzliche Sicherheitsmechanismen umsetzen, wie z.B. VPN, Firewall-Systeme und IDS/IPS.

D.7 Literatur und Links

Diese Liste stellt eine wertungsfreie Auswahl ohne Anspruch auf Vollständigkeit dar.

[BARB05] Michel Barbeau, „WiMAX/802.16 Threat Analysis“, Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks, Montreal, Kanada, 2005, http://www.scs.carleton.ca/~barbeau/Publications/2005/iq2-barbeau.pdf

[BNA06] Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, „Drei neue bundesweite Breitband-Dienstleister“, Pressemitteilung vom 15. Dezember 2006, verfügbar unter http://bwa-versteigerung.bundesnetzagentur.de

[DEIN07] Andreas Deininger et al., „Security Vulnerabilities and Solutions in Mobile WiMAX“, International Journal of Computer Science and Network Security, VOL.7 No.11, 2007

[GSK] Bundesamt für Sicherheit in der Informationstechnik, „IT-Grundschutz-Kataloge“, verfügbar unter https://www.bsi.bund.de/cln_155/DE/Themen/weitereThemen/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

[HAN08] Tao Han et al., „Analysis of mobile WiMAX security: Vulnerabilities and solutions”, 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, 2008

[IEEE04] IEEE Std 802.16-2004, „Part 16: Air Interface for Fixed Broadband Wireless Access Systems“, 2004, verfügbar unter http://www.ieee.org

[IEEE05] IEEE Std 802.16e-2005, „Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems – Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands“, 2006, verfügbar unter http://www.ieee.org

[RFC3748] RFC 3748, “Extensible Authentication Protocol (EAP)”, IETF Proposed Standard, Juni 2004, http://www.ietf.org/rfc/rfc3748.txt

[RFC4017] RFC 4017, „Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs“, IETF Informational, Juni 2005, http://www.ietf.org/rfc/rfc4017.txt

[WiMAX] WiMAX Forum, http://www.wimaxforum.org

D.8 Abkürzungen

3DES	Triple Data Encryption Standard
AAA	Authentication, Authorization, and Accounting
AES	Advanced Encryption Standard
AK	Authorization Key
ASN	Access Service Network
ATM	Asynchronous Transfer Mode
BFWA	Broadband Fixed Wireless Access
BWA	Broadband Wireless Access
CA	Certificate Authority
CBC	Cipher Block Chaining
CBC-MAC	CBC with Message Authentication Code
CCM	Counter with CBC-MAC
CID	Connection Identifier
CMAC	Cipher-based Message Authentication Code
CPS	Common Part Sublayer
CRC	Cyclic Redundancy Check
CS	Convergence Sublayer
CTR	Counter
DECT	Digital Enhanced Cordless Telecommunications
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
DSL	Digital Subscriber Line
DSLAM	DSL Access Multiplexer
EAP	Extensible Authentication Protocol
EAP-TTLS	EAP-Tunneled Transport Layer Security
ECB	Electronic Code Book
EDE	Encrypt-Decrypt-Encrypt
EMSK	Extended Master Session Key
ETSI	European Telecommunications Standards Institute
GKEK	Group Key Encryption Key
GSA	Group Security Association
GTEK	Group Traffic Encryption Key
HIPERMAN	High Performance Radio Metropolitan Area Network
HMAC	Hashed Message Authentication Code
HA	Home Agent

HSDPA	High Speed Downlink Packet Access
HSUPA	High Speed Uplink Packet Access
HUMAN	High-speed Unlicensed MAN
ID	Identification, Erkennungsnummer
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMS	IP Multimedia System
IMT	International Mobile Telecommunication
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Informationstechnik
ITU	International Telecommunication Union
KEK	Key Encryption Key
LAN	Local Area Network
LOS	Line-of-Sight
LTE	Long Term Evolution
MAC	Medium Access Control
MAK	MBS Authorization Key
MAN	Metropolitan Area Network
MBS	Multicast-/Broadcast-Service
MIP	Mobile IP
MITM	Man in the Middle
MS	Mobile Station
MSK	Master Session Key
MTK	MBS Traffic Key
NLOS	Non-Line-of-Sight
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open System Interconnection
PAK	Primary Authorization Key
PHY	Physical Layer (IEEE)
PDU	Protocol Data Unit
PKM	Privacy Key Management
PMK	Pairwise Master Key
QoS	Quality of Service
RFC	Request for Comments
RSA	Rivest, Shamir und Adleman
SA	Security Association
SAID	SA Identifier
SC	Single Carrier

SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
TFTP	Trivial File Transfer Protocol
TEK	Traffic Encryption Key
UMTS	Universal Mobile Telecommunications System
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network

D.9 Glossar

3DES

Siehe Triple DES

Advanced Encryption Standard (AES)

Symmetrisches Verschlüsselungsverfahren mit einer variablen Schlüssellänge von 128, 192 oder 256 Bit.

Authentisierung

Verifizierung der Identität einer Instanz, z.B. eines Benutzers oder eines Geräts. Zweck ist oft die anschließende Autorisierung für Zugriffe. Ohne Authentisierung ist im Allgemeinen keine sinnvolle Autorisierung möglich.

Certificate Authority (CA)

Siehe Zertifizierungsstelle

Cipher Block Chaining Mode (CBC)

Betriebsart, in der Blockchiffrierungsalgorithmen arbeiten: ein Klartextblock wird zuerst mit dem im vorhergehenden Schritt erzeugten Geheimtextblock per XOR (exklusives Oder) verknüpft und danach verschlüsselt.

Counter with CBC-MAC (CCM)

CBC-MAC = Cipher Block Chaining with Message Authentication Code; CCM ist eine generische Methode für die Verschlüsselung und Integritätsprüfung von Daten, die für die Verwendung einer 128-Bit-Blockchiffrierung (z.B. AES) spezifiziert ist.

Cyclic Redundancy Check (CRC)

Prüfsumme über die zu übertragenden Daten, die in der Nachricht mitgeschickt wird und es dem Empfänger gestattet, Bitfehler, die auf dem Kommunikationskanal entstanden sind, zu erkennen.

Data Encryption Standard (DES)

Weit verbreiteter symmetrischer Verschlüsselungsalgorithmus; wird aufgrund der verwendeten Schlüssellänge von nur 56 Bit für viele Anwendungen als nicht ausreichend sicher erachtet. Die effektive Schlüssellänge kann durch Mehrfachanwendung des DES (siehe Triple DES, kurz 3DES) vergrößert werden.

Denial of Service (DoS)

Ein Angriff vom Typ Denial of Service hat zum Ziel, die Arbeitsfähigkeit des angegriffenen Objekts möglichst stark zu reduzieren. Dies beinhaltet beispielsweise die systematische Überlastung eines Netzknotens durch unsinnigen Verkehr (Dummy Traffic) oder die beabsichtigte Herbeiführung eines Fehlerzustands durch das Einspielen fehlerhafter Nachrichten.

Dictionary-Attacke

Siehe Wörterbuchattacke

Electronic Code Book Mode (ECB)

Betriebsart, in der Blockchiffrierungsalgorithmen arbeiten; einfachster und zugleich unsicherster Modus, denn es werden die Teile des Klartextblocks nacheinander und unabhängig voneinander in den Geheimtextblock überführt.

Extensible Authentication Protocol (EAP)

Rahmen (Framework) für die Verwendung von Authentisierungsmethoden. Es wird u.a. für PPP oder auch in Verbindung mit EAPOL unter IEEE 802.1X verwendet.

Fresnel Zone

Siehe LOS

Handover

Wechsel von einem (physikalischen) Kommunikationskanal auf einen anderen unter Aufrechterhaltung der Ende-zu-Ende-Kommunikationsbeziehung.

LOS

LOS ist eine Abkürzung für Line-of-Sight: Sichtverbindung bedeutet hier stets eine funktechnische (nicht optische) Sichtverbindung. Dabei muss ein spezielles Ellipsoid mit einer gewissen Ausdehnung zwischen Sender und Empfänger weitestgehend frei von Hindernissen sein. Dies ist die sogenannte Fresnel Zone.

Man in the Middle

Der Angreifer positioniert sich zwischen zwei Kommunikationspartner und täuscht beiden Parteien vor, der jeweils erwartete eigentliche Partner zu sein. Dabei kann der Man in the Middle den Dialog zwischen den beiden Parteien belauschen oder auch verfälschen. Ziel ist oft die Ermittlung von Passwörtern.

Triple DES (3DES)

Bei 3DES werden drei DES-Chriffrierer hintereinander geschaltet, wobei der mittlere DES-Chriffrierer invers eingebaut ist (Encrypt-Decrypt-Encrypt, kurz: EDE).

WiMAX-Forum

Vereinigung von Herstellern von WiMAX-Komponenten nach IEEE 802.16

Wörterbuchattacke

Eine Wörterbuchattacke (auch als Dictionary-Attacke bezeichnet) wird typischerweise zum Raten eines Passworts oder Schlüssels eingesetzt. Die Annahme für eine Wörterbuchattacke ist, dass Passwörter oder Schlüssel aus einer sinnvollen oder in Wörterbüchern bekannten Zeichenkombination bestehen. In diesem Falle kann das Verfahren schnell zum Erfolg führen.

Zertifikat

Von einer Zertifizierungsstelle (Certificate Authority, CA) beglaubigter öffentlicher Schlüssel, der einer Person oder einem Objekt zugeordnet ist.

Zertifizierungsstelle

Element einer PKI, welche für das Ausstellen von digitalen Zertifikaten zuständig ist.

E. Richtfunktechniken

Inhaltsverzeichnis des Abschnitts

E.1 Grundlagen und Funktionalität

Die Planer von modernen Kommunikationsanlagen mit lokal begrenzten Reichweiten, wie sie in einem Local Area Network (LAN) oder einem Metropolitan Area Network (MAN) vorzufinden sind, stehen bei der Planung eines gebäudeübergreifenden Primärnetzes immer wieder vor dem gleichen Problem: Wie kann zwischen zwei Gebäuden eine hohe Datenrate mit möglichst geringem Verkabelungsaufwand realisiert werden? Entspricht die Verkabelung nicht den Anforderungen bzw. sind die Betriebskosten von angemieteten Leitungen zu hoch, gibt es die Alternativen Neuverkabelung, Freiraumübertragung oder Nutzung des Internets mit Hilfe von VPN. Immer häufiger wird auch bei hochperformanten Verbindungen aus Kostengründen die Freiraumübertragung gewählt.

Bei der Freiraumübertragung wird unterschieden in

- Richtfunk in nicht genehmigungspflichtigen Frequenzbereichen (z.B. WLAN nach IEEE 802.11),
- genehmigungspflichtigen Richtfunk und
- anmeldepflichtigen optischen Richtfunk (Free Space Optics, FSO).

Streng genommen stellt die FSO-Übertragung eine Infrarot-Technik dar und ist damit im eigentlichen Sinne keine „Funktechnik“. Da der allgemeine Sprachgebrauch jedoch auch den Begriff „optischer Richtfunk“ vorsieht, wird nachfolgend als Oberbegriff für die drei oben genannten Techniken der Begriff „Richtfunk“ verwendet.

Alle betrachteten funkbasierten Techniken werden in der klassischen Hochfrequenztechnik als „mikrowellenbasiert“ bezeichnet, da sie in einem Frequenzbereich mit sehr kurzen Wellenlängen arbeiten. Da jedoch mit dem Begriff Mikrowellen-Richtfunk im Allgemeinen die Verwendung einer Übertragungstechnik mit Trägerfrequenzen oberhalb von 6 GHz assoziiert wird, wird nachfolgend WLAN als Richtfunk-Technik nicht näher betrachtet. Weitergehende Informationen zur Verwendung von WLAN als Richtfunktechnik sind in Kapitel A.4.4.5 aufgeführt.

Der breitbandige drahtlose Netzzugang mittels Richtfunk im Punkt-zu-Mehrpunkt-Betrieb, auch als Broadband Wireless Access (BWA) bekannt, wird in diesem Kapitel nicht berücksichtigt. Hier wird auf die weiteren Kapitel dieses Dokuments verwiesen, speziell auf Kapitel D. WiMAX, IEEE 802.16 und Kapitel I.3 IEEE 802.22 – Wireless Regional Area Network (WRAN).

Richtfunksysteme mit WLAN-Technik nach IEEE 802.11 liefern in den meisten Fällen eine Ethernet-Schnittstelle (gemäß IEEE 802.3) zum Anschluss an das kabelbasierte Netz. Die Schnittstellen von Mikrowellen-Richtfunksystemen zum kabelbasierten Netz dagegen sind meistens technologieneutral, sie erlauben beispielsweise sowohl Ethernet- als auch TDM-basierte Dienste. Derartige transparente Systeme bieten den Vorteil, dass an die Schnittstelle zum kabelbasierten Netz jede Übertragungstechnik angeschlossen werden kann. Das Richtfunk-System erkennt jeden beliebigen Bitstrom und überträgt ihn in den Freiraum. Damit besteht die Möglichkeit, die Schnittstelle zum kabelbasierten Netz für unterschiedlichste Übertragungsverfahren zu nutzen; bei Wechsel der kabelgebundenen Übertragungstechnik muss das Mikrowellen-Richtfunksystem nicht ausgetauscht werden.

E.1.1 Mikrowellen-Richtfunksysteme

Im Unterschied zu optischen Richtfunksystemen nutzen Mikrowellen-Richtfunksysteme elektromagnetische Signale als Informationsträger.

Abhängig von der zu überbrückenden Entfernung stehen bei Mikrowellen-Richtfunksystemen verschiedene genehmigungspflichtige und genehmigungsfreie Frequenzbänder zur Verfügung. Die in Deutschland genutzten genehmigungspflichtigen Trägerfrequenzen liegen bei 4, 6, 7, 13, 15, 18, 23, 26, 28, 32 und 38 GHz[1]. Diese Frequenzen sind teilweise noch in weitere Frequenzbereiche unterteilt, die jeweils einen oder mehrere Kanäle der Richtfunkstrecke bilden. Seit 2008 liegt eine Allgemeinzuteilung für den Punkt-zu-Punkt Richtfunk im Frequenzbereich von 59 GHz bis 63 GHz der Bundesnetzagentur [BNA08] vor. Dies ermöglicht einen genehmigungsfreien Betrieb von Richtfunksystemen im 60-GHz-Bereich für Reichweiten bis ca. 1 km und Datenraten von ca. 100 Mbit/s.

Die Übertragungsfrequenz bestimmt zusammen mit dem Antennendurchmesser und der Sendeleistung die maximal zu überbrückende Distanz; Reichweiten von mehr als 50 km mit einer Datenrate von über 600 Mbit/s sind nutzbar. Die Systeme arbeiten in von der Bundesnetzagentur koordinierten Frequenzbändern und weisen folgende Vorteile gegenüber den Frequenzbändern von WLAN-Systemen auf:

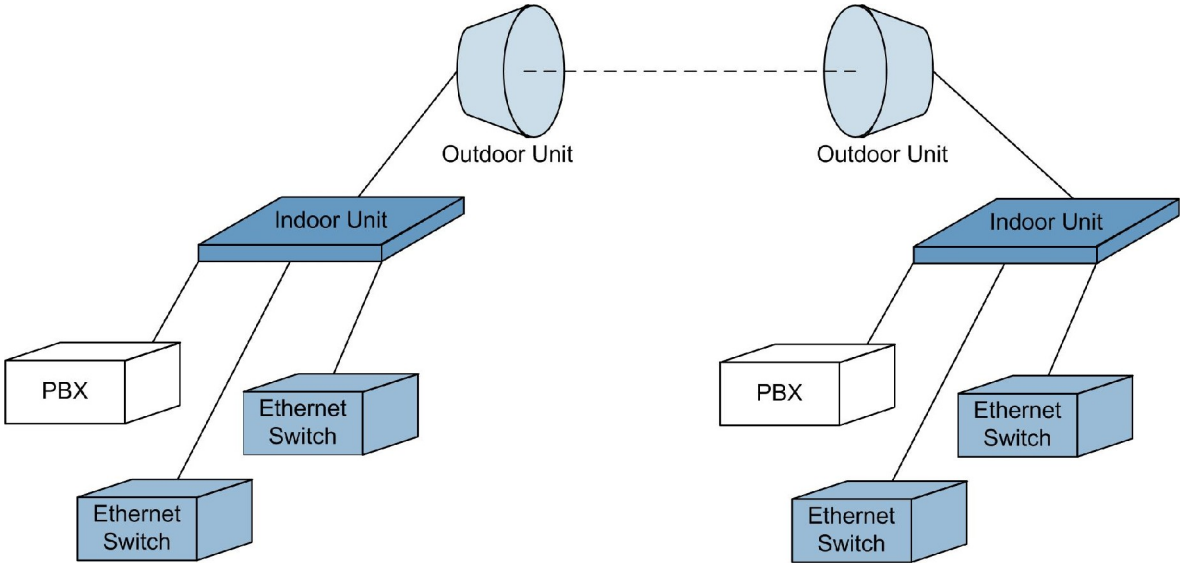
- Exklusive Zuweisung der Betriebsfrequenz an nur einen Nutzer
- Koordinierter Betrieb der Richtfunksysteme, dadurch keine Störungen durch andere Nutzer im selben Frequenzband

Eine Ausnahme bildet hierbei der erwähnte Frequenzbereich um 60 GHz. Aufgrund der beschränkten Reichweite ist die Wahrscheinlichkeit für eine Störung durch andere Nutzer jedoch geringer. Ein Schutz vor Beeinträchtigungen lässt sich hieraus jedoch nicht ableiten.

Die meisten Mikrowellen-Richtfunksysteme bestehen aus einer Innen- und einer Außeneinheit. Die Inneneinheit (Indoor Unit) enthält die Schnittstellenelektronik (z.B. Ethernet-Schnittstellen), den internen Multiplexer und die Stromversorgung für die Außeneinheit. Die Außeneinheit (Outdoor Unit) erzeugt das hochfrequente Sendesignal und gibt es an die Antenne ab. Diese wird zusammen mit der Antenne an einem Antennenträger auf dem Dach eines Gebäudes oder an einem Mast installiert. Sie enthält den Empfänger mit der zugehörigen Signalverarbeitung. Als Antennen werden Parabolantennen eingesetzt, die ein hohes Maß an Bündelung und Parallelität der Strahlen sicherstellen. Die Polarisation des Funkfeldes ist über eine Drehung der Antenne vertikal oder horizontal einstellbar. Mit Hilfe eines Koaxialkabels werden beide Einheiten miteinander verbunden; auch die Spannungsversorgung der Außeneinheit erfolgt über dieses Koaxialkabel.

[1] Informationen zu den Nutzungsbedingungen sowie der aktuelle Frequenznutzungsplan sind über die Web-Seiten der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (http://www.bundesnetzagentur.de) verfügbar.

Abbildung E-1: Komponenten eines Mikrowellen-Richtfunksystems (Punkt-zu-Punkt)



Falls zwischen den Endpunkten keine direkte Sichtverbindung besteht, lässt sich ein indirekter Weg über aktive oder passive Relaisstellen herstellen (Richtfunkrelais). Beispielsweise gibt es passive Umlenkantennen, d.h. direkt über Hohlleiter gekoppelte Antennen, die keine aktiven Elemente enthalten und demzufolge keinen Stromanschluss benötigen.

Mikrowellen-Richtfunksysteme werden grundsätzlich für Punkt-zu-Punkt-Verbindungen oder Punkt-zu-Mehrpunkt-Verbindungen verwendet. Die Punkt-zu-Punkt-Richtfunksysteme verbinden zwei Stationen über eine Richtfunkstrecke, sie werden häufig in Weitverkehrsnetzen und zur Überbrückung großer Distanzen verwendet. Jedoch auch geringe Distanzen, z.B. zur Kopplung zweier Nachbargebäude sind ein häufiger Anwendungsfall von Punkt-zu-Punkt-Verbindungen. Bei Punkt-zu-Mehrpunkt-Verbindungen versorgt ein Richtfunksystem sternförmig mehrere Teilnehmer gleichzeitig.

Die Hersteller nutzen unterschiedliche Modulationsverfahren, sodass eine Kombination von verschiedenen Herstellern kaum möglich ist.

Die Datenübertragung in Richtfunksystemen geschieht typischerweise ausschließlich auf physikalischer Ebene. PDH (Plesiochronous Digital Hierarchy) arbeitet mit Asynchron-Übertragung ohne identischem Takt und SDH (Synchronous Digital Hierarchy) mit Synchron-Übertragung, wobei die Synchronisierung über ein zentrales Taktsignal erfolgt. Das PDH-Verfahren hat diverse Nachteile beim Multiplexen bzw. Demultiplexen, deshalb wird PDH zunehmend durch SDH abgelöst.

E.1.2 Broadband Fixed Wireless Access (BFWA)

Für Mikrowellen-Richtfunk hat die Bundesnetzagentur im August 2007 eine Allgemeinzuteilung der Frequenzen im Bereich von 5755 MHz bis 5875 MHz für gewerblich öffentliche, breitbandige und ortsfeste Verteilsysteme erlassen [BNA07]. Die Frequenzen können sowohl für Punkt-zu-Punkt- als auch Punkt-zu-Mehrpunkt-Richtfunk, vermaschte Netze oder Kombinationen aus diesen genutzt werden.

Die Nutzung der Frequenzen ist hierbei nicht an einen bestimmten technischen Standard gebunden, sondern explizit als technologieneutral gekennzeichnet. Somit ist dieser Frequenzbereich beispielsweise sowohl für WLAN als auch WiMAX geeignet. Ziel ist es auch hier, die Versorgung in ländlichen Regionen mit Breitbandanschlüssen zu fördern. Weiterhin ist die Nutzung der Frequenzen nicht genehmigungspflichtig und damit kostenfrei. Da der Frequenzbereich jedoch für die gewerbliche und öf-

fentliche (d.h. nicht firmeninterne) Nutzung vorgesehen ist, erfordert dies eine Anmeldung gemäß § 6 des Telekommunikationsgesetzes (TKG). Gemeldet werden müssen beispielsweise Aufnahme, Änderung und Beendigung des Betriebs. Weiterhin gelten die in Tabelle E-1 wiedergegebenen Frequenznutzungsparameter.

Da der Frequenzbereich bereits durch andere Anwendungen genutzt wird, wie beispielsweise militärische Radarsysteme und Anwendungen des Festen Funkdienstes (Funkdienst zwischen bestimmten festen Punkten), ist BFWA nur ein Sekundärnutzer. Entsprechend sind Mechanismen zum Schutz des Primärnutzers bei BFWA zwingend vorgeschrieben. Hierzu gehören Verfahren für den automatischen Frequenzwechsel (Dynamic Frequency Selection, DFS) bei Erkennung von z.B. Radarsignalen sowie Anpassungen der Sendeleistung (Transmit Power Control, TPC). Generell gilt bei der Nutzung des Frequenzbereiches die europäische Norm ETSI EN 302 502 (siehe [EN302502]).

Insbesondere WLAN-Systeme nach IEEE 802.11a/n können diese Frequenzen bereits nutzen. Auf diese Weise können Outdoor-WLAN-Systeme im Punkt-zu-Mehrpunkt- oder Punk-zu-Punkt-Betrieb mit bis zu 4 Watt (36 dBm) betrieben werden. Hier bieten einige Hersteller bereits entsprechend aktualisierte Firmware an, sodass ein Umstieg auf eine andere Hardware entfällt.

Bezüglich der Gefährdungen und Maßnahmen wird auf das Kapitel der jeweils genutzten Technik verwiesen, beispielsweise WLAN oder WiMAX.

Tabelle E-1: Frequenznutzungsparameter bei BFWA

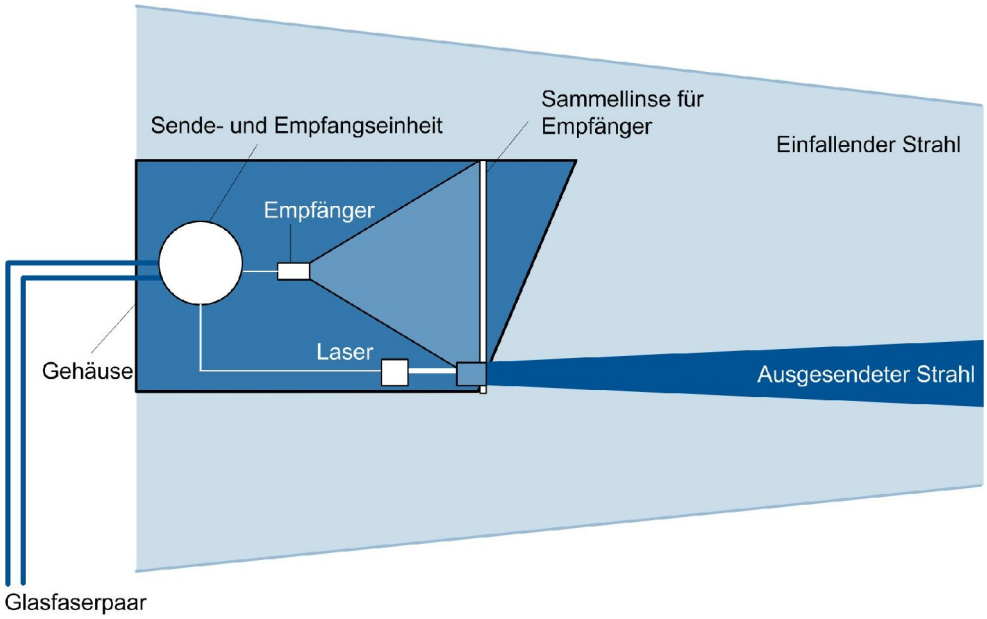
	Punkt-zu-Mehrpunkt	**Punkt-zu-Punkt**	**Mesh-Netze**	**Kombinierte Netze**
Maximal zulässige mittlere äquivalente isotrope Strahlungsleistung in dBm (EIRP[2])	36	36	33	33
Maximal zulässige spektrale Strahlungsleistungsdichte in dBm/MHz (EIRP)	23	23	20	20
Bereich der Leistungsregelung (TPC) in dB	12	12	12	12
Weitere Bestimmungen für den Frequenzbereich 5755 MHz bis 5850 MHz	Dynamisches Frequenzwahlverfahren (DFS)	Dynamisches Frequenzwahlverfahren (DFS)	Dynamisches Frequenzwahlverfahren (DFS)	Dynamisches Frequenzwahlverfahren (DFS)

E.1.3 Optische Systeme

Im Unterschied zu Mikrowellen-Richtfunksystemen nutzen FSO-Systeme für die Übertragung im Freiraum Licht im infraroten Spektrum mit einer Wellenlänge zwischen 760 nm und 1550 nm. Der von einer Datenquelle wie z.B. einem Switch gelieferte Datenstrom wird mit Hilfe einer Strahlenquelle in Form einer Leuchtdiode oder Laserdiode direkt durch den Freiraum zu einer Empfangsstation gesendet. Im Empfänger befinden sich Fotodioden, welche die optischen Impulse in elektrische Impulse zurückverwandeln.

2 EIRP = Equivalent Isotropically Radiated Power

Abbildung E-2: Aufbau eines optischen Richtfunksystems

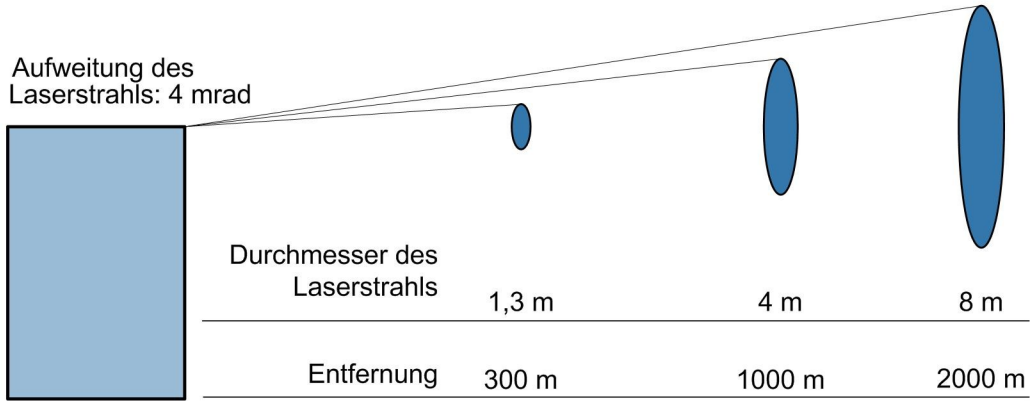


Auf dem optischen Kanal bedient man sich eines einfachen binären Kodierungsverfahrens, der Verwendung eines „Licht an/Licht aus“-Schemas. Der an- bzw. abgehende kabelbasierte Kanal ist abhängig von dem verwendeten Übertragungsverfahren. Bei FSO-Systemen ist meistens nur die kabelbasierte Schnittstelle standardisiert (z.B. 100BaseFX oder 1000BaseSX/LX), die Freiraumschnittstelle dagegen ist herstellerabhängig. Somit setzt der Aufbau von optischen Richtfunkstrecken derzeit immer zwei Geräte von einem Hersteller und aus der gleichen Produktreihe voraus.

Im Vergleich zu Mikrowellen-Richtfunksystemen zeichnen sich FSO-Systeme durch eine deutlich höhere nutzbare Datenrate aus, Systeme mit über 1 Gbit/s sind auf dem Markt erhältlich. Dagegen ist die nutzbare Reichweite im Vergleich zu Funktechniken in genehmigungspflichtigen Frequenzbändern deutlich geringer: Mit FSO-Technik kann deutlich weniger als 5 km überbrückt werden, bei Mikrowellenrichtfunk können zum Vergleich 50 km und mehr überbrückt werden.

Der Durchmesser eines Lichtstrahls hat die Eigenschaft, bei zunehmender Entfernung von der Lichtquelle größer zu werden, dies gilt auch für kohärentes Licht, wie es z.B. eine Laserquelle aussendet. Die übliche Aufweitung des Strahls am Sender von 2 mrad bis 10 mrad führt z.B. bei einer Entfernung von ca. 1 km zu einer ausgeleuchteten Kreisfläche von 2 m bis 10 m Durchmesser. Erhöht sich die Distanz z.B. auf 2 km, beträgt der Kreisdurchmesser 4 m bis 20 m. Diese Strahlaufweitung (Divergenz) ist notwendig, um mögliche physikalische Schwankungen des Sendesystems, bedingt z.B. durch Windeinflüsse, auf der Empfangsseite kompensieren zu können.

Abbildung E-3: Aufweitung eines Laserstrahls



Alle Systeme überbrücken die Sichtweite auch bei Regen, Schneefall oder Dunst. Je nach Wetterlage kann es allerdings sein, dass die Bitfehlerrate ansteigt und im Extremfall die Verbindung vollkommen ausfällt. Als grober Richtwert für den Beginn eines Totalausfalls wird die Sichtweite des menschlichen Auges herangezogen: Ist die Gegenstation nicht mehr zu sehen, so muss mit einer Kommunikationsunterbrechung gerechnet werden.

E.2 Sicherheitsmechanismen

Mikrowellen- und FSO-Richtfunksysteme haben ihre Wurzeln im Bereich der Telekommunikation auf der Ebene der physikalischen Übertragung. In diesem Sinne wird eine Richtfunkstrecke wie ein Kabel behandelt.

Daher werden von Anbietern auf Mikrowellen- oder FSO-Technik basierter Richtfunksystemen oft keine Mechanismen zur Absicherung der Kommunikation (Authentisierung, Verschlüsselung und Integritätsprüfung) eingesetzt. Wenn dennoch Sicherheitsmechanismen in den Produkten integriert sind, handelt es sich teilweise um proprietäre Eigenentwicklungen, deren Funktionsweise der Hersteller gar nicht oder nur sehr begrenzt offenlegt.

Es wird bei diesen Richtfunksystemen also davon ausgegangen, dass eine höhere Protokollschicht die notwendigen Sicherheitsfunktionen implementiert.

E.3 Gefährdungen

Nachfolgend werden die Gefährdungen für Mikrowellen-Richtfunksysteme und FSO-Systeme beschrieben. Entsprechende Maßnahmen, um diese Gefährdungen zu minimieren oder auszuschließen, sind in Kapitel E.4 beschrieben.

E.3.1 Ausfall durch höhere Gewalt

Allgemein

Wie im kabelgebundenen LAN kann es auch im Richtfunk durch Überspannungen zum Ausfall von Richtfunk-Komponenten kommen.

Bei allen außen montierten Systemen ist darauf zu achten, dass Überspannungen in Folge eines direkten oder indirekten Blitzeinschlags zu einer Beschädigung der Systeme führen können. Neben der Beschädigung der Richtfunksysteme selber besteht zusätzlich die Gefahr, dass eine Überspannung ins Gebäude eintritt und dort weitere Schäden wie z.B. die Zerstörung der aktiven Netzwerkkomponenten anrichtet.

Mikrowellen-Richtfunk

Beim Mikrowellen-Richtfunk spielen Wettereinflüsse nur eine untergeordnete Rolle. Mit Ausnahme von extrem starkem Regen wird die Datenübertragung durch Wettereinflüsse nicht beeinflusst.

FSO-Systeme

Bei FSO-Systemen müssen witterungsbedingte Einflüsse von z.B. Regen, starkem Nebel oder Schneefall besonders berücksichtigt werden. Diese sind wiederum direkt abhängig von der Entfernung zwischen Sender und Empfänger.

E.3.2 Mangelhafte Planung

Da alle richtfunkbasierten Systeme bei einer LAN-Kopplung prinzipiell wie Kabelverbindungen einzustufen sind, müssen bei ring- oder maschenförmigen Topologien zusätzliche Mechanismen eingesetzt werden, um eine Schleife (Loop) zu verhindern. Durch Einsatz solcher Mechanismen wie z.B. Spanning Tree Protocol oder Routing-Redundanzen können weitere Gefahren entstehen; zu nennen sind z.B. falsch konfigurierte Spanning-Tree-Topologien.

E.3.3 Bedrohung der Verfügbarkeit

Mikrowellen-Richtfunk

Der Einsatz von Richtfunksystemen in genehmigungspflichtigen Frequenzbereichen bietet prinzipiell eine hohe Störunempfindlichkeit, da eine Nutzung der Frequenz nur nach Freigabe durch die Bundesnetzagentur möglich ist.[3]

FSO-Systeme

FSO-Systeme kommen – bezogen auf Störunempfindlichkeit – der kabelbasierten Übertragung am nächsten und können in manchen Fällen als Ersatz für Glasfaserverbindungen in Erwägung gezogen werden.

Kurze Unterbrechungen, beispielsweise durch Vögel, die den Strahl kreuzen, korrigiert das übergeordnete Protokoll oder bei Mehrkanalsystemen auch das FSO-System selber. Im ersten Fall werden die Daten automatisch erneut übertragen. Allerdings ist ein FSO-System sehr wetterempfindlich (siehe Kapitel E.3.1).

Für FSO-Systeme besteht weiterhin für große Übertragungsstrecken ab 1000 m bei starkem Nebel die Gefahr einer Kommunikationsunterbrechung. Aus diesem Grunde bieten einige Hersteller funkbasierte Backup-Systeme, auf die automatisch umgeschaltet werden kann.

FSO-Systeme sind generell anfällig gegenüber Einflüssen durch das Wetter. Die Schwierigkeit der Einschätzung des Einflusses auf die Verfügbarkeit liegt insbesondere darin, dass die wetterabhängige Schwankungsbreite nicht verifizierbar und regional sehr unterschiedlich ist. Wer eine hohe Verfügbarkeit des Systems erreichen will oder muss, sollte mit geringeren Reichweiten kalkulieren.

Weiterhin muss der Wartungsaufwand von FSO-Systemen berücksichtigt werden, da diese Geräte zum Teil an sehr exponierten Stellen montiert werden und zur Wartung hohe Leitern oder gar Steiger notwendig sind. Dies muss in der Planung besonders berücksichtigt werden.

E.3.4 Abhören

Allgemein

Eine Verschlüsselung der Luftschnittstelle ist bei den Richtfunktechniken weder vorgeschrieben noch standardisiert.

Mikrowellen-Richtfunk

Obwohl beim Mikrowellen-Richtfunk sehr stark bündelnde Parabolantennen eingesetzt werden, kann eine absolute Parallelität der Strahlen bedingt durch äußere Störeinflüsse nicht sichergestellt werden. Die daraus resultierende Streuung der Strahlen ermöglicht ein Belauschen der Verbindung, was keine Signalbeeinflussung zur Folge hat und demzufolge nur schwierig festgestellt werden kann. Allerdings muss der potenzielle Lauscher zum Abhören neben der Sende- und Empfangsfrequenz auch die Polarisation, das Modulationsverfahren sowie Typ und Rahmenkodierung kennen.

[3] Richtfunkvarianten in nicht genehmigungspflichtigen Frequenzbereichen haben den Nachteil, dass ihre Anfälligkeit gegen Störungen durch andere, im gleichen Frequenzbereich arbeitende Übertragungssysteme im Einzelfall sehr groß sein kann. Das 2,4-GHz-Band wird beispielsweise auch von privaten WLANs, Bluetooth, Bewegungsmeldern und weiteren Systemen genutzt.

FSO-Systeme

Generell erschweren optische Richtfunksysteme im Vergleich zu funkbasierten Systemen aus folgenden Gründen das Aufzeichnen eines Signalstroms:

- Der Strahlengang ist scharf gebündelt.
- Ein Abhören ist praktisch nur durch Unterbrechen bzw. Umlenken des Strahls möglich, dabei muss natürlich die weitere Kommunikation aufrechterhalten werden.
- Der Strahlenverlauf verläuft in der Regel in erheblicher Höhe über dem Erdboden.

Trotz der scharfen Bündelung des Strahls muss davon ausgegangen werden, dass sich der Strahl mit zunehmender Entfernung aufweitet. Es ist somit denkbar, dass insbesondere am Empfangspunkt ein Fremdsystem in den aufgeweiteten Strahl montiert wird und die Funkdaten ausliest, ohne dass die produktive Kommunikation unterbrochen und die Störung bemerkt wird.

FSO-Systeme mit automatischem Funk-Backup bei Wetterverschlechterung bergen das Risiko, dass für die Backup-Verbindung keine ausreichenden Maßnahmen zur Abhörsicherheit getroffen wurden. In diesem Fall ist dann ein gezieltes Aufzeichnen des Signalstromes und Mitlesen der Daten denkbar. Man kann sich ein Szenario vorstellen, bei dem z.B. durch gezielte Raucheinwirkung am Empfangsteil das sendende FSO-System zum Umschalten auf die nicht geschützte Funkstrecke gezwungen wird.

E.3.5 Verletzungsgefahr

Jeder Laser stellt insbesondere für das menschliche Auge eine Gefahrenquelle dar: Ist z.B. die Leistung des Lasers zu hoch, so besteht die Gefahr einer Verletzung der Netzhaut. Die unterschiedlichen Eigenschaften, bezogen auf den Schutz der Augen, wurden von internationalen Standardisierungsgremien durch Einführung von Laserleistungsklassen berücksichtigt[4] (z.B. [IEC60825-1]).

E.3.6 Unsichere Konfiguration der Inneneinheit

Insbesondere Inneneinheiten mit einer Ethernet-Schnittstelle für das Management auf Basis von TCP/IP-Protokollen stellen eine Gefährdung dar, wenn diese Schnittstelle nicht angemessen abgesichert ist.

Die folgenden Punkte sollten hierbei berücksichtigt werden:

- Die Administration erfolgt in der Regel über unverschlüsselte Protokolle wie z.B. HTTP.
- Durch die Nutzung von IP ist für den Zugriff auf die Administrationsschnittstellen kein direkter lokaler Zugriff nötig, im Gegensatz zu beispielsweise einem direkten Konsolenanschluss. Dies ermöglicht bei fehlender Absicherung der IP-basierten Kommunikation auch einen Fernzugriff durch nicht autorisierte Personen.

Ebenso stellen aktivierte, aber nicht genutzte Funktionen generell eine Gefährdung dar, da die Angriffsfläche hierbei unnötig vergrößert wird.

Weitere Informationen hierzu können den IT-Grundschutz-Katalogen des BSI entnommen werden (siehe [GSK]). Als Grundlage des auszuwählenden IT-Systems kann hierfür der Baustein „Router und Switches“ betrachtet werden.

---

4 Siehe auch http://de.wikipedia.org/wiki/Laser#Laser-Klasse.

E.4 Schutzmaßnahmen

Nachfolgend werden entsprechende Maßnahmen beschrieben, um die aufgeführten Gefährdungen zu minimieren oder auszuschließen.

E.4.1 Sorgfältige Planung

Montage der Richtfunk-Systeme optimieren

Wichtigste Voraussetzung für den zuverlässigen Betrieb aller Systeme ist eine sichere Montage. Bereits bei der Planung des Standortes für Richtfunk-Systeme kann das Risiko einer Sabotage erheblich reduziert werden, indem – sofern möglich – die Systeme versteckt aufgestellt werden und damit nicht einfach zu entdecken sind. Beispielsweise erlauben FSO-Systeme auch eine Montage im Innenbereich hinter einem Fenster.

Außerdem sollten die Systemteile in Bereichen montiert werden, in denen ein unkontrollierter Zugang ausgeschlossen werden kann. Dies impliziert bei Einsatz von FSO-Systemen auch den Bereich des aufgeweiteten Lichtstrahls, auch hier sollte ein unautorisierter Zugang ausgeschlossen werden.

Schutz gegen Überspannungen durch Blitzeinschlag

Zum Schutz gegen Überspannungen durch Blitzeinschlag sind zwei wesentliche Maßnahmen zu treffen: Zum einen sind die Systeme durch Blitzfangstangen und weitere Maßnahmen gegen direkten Einschlag zu schützen. Zusätzlich ist durch geeignete Wahl der Datenleitungen (bevorzugt werden Lichtwellenleiter) oder Überspannungsschutzgeräte bei Kupferleitungen der Eintritt von Überspannungen ins Gebäude zu unterbinden (indirekte Blitzeinschlagwirkung). Dies gilt in gleicher Form für die Stromversorgung der Geräte.

Der kupferbasierte Datenanschluss eines außenmontierten Richtfunksystems ist nach Möglichkeit zu vermeiden, stattdessen sollten glasfaserbasierte Anschlüsse präferiert werden.

Untersuchung der Einsatzumgebung auf mögliche Störungen

Bei den meisten Richtfunk-Systemen benötigt man eine uneingeschränkte Sichtverbindung zwischen den beiden Standorten.

Im Falle einer Nutzung von mikrowellenbasierten Techniken ist eine Abwesenheit von Hindernissen innerhalb der sogenannten Fresnel-Zone[5] gefordert.

Planung von Backup-Mechanismen

Um bei wetterbedingten Verschlechterungen des Übertragungskanals einen alternativen Kommunikationskanal bereitzustellen, sollten Backup-Mechanismen eingeplant werden.

Bei optischen Systemen bieten sich nicht-optische, funkbasierte Backup-Lösungen an, sowohl herstellerspezifische als auch standardisierte WLAN-Lösungen. Alternativ können Backup-Lösungen durch

[5] Die Fresnel-Zone ist ein spezielles Ellipsoid mit einer gewissen Ausdehnung, der zwischen Sender und Empfänger weitestgehend frei von Hindernissen sein sollte, damit es nicht zu Verschlechterungen der Übertragungsqualität kommt.

Einsatz von terrestrischen Leitungen geschaffen werden. Hier ist möglicherweise ein geringerer Datendurchsatz zu berücksichtigen, z.B. beim Einsatz von ISDN-Leitungen.

Planung der rechtzeitigen Umschaltung auf Backup-Mechanismen

Um frühzeitig das wetterbedingte Absinken eines Signalpegels erkennen zu können und bereits vor dem Ausfall Vorbereitungen zu treffen, die z.B. eine Umschaltung auf alternative Verbindungen möglich machen (beispielsweise auf klassische terrestrische Leitungen), sollten die Systeme über integrierte Überwachungsfunktionen verfügen. Viele Systeme auf dem Markt bieten z.B. SNMP-Agenten an, die bei Unterschreitung eines zuvor definierten Schwellpegels einen Alarm generieren.

Die Überwachung der Systeme muss sich auf zwei Hauptaufgaben fokussieren: Kontrolle der Übertragungsqualität (z.B. Bitfehlerrate) und Kontrolle des Empfangspegels. Die ausschließliche Kontrolle der letztendlich relevanten Übertragungsqualität erlaubt dem Betreiber der Strecke ein Eingreifen erst bei beginnender Einbuße der Übertragungsqualität. Wird dagegen der Empfangspegel direkt überwacht, so kann mit entsprechender Schwellwertsetzung bereits vorher auf eine sich verändernde Wetterlage reagiert werden. Deshalb ist eine Pegelkontrolle mit automatischer Meldung bei Schwellwertunterschreitung ein absolutes Muss an Management-Funktionalität.

E.4.2 Sichere Konfiguration der Inneneinheit

Da die Systeme oft auch mit Ethernet-Schnittstellen ausgestattet sind und TCP/IP nutzen, sind entsprechende Maßnahmen zur Absicherung nötig. Generell wird hier auf die IT-Grundschutz-Kataloge verwiesen. Die Maßnahmen zielen dabei beispielsweise auf die folgenden Punkte:

- Deaktivierung nicht benötigter Funktionen und Schnittstellen, beispielsweise SNMPv1/v2, HTTP oder Telnet. Alternativ könnte die Administration über eine serielle Schnittstelle erfolgen.
- Deaktivierung bzw. restriktive Handhabung von Fernwartungsfunktionen
- Beschränkung von IP-basierten Administrationszugriffen auf das System auf ein (physikalisch oder logisch) separates Netz
- Verwendung von verschlüsselten Protokollen wie z.B. SNMPv3 mit Authentisierung/Verschlüsselung, HTTPS oder SSH
- Kennwortschutz und Rechteverwaltung

Weitere zu berücksichtigende Themen sind:

- Überwachung des Gesamtsystems mit Hilfe von Management-Werkzeugen
- Datensicherung und Wiederherstellung
- Software-Pflege

E.4.3 Überwachung der Systeme zur Erkennung von Lauschangriffen

Zur Erkennung eines Lauschangriffs auf eine Richtfunk-Verbindung kann insbesondere bei FSO-Systemen in Betracht gezogen werden, mit Hilfe einer Videokamera den Übertragungsweg permanent zu überwachen.

E.4.4 Zusätzliche Sicherheitsmechanismen

Die Möglichkeit einer Datenverschlüsselung wird durch die Systeme in der Regel nicht geboten und ein Abhören des Signalstroms kann nicht ausgeschlossen werden. Deshalb wird für alle beschriebenen Richtfunksysteme empfohlen, durch Zusatzmaßnahmen, wie beispielsweise durch die Nutzung eines VPN, für Authentisierung, Verschlüsselung und Integritätsschutz zu sorgen. Diese Verschlüsselung muss bereits im kabelbasierten Netz stattfinden, damit die Funksysteme ausschließlich verschlüsselte Informationen konvertieren und übertragen können.

E.4.5 Schutz vor Verletzungen

Für optische Freiraumsysteme wird in der Regel die Anforderung gestellt, Systeme zu spezifizieren, die für die Augen sicher sind und ohne zusätzliche Zugangsbeschränkungen für nicht ausgebildetes Personal (wie z.B. Fensterputzer oder Wartungspersonal auf dem Dach) betrieben werden können. Dadurch reduzieren sich die in Frage kommenden Lasersicherheitsklassen nach IEC auf 2 Klassen:

- Klasse 1: Laser, die unter normalen Umständen sicher zu benutzen sind und mit optischen Instrumenten zur Strahlverlaufsverfolgung (Zielfernrohr, Fernglas oder Lupe) eingemessen werden können.

- Klasse 1M: Laser mit Wellenlängen von 302,5 nm bis 4000 nm, die ausreichend sicher sind, aber nicht mit optischen Instrumenten zur Strahlverfolgung ausgemessen werden können.

Dies bedeutet de facto, dass bei beiden Typen für einen Menschen, der in einen Laserstrahl mit dem bloßen Auge hineinblickt, keine Gefahr besteht.

In Einzelfällen sind auch noch Systeme entsprechend der alten Laserklasse 3R im Einsatz. Geräte der Laserklasse 3R sind gefährlicher und sollten bei neuen Strecken nicht mehr zum Einsatz kommen.

E.5 Ausblick

Optische und Mikrowellen-Richtfunksysteme werden auch künftig eingesetzt werden, wenn ein Bedarf nach hohen Datenraten und/oder der Überbrückung größerer Entfernungen besteht. Da diese Richtfunksysteme rein auf der physikalischen Übertragungsebene arbeiten, sind standardisierte Sicherheitsmechanismen zwischen den Sende- und Empfangseinheiten nicht zu erwarten. Die Hersteller von Richtfunksystemen werden auch in Zukunft wahrscheinlich eher selten eine Verschlüsselung auf Ebene der Richtfunksysteme anbieten und der Nutzer bleibt für die Absicherung selbst verantwortlich.

E.6 Fazit

Die Nutzung der drahtlosen Techniken auf Basis von optischem und mikrowellenbasiertem Richtfunk stellen eine – unter Kenntnis der wetterbedingten Risiken – zuverlässige Technik zur Verbindung von Gebäuden dar. Vorteilhaft ist die Transparenz der Richtfunksysteme, welche die Nutzung durch unterschiedlichste Übertragungsverfahren gestattet. Durch die Bündelung der Funkwellen bzw. des Lichtstrahls wird das Aufzeichnen des Signalstroms im Vergleich zur WLAN-Technik zwar erschwert, kann aber dennoch nicht ausgeschlossen werden. Daher sind bei entsprechendem Schutzbedarf zusätzliche Schutzmaßnahmen wie Verschlüsselung, Integritätssicherung und Authentisierung, z.B. durch VPN-Technik, notwendig. Diese Schutzmaßnahmen sind oft nicht Bestandteil des Richtfunksystems, sondern müssen auf höheren Protokollebenen umgesetzt werden.

Die Verfügbarkeit von mikrowellenbasierten Richtfunksystemen oder FSO-Systemen ist durch die Nutzung von genehmigungspflichtigen Frequenzbereichen bzw. der völligen Vermeidung von Funktechniken höher einzustufen als bei WLAN-basierten Techniken. Im Vergleich der beiden vorgestellten Richtfunktechniken haben FSO-Systeme eine wesentliche Einschränkung gegenüber den mikrowellenbasierten Technologien, denn Regen, Nebel oder Schneefall erhöhen die Dämpfung im Freiraum und beeinflussen die Reichweite der FSO-Systeme besonders stark.

E.7 Literatur und Links

Eine genaue Beschreibung des Prinzips von Optischem Richtfunk ist z.B. in [WBG03] enthalten. Technische Details sind in der Regel herstellerspezifischen Quellen zu entnehmen.

Dokumente zu den Nutzungsbedingungen von regulierten Frequenzen sowie der aktuelle Frequenznutzungsplan können der Homepage der Bundesnetzagentur (http://www.bundesnetzagentur.de) entnommen werden.

[BNA07] Mitteilung 47 / 2007 „Allgemeinzuteilung der Frequenzen im Frequenzbereich 5755 MHz – 5875 MHz für gewerblich öffentliche, breitbandige, ortsfeste Verteilsysteme; Broadband Fixed Wireless Access (BFWA)“, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, 2007

[BNA08] Mitteilung 217 / 2008 „Allgemeinzuteilung für Punkt-zu-Punkt Richtfunk im Frequenzbereich 59 GHz – 63 GHz“, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, 2008

[EN302502] ETSI EN 302 502, „Broadband Radio Access Networks (BRAN); 5,8 GHz fixed broadband data transmitting systems; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive“, verfügbar unter http://www.etsi-org/

[GSK] Bundesamt für Sicherheit in der Informationstechnik, „IT-Grundschutz-Kataloge“, verfügbar unter https://www.bsi.bund.de/cln_155/DE/Themen/weitereThemen/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

[IEC60825-1] IEC 60825-1, „Safety of laser products - Part 1: Equipment classification and requirements“, 2007

[WBG03] H. Willebrand, Baksheesh S. Ghuman, „Optischer Richtfunk“, Hüthig Verlag, 2003

E.8 Abkürzungen

BFWA	Broadband Fixed Wireless Access
BWA	Broadband Wireless Access
DFS	Dynamic Frequency Selection
EIRP	Equivalent Isotropically Radiated Power
ETSI	European Telecommunications Standards Institute
FSO	Free Space Optics
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISDN	Integrated Services Digital Network
IT	Informationstechnik
LAN	Local Area Network
MAN	Metropolitan Area Network
PBX	Private Branch Exchange
PDH	Plesiochronous Digital Hierarchy
SDH	Synchronous Digital Hierarchy
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TCP	Transmission Control Protocol
TDM	Time Division Multiplex, Zeitmultiplex
TKG	Telekommunikationsgesetzes
TPC	Transmit Power Control
VPN	Virtual Private Network
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network

E.9 Glossar

Divergenz

Siehe Strahlaufweitung

Free Space Optics (FSO)

Optischer Richtfunk, der für die Übertragung im Freiraum Licht im infraroten Spektrum nutzt.

Indoor Unit (Inneneinheit)

Die Indoor Unit des Mikrowellen-Richtfunksystems enthält die Schnittstellenelektronik, den internen Multiplexer und die Stromversorgung für die Außeneinheit.

Outdoor Unit (Außeneinheit)

Die Outdoor Unit des Mikrowellen-Richtfunksystems enthält Sender und Empfänger mit der zugehörigen Signalverarbeitung. Sie wird zusammen mit der Antenne an einem Antennenträger auf dem Dach eines Gebäudes oder an einem Mast installiert.

Plesiochronous Digital Hierarchy (PDH)

PDH ist eine international standardisierte Technik zur Übertragung von digitalen Datenströmen, in annähernd synchronen Datenströmen (griechisch plesio = fast) auf Weitverkehrsstrecken (Multiplexing). PDH definiert eine Hierarchie von unterstützten Bitraten (z.B. E1 mit 2 Mbit/s und E3 mit 34 Mbit/s). Für Bitraten von mehr als 45 Mbit/s wird derzeit meist SDH verwendet.

Strahlaufweitung (Divergenz)

Mit steigendem Abstand zwischen Sender und Empfänger eines FSO-Systems weitet sich je nach Einstellung am Sender der Strahl mehr oder weniger auf. Eine gewisse Strahlaufweitung ist notwendig, um mögliche physikalische Schwankungen des Sendesystems, bedingt z.B. durch Windeinflüsse, auf der Empfangsseite kompensieren zu können.

Synchronous Digital Hierarchy (SDH)

SDH ist ein international standardisiertes synchrones Zeitmultiplexverfahren, das ähnlich zu PDH eine Multiplex-Hierarchie beinhaltet. Beispiele für die Hierarchie sind die Stufen STM-1 (155,52 Mbit/s) und STM-16 (2.488,32 Mbit/s). Die Daten werden transparent durch das SDH-Netz übertragen.

F. ZigBee, IEEE 802.15.4

Inhaltsverzeichnis des Abschnitts

F.1 Grundlagen und Funktionalität

ZigBee[1] ist ein Industriestandard für drahtlose Sensor- und Steuernetzwerke und stellt einen speziellen Typ von Wireless Personal Area Networks (WPANs) dar, zu denen Bluetooth und im weitesten Sinne auch WLAN zählen. ZigBee wurde von dem im Jahr 2002 gegründeten Herstellerkonsortium ZigBee Alliance spezifiziert und basiert auf dem Standard IEEE 802.15.4, von dem die physikalische Übertragung und der Kanalzugriff übernommen wurde. ZigBee-Geräte sind für einen geringen Stromverbrauch ausgelegt, um batteriebetriebenen Endgeräten lange Laufzeiten zu ermöglichen. Hierzu operieren ZigBee bzw. IEEE 802.15.4 (im Vergleich zu WLAN und Bluetooth) bewusst mit einer vergleichsweise geringen Datenrate. Weiterhin ist ein sehr kompakter, kleiner Aufbau von ZigBee-Geräten möglich.

Aktuelle Informationen zu ZigBee finden sich auf der Internet-Seite der ZigBee Alliance (siehe [ZA08]).

Anwendungen von ZigBee liegen unter anderem in folgenden Bereichen:

- Automatisierungstechnik, z.B. Anlagensteuerung und Sensorabfrage
- Logistik, z.B. Barcode Scanner und RFID-Lesegeräte (Radio Frequency Identification)
- Heim- und Gebäudeautomatisierung, z.B. Steuerung von Lichtschaltern, Türöffnern, Alarmierung durch Bewegungsmelder und Abfrage von Temperaturfühlern
- Medizintechnik, z.B. Steuerung, Alarmierung und Abfrage von medizinisch-elektrischen Geräten
- Spielzeug, z.B. Vernetzung und Steuerung von elektrischen Spielzeugelementen

Neben ZigBee, welches auf IEEE 802.15.4 basiert, existieren verschiedenste proprietäre Funktechnologien für den Steuerungs- und Sensorbereich (siehe auch [VDI07]).

Aufgrund der vergleichsweise geringen Verbreitung derartiger Funksysteme in Unternehmen und Behörden wird an dieser Stelle nicht weiter auf solche speziellen Systeme eingegangen. Weitere nicht offengelegte, d.h. proprietäre Systeme sind in großer Anzahl für jeden Einsatzbereich eines Sensor- und Steuerungs-WPAN verfügbar. Eine allgemeine Sicherheitsbetrachtung dieser Systeme ist nur sehr eingeschränkt möglich.

2008 wurde mit WirelessHART ein weiteres Funksystem spezifiziert und offengelegt, welches auf IEEE 802.15.4 (Physical Layer) und IEEE 802.15.1 basiert und eine Verschlüsselung mittels AES (Advanced Encryption Standard) unterstützt. WirelessHART ist für die Fertigungs- und Prozessautomatisierung, speziell auch für explosionsgefährdete, sogenannte EX-Bereiche vorgesehen[2]. Da zum jetzigen Zeitpunkt kaum Produkte für WirelessHART verfügbar sind, ist eine spezielle Sicherheitsbetrachtung dieses Ansatzes nur schwer möglich. Aufgrund der gemeinsamen IEEE-Basis sind jedoch viele Punkte der folgenden Sicherheitsbetrachtungen für ZigBee auch auf WirelessHART übertragbar. Daher wird WirelessHART hier nicht separat betrachtet.

---

1 Auf Englisch wird die Tanzsprache der Honigbiene, mit der Informationen über Futterquellen (wie Entfernung, Richtung und Ergiebigkeit) ausgetauscht werden, als ZigBee Principle bezeichnet, denn bei einer der beiden bekannten Tanzformen, dem sogenannten Schwänzeltanz, verwendet die Biene ein zick-zack-förmiges (engl. zig-zag) Bewegungsmuster zur Informationskodierung.

2 Die Gesamtheit aller Bereiche, die durch verschiedenste Bedingungen wie z.B. Gase, Stäube oder elektrische Ladungen explosionsgefährdet sind, wird als EX-Bereich bezeichnet.

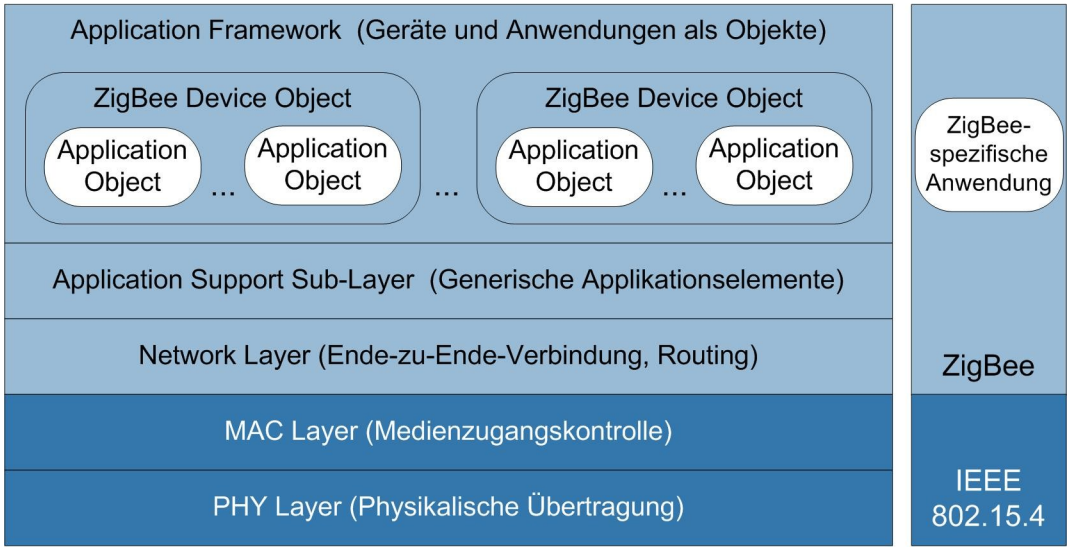
Die Kommunikation erfolgt bei ZigBee und vergleichbaren WPAN-Systemen über Funk und daher bestehen grundsätzlich die Gefahren der Abhörbarkeit, des unerlaubten Zugangs zum WPAN und der möglichen Störbarkeit von Übertragungen (beabsichtigt oder nicht). Da ZigBee zur Sensorabfrage und zu Steuerungszwecken eingesetzt werden soll, kommt der Forderung der Integrität der Daten (im Vergleich zu anderen Funknetzen) eine besonders hohe Bedeutung zu, da durchaus Szenarien denkbar sind, in denen manipulierte oder unterdrückte Steuerkommandos bzw. Messwerte zu einem erheblichen Schaden führen können.

F.1.1 Architektur

In der Architektur eines ZigBee-Systems werden die folgenden Schichten spezifiziert (siehe auch Abbildung F-1 und [ZA08]):

- Die physikalische Übertragung (PHY Layer) und der Kanalzugriff (Medienzugangssteuerung, Media Access Control Layer, kurz: MAC Layer) basieren auf der unter IEEE 802.15.4 beschriebenen Funkschnittstelle (siehe [IEEE06]).
- Der ZigBee Network Layer (NWK) dient der Bereitstellung einer Ende-zu-Ende-Kommunikation, die gegebenenfalls ein Routing über mehrere Zwischenknoten erfordern kann.
- Aufbauend auf dem Network Layer bietet der Application Support Sub-Layer (APS) einen Satz von allgemein verwendbaren Applikationselementen.
- Geräte und Anwendungen werden als Objekte spezifiziert, d.h. sie werden über einen Satz von Attributen beschrieben, deren Zustand nur über die für das Objekt spezifizierte Schnittstelle geändert werden kann. ZigBee Device Objects (ZDOs) repräsentieren ZigBee-Geräte, auf denen die eigentlichen Anwendungen laufen. Die Anwendungen werden als Application Objects dargestellt, die über die ZDOs kontrolliert und verwaltet werden. Das hierzu notwendige Rahmenkonzept – z.B. die Festlegung von Mechanismen zur Adressierung von Objekten – wird im ZigBee Application Framework bereitgestellt.

Abbildung F-1: ZigBee-Architektur (vereinfacht)



F.1.2 IEEE 802.15.4

Für IEEE 802.15.4 sind drei Frequenzen vorgesehen (siehe auch Tabelle F-1):

- Im weltweit verfügbaren ISM-Band bei 2,4 GHz können 16 Kanäle mit einem Kanalabstand von 5 MHz verwendet werden. Die Datenrate beträgt 250 kbit/s und die Modulation erfolgt mit einer Variante von QPSK (Quadrature Phase Shift Keying).
- In Europa ist im Frequenzbereich 868 MHz bis 868,6 MHz ein weiterer Kanal für IEEE 802.15.4 vorgesehen. Hier wird als Modulation BPSK (Binary Phase Shift Keying) verwendet. Die erreichbare Datenrate beträgt 20 kbit/s.
- In Amerika steht mit dem Frequenzbereich 902 MHz bis 928 MHz ein weiteres ISM-Band zur Verfügung, das 10 Kanäle für IEEE 802.15.4 bei einer Datenrate von 40 kbit/s unter Verwendung von BPSK liefert.

Tabelle F-1: Physikalische Übertragungsparameter

Frequenz	Verfügbarkeit	Datenrate	Anzahl Kanäle
2,4 – 2,4835 GHz (ISM)	weltweit	250 kbit/s	16
868 – 868,6 MHz	Europa	20 kbit/s	1
902 – 928 MHz (ISM)	Amerika	40 kbit/s	10

Um das System gegenüber schmalbandigen Störungen robust zu gestalten, werden die Nutzdaten zur Übertragung mit einer Spreizsequenz überlagert. Hierzu wird das zu übertragende Binärsignal mit einer Rate abgetastet (der sogenannten Chiprate), die größer als die zugrunde liegende Datenrate des Binärsignals ist. Dieses Signal wird mit einer anderen Bitfolge in der gegebenen Chiprate verknüpft, der sogenannten Spreizsequenz. Dieses Verfahren wird als Direct-Sequence-Spread-Spectrum-Verfahren (DSSS) bezeichnet.

Der Standard IEEE 802.15.4 erwartet Sendeleistungen zwischen 0,5 mW bis 10 mW, wobei wahrscheinlich meist mit 1 mW operiert wird. Dabei kann eine Reichweite von ca. 10 Metern (bei 1 mW Sendeleistung) bis ca. 70 Metern (unter idealen Bedingungen bei 10 mW Sendeleistung) erzielt werden.

Neben ZigBee operieren auch diverse andere Funksysteme im Frequenzbereich von 2,4 GHz, z.B. WLAN und Bluetooth. Speziell WLAN-Systeme, die eine deutlich höhere Sendeleistung als ZigBee-Systeme nutzen, können Interferenzen zu ZigBee aufweisen, die zwangsläufig aus einer Überlappung der Sendekanäle resultieren. Die Meinungen hinsichtlich der Auswirkungen dieser Störungen gehen allerdings auseinander und rangieren von extremen Störungen (siehe [ZW07]) bis hin zu nachweisbaren, aber nicht signifikanten Störungen (siehe [ZA07]). In der Praxis bedeutet dies jedoch, dass jeweils eine Einzelfallbetrachtung erforderlich ist, welche die konkreten Einsatzszenarien unter den gegebenen speziellen Bedingungen bewertet (siehe auch [IEEE06] und [FS06]).

IEEE 802.15.4 unterscheidet zwei Gerätetypen:

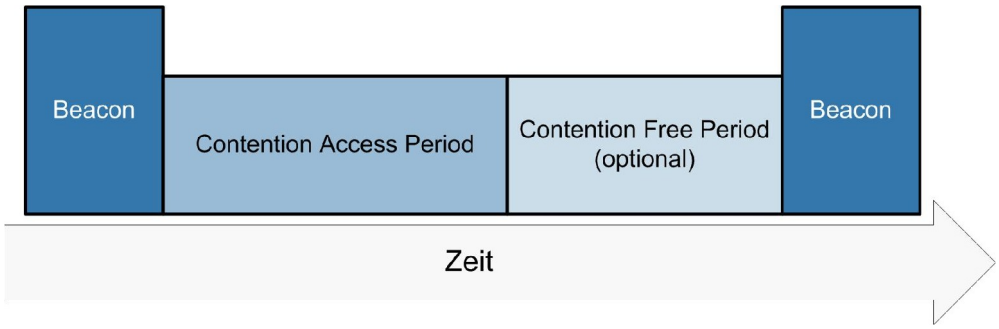
- Full Functional Device (FFD)
- Reduced Functional Device (RFD)

Eine FFD ist vereinfacht gesagt ein Gerät, das alle Betriebsfunktionen für ein WPAN implementiert hat und in diesem Sinne komplett ist, wohingegen ein RFD nur eingeschränkte Kommunikationsmittel hat. FFDs können unmittelbar miteinander kommunizieren, ein RFD kann dagegen nur mit einem FFD kommunizieren. RFDs sind für extrem einfache Applikationen gedacht, die nur geringe Datenvolumen übertragen müssen und nur bei Bedarf aktiv werden. Ein Beispiel ist ein über ZigBee gesteuerter Lichtschalter.

In einem WPAN nach IEEE 802.15.4 gibt es stets ein Gerät mit einer speziellen Rolle: den sogenannten PAN Coordinator. Der PAN Coordinator ist stets ein FFD; die anderen Geräte im WPAN können FFDs oder RFDs sein. Typischerweise wird ein FFD als PAN Coordinator vorkonfiguriert oder das erste aktive FFD wird automatisch zum PAN Coordinator. Der PAN Coordinator verwaltet die Identifikation des WPAN, koordiniert die Anmeldung weiterer Geräte (FFD oder RFD) an das WPAN und kann gewisse Parameter beim Kanalzugriff steuern. Bei Ausfall des PAN Coordinator muss das Netz erneut aufgebaut werden und einen neuen PAN Coordinator auswählen.

In regelmäßigen Abständen senden Stationen, welche die Rolle eines sogenannten Coordinator haben oder der PAN Coordinator selbst sind, ein spezielles Paket, das als Beacon Frame bezeichnet wird. In diesem Paket wird unter anderem die Identifikation des WPAN mitgeteilt[3]. Die Zeit zwischen zwei Beacon Frames wird in zwei Phasen eingeteilt: eine Phase, in der um den Funkkanal konkurriert wird (Contention Access Period) und eine optionale, wettbewerbsfreie Phase (Contention Free Period). In der Contention Access Period erfolgt der Kanalzugriff über ein zufallsgesteuertes CSMA/CA-Verfahren (Carrier Sense Multiple Access with Collision Avoidance).

Abbildung F-2: Aufteilung der Zeit für den Kanalzugriff

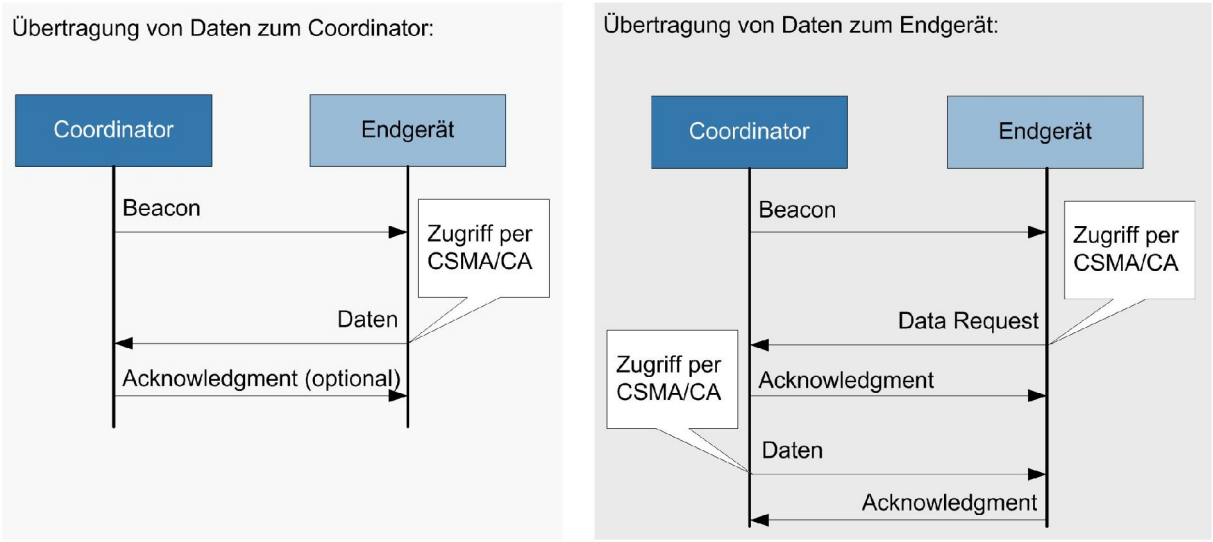


Eine Besonderheit des ZigBee-Kanalzugriffs ist, dass auf das Acknowledgment eines Pakets, welches von einem Gerät an den Coordinator geschickt wird, optional verzichtet werden kann. In diesem Fall erfährt ein Gerät nicht, ob ein gesendetes Paket angekommen ist oder auf dem Funkweg verloren gegangen ist, und es gibt keine Möglichkeit der Neuübertragung bei Paketverlust. Potenzielle Anwendung ist hier die periodische Übertragung von Nachrichten (z.B. Messwerten), bei denen es nichts ausmacht, wenn ein einzelnes Paket verloren geht, sofern früher oder später eine aktuelle Nachricht empfangen werden kann.

Eine weitere Besonderheit ist der richtungsabhängige Transfer von Daten, wie in Abbildung F-3 gezeigt. Wenn ein Coordinator Daten zur Übertragung an ein spezielles Gerät vorliegen hat, zeigt der Coordinator dies im Beacon Frame an. Das durch die Parameter im Beacon Frame angesprochene Gerät fordert dann die Daten explizit vom Coordinator an. Auf diese Weise muss ein Gerät lediglich Beacon Frames verarbeiten und kann stromsparend alle anderen nicht für dieses Gerät bestimmte Pakete ignorieren. Weiterhin können ZigBee-Geräte in einen besonders energiesparenden Schlafzustand (Sleep Mode) versetzt werden, aus dem sie über das Netz wieder aufgeweckt werden können.

[3] Die Steuerung des Kanalzugriffs mittels Beacon Frames ist optional und kann in gewissen Situationen deaktiviert werden.

Abbildung F-3: Richtungsabhängige Übertragung auf MAC Layer

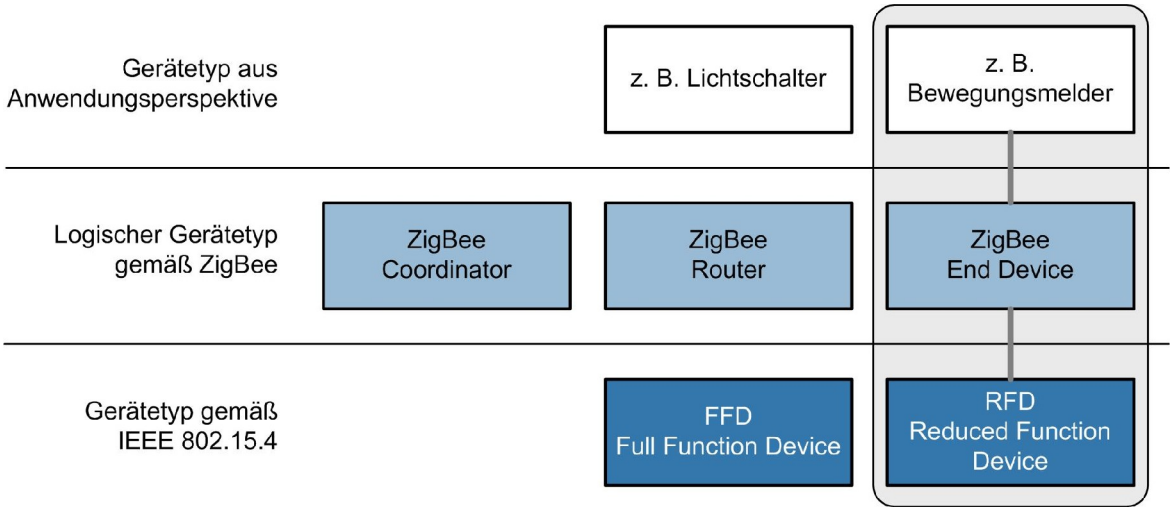


F.1.3 Network Layer

Der ZigBee Network Layer stellt alle Grundfunktionen für ein sich selbst organisierendes Netzwerk bereit. Hierzu werden drei logische Gerätetypen (d.h. Rollen) unterschieden (siehe Abbildung F-4):

- Der ZigBee Coordinator entspricht dem PAN Coordinator in IEEE 802.15.4, muss somit ein FFD sein und ergänzt diesen um Funktionen auf dem Network Layer.
- Ein FFD kann zusätzlich die Rolle eines ZigBee Router übernehmen, der Pakete zwischen ZigBee-Knoten vermittelt. Der logische Gerätetyp ZigBee Router entspricht dem Coordinator in IEEE 802.15.4.
- Ein ZigBee End Device ist ein reines Endgerät und kann sowohl FFD als auch RFD sein.

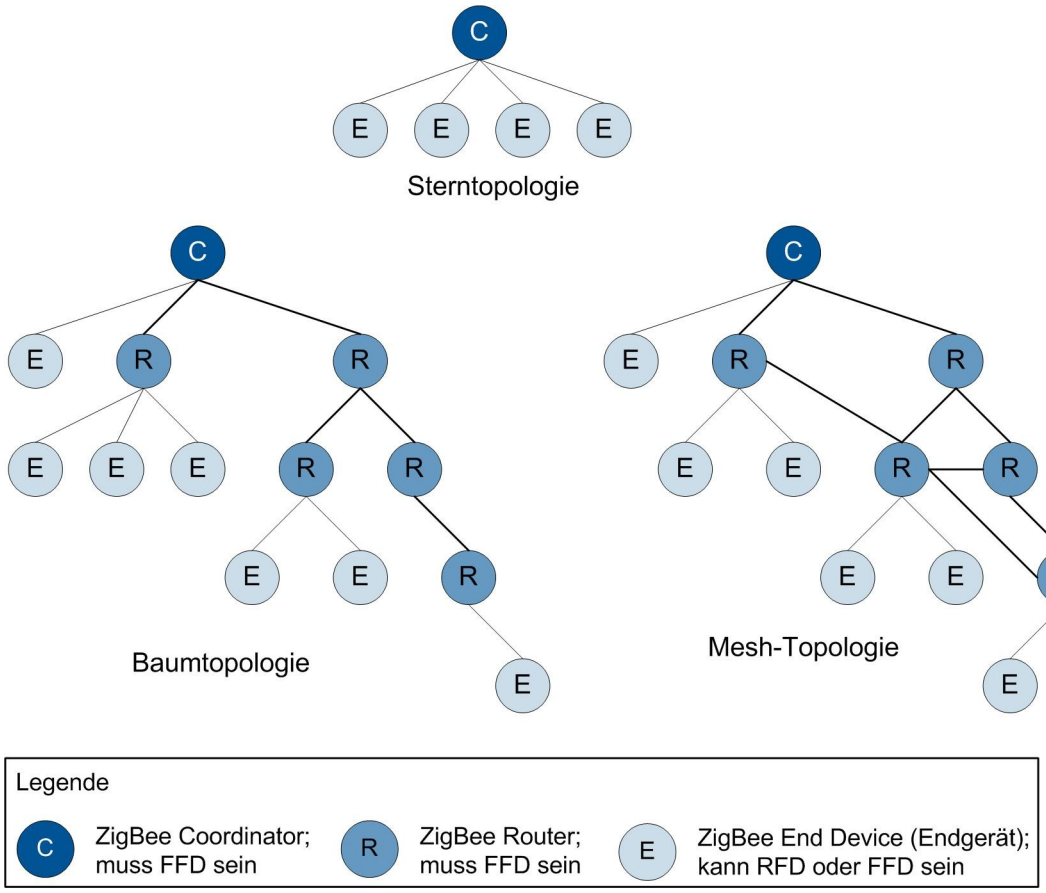
Abbildung F-4: Gerätetypen



Dabei ergeben sich anwendungs- und gerätespezifische Profile, wie in der Abbildung F-4 am Beispiel eines Bewegungsmelders skizziert.

Über die Mechanismen des Network Layer können unterschiedliche Topologien in einem ZigBee WPAN aufgebaut werden, wie in Abbildung F-5 gezeigt. Dabei sind auch redundante Verbindungen zwischen ZigBee Router möglich. Die Vermaschung kann sich dynamisch durch die Mobilität von Geräten ändern. ZigBee spezifiziert aber keine Mechanismen zur Aufrechterhaltung einer Ende-zu-Ende-Kommunikation bei einer durch Mobilität verursachten Konnektivitätsänderung.

Abbildung F-5: Mögliche Netztopologien



F.1.4 Application Layer

Der ZigBee Application Layer setzt sich aus dem Application Support (APS) Sub-Layer, den ZigBee Device Objects (ZDOs) und den außerhalb von ZigBee durch den Hersteller eines Geräts definierten Application Objects zusammen.

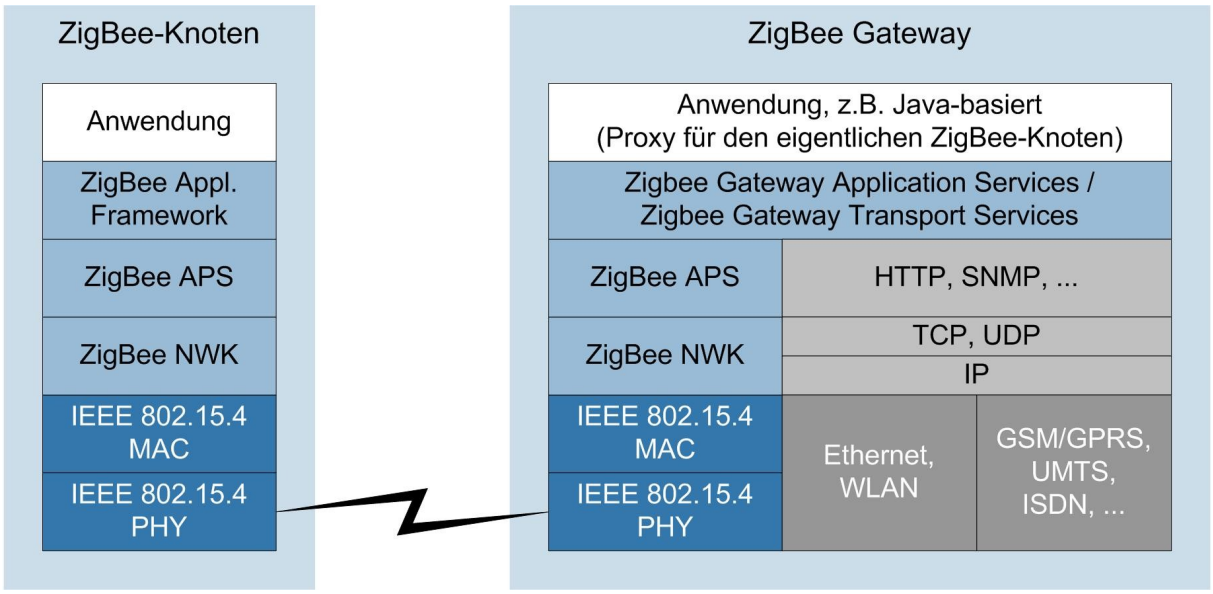
Wenn ein Gerät eingeschaltet wird bzw. in ein ZigBee WPAN eingebracht werden soll, führt der APS Sub-Layer des Geräts zunächst ein sogenanntes Discovery aus. Dabei stellt das Gerät fest, welche anderen Geräte in der Nachbarschaft operieren, zu denen eine Verbindung aufgebaut werden kann. Der APS Sub-Layer übernimmt anschließend auch die Verwaltung der Liste der Geräte, zu denen eine Bindung (Binding) besteht, sowie die Verteilung von Nachrichten zwischen diesen Geräten.

Zu den Verantwortlichkeiten eines ZDO gehören die Festlegung der Rolle des Geräts (z.B. Endgerät oder ZigBee Coordinator) sowie die Initiierung eines Binding bzw. die Antwort auf ein Binding Request. In dieser Phase werden auch die Parameter für eine gesicherte Kommunikationsbeziehung zwischen den Geräten festgelegt.

F.1.5 Verbindung zu anderen Netzwerken

Diverse ZigBee-Anwendungen benötigen neben der Funkvernetzung eine Anbindung an eine IP-basierte Infrastruktur. Hierzu dient das Konzept des ZigBee Gateway, welches auf der einen Seite über einen kompletten ZigBee-Protokoll-Stack als ZigBee Router die Verbindung zum ZigBee-Netz hält und über eine spezielle Anwendung auf der anderen Seite die Übertragung von Daten von und zur Infrastruktur durchführt (siehe Abbildung F-6). Ein Beispiel ist die Abfrage des Zustands von ZigBee-Geräten und deren Konfiguration über eine zentrale Management-Konsole, die als Festnetzstation in einem kabelbasierten LAN über IP mit einem ZigBee Gateway kommuniziert. In einem WPAN können durchaus mehrere ZigBee Gateways positioniert sein.

Abbildung F-6: Anbindung an die Infrastruktur über ein ZigBee Gateway



F.1.6 Anwendungsprofile der ZigBee Alliance

Die Aktivitäten der ZigBee Alliance umfassen auch die Spezifikation von Profilen für die möglichen Einsatzgebiete von ZigBee. Die ZigBee Application Profiles (ZAP) beschreiben jeweils typische ZigBee-Geräte (Devices) für bestimmte Einsatzszenarien vollständig mit allen zwingenden und optionalen Charakteristika. Das erklärte Ziel ist es, eine umfassende Interoperabilität zwischen verschiedenen Herstellern und die Möglichkeit von großen heterogenen Netzen zu schaffen.

Folgende ZigBee-Anwendungsprofile sind zum jetzigen Zeitpunkt definiert:

- Home Automation Profile

  Das Profil wurde im Oktober 2007 spezifiziert und beschreibt die Kommunikation und Steuerung von Geräten wie Lichtanlagen, Heizungssteuerung, Ton- und Bildanlagen, Alarmanlagen, elektrische Rollläden usw. Zielgruppe dieses Profils sind kleinere Installationen, bei denen ein ZigBee-Netz nur ein Gebäude mit etwa 2 bis 500 Geräten und mit bis zu 2000 qm umfasst. Eine gebäudeübergreifende Kommunikation ist nicht vorgesehen.

  Für dieses Profil sind nur minimale Sicherheitsanforderungen spezifiziert.

- Smart Energy Profile

  Das Profil wurde im Dezember 2008 spezifiziert und beschreibt die Kommunikation und Steuerung von Geräten im Energiebereich wie z.B. Stromzähler. Ein solches ZigBee-Netz umfasst Installationen mit bis zu 500 Geräten pro Gebäude, wobei die Kommunikation zusätzlich auch gebäudeübergreifend erfolgt, z.B. eine automatische Übermittlung von Zählerständen an eine zentrale Stelle.

  Für den Smart-Energy-Bereich sind erhöhte Sicherheitsanforderungen spezifiziert, z.B. muss die Datenübertragung zwingend verschlüsselt werden und eine Schlüsselübertragung im Klartext ist nicht zulässig.

- Health Care Profile

  Das Profil wurde im März 2009 abgeschlossen und beschreibt die Kommunikation und Steuerung von Geräten für unkritische und wenig akute Gesundheitsdienste. Ein solches ZigBee-Netz umfasst neben dem Home-Bereich auch alle Einrichtungen der Gesundheitsvorsorge und unterstützt mobile und fest installierte Geräte.

  Auch für den Health-Care-Bereich sind erhöhte Sicherheitsanforderungen spezifiziert.

- RF4CE Profile (Radio Frequency for Consumer Electronics)

  Die Spezifikation für dieses Profil wurde im September 2009 veröffentlicht. Dieses Profil ermöglicht eine Hersteller-übergreifende Kontrolle und Steuerung von Geräten der Unterhaltungsbranche und soll mittelfristig die Kommunikation via Infrarot im Bereich der Consumer Electronics (CE) ablösen. Langfristig soll mit Hilfe dieses Profils auch die Kommunikation in weiteren haushaltsnahen Bereichen, z.B. zur Raumüberwachung und zur Kontrolle von Lichtanlagen, ermöglicht werden.

  Für den CE-Bereich sind Maßnahmen für erhöhte Sicherheitsanforderungen spezifiziert, z.B. erfolgt die Datenübertragung verschlüsselt und eine Authentisierung der Teilnehmer ist vorgesehen.

Weitere Profile sind in Entwicklung und enthalten ebenfalls spezifische Sicherheitsanforderungen für die jeweilige Einsatzumgebung.

- Building Automation Profile

  Im Unterschied zur Home Automation sollen hier alle zu kontrollierenden und zu steuernden Geräte in größeren Gebäuden, z.B. Bürogebäude, erfasst werden.

- Telecommunication Services Profile

  Dieses Profil soll eine Hersteller-übergreifende Kontrolle und Steuerung von Geräten der Telekommunikation gewährleisten.

F.2 Sicherheitsmechanismen

Die für ZigBee spezifizierten Sicherheitsmechanismen beinhalten Methoden für den Austausch von Schlüsselmaterial und für den Schutz der Nachrichten, die über ZigBee übertragen werden. Das dabei erreichbare Sicherheitsniveau hängt primär von der Sicherheit der verwendeten symmetrischen Schlüssel ab, d.h. ein Gerät muss entweder auf eine sichere Weise (bei der Herstellung des Geräts oder manuell durch den Nutzer) mit einem Schlüssel vorkonfiguriert werden, oder die Übertragung des Schlüsselmaterials muss geeignet abgesichert sein.

Dies ist allerdings nicht generell gewährleistet, da beispielsweise mit sehr einfachen Endgeräten zu rechnen ist, die eine manuelle Schlüsselkonfiguration nicht gestatten und für die ein initialer Schlüssel ungesichert über Funk übertragen werden muss. In diesem Fall ist das System für einen kurzen Moment sehr verwundbar.

In ZigBee gilt das Prinzip, dass diejenige Protokollebene, die ein Paket erzeugt, zunächst auch für die Absicherung des Pakets verantwortlich ist. Insbesondere entscheidet auch diese Protokollebene bzw. die Applikation, welches Sicherheitsniveau erfüllt werden muss. Vorgaben für die mindestens zu unterstützenden Sicherheitsmechanismen definieren die von der ZigBee Alliance spezifizierten Application Profiles (siehe Kapitel F.1.6). Die entsprechenden Sicherheitsmechanismen werden in ZigBee auf mehreren Protokollebenen realisiert, wie im Folgenden kurz vorgestellt wird.

F.2.1 Schlüsselmanagement

Die Sicherheit in einem Netzwerk von ZigBee-Geräten basiert auf sogenannten Link Keys (Verbindungsschlüsseln) und einem Network Key (Netzwerkschlüssel). Die Unicast-Kommunikation zwischen zwei Applikationselementen (APL Peer Entities) wird unter Verwendung eines Link Keys abgesichert. Dieser symmetrische Schlüssel muss in den beiden APL Peer Entities vorliegen. Broadcasts werden mit dem Network Key verschlüsselt. Der Network Key ist allen ZigBee-Stationen im Netz bekannt. Alle Schlüssel haben eine Länge von 128 Bit.

Ein ZigBee-Gerät erhält einen Link Key entweder über eine Übertragung des Schlüssels oder durch die Ableitung des Schlüssels[4], oder der Schlüssel ist werksseitig oder manuell durch den Nutzer vorkonfiguriert.

Grundlage für die Ableitung eines Link Key ist ein Master Key, der seinerseits auf die ZigBee-Geräte durch eine Netzwerkübertragung oder eine Vorkonfiguration gelangt.

Der Network Key wird entweder übertragen oder er ist vorkonfiguriert. Der Network Key kann von jeder Protokollschicht, die Sicherheitsfunktionen beinhaltet, verwendet werden, d.h. von MAC, NWK und APL. Ein Link Key oder ein Master Key darf dagegen nur vom APS genutzt werden.

Für die Verteilung der Schlüssel ist in ZigBee ein sogenanntes Trust Center verantwortlich, das außerdem Aufgaben im Bereich des Configuration Management auf Netzwerk- und Applikationsebene wahrnimmt. In einem abgesicherten ZigBee-Netzwerk ist genau ein Trust Center vorgesehen. Sofern nicht explizit auf den Geräten im Netzwerk anders vorkonfiguriert, übernimmt der PAN Coordinator auch die Rolle des Trust Centers. Alternativ kann der PAN Coordinator diese Rolle auch an ein anderes Gerät delegieren.

---

[4] Der Link Key wird dazu nicht explizit übertragen, sondern Informationen, aus denen ein gemeinsamer Schlüssel abgeleitet werden kann.

Im Detail unterscheidet ZigBee hinsichtlich der Rolle des Trust Center zwischen zwei Modi, für die das Trust Center konfiguriert sein kann und denen auch unterschiedliche Sicherheitsniveaus zugeordnet sind: dem Commercial Mode, der meist für Applikationen, die hohe Sicherheitsanforderungen haben, genutzt wird und dem Residential Mode, der durch Anwendungen mit typischerweise geringeren Sicherheitsanforderungen charakterisiert ist.

F.2.2 Application Layer

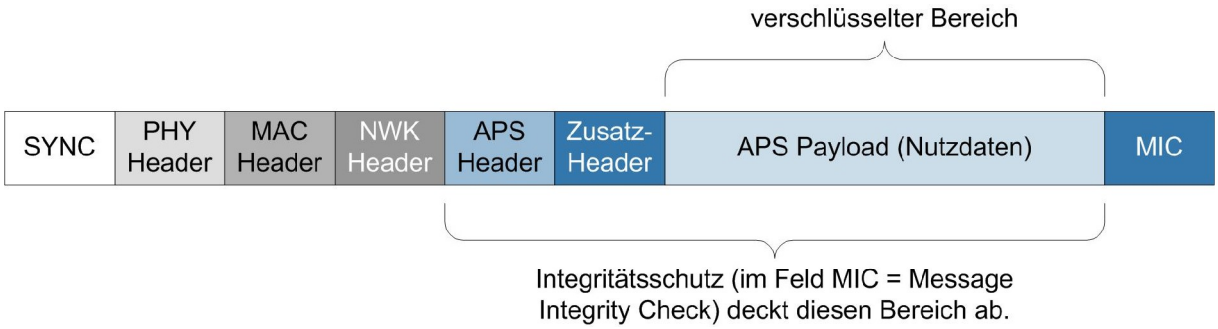
Das APS bietet für die eigentlichen Anwendungsobjekte die zur Absicherung der Kommunikation notwendigen Dienste (Security Primitives) an. Dies beinhaltet Operationen für die sichere Übertragung, für den Empfang von abgesicherten Paketen sowie zur Etablierung und Verwaltung von Schlüsseln. Die Anwendungsobjekte sind verantwortlich für die Auswahl eines geeigneten Niveaus der Absicherung einer ausgehenden Übertragung.

Wenn ein Paket auf Anwendungsebene verschlüsselt werden soll, so geschieht dies durch AES-CCM*, einer Erweiterung von CCM, welche die Auswahl gestattet

- ein Paket nur zu verschlüsseln,
- für ein Paket nur eine Integritätsprüfung vorzunehmen
- oder beides zusammen durchzuführen.

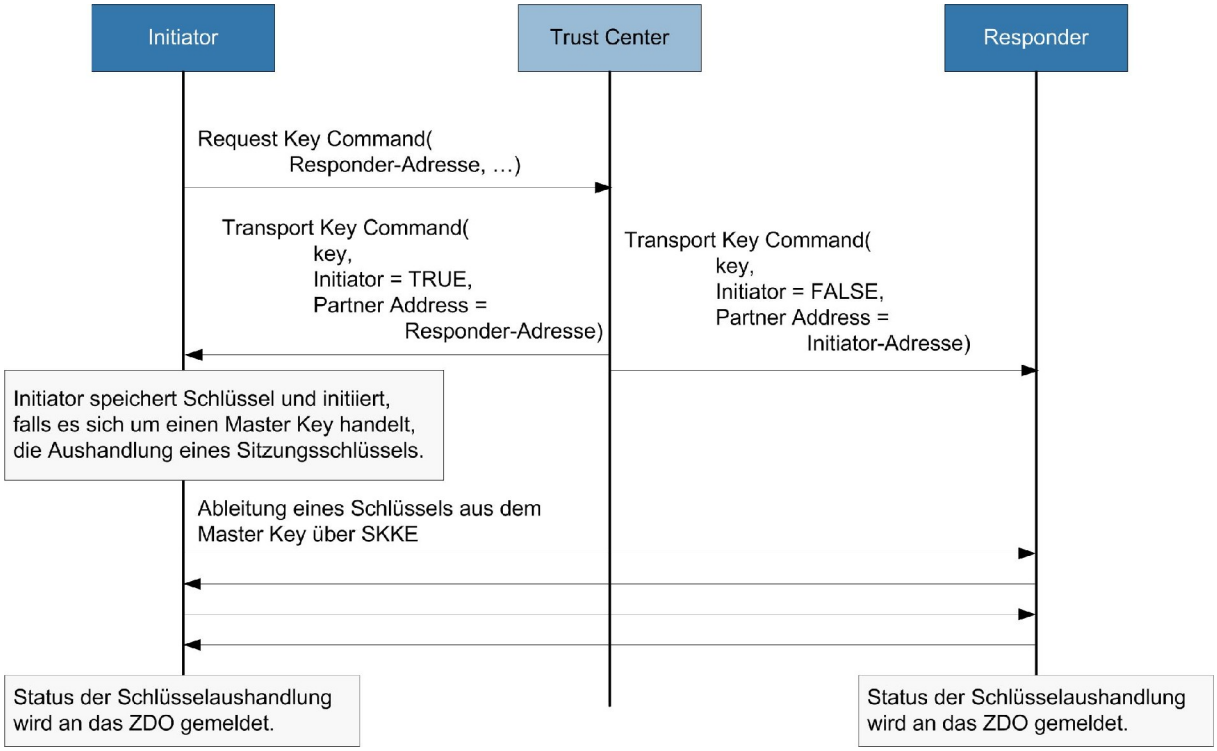
CCM ist eine Abkürzung für Counter with CBC-MAC (CBC-MAC = CBC with Message Authentication Code, CBC = Cipher Block Chaining). CCM ist eine generische Methode für die Verschlüsselung und Authentisierung von Daten, die für die Verwendung einer 128-Bit-Blockchiffrierung spezifiziert ist. Hier wird AES als Blockchiffrierung benutzt. Im WLAN-Kapitel dieses Dokuments ist diese Methode kurz beschrieben. Abbildung F-7 zeigt die in einem Paket auf dem Application Layer abgesicherten Bereiche.

Abbildung F-7: Abgesicherte Bereiche bei Verschlüsselung und Integritätsprüfung auf Application Layer



Der zur Ver- und Entschlüsselung notwendige symmetrische Schlüssel kann, wie in Abbildung F-8 am vereinfachten Beispiel für eine Ende-zu-Ende-Schlüsselverteilung gezeigt, abgeleitet werden. Dabei wendet sich diejenige APS Entity, welche die Kommunikationsbeziehung initiiert (Initiator), zunächst an das Trust Center, um einen Schlüsseltransfer zu initiieren. Das Trust Center überträgt dann das gewünschte Schlüsselmaterial. Wenn es sich dabei um einen Master Key handelt, wird in einem zweiten Schritt der Sitzungsschlüssel im Rahmen des Protokolls Symmetric-Key Key Establishment (SKKE) vereinbart. Über das SKKE wird ein 4-Way-Handshake durchgeführt, ähnlich wie er auch in anderen Kommunikationssystemen (z.B. WLAN) für die Schlüsselaushandlung verwendet wird.

Abbildung F-8: Beispiel für die Ende-zu-Ende-Ableitung eines Schlüssels auf Anwendungsebene

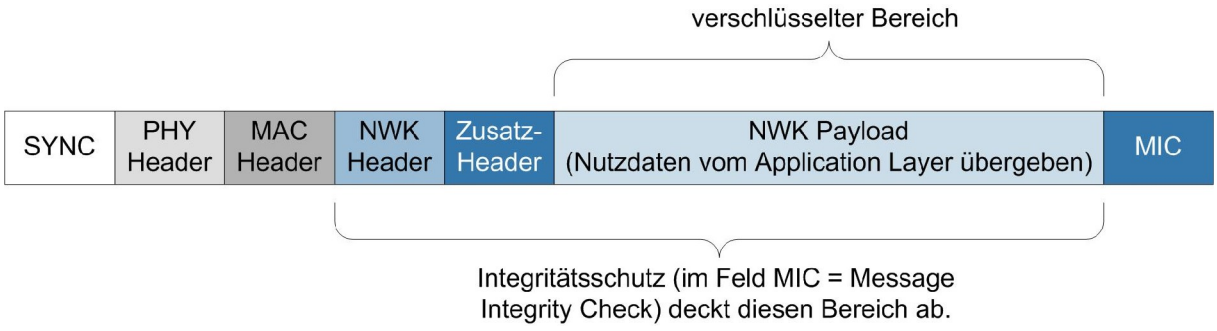


F.2.3 Network Layer

Für Pakete, die auf dem Network Layer verschlüsselt werden sollen, wird ebenfalls das Verfahren CCM* verwendet. Die Anforderung zur Verschlüsselung auf Network Layer kann dabei beispielsweise vom Application Layer durch Angabe eines Parameters geschehen. Abbildung F-9 zeigt die in einem Paket auf dem Network Layer abgesicherten Bereiche.

Eine Aufgabe des Network Layer ist das Routing von Nachrichten ggf. über mehrere Zwischenknoten (Hops) hinweg. Pakete des Routing-Protokolls (d.h. Signalisierungspakete zur Bestimmung und Auswahl des Übertragungswegs) beinhalten Broadcast- und Unicast-Nachrichten. Die Unicast-Nachrichten werden mit dem entsprechenden Link Key verschlüsselt, sofern dieser verfügbar ist. Zumindest wird für ein Paket der Network Key angewendet.

Abbildung F-9: Abgesicherte Bereiche bei Verschlüsselung und Integritätsprüfung auf Network Layer



F.2.4 IEEE 802.15.4

Die MAC-Ebene von IEEE 802.15.4 bietet einen Satz von Basis-Sicherheitsdiensten bestehend aus den folgenden Elementen:

- Zugangskontrolle
- Verschlüsselung
- Integritätsprüfung
- Sequenzkontrolle

Diese Elemente werden in sogenannten Security Suites zusammengestellt. Tabelle F-2 zeigt die in IEEE 802.15.4 festgelegten Security Suites.

Tabelle F-2: Sicherheitsmechanismen in IEEE 802.15.4

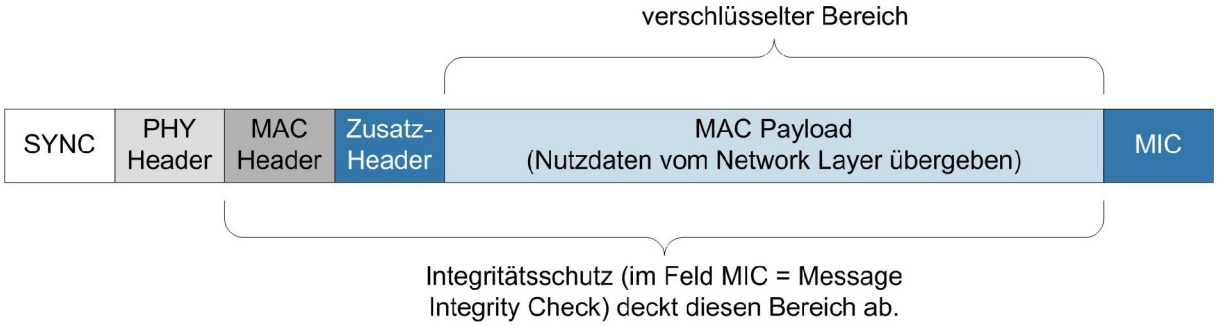
Identifikation	Name der Security Suite	Security Service			
		Zugangskontrolle	Verschlüsselung	Frame-Integritätsprüfung	Frame-Sequenzkontrolle (optional)
0x00	-				
0x01	AES-CTR	X	X		X
0x02	AES-CCM-128	X	X	X	X
0x03	AES-CCM-32	X	X	X	X
0x04	AES-CCM-64	X	X	X	X
0x05	AES-CBC-MAC-128	X		X	
0x06	AES-CBC-MAC-64	X		X	
0x07	AES-CBC-MAC-32	X		X	

Der Nutzer von IEEE 802.15.4 (also die höheren Protokollebenen, potenziell bis hin zum eigentlichen Nutzer des ZigBee-Systems) ist verantwortlich für die geeignete Auswahl und Nutzung der Security Suites. Dies beinhaltet insbesondere die sichere Übertragung und Ableitung bzw. Konfiguration von Schlüsselmaterial. Im Extremfall wird mit der Suite 0x00 kein Sicherheitsmechanismus eingesetzt.

Der Standard IEEE 802.15.4 legt für ein Gerät drei verschiedene Sicherheitsmodi fest:

- Im Unsecured Mode werden keine Sicherheitsmechanismen genutzt (entspricht der Security Suite 0x00)
- Im ACL Mode erfolgt lediglich eine Zugangskontrolle über eine Access Control List (ACL), siehe Kapitel F.2.4.1.
- Nur im Secured Mode sind alle oben genannten Basis-Sicherheitsdienste verfügbar. Abbildung F-10 zeigt die dabei in einem Paket auf der MAC-Ebene abgesicherten Bereiche.

Abbildung F-10: Abgesicherte Bereiche bei Verschlüsselung und Integritätsprüfung auf der MAC-Ebene



F.2.4.1 Zugangskontrolle

Die Zugangskontrolle ist ein Dienst, der einem Gerät die Auswahl des Kommunikationspartners ermöglicht. In einer Access Control List (ACL) werden im Sinne einer sogenannten White List die MAC-Adressen derjenigen Stationen verzeichnet, mit denen eine Kommunikation gestattet ist. Empfängt eine Station ein Paket, wird geprüft, ob die Quell-MAC-Adresse in der ACL verzeichnet ist. Wenn nein, wird das Paket verworfen.

Dieser Mechanismus erscheint auf den ersten Blick sehr einfach, die Komplexität besteht allerdings in der Verwaltung der ACLs. Wenn beispielsweise ein Gerät oder der entsprechende Adapter ausgetauscht werden muss, ist es auch unmittelbar erforderlich, die zugehörigen Einträge der ACLs zu aktualisieren. Dies ist sehr fehleranfällig. Eine zentrale Verwaltung von MAC-Adressen wäre daher (speziell bei größeren Netzen) wünschenswert. Der Standard IEEE 802.15.4 gibt hierzu jedoch keine Empfehlungen.

F.2.4.2 Verschlüsselung

Zur Verschlüsselung sind zwei auf dem Advanced Encryption Standard (AES) basierende symmetrische Verfahren unter Verwendung einer Schlüssellänge von 128 Bit spezifiziert:

- AES-CTR: Im Counter (CTR) Mode wird der Wert eines Zählers mit AES verschlüsselt. Dieser verschlüsselte Zählerwert und ein entsprechend großer Block des Klartextes dienen dann als Eingabe in eine XOR-Operation, die dann das Verschlüsselungsergebnis liefert.
- AES-CCM: Siehe Kapitel F.2.2.

Es ist grundsätzlich gestattet, dass eine Gruppe von mehr als zwei Stationen einen gemeinsamen Schlüssel verwendet. Mechanismen zum Schlüsselmanagement sind allerdings nicht Bestandteil von IEEE 802.15.4.

F.2.4.3 Integritätsprüfung

Die im vorangegangenen Kapitel F.2.4.2 genannte Methode AES-CCM wird auch zur Integritätsprüfung verwendet. Bei Anwendung von AES-CCM erhält man neben dem verschlüsselten Text auch einen verschlüsselten Integritäts-Code. Der Standard IEEE 802.15.4 spezifiziert drei Längen für diesen Integritäts-Code: 32 Bit (AES-CCM-32), 64 Bit (AES-CCM-64) und 128 Bit (AES-CCM-128). Jede Implementierung, die den Secure Mode anbietet, muss zumindest AES-CCM-64 unterstützen.

Es sind auch Security Suites spezifiziert, die als kryptographische Mechanismen keine Verschlüsselung, sondern lediglich eine Integritätsprüfung mit verschiedenen Längen für den Integritäts-Code un-

terstützen (32 Bit, 64 Bit und 128 Bit, siehe Tabelle F-2). Dabei wird AES-CBC-MAC eingesetzt, d.h. AES dient hier nur zur Berechnung einer kryptographischen Prüfsumme der zu übertragenden Daten.

In diesem Zusammenhang ist es wichtig zu erwähnen, dass die ZigBee-Spezifikation in Ergänzung zu IEEE 802.15.4 zusätzlich auch für die MAC-Ebene die Unterstützung von AES-CCM* fordert.

F.2.4.4 Sequenzkontrolle

Die zu übertragenen Pakete werden nummeriert und die Paketnummer wird im Paket mit übertragen. Bei Empfang eines Pakets wird durch Betrachtung der Paketnummer geprüft, ob das Paket neuer ist als das zuvor empfangene Paket. Wenn nein, kann es sich um eine Replay-Attacke handeln und das entsprechende Paket sollte verworfen werden. Die Paketnummer wird verschlüsselt übertragen. Die Sequenzkontrolle ist optional und steht nur in den Security Suites zur Verfügung, die eine Verschlüsselung unterstützen.

F.3 Gefährdungen

Dieses Kapitel beschreibt typische Gefährdungen, denen ein ZigBee-System ausgesetzt sein kann. Da bisher ZigBee-Geräte nur in vergleichsweise geringem Umfang produktiv eingesetzt werden, gibt es noch wenig Erfahrung.

F.3.1 Ausfall durch Umgebungseinflüsse

Wie in einem kabelgebundenen Netz kann es auch in einem ZigBee-Netz durch Überspannungen zum Ausfall von Netzkomponenten kommen. Insbesondere sind Außeninstallationen durch Blitz und Witterungseinflüsse gefährdet. In Produktions- und Logistikumgebungen können ZigBee-Komponenten in einer rauen Umgebung durch Staub, Feuchtigkeit und Erschütterungen beschädigt werden.

F.3.2 Mangelhafte Planung

ZigBee-Netze mit der Möglichkeit eines flexiblen Routing von Nachrichten über ZigBee Router können schnell eine Dimension erreichen, die eine sorgfältige Planung der Flächendeckung und der Länge möglicher Routing-Pfade erfordern. Folgende Beispiele illustrieren die Gefährdungen durch Planungsfehler:

- Durch eine mangelhafte Planung können sich z.B. Performance-Einbußen ergeben, die durch Störungen oder auch durch Funklöcher entstehen können.
- Die Anzahl der passierten ZigBee Router bis zur Auslieferung einer Nachricht an den Adressaten im ZigBee-Netz bzw. bis zum Erreichen eines ZigBee Gateway ist ein kritischer Parameter. Bei jeder Übertragung zum nächsten Hop über die störanfällige Funkstrecke steigt die Wahrscheinlichkeit eines Paketverlusts an und es kommt zu einer zusätzlichen Verzögerung. Ein Planungsfehler kann zu einer zu großen Anzahl von Hops führen, sodass als Folge Abstriche in der Verfügbarkeit und in der Dienstgüte hingenommen werden müssen.
- Im Rahmen der Netzplanung werden auch die eingesetzten Sicherheitsmechanismen festgelegt. Fehlerhafte Einschätzungen der Risikolage und Planungsfehler können dazu führen, dass ein unnötig geringes Sicherheitsniveau (z.B. der Verzicht auf Verschlüsselung und Integritätsprüfung) eingestellt wird oder beispielsweise Geräte eingesetzt werden sollen, die keine geeignete Absicherung unterstützen (beispielsweise weil sie die ungesicherte Übertragung eines Master Keys erfordern).

F.3.3 Fehlende Regelungen zur Nutzung von Frequenzen und Störung durch Fremdsysteme

Das ISM-Band bei 2,4 GHz, das für die ZigBee-Funkübertragung unter anderem in Frage kommt, wird von diversen Systemen genutzt, z.B. WLAN, Bluetooth, Bewegungsmeldern, weiteren WPANs und Mikrowellenherden. Insbesondere können die mittlerweile flächendeckend genutzten WLANs entsprechend IEEE 802.11 die ZigBee-Kommunikation erheblich beeinträchtigen (siehe [IEEE06], [ZA07] und [ZW07]). Wenn in dem Bereich, in dem ein ZigBee-Netz betrieben wird, keine detaillierten Festlegungen hinsichtlich des Parallelbetriebs zu anderen Funksystemen getroffen werden, kann es zu signifikanten Störungen der Datenübertragung im ZigBee-Netz kommen. Werden diese Störungen durch einen anderen Nutzer (außerhalb der Behörde oder des Unternehmens) verursacht, der berech-

tigterweise ebenfalls im 2,4-GHz-Bereich operiert, müssen die Störungen sogar hingenommen werden.

F.3.4 Sicherheitskritische Einstellung

ZigBee überlässt die Wahl von Verschlüsselung und Integritätsprüfung der Applikation bzw. dem Nutzer. Gegebenenfalls kann der Benutzer selbst entscheiden, ob eine Übertragung gesichert wird oder nicht. Weiterhin können die Voreinstellungen des Herstellers eine unsichere Konfiguration bedeuten. Es besteht damit die Gefahr, dass Übertragungen unzureichend abgesichert sind.

F.3.5 Schwächen im Schlüsselmanagement

Schlüssel (insbesondere Master Keys) werden entweder vorkonfiguriert – manuell durch den Nutzer oder bei der Produktion des ZigBee-Geräts – oder zu den ZigBee-Geräten übertragen. Damit besteht zunächst unmittelbar die Gefahr, dass Informationen über einen Master Key nach außen dringen. Ein manuell eingetragener Schlüssel kann (ggf. unbeabsichtigt) eine Systematik aufweisen, die ein Angreifer bei einer Brute-Force-Attacke im Sinne eines geschickten Ratens des Schlüssels ausnutzen kann.

Bei durch den Hersteller vorkonfigurierten Master Keys muss dem Hersteller vertraut werden, dass der Schlüssel einen genügend zufälligen Charakter aufweist.

Kritisch ist das Ausrollen neuer Master Keys, da der Standard hier keine Hilfsmittel spezifiziert. Manuelles Verteilen neuer Schlüssel kann zu Fehlkonfigurationen führen und sehr aufwändig sein. Dies birgt die Gefahr, dass Nutzer mit möglichst wenigen Master Keys arbeiten und die Master Keys weitestgehend über das ZigBee-Netz verteilen[5]. Weiterhin können Nutzer versucht sein, die regelmäßige Verteilung neuer Master Keys zu vermeiden, was automatisch mit dem Problem der Überalterung der Master Keys verbunden ist[6].

Das Schlüsselmanagement weist insgesamt die Schwäche auf, dass die Übertragung von Schlüsselmaterial nicht in eine Authentisierung eingebettet und nicht durch die dabei eingesetzten kryptographischen Mittel geschützt ist. Trotz der Forderung der Unterstützung sehr einfacher Geräte, die keine komplexen Authentisierungsverfahren unterstützen, hätte dies nicht dagegen gesprochen, den ZigBee-Standard um ein weiteres Sicherheitsprofil zu erweitern, das eine Authentisierung mit integrierter Übertragung von Schlüsselmaterial unterstützt.

F.3.6 Unkontrollierte Ausbreitung der Funkwellen

Die Funkwellen der ZigBee-Komponenten breiten sich auch über räumliche Grenzen des ZigBee-Nutzungsbereichs aus. Hier ist dann eine Aufzeichnung grundsätzlich möglich. Werden Richtantennen für einen Lauschangriff verwendet, ist ein ZigBee-Netz trotz der üblicherweise sehr geringen Sendeleistungen seiner Komponenten auch über größere Entfernungen verwundbar.

---

5 Die Gefahr besteht in folgendem Sachverhalt: Je weniger Master Keys im Netz vorliegen, desto weniger Schlüssel muss ein Angreifer „erraten“, d.h. desto geringer ist der Aufwand für den Angreifer. Außerdem bedeutet jede Übertragung eines Master Key die Gefahr, dass der Schlüssel von einem Angreifer abgefangen wird.

6 Je seltener ein Master Key erneuert wird, desto mehr Zeit hat ein Angreifer, sich den Schlüssel durch geeignete Techniken zu beschaffen. Je länger ein bereits kompromittierter Schlüssel noch gültig ist, desto mehr Möglichkeiten hat ein Angreifer durch Abhören, Fälschen oder durch Zugriff auf Infrastruktur-Ressourcen Schaden zu stiften.

F.3.7 Abhören der ZigBee-Kommunikation

Da es sich bei Funk um ein Shared Medium handelt, können die über ZigBee übertragenen Daten aufgezeichnet werden. Der Lauschangriff wird erleichtert, wenn keine Verschlüsselung verwendet wird, oder wenn es gelingt, einen Schlüssel zu kompromittieren. Weiterhin sind Daten, die beispielsweise mit dem im gesamten Netz identischen Network Key verschlüsselt werden, vergleichsweise schwach geschützt.

Die Gefährdung der Vertraulichkeit muss anwendungsspezifisch gewichtet werden. Die Übertragung von Statusinformationen oder Messergebnissen mag zwar in vielen Fällen (beispielsweise in Produktion und Logistik) nur geringe Anforderungen an die Vertraulichkeit stellen, werden dagegen in einer medizinisch-technischen Anwendung Daten übertragen, die auf das Krankheitsbild einer Person Rückschlüsse gestatten, ist der Schutz der Vertraulichkeit immens wichtig.

F.3.8 Replay und Manipulation von Nachrichten

Ein Angreifer kann zunächst Nachrichten von dem Shared Medium Funk aufzeichnen und wieder in das Netz einspielen. Weiterhin kann der Angreifer dabei Pakete manipulieren. Ohne einen geeigneten und aktivierten Integritätsschutz besteht eine hohe Wahrscheinlichkeit, dass Replay und Manipulation von Nachrichten unerkannt bleiben. Die Verletzung des Sicherheitsziels der Integrität der Nachrichten ist für ZigBee dabei besonders kritisch, da ZigBee zur Sensorabfrage und zu Steuerungszwecken eingesetzt werden soll. Fehlerhafte Messergebnisse oder Steuerkommandos können je nach Anwendung zu einem erheblichen Schaden führen.

F.3.9 Vortäuschen eines gültigen Netzelements

Sofern keine geeigneten Authentisierungsverfahren eingesetzt werden, kann im Netz eine Fremdstation nur schwer identifiziert werden. Die alleinige Verwendung einer MAC-Adresse für die Zugangskontrolle, wie in ZigBee vorgesehen, kann nicht verhindern, dass eine Station die MAC-Adresse einer anderen (aktuell nicht aktiven) Station übernimmt und sich als gültiges Netzelement ausgibt. Wenn in dieser Situation nicht vorkonfigurierte Schlüssel genutzt werden, kann es sogar passieren, dass eine solche Station mit Schlüsselmaterial versorgt wird und aktiv am Netz teilnehmen kann. Weiterhin ist zu bedenken, dass Multi-Hop-Netze generell eine gewisse Anfälligkeit gegenüber Man-in-the-Middle-Attacken haben. Denkbar ist, dass ein Angreifer einen ZigBee Router vortäuscht und versucht, einen gewissen Anteil des Netzverkehrs über sich zu leiten.

F.3.10 Bedrohung der Verfügbarkeit

Geräte, die in das Frequenzspektrum einstrahlen, in dem ein ZigBee-Netz operiert, können die Kommunikation empfindlich stören und im Extremfall unmöglich machen. Die Ursache können andere Funkgeräte sein (siehe Kapitel F.3.3).

Solche Störungen können auch bewusst durch einen Störsender erzeugt werden; generell können aber alle möglichen elektrischen Geräte Störstrahlungen aussenden. Dieser Faktor muss insbesondere in industriellen Umgebungen in Betracht gezogen werden, die ja wesentliche Einsatzbereiche von ZigBee sein sollen. Prüfungen hinsichtlich der elektromagnetischen Verträglichkeit können lediglich die Wahrscheinlichkeit einer Störung reduzieren, ausschließen können sie eine Störung nicht. Eine solche Störquelle kann sich bei ausreichender Sendeleistung auch außerhalb des Geländes befinden, auf dem ZigBee genutzt wird.

Grundsätzlich können in Funknetzen Angriffe vom Typ Denial of Service (DoS) nie ausgeschlossen werden. Ein Übertragungssystem, das robust gegenüber Störungen gestaltet ist, kann lediglich mildernd wirken.

Abhängig von Größe, Art der Applikation und Installation kann der ZigBee Coordinator einen Single-Point-of-Failure darstellen. Fällt dieser durch Umgebungseinflüsse oder durch einen gezielten Angriff aus, so ist das gesamte ZigBee-Netz gegebenenfalls nicht mehr kommunikationsfähig.

F.3.11 Erstellung von Bewegungsprofilen

Da die MAC-Adresse eines ZigBee-Geräts, die normalerweise die Hardware-Adresse des Geräts ist, bei jeder Datenübertragung mit versendet wird, ist ein eindeutiger Bezug zwischen MAC-Adresse des Geräts, Ort und Uhrzeit der Datenübertragung herstellbar. Auf diese Weise können grundsätzlich Bewegungsprofile über mobile Nutzer erstellt werden. Die Wertung dieser Eigenschaft von lokalen Funksystemen als Gefährdung ist anwendungsabhängig[7].

[7] Ein ZigBee-Gerät ist nicht notwendig mit einer Person assoziiert. Es gibt außerdem Anwendungen, in denen die Lokalisierung eines Geräts die Sicherheit von Arbeitsabläufen sogar steigern kann. Das Wissen um die Position einer Person ist beispielsweise bei einem Unfall oft von entscheidender Bedeutung. Hier wäre es eher eine Gefahr, wenn die Lokalisierung nicht zuverlässig und genau genug ist.

F.4 Schutzmaßnahmen

ZigBee wird sich durch vielfältige und sehr heterogene Anwendungen auszeichnen, verbunden mit einer großen Palette an unterschiedlich intelligenten Geräten. Es gibt also keine allgemeingültige Empfehlung zur Absicherung, sondern die einzelne Anwendung (bzw. Anwendungsgruppe) muss betrachtet werden. In diesem Sinne ist ZigBee auch spezifiziert, denn jede Protokollschicht ist für die Absicherung eines in der entsprechenden Protokollschicht erzeugten Pakets zunächst selbst verantwortlich und in speziellen Applikationsprofilen werden Sicherheitsniveaus festgelegt. Daher ist die Analyse des Schutzbedarfs der Anwendungen und der zugehörigen Daten eine fundamentale Grundlage.

F.4.1 Absicherung der Datenkommunikation

Generell gilt, dass jede Kommunikationsbeziehung in ZigBee immer die höchstmögliche anwendbare Absicherung verwenden sollte. ZigBee-Netze sollten dabei möglichst auf jeder Funkstrecke eine Verschlüsselung und eine Integritätssicherung verwenden. Die Priorisierung von Verschlüsselung und Integritätssicherung ist dabei anwendungsspezifisch am Schutzbedarf orientiert.

Auf die ungesicherte Übertragung von Master Keys sollte stets verzichtet werden. Sofern möglich, sollten Master Keys in regelmäßigen Abständen gewechselt werden. Die Häufigkeit muss im Einzelfall festgelegt werden.

Die Absicherung der zu übertragenden Pakete sollte möglichst bereits auf Anwendungsebene geschehen. Die Verschlüsselungsmechanismen der unteren Ebenen sollten nur zur Absicherung von Kontrollpaketen genutzt werden, die auf NWK Layer oder MAC Layer erzeugt werden. Auf diese Weise ist zugesichert, dass Nutzdaten auch bei der Übertragung über ZigBee Router stets gesichert sind.

F.4.2 Geeignete Produktauswahl

Allgemein sollte wie in Maßnahme F.4.1 ein höchstmögliches Sicherheitsniveau erreicht bzw. das Sicherheitsniveau des gewünschten ZigBee Application Profile unterstützt werden. Dies bedingt eine Auswahl von Produkten, die die hierfür erforderlichen Sicherheitsmechanismen zuverlässig und interoperabel unterstützen.

Die ZigBee Alliance bietet durch die ZigBee-Zertifizierung (ZigBee Certified Products[8]) für die spezifizierten Application Profiles Hilfen bei der Auswahl von geeigneten Produkten.

F.4.3 Zugangskontrolle

Die Zugangskontrolle über ACLs aus MAC-Adressen gemäß IEEE 802.15.4 sollte für ZigBee Router und ZigBee Gateways genutzt werden. Auf diese Weise ist zunächst das Risiko minimiert, dass sich unbeabsichtigt eine Fremdstation in das Netz integriert. Außerdem kann durch MAC-Filter die Vielfalt der möglichen Netzverbindungen bewusst eingeschränkt und damit übersichtlich gehalten werden. Dies ist insbesondere für ZigBee Router wichtig.

---

8 Diese Zertifizierung ist nicht zu verwechseln mit der Kennzeichnung von Produkten als „Designed For ZigBee“, die von der ZigBee Alliance als Vorstufe zur Zertifizierung angesehen wird. Derartige Produkte unterstützen die erforderlichen Mechanismen nicht zwingend.

Der effektive Sicherheitsgewinn durch eine Zugangskontrolle basierend auf MAC-Adressen ist allerdings eher gering.

F.4.4 Frequenzstandard und Frequenzmanagement

Durch die zunehmend flächendeckende Nutzung von Funktechnologien im 2,4-GHz-Bereich können Interferenzen zwischen diesen auftreten. Insbesondere kann die Kommunikation von ZigBee-Geräten hierdurch gestört werden. Prinzipiell besteht diese Gefährdung für alle Frequenzbereiche. Eine Minimierung dieser Gefährdung kann durch die folgenden Maßnahmen erreicht werden (siehe auch [VDI08] und [ZVEI08]):

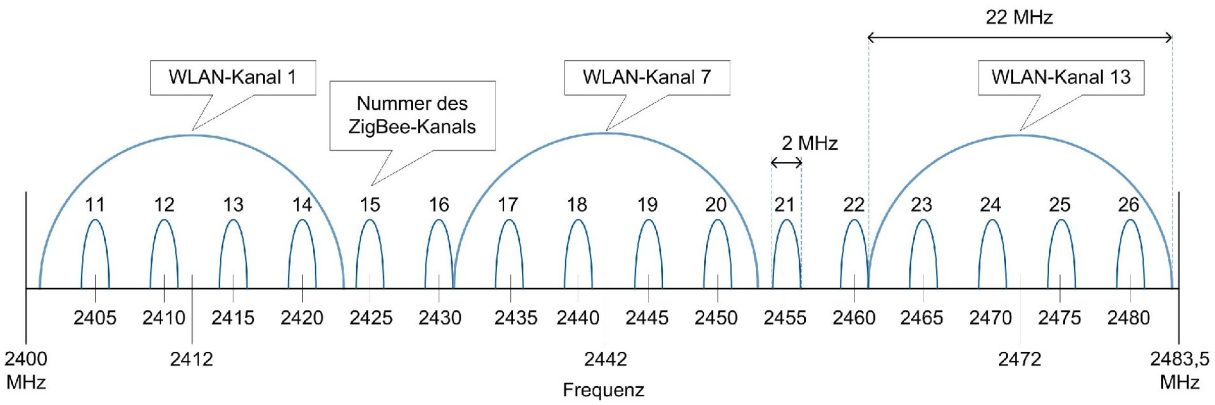
- Eine Planung der Frequenzen für alle eingesetzten Funktechnologien – ZigBee, WLAN und Bluetooth usw. – ist möglichst vor Einsatz der Technologien vorzunehmen. Zwingend ist eine solche Planung im Bereich der industriellen Automatisierung. Dabei muss berücksichtigt werden, dass ggf. auch Systeme, die keine Kommunikationssysteme darstellen, wie Mikrowellenherde, Schweißbrenner usw. in den genannten Frequenzbereichen eingesetzt werden können.

- Mit der Frequenzplanung geht eine Planung der Abdeckungsbereiche einher. Mit zunehmendem Abstand zwischen WLAN- und ZigBee-Bereichen wird die Gefährdung durch Interferenzen geringer.

- Bei der Auswahl der ZigBee-Geräte kann bereits darauf geachtet werden, dass Geräte zum Einsatz kommen, die eine automatische Kanalwahl unterstützen und dabei die von einem WLAN genutzten Bereiche vermeiden. Wenn dies nicht möglich ist, muss durch eine manuelle Konfiguration der Kanäle eines ZigBee-Systems darauf geachtet werden, dass nur Kanäle verwendet werden, die von einer WLAN-Installation am wenigsten betroffen sind. Werden beispielsweise in einem WLAN flächendeckend die Kanäle 1, 7 und 13 verwendet, kommen für ZigBee, wie in Abbildung F-11 gezeigt, eigentlich nur die Kanäle 15, 16, 21 und 22 in Frage, da diese am geringsten von WLAN-Übertragungen betroffen sind[9].

- Ist ein flächendeckender, ortsnaher Einsatz von WLAN und ZigBee im 2,4-GHz-Bereich unumgänglich, so sollte ZigBee nur für unkritische Applikationen verwendet werden. Grundsätzlich sind umfangreiche eigene Tests für die vorgesehenen Applikationen vorzusehen.

Abbildung F-11: Kanalaufteilung bei ZigBee im Vergleich zu WLAN



[9] Für die Übertragung bei ZigBee stehen bei 2,4 GHz 16 Kanäle zur Verfügung, die jeweils 2 MHz breit sind und von 11 bis 26 nummeriert werden.

F.4.5 Redundante Planung des ZigBee Coordinator

Die herausragende Stellung des ZigBee Coordinator erfordert eine besondere Planung der Verfügbarkeit dieses Knotens. Grundsätzlich sollten die ZigBee-Geräte derart ausgewählt und konfiguriert werden, dass ein weiteres ZigBee-Gerät als FFD im Fehlerfall den primären ZigBee Coordindator ersetzen kann.

F.4.6 Absicherung der ZigBee Gateways

Über ZigBee Gateways können sich prinzipiell Angriffe über Netze hinweg ausbreiten. Die Gefährdung besteht dabei in beiden Richtungen, denn auch ZigBee-Geräte können über ein Gateway angegriffen werden. Ein ZigBee Gateway kommuniziert allerdings auf Anwendungsebene und damit besteht die Möglichkeit – im Sinne eines Application Layer Gateway – hier ein hohes Niveau an Sicherheit zu schaffen. Dazu muss ein ZigBee Gateway entsprechend gehärtet sein, zumindest sofern auf dem Gateway ein Standard-Betriebssystem (z.B. Windows oder Linux) genutzt wird.

F.4.7 Planung der ZigBee Router

Die Verwendung eines ZigBee Router sollte mit Bedacht geplant werden, da jeder Hop die Gesamtverfügbarkeit reduziert. Die möglichen Kommunikationsbeziehungen zu anderen Routern sollten durch MAC ACLs gemäß IEEE 802.15.4 festgelegt werden (siehe auch Kapitel F.4.2).

F.4.8 Nicht benötigte Funkschnittstellen deaktivieren

Bei Nichtbenutzung von ZigBee-Komponenten sollte deren Funktion deaktiviert werden bzw. zumindest in den Schlafzustand gewechselt werden.

F.4.9 Restrisiko

Unabhängig von den beschriebenen Sicherheitsmaßnahmen sind mit der Verwendung von ZigBee-Systemen immer folgende Restrisiken verbunden:

- Das Erstellen von Bewegungsprofilen mobiler Geräte (siehe Kapitel F.3.11) kann nicht verhindert werden.
- Die Bedrohung der Verfügbarkeit (siehe Kapitel F.3.1 und F.3.10) ist ebenfalls nicht vollständig vermeidbar.

F.5 Ausblick

ZigBee setzt sich als Industriestandard zunehmend im Bereich der Sensortechnik durch. Dieser ist bisher durch sehr heterogene Produkte mit vielen verschiedenen, proprietären Protokollansätzen für die Funkkommunikation gekennzeichnet. Zum Zeitpunkt der Erstellung dieses Dokuments ist bereits eine deutlich steigende Anzahl von Produkten verfügbar, jedoch hat ZigBee noch keine Dominanz erreicht. Lücken in den Sicherheitsmechanismen und deren Implementierung zeigen sich jedoch meist erst bei entsprechender Verbreitung der Produkte. Derzeit sind für ZigBee aufgrund der geringen Verbreitung im produktiven Betrieb nur wenige relevante Sicherheitsvorfälle bekannt. Hinsichtlich der Entwicklung der Gefährdungen und der Sicherheit ist ein weiterer Ausblick daher nicht möglich.

Klar erkennbar ist zum jetzigen Zeitpunkt eine Gefährdung der Verfügbarkeit durch Überlappung der Frequenzbereiche, insbesondere falls ZigBee im 2,4-GHz-Spektrum genutzt wird. Derartige Gefährdungen resultieren aus der Zunahme parallel genutzter Funksysteme auf Basis von WLAN, Bluetooth oder ZigBee, die im selben Frequenzbereich ggf. sogar flächendeckend operieren. Diese Gefährdung der Verfügbarkeit wird mit zunehmender Verbreitung von Funktechnologien noch erheblich an Bedeutung gewinnen und erfordert für alle Systeme eines Unternehmens bzw. einer Behörde eine sorgfältige Planung der genutzten Frequenzen und der Funkversorgung.

F.6 Fazit

ZigBee ist ein für Sensor- und Steuerungsaufgaben zugeschnittenes drahtloses Kommunikationssystem, das sowohl einen punktuellen als auch einen flächendeckenden Aufbau gestattet. ZigBee ist von der ZigBee Alliance als Industriestandard spezifiziert und nutzt auf den unteren Protokollebenen den Standard IEEE 802.15.4.

Die Verschlüsselung und/oder die Integritätssicherung kann auf Application Layer, Network Layer und MAC Layer durchgeführt werden und setzt AES ein. Schlüssel werden vorkonfiguriert oder über das Netz übertragen. Das Schlüsselmanagement weist die Schwäche auf, dass die Schlüsselvereinbarung nicht in eine Authentisierung eingebettet und nicht durch die dabei eingesetzten kryptographischen Mittel geschützt ist.

Unter der Annahme sicher konfigurierter Schlüssel gestattet ZigBee allerdings eine vergleichsweise solide Absicherung der Kommunikation (hinsichtlich des Sicherheitsziels der Vertraulichkeit). Voraussetzung ist, dass die im Standard unterstützten Mechanismen auch in den Produkten angeboten werden, der Einsatz dieser Mechanismen geeignet geplant und im Netz auch konfiguriert wird.

ZigBee bietet ein breites Einsatzspektrum im Sensor- und Steuerungsbereich und hat als offener Standard zunehmend Akzeptanz erreicht. Insbesondere beim Einsatz von ZigBee ist ein umfassendes Frequenzmanagement für den gesamten Unternehmens- bzw. Behördenbereich wichtig, um die Gefährdung der Verfügbarkeit zu minimieren.

Aufgrund der genannten Restrisiken, insbesondere der Gefährdung durch Interferenz mit WLAN-Systemen, sollte ZigBee, aber auch jegliche andere Funktechnologie im Sensor- und Steuerungsbereich, nur nach geeigneten Tests oder für unkritische Applikationen eingesetzt werden.

F.7 Literatur und Links

Ausführliche technische Informationen zur Funktionsweise von ZigBee können der Homepage der ZigBee Alliance (http://www.zigbee.org) entnommen werden. Neben der ZigBee-Spezifikation sind hier auch Präsentationen und White Papers verfügbar.

[FS06] Funkschau, “WLAN/Zigbee: Koexistenz nicht gewährleistet”, Dezember 2006

[IEEE06] IEEE Std 802.15.4 – 2006, “Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)”, 2006, verfügbar unter http://www.ieee.org

[VDI07] VDI/VDE 2185, Blatt 1, „Funkgestützte Kommunikation in der Automatisierungstechnik“, September 2007

[VDI08] VDI/VDE 2185, Blatt 2, „Funkgestützte Kommunikation in der Automatisierungstechnik – Koexistenzmanagement von Funklösungen“, Entwurf, August 2008

[ZA07] ZigBee Alliance, „ZigBee and Wireless Frequency Coexistances“ White Paper, Juni 2007, verfügbar unter http://www.zigbee.org/

[ZA08] ZigBee Alliance, „ZigBee Specification 2007“, Januar 2008, verfügbar unter http://www.zigbee.org/

[ZVEI08] ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e.V., „Koexistenz von Funksystemen in der Automatisierungstechnik“, November 2008, verfügbar unter http://www.zvei.de

[ZW07] Z-Wave Alliance, „WLAN Interference with IEEE 802.15.4“, März 2007, verfügbar unter http://www.z-wavealliance.org

F.8 Abkürzungen

ACL	Access Control List
AES	Advanced Encryption Standard
APL	Application
APS	(ZigBee) Application Support Sub-Layer
BPSK	Binary Phase Shift Keying
CBC	Cipher Block Chaining
CBC-MAC	CBC with Message Authentication Code
CCM	Counter with CBC-MAC
CE	Consumer Electronics
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTR	Counter
DoS	Denial of Service
DSSS	Direct Sequence Spread Spectrum
FAQ	Frequently Asked Question
FFD	Full Functional Device
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISM	Industrial, Scientific, and Medical
LAN	Local Area Network
MAC	Medium Access Control
MIC	Message Integrity Check
NWK	(ZigBee) Network Layer
PAN	Personal Area Network
PHY	Physical Layer (IEEE)
QPSK	Quadrature Phase Shift Keying
RF4CE	Radio Frequency for Consumer Electronics
RFD	Reduced Functional Device
RFID	Radio Frequency Identification
SKKE	Symmetric-Key Key Establishment
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

UMTS	Universal Mobile Telecommunications System
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
ZAP	ZigBee Application Profile
ZDO	ZigBee Device Object

F.9 Glossar

Access Control List (ACL)

Zugriffskontrollliste für die Filterung von zugelassenen IP-/MAC-Adressen

Advanced Encryption Standard (AES)

Symmetrisches Verschlüsselungsverfahren mit einer variablen Schlüssellänge von 128, 192 oder 256 Bit.

Application Support Sub-Layer (APS)

Bestandteil des ZigBee Application Layer, das aufbauend auf dem ZigBee Network Layer (NWK) einen Satz von allgemein verwendbaren Applikationselementen anbietet.

Authentisierung

Verifizierung der Identität einer Instanz, z.B. eines Benutzers oder eines Geräts. Zweck ist oft die anschließende Autorisierung für Zugriffe. Ohne Authentisierung ist im Allgemeinen keine sinnvolle Autorisierung möglich.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

Kanalzugriffsverfahren in ZigBee (und WLAN nach IEEE 802.11), welches auf dem Prinzip der zufälligen Verzögerung des Sendeversuchs und des Abhörens des Funkkanals vor einer Übertragung basiert. Erlaubt mehreren Stationen die simultane Nutzung des Shared Medium Funk mit einem vergleichsweise geringen Kollisionsrisiko.

Cipher Block Chaining Mode (CBC)

Betriebsart, in der Blockchiffrierungsalgorithmen arbeiten; ein Klartextblock wird zuerst mit dem im vorhergehenden Schritt erzeugten Geheimtextblock per XOR (exklusives Oder) verknüpft und danach verschlüsselt.

Counter with CBC-MAC (CCM)

CBC-MAC = Cipher Block Chaining with Message Authentication Code; CCM ist eine generische Methode für die Verschlüsselung und Integritätsprüfung von Daten, die für die Verwendung einer 128-Bit-Blockchiffrierung (z.B. AES) spezifiziert ist.

Denial of Service (DoS)

Ein Angriff vom Typ Denial of Service hat zum Ziel die Arbeitsfähigkeit des angegriffenen Objekts möglichst stark zu reduzieren. Dies beinhaltet beispielsweise die systematische Überlastung eines Netzknotens durch unsinnigen Verkehr (Dummy Traffic) oder das beabsichtigte Herbeiführen eines Fehlerzustands durch das Einspielen fehlerhafter Nachrichten.

Dictionary-Attacke

Siehe Wörterbuchattacke

Full Functional Device (FFD)

ZigBee-Gerät, das alle Betriebsfunktionen für ein WPAN implementiert (z.B. die Funktion eines PAN-Coordinator).

Funkzelle

Geografischer Bereich um einen Sender herum, in dem ein genügend guter Empfang besteht. Was als „genügend gut“ zu bezeichnen ist, ist Festlegungssache. Die Ausdehnung einer Funkzelle wird weiterhin durch den verwendeten Frequenzbereich, die Sendeleistung und insbesondere durch die

jeweiligen Umgebungsbedingungen (z.B. Material von Wänden, Türen, Fenstern und Decken) beeinflusst.

ISM-Frequenzband

Lizenzfrei nutzbare Frequenzbänder, die für industrielle, wissenschaftliche und medizinische Zwecke verwendet werden können (ISM = Industrial, Scientific and Medical)

Man in the Middle

Der Angreifer positioniert sich zwischen zwei Kommunikationspartner und täuscht beiden Parteien vor, der jeweils erwartete eigentliche Partner zu sein. Dabei kann der Man in the Middle den Dialog zwischen den beiden Parteien belauschen oder auch verfälschen. Ziel ist oft die Ermittlung von Passwörtern.

Message Integrity Check (MIC)

Kryptographischer Integritätsschutzmechanismus

PAN Coordinator

Spezielle Rolle eines Full Functional Device in einem WPAN nach IEEE 802.15.4. Der PAN Coordinator verwaltet die Identifikation des WPAN, koordiniert die Anmeldung an das WPAN und kann gewisse Parameter beim Kanalzugriff steuern.

Personal Area Network (PAN)

Netz, welches im Nahbereich (in einem Radius von wenigen Metern) operiert und Kleingeräte wie Drucker, PDAs oder Mobiltelefone untereinander oder mit einer Zentralstation (z.B. PC, Router) vernetzt. Dabei können verschiedene drahtgebundene Übertragungstechniken (z.B. USB, FireWire) oder drahtloser Techniken, wie IrDA, Bluetooth oder ZigBee verwendet werden. Bei Verwendung drahtloser Techniken spricht man von einem Wireless PAN (WPAN).

Reduced Functional Device (RFD)

ZigBee-Gerät mit eingeschränkten Kommunikationsmitteln. RFDs sind für einfache Applikationen gedacht (z.B. ein über ZigBee gesteuerter Lichtschalter).

Spoofing

Vortäuschen einer in der Regel vertrauenswürdigen Identität (z.B. durch Manipulation von Adressen) mit dem Ziel Schaden anzurichten oder unerlaubten Zugriff zu erhalten.

Wireless PAN (WPAN)

Siehe PAN

Wörterbuchattacke

Eine Wörterbuchattacke (auch als Dictionary-Attacke bezeichnet) wird typischerweise zum Raten eines Passworts oder Schlüssels eingesetzt. Die Annahme für eine Wörterbuchattacke ist, dass Passwörter oder Schlüssel aus einer sinnvollen oder in Wörterbüchern bekannten Zeichenkombination bestehen. In diesem Falle kann das Verfahren schnell zum Erfolg führen.

Zelle

Siehe Funkzelle

ZigBee Device Object (ZDO)

Modelliert auf Anwendungsebene ein ZigBee-Gerät. ZigBee Anwendungen werden als Application Objects dargestellt, die über die ZDOs kontrolliert und verwaltet werden.

ZigBee Coordinator

Entspricht dem PAN Coordinator in IEEE 802.15.4 und ergänzt diesen um Funktionen auf dem Network Layer

ZigBee Router

Spezielle Full Functional Devices, die zusätzlich Pakete zwischen ZigBee-Knoten vermitteln kann. Der logische Gerätetyp ZigBee Router entspricht dem Coordinator in IEEE 802.15.4.

G. UWB

Inhaltsverzeichnis des Abschnitts

G.1 Grundlagen / Funktionalität

Der Begriff UWB (Ultra Wideband) bezeichnet Funksysteme, die – bezogen auf die Betriebsfrequenz – eine hohe Bandbreite nutzen. Im Allgemeinen belegt bei UWB das Spektrum der Aussendung eine Bandbreite, die mindestens 25% der Bandmittenfrequenz beträgt. UWB-Systeme verteilen ihre Sendeenergie auf einen sehr großen Frequenzbereich und sind somit für herkömmliche schmalbandige Empfangssysteme nur noch als Hintergrund-Rauschen wahrnehmbar oder gar vollständig hinter deren Eigenrauschen verschwunden. Somit ist also in bestimmten Grenzen ein ungestörter Parallelbetrieb herkömmlicher Funkanwendungen und UWB möglich.

UWB ist eine Technik, die zur Übertragung hoher Datenraten über kurze Entfernungen genutzt werden kann. Der Abstand zwischen Sender und Empfänger wird im Allgemeinen kleiner als 10 Meter sein. Auch im Hinblick auf eine lange Standzeit batteriebetriebener Geräte wird mit geringen Sendeleistungen gearbeitet. So verwundert es nicht, dass man die UWB-Technik als Möglichkeit sieht, Bluetooth in Richtung höherer Datenraten zu erweitern (siehe Kapitel B. Bluetooth). Als weiteres praktisches Anwendungsfeld wird der Ersatz der drahtgebundenen USB-Schnittstelle durch UWB gesehen. Die Vorteile des UWB-Verfahrens werden in der Literatur wie folgt zusammengefasst:

- geringer Energieverbrauch – Voraussetzung für eine hohe Batterielebensdauer in mobilen Endgeräten
- skalierbare hohe Datenraten
- verbesserte Störfestigkeit
- robust gegen Mehrwegeausbreitung (Frequenz-Diversität)
- kleine, kostengünstige, skalierbare und flexible Chipsätze in CMOS-Technologie realisierbar

Die ersten Ansätze für UWB fußten auf sogenannten gepulsten Signalen. Jeder Puls dauert dabei nicht länger als eine Milliardstelsekunde (10^{-9} s) und ähnlich wie bei einem ultraschnellen Morse-Code enthält die Abfolge der Pulse die zu übertragende Information.

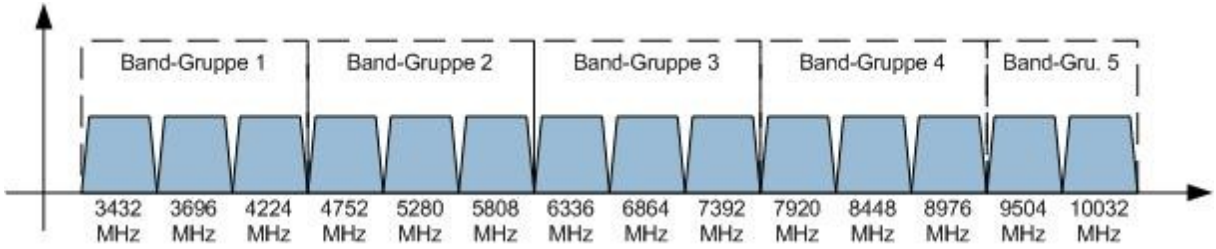
In der Zwischenzeit wurden zwei Varianten für eine technische Realisierung von UWB vorgestellt: Direct Sequence UWB (DS-UWB) und Multiband OFDM (MB-OFDM). Beide Verfahren wurden von der Task Group IEEE 802.15.3a diskutiert (siehe [IEEE153a]). Eine Einigung auf einen gemeinsamen Standard konnte die Task Group nicht erwirken, stattdessen löste sie sich im Januar 2006 auf. Die hinter den genannten Verfahren stehenden Konsortien bekräftigten jedoch zunächst ihr Interesse an einer weiteren Entwicklung der Technik:

- Das UWB-Forum hat ein Verfahren namens DS-UWB propagiert. Nachdem in 2006 zwei wichtige Mitglieder ihre Mitarbeit aufkündigten, hat sich das UWB-Forum jedoch aufgelöst.
- Die WiMedia Alliance (seit März 2005 verschmolzen mit der Multiband OFDM Alliance, MBOA) propagiert MB-OFDM. Sie erreichte in Zusammenarbeit mit der ECMA International die Herausgabe eines Standards für UWB-Systeme auf der Basis von MB-OFDM. Die Spezifikation wurde als ECMA-368 veröffentlicht (siehe [ECMA05]) und wurde in 2007 auch als ISO/IEC 26907 verabschiedet. MB-OFDM wurde darüber hinaus im März 2006 von der Bluetooth Special Interest Group als Basis für zukünftige Bluetooth-Geräte ausgewählt (siehe [BTSIG06]). Im März 2009 kündigte die WiMedia Alliance an, ihr Know-how im Rahmen entsprechender Verträge an die Bluetooth SIG, an das USB Implementers Forum sowie an die Wireless USB Promoter Group zu transferieren (siehe [WIME09]). Danach will sich auch die WiMedia Alliance auflösen.

G.1.1 Multiband-OFDM

Der Standard ECMA-368 spezifiziert Multiband-OFDM im Frequenzbereich von 3.1 bis 10.6 GHz (siehe [ECMA05]). Der Bereich ist in 14 Frequenzbänder mit einer Bandbreite von je 528 MHz unterteilt. Die Bänder werden in 4 Gruppen à 3 Bänder sowie einer Gruppe à 2 Bänder zusammengefasst (siehe Abbildung G-1).

Abbildung G-1: Frequenzbänder in MB-OFDM gemäß ECMA-368



Jedes Band besteht aus 128 Unterkanälen, von denen 100 zur Datenübertragung genutzt werden. Die Symbolrate beträgt 3,2 Megasymbole pro Sekunde. Die Modulation erfolgt mit einem vierwertigen Verfahren (Quadrature Phase Shift Keying, QPSK oder Dual Carrier Modulation, DCM, siehe [ECMA05]), entsprechend zwei Bits pro Symbol.

Zur Verbesserung der Robustheit gegen Bitfehler werden drei Verfahren vorgeschlagen:

- Verwendung eines Faltungs-Code mit unterschiedlichen Code-Raten (Forward Error Correction, FEC)
- Aussenden gleicher Information auf zwei unterschiedlichen Unterträgern (Frequency-Domain Spreading, FDS)
- Aussenden desselben Symbols zweimal zu unterschiedlichen Zeiten (Time-Domain Spreading, TDS)

Insgesamt ergibt sich aus der Kombination dieser drei Parameter die in Tabelle G-1 dargestellte Matrix der Datenraten.

Tabelle G-1: Datenraten bei MB-OFDM

Datenrate	Code-Rate	Modulation	FDS	TDS	Bits/Symbol
53,3 Mbit/s	⅓	QPSK	Ja	Ja	50
80 Mbit/s	½	QPSK	Ja	Ja	50
106,7 Mbit/s	⅓	QPSK	Nein	Ja	100
160 Mbit/s	½	QPSK	Nein	Ja	100
200 Mbit/s	⅝	QPSK	Nein	Ja	100
320 Mbit/s	½	DCM	Nein	Nein	200

Datenrate	Code-Rate	Modulation	FDS	TDS	Bits/Symbol
400 Mbit/s	5/8	DCM	Nein	Nein	200
480 Mbit/s	3/4	DCM	Nein	Nein	200

Beispiel (2. Tabellenzeile):

Die OFDM ermöglicht in Kombination mit QPSK das gleichzeitige Übertragen von 200 Bits in einem Symbol. Wird FDS eingesetzt, halbiert sich diese Zahl auf 100, da immer zwei Unterträger für ein Bit benötigt werden. Infolge von TDS wird das gleiche Symbol zweimal ausgesandt, die Zahl halbiert sich zu 50 Bits pro Symbol. Bei 3,2 Megasymbolen pro Sekunde ergibt sich eine Bitrate von 160 Mbit/s. Bei einer Code-Rate von ½ ergibt sich eine tatsächlich nutzbare Datenrate von ca. 80 Mbit/s.

Die Unterscheidung verschiedener Kanäle geschieht mittels eines Frequenzsprungverfahrens. Dabei wird jedes Symbol in einem unterschiedlichen Band einer Bandgruppe ausgesandt. In jeder der 4 unteren Bandgruppen sind 7 unterschiedliche Sprungsequenzen (Time-Frequency Codes, TFC) definiert, in der Bandgruppe 5 lediglich 2 Sprungsequenzen.

Im Gegensatz zu vielen anderen Nahfunktechniken verwenden UWB-Systeme bei der Datenübertragung temporäre Geräteadressen, deren Gültigkeit sich auf die aktuelle Kommunikationsbeziehung beschränkt.

G.1.2 Regulierende Vorschriften für UWB

Seit März 2003 gibt es eine kommerzielle Nutzungserlaubnis für UWB in den USA. Die FCC (Federal Communications Commission) nennt als Grenzwert für die Sendeleistung[1] einen Wert von -41,3 dBm/MHz im Frequenzbereich von 3,1 bis 10,6 GHz (siehe [FCCUWB]). Zu beachten ist, dass dieser Wert auf die Leistung bezogen ist, die sich auf einen 1 MHz breiten Bereich um die betreffende Messfrequenz verteilt. Im gesamten genannten Frequenzbereich kann also ein UWB-Gerät mit maximal 0,5 mW EIRP[2] strahlen.

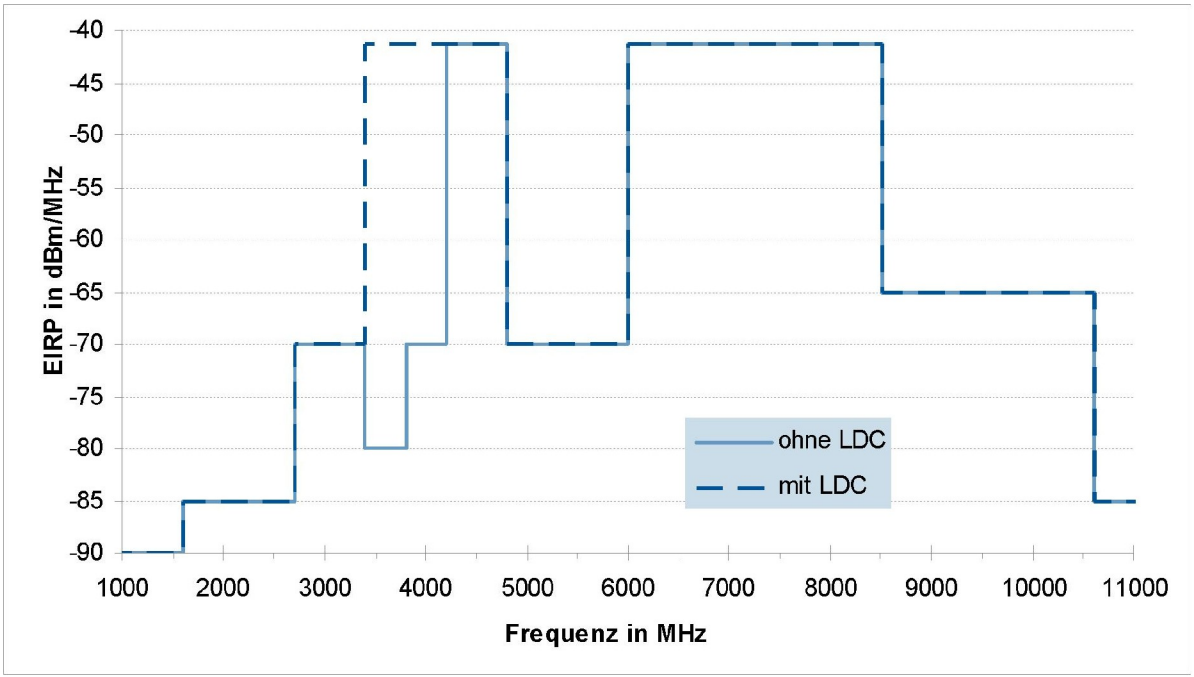
In Europa ist die Regulierung restriktiver, insbesondere wurde der Bereich von 4,8 bis 6 GHz besonders geschützt (siehe [ETSI08]). Die Abbildung G-2 zeigt die maximale effektive Strahlungsleistung in dBm/MHz als Funktion der Frequenz im Bereich 1 bis 11 GHz. Man erkennt, dass es einen besonderen Modus namens LDC (Low Duty Cycle) gibt, der – falls aktiv – eine höhere Leistung im Frequenzbereich 3,4 bis 4,2 GHz erlaubt. Unter LDC versteht die ETSI ein UWB-Gerät, das höchstens für eine Zeitspanne von 5 Millisekunden sendet und dann eine Pause von ca. 1 Sekunde macht. Anders ausgedrückt darf das UWB-Gerät während einer Stunde nur max. 18 Sekunden lang senden.

Über diese Maßnahmen hinaus sieht die ETSI eine Sendeleistungsregelung (Transmit Power Control, TPC) für in Fahrzeugen betriebenen UWB-Geräte vor. TPC muss im Frequenzbereich 4,2 bis 8,5 GHz wirken und einen Regelumfang von 12 dB aufweisen.

1 Effektive Strahlungsleistung EIRP (Equivalent Isotropically Radiated Power)

2 Diese Sendeleistung liegt in der Größenordnung der Bluetooth Klasse 3.

Abbildung G-2: Leistungsgrenzen für UWB-Systeme innerhalb von Gebäuden in Europa



G.1.3 Wireless USB

Wireless USB wurde im Jahre 2005 vom USB Implementers Forum spezifiziert (siehe [WUSB05]) und später auch als Certified Wireless USB (CWUSB) bezeichnet. Das USB Implementers Forum sieht in CWUSB eine Weiterentwicklung der drahtgebundenen Schnittstelle USB 2.0. Das Konzept des intelligenten Rechners (englisch Host), an den mittels USB vergleichsweise einfache Peripheriegeräte (englisch Devices) angebunden werden, wird durch CWUSB nicht verändert. Auch die Treiber-Struktur für die Ansteuerung der Peripheriegeräte bleibt bei CWUSB unverändert, das USB-Kabel wird jedoch durch eine Funkverbindung ersetzt. Die Spezifikation definiert sogar Adapter zur Verbindung von drahtgebundenen USB-Geräten mittels CWUSB (Device Wire Adapter und Host Wire Adapter).

CWUSB ist die erste Anwendung der UWB-Technik. Die Spezifikation setzt eine UWB-Funkverbindung nach dem von der WiMedia Alliance entwickelten Standard MB-OFDM voraus. Sie ergänzt diesen Standard um die für eine funktionierende Kommunikation fehlenden Teile, insbesondere um ein Medienzugangsverfahren, Paketformate und Sicherheitsmechanismen (siehe [ECMA05]).

CWUSB unterstützt alle in MB-OFBM unterstützten Datenraten gemäß Tabelle G-1. Somit kann maximal auf eine Rate von 480 Mbit/s zurückgegriffen werden; das entspricht der im drahtgebundenen USB 2.0 spezifizierten maximalen Bitrate. Auch alle Frequenzbänder gemäß Abbildung G-1 können von CWUSB-Geräten verwendet werden. Die vorliegende Spezifikation fordert, dass CWUSB-Geräte mindestens die Bandgruppe 1 der Abbildung G-1 unterstützen[3].

Wireless USB verwendet temporäre Geräteadressen, die erst nach erfolgreicher Assoziation den Geräten zugewiesen werden.

[3] In Europa wird für die Bandgruppe 1 die Umsetzung von LDC gefordert (siehe Abbildung G-2), was einer Verbreitung von CWUSB in Europa zum Zeitpunkt der Veröffentlichung dieser Broschüre noch im Wege steht.

G.2 Sicherheitsmechanismen

G.2.1 Kryptographische Sicherheitsmechanismen bei MB-OFDM

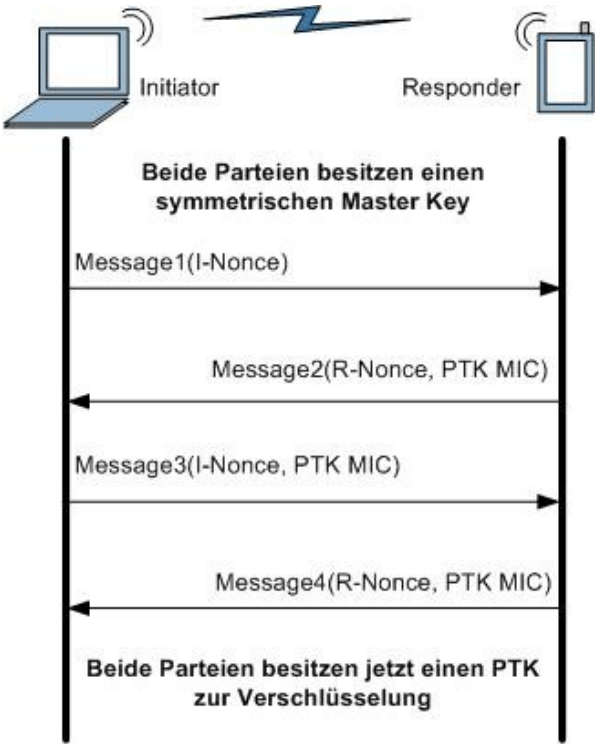
Der ECMA-Standard 368 definiert zwei Sicherheitsebenen: keine Sicherheit und hohe Sicherheit. Geräte wählen zwischen diesen Ebenen abhängig von einem Sicherheitsmodus, in dem sie arbeiten:

- Security mode 0: Das Gerät verwendet grundsätzlich keine Sicherheit bei der Datenübertragung.
- Security mode 1: Das Gerät verwendet keine Sicherheit, wenn es mit Geräten des Modus 0 oder 1 kommuniziert. Bei Kommunikation mit Geräten im Modus 2 wird hohe Sicherheit eingesetzt.
- Security mode 2: Das Gerät verwendet grundsätzlich hohe Sicherheit und kommuniziert somit nur mit Geräten im Modus 1 oder 2.

Eine hohe Sicherheit wird erreicht durch eine starke Verschlüsselung, Integritätsprüfung und einen Schutz gegen Einspielen zuvor aufgezeichneter Frames (replay attack protection). Dabei werden nicht nur Datenpakete geschützt, sondern auch ausgewählte Signalisierungspakete.

Ausgehend von einem symmetrischen geheimen Schlüssel (Pairwise Master Key, PMK) werden temporäre Schlüssel für die Punkt-zu-Punkt-Übertragung zwischen Stationspaaren (Pairwise Transient Key, PTK) abgeleitet. Zum Einsatz kommt ein Verfahren, das als 4-Way-Handshake (siehe Abbildung G-3) bezeichnet wird. Es ähnelt dem gleichnamigen Verfahren bei WLAN und ermöglicht das Generieren der temporären Schlüssel, ohne dass diese zwischen den Stationen übertragen werden müssen. Das Verfahren dient gleichzeitig der gegenseitigen Authentisierung der Kommunikationspartner, hier Initiator und Responder genannt.

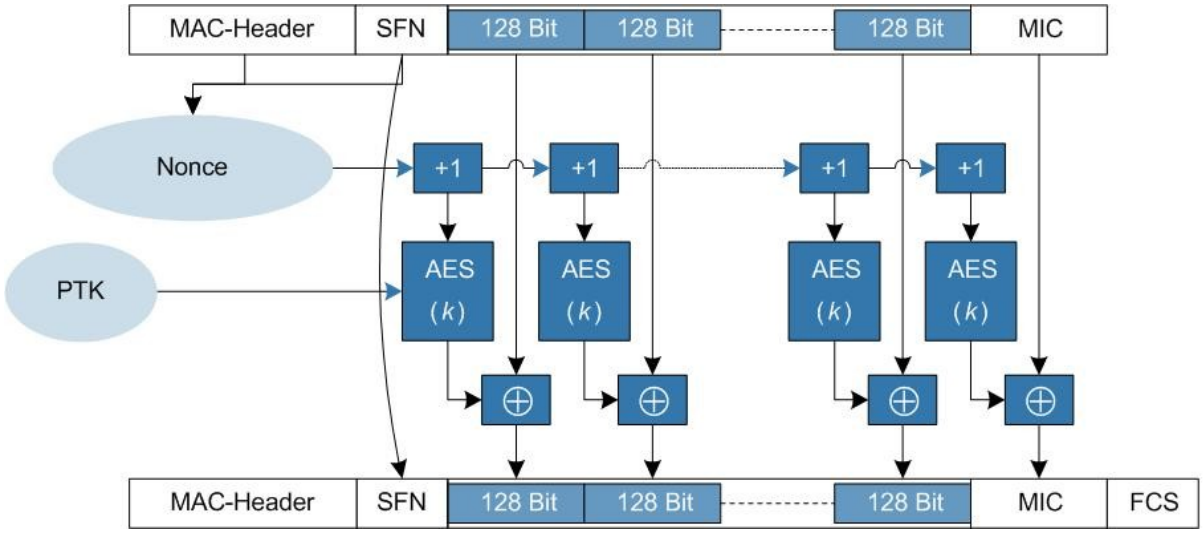
Abbildung G-3: 4-Way-Handshake



Zu diesem Zweck tauschen Initiator und Responder je eine Zufallszahl (I-Nonce bzw. R-Nonce) aus. Beide Stationen bilden unter Zuhilfenahme der beiden Zufallszahlen, der Geräteadressen sowie dem PMK eine neue 256 Bit lange Pseudozufallszahl. Sofern beide PMK identisch waren, gilt dies auch für die Pseudozufallszahl, deren eine Hälfte (128 Bit) nun als PTK dient. Die andere Hälfte wird zur Errechnung eines Prüfwertes (PTK Message Integrity Code, PTK MIC) herangezogen, der an den jeweiligen Kommunikationspartner übertragen und dort zur Prüfung der Authentizität der Gegenseite verwendet wird. Abbildung G-3 zeigt das vollständige Handshake. Wie die Stationen in den Besitz des PMK gelangen, der als Basis für das 4-Way-Handshake dient, ist nicht Gegenstand des Standards.

Auf Basis der temporären Schlüssel erfolgt eine Verschlüsselung mittels Advanced Encryption Standard (AES) in einem speziellen Modus CCM (siehe Abbildung G-4). CCM steht für CTR mode (Counter Mode) with CBC-MAC Protocol (Cipher Block Chaining Message Authentication Code). Hierbei wird nicht direkt der Klartext verschlüsselt, sondern ein Pseudozufallswert (Nonce), der unter anderem aus einem Paketzähler (Secure Frame Number, SFN) gebildet wird. Das eigentliche Verschlüsselungsergebnis entsteht dann aus der XOR-Verknüpfung eines Blocks des Klartextes mit dem AES-verschlüsselten Nonce. Die Methode Cipher Block Chaining (CBC) wird zur Integritätssicherung der Daten verwendet; sie dient der Berechnung einer Prüfsumme (Message Integrity Code, MIC).

Abbildung G-4: Verwendung von AES bei MB-OFDM (vereinfacht)



Der Standard sieht auch die Aussendung von Nachrichten an mehrere Geräte per Broadcast und Multicast vor. Zu diesem Zweck tauschen die Geräte Gruppenschlüssel (Group Temporary Key, GTK) mittels spezieller Nachrichten aus, die über den mit PTK verschlüsselten Kanal versendet werden.

G.2.2 Sicherheitsmechanismen bei Wireless USB

Wireless USB (CWUSB) setzt bei der Verschlüsselung der Daten auf das bei MB-OFDM angewandte Verfahren. Die Spezifikation von Verschlüsselung und 4-Way-Handshake (siehe [WUSB05]) entspricht in weiten Teilen dem ECMA-Standard 368 (siehe [ECMA05]), ohne dass darauf explizit Bezug genommen wird. CWUSB führt jedoch Verfahren zur Authentisierung der Geräte ein. Demnach etablieren die Geräte einen Verbindungskontext (Connection Context, CC), der neben eindeutigen Geräteadressen einen symmetrischen Verbindungsschlüssel (Connection Key, CK) umfasst. Der CK dient schließlich als Eingangswert für das 4-Way-Handshake und entspricht somit dem PMK in Kapitel G.2.1.

Für die praktische Umsetzung relevant ist ein Nachtrag zur CWUSB-Spezifikation aus dem Jahre 2006 (siehe [WUAM06]). Darin werden zwei Modelle für die Assoziation von Gerät und Computer beschrieben:

- Kabelbasierte Assoziation: Zunächst werden Gerät und Rechner mit einem herkömmlichen USB-Kabel verbunden. Der Rechner erkennt darüber, dass das Peripheriegerät Wireless USB unterstützt und übermittelt dem Gerät seine eigene Geräteadresse. Das Peripheriegerät antwortet mit dem dazu passenden Verbindungskontext, wenn zuvor bereits eine Verbindung bestanden hatte. Andernfalls übermittelt das Peripheriegerät nur seine Geräteadresse an den Rechner, der daraus einen Verbindungskontext generiert und ihn an das Gerät übermittelt. Im Rahmen dieser Aushandlung können die Geräte außerdem Daten über die unterstützten Frequenzbänder untereinander austauschen.

- Numerische Assoziation: Dieses Verfahren basiert auf einem Diffie-Hellman-Schlüsselaustausch, der über die UWB-Schnittstelle durchgeführt wird. Aus dem geheimen Schlüssel, der als Ergebnis des Schlüsselaustausches entsteht, wird über eine Hash-Funktion der Verbindungsschlüssel abgeleitet. Da Diffie-Hellman-Verfahren anfällig gegen Man-in-the-Middle-Angriffe sind, erfolgt eine Erfolgskontrolle der Assoziation durch den Anwender. Auf Peripheriegerät und Rechner wird je eine Zahl angezeigt, deren Gleichheit durch den Anwender zu bestätigen ist. Das Verfahren ähnelt in seiner Funktionsweise dem Assoziations-Modell Numeric Comparison des Secure Simple Pairing bei Bluetooth 2.1 + EDR (siehe Kapitel B. Bluetooth). Die zu vergleichende Zahl ist bei CWUSB jedoch nur zwei-, drei- oder vierstellig.

Die in [WUAM06] dargelegte Spezifikation formuliert neben den für die genannten Verfahren benötigten Protokollen und Datentypen auch Anforderungen an die einzusetzenden Zufallszahlengeneratoren. Demnach dürfen Zufallszahlen weder fest in CWUSB-Geräten kodiert noch mehrfach verwendet werden. Stattdessen soll den Empfehlungen des RFC 4086 gefolgt werden (siehe [RFC4086]). Insbesondere wird gefordert, dass die Basis für Zufallszahlen nicht deterministisch sein soll (z.B. Ableitung von einer physikalischen Rauschquelle).

Auch die Erkennbarkeit von Rechnern durch CWUSB-Geräte ist in der Spezifikation (siehe [WUAM06]) geregelt. Demnach soll ein Rechner bei der Numerischen Assoziation für die Erkennung durch Peripheriegeräte aktiviert werden. Dieser Zustand soll mindestens 1 Minute, keinesfalls aber mehr als 5 Minuten anhalten. Eine dauerhafte Erkennbarkeit, die z.B. bei Bluetooth verschiedene Sicherheitslücken geöffnet hat, soll dadurch offensichtlich vermieden werden.

G.3 Gefährdungen

Dieses Kapitel beschreibt typische Gefährdungen, denen ein UWB-System ausgesetzt sein kann. Da UWB noch eine sehr junge Technik ist, gibt es kaum praktische Erfahrungen mit diesen Systemen. Darüber hinaus gibt es über die in Kapitel G.2.1 genannten Verfahren keine stabilen Spezifikationen von Sicherheitsmechanismen.

G.3.1 Fehlende Regelungen zur Nutzung von Frequenzen

UWB-Systeme sind für den Einsatz parallel zu anderen Funksystemen prädestiniert. Die vorliegenden Regulierungen beschäftigen sich mit der Frage, inwieweit herkömmliche Systeme durch UWB beeinträchtigt werden. Dagegen ist ein Schutz von UWB-Systemen vor Störungen durch andere Funksysteme auf Basis einer Regulierung ebenso wenig möglich wie vorgesehen. Es ist somit beim Betrieb von Anwendungen auf der Basis von UWB grundsätzlich mit der Möglichkeit zu rechnen, dass Störungen auftreten. Eine Verfügbarkeit der Anwendungen kann unter diesen Bedingungen kaum garantiert werden (siehe auch Kapitel G.3.2).

G.3.2 Denial of Service (DoS)

UWB-Systeme übertragen Informationen mittels elektromagnetischer Funkwellen. Strahlen andere elektromagnetische Quellen im gleichen Frequenzspektrum Energie ab, können diese die UWB-Kommunikation stören und im Extremfall verhindern. Dies kann unbeabsichtigt oder aber durch absichtliches Betreiben einer Störquelle als Denial-of-Service-Angriff erfolgen. Eine solche Störquelle kann sich bei ausreichender Sendeleistung auch außerhalb des Gebäudes befinden, in dem UWB genutzt wird.

G.3.3 Schwachstellen der Authentisierungsverfahren

Die im ECMA-Standard vorgesehenen kryptographischen Sicherheitsmaßnahmen basieren auf einem symmetrischen Schlüssel (PMK), der allen beteiligten Komponenten bekannt sein muss (siehe Kapitel G.2.1). Ein Verfahren zur Generierung und Verteilung des PMK ist im ECMA-Standard nicht vorgegeben. Zukünftige Anwendungen, die auf UWB basieren, sind also bezüglich des verwendeten Authentisierungsverfahrens noch zu bewerten.

Bei Wireless USB (CWUSB) sind solche Verfahren spezifiziert. Dabei ist insbesondere die kabelbasierte Assoziation robust gegen Angriffe, da ein vertrauenswürdiger und physisch sicherer Kanal für den Schlüsselaustausch bereitsteht. Die Numerische Assoziation bietet mit dem Anwender ebenfalls eine vertrauenswürdige Instanz zur Prüfung einer sicheren Authentisierung. Allerdings besteht bei der Verwendung von nur zweistelligen Anzeigen auf CWUSB-Geräten eine nicht mehr zu vernachlässigende Wahrscheinlichkeit (1:100) dafür, dass ein Man-in-the-Middle-Angriff erfolgreich abgeschlossen werden kann.

G.3.4 Unkontrollierte Ausbreitung der Funkwellen

Die Funkwellen der UWB-Systeme breiten sich auch über die räumlichen Grenzen der Geräte aus. Dabei kann auch in nicht vom Anwender kontrollierten Bereichen ein Empfang möglich sein. Durch die

Verwendung einer Richtantenne lassen sich auch in größerer Entfernung schwache Signale empfangen und letztlich auswerten. Während Wireless USB eine Verschlüsselung der Daten vorschreibt, sind zukünftig auch UWB-Anwendungen denkbar, bei denen das nicht der Fall ist.

G.3.5 Diebstahl eines Endgeräts

Ein Dieb kann über die in dem gestohlenen Gerät enthaltenen Informationen ungehindert und unbemerkt Basisinformationen für eine weitere Kompromittierung erlangen, z.B. auf dem Wege des Auslesens des geheimen Schlüssels (PMK) bzw. des Verbindungskontextes (CC).

G.4 Schutzmaßnahmen

G.4.1 Absicherung von UWB

UWB-Systeme sollten grundsätzlich mit Verschlüsselung betrieben werden. Sofern Geräte gemäß ECMA-368 zum Einsatz kommen, sollten diese in den Security Mode 2 versetzt werden, da sie nur unter dieser Bedingung jegliche unverschlüsselte Kommunikationsbeziehung ablehnen. Die Unterstützung des Security Mode 2 wird somit zu einem Auswahlkriterium für UWB-Systeme entsprechend ECMA-368.

Die UWB-Schnittstellen der Geräte sollten bei Nichtbenutzung deaktiviert werden.

G.4.2 Absicherung von Wireless USB

Wireless USB (CWUSB) sollte nach Möglichkeit mit der kabelbasierten Assoziation betrieben werden. Geräte mit Numerischer Assoziation sollten die größtmögliche Anzeige mit 4 Ziffern besitzen, damit ein guter Schutz gegen Angriffe auf die Authentisierung besteht.

G.4.3 Weitere Schutzmaßnahmen

Über die oben genannten Maßnahmen hinaus sollten auf UWB-Systemen und CWUSB-Rechnern – falls dies technisch möglich ist – weitere lokale Schutzmaßnahmen implementiert werden. Dazu zählen:

- Zugriffsschutz (materielle Sicherungsmaßnahmen)
- Benutzerauthentisierung
- Virenschutz
- Personal Firewall
- restriktive Datei- und Ressourcenfreigabe auf Betriebssystemebene
- lokale Verschlüsselung

Informationen hierzu findet man in den IT-Grundschutz-Katalogen des BSI (siehe [GSK]). Im Zweifel orientiere man sich am Baustein „Internet-PC“ und wende die zugehörigen Maßnahmen sinngemäß an.

Als Schutzmaßnahme gegen das Abhören von Raumgesprächen ist ein Verbot des Einbringens von Funktechnik in den zu schützenden Raum zu empfehlen.

G.4.4 Restrisiko

Unabhängig von den beschriebenen Sicherheitsmaßnahmen ist mit der Verwendung von UWB-Systemen immer das Restrisiko einer Bedrohung der Verfügbarkeit (siehe Kapitel G.3.2) verbunden.

G.5 Ausblick

Wireless USB auf Basis von UWB mit MB-OFDM ist inzwischen am Markt verfügbar; Versionen für den Betrieb in Europa sind zum Zeitpunkt der Veröffentlichung dieser Broschüre bereits von verschiedenen Herstellern angekündigt worden. Als zweites Anwendungsfeld für UWB kann ein zukünftiges Bluetooth angesehen werden, und es ist davon auszugehen, dass die dort bereits bestehenden Sicherheitsmechanismen auch in diesen Varianten zum Einsatz kommen werden. Weitere Einsatzfelder von UWB sind in Anbetracht der Auflösung von UWB-Forum und WiMedia Alliance ungewiss.

G.6 Fazit

Funktechniken auf Basis von UWB (Ultra Wideband) befinden sich in der Entwicklung; erste serienreife Produkte sind verfügbar. Sicherheitsmechanismen sind spezifiziert und die Regulierung der Nutzung von UWB ist weitgehend abgeschlossen. Die Einsatzreichweite und Sicherheitsmaßnahmen ähneln denen von Bluetooth 2.1+EDR.

G.7 Literatur und Links

Deutschsprachige Literatur, die eine leicht verständliche Einführung in das Thema geben, sucht man noch vergeblich. Stattdessen ist man auf Informationen in Zeitschriftenartikeln angewiesen, z.B. [HEI03] und [ZIBA05]. Eine komprimierte Beschreibung der physikalischen Schicht sowie des Medienzugangs bei MB-OFDM findet sich in [HiZa05]. Dort wird auch über Simulationsergebnisse berichtet. Ansonsten erhält man Informationen aus erster Hand in den entsprechenden Standards, insbesondere [ECMA05] und [WUSB05].

[BTSIG06] „Bluetooth SIG selects WiMedia Alliance Ultra-Wideband Technology For High Speed Bluetooth® Applications", Pressemitteilung der Bluetooth SIG, März 2006, verfügbar unter http://www.bluetooth.com/Bluetooth/Press/SIG

[ECMA05] „High Rate Ultra Wideband PHY and MAC Standard", ECMA-368, Dezember 2005, http://www.ecma-international.org/publications/files/ECMA-ST/ECMA-368.pdf

[FCCUWB] Federal Comminications Commission, Part 15 of the Commission's Rules: "§15.517 Technical requirements for indoor UWB systems, http://edocket.access.gpo.gov/cfr_2005/octqtr/pdf/47cfr15.517.pdf

[GSK] Bundesamt für Sicherheit in der Informationstechnik, „IT-Grundschutz-Kataloge", verfügbar unter https://www.bsi.bund.de/cln_155/DE/Themen/weitereThemen/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

[HaZi06] Dr. Till Harbaum, Dušan Živadinović, Weitsprung Ultrabreitbandfunk – erste Netzwerkkarten im Kurztest, c't 7/2006, Seite 188, März 2006

[HEI03] Supermanns Röntgenblick für Notfallretter, Heise News, Februar 2003, http://www.heise.de/newsticker/meldung/34548

[HiZa05] Guido R. Hiertz, Yunpeng Zang, Jörg Habetha, Hanza Sirin, IEEE 802.15.3a Wireless Personal Area Networks - The MBOA Approach, In Proceedings of 11th European Wireless Conference 2005, Volume 1, p.p. 204-210, April 2005

[IEEE153a] Webseite der IEEE 802.15 WPAN High Rate Alternative PHY Task Group 3a (TG3a), http://www.ieee802.org/15/pub/TG3a.html

[RFC4086] RFC 4086, Randomness Requirements for Security, IETF BEST CURRENT PRACTICE, Juni 2005, http://www.ietf.org/rfc/rfc4086.txt

[WIME09] WiMedia Alliance: WiMedia Announces New Agreements with Bluetooth SIG and Wireless USB, Pressemitteilung, März 2009

[WUAM06] USB Implementers Forum: Association Models Supplement to the Certified Wireless Universal Serial Bus Specification, Revision 1.0, März 2006, http://www.usb.org/developers/wusb/wusb_2007_0214.zip

[WUSB05] USB Implementers Forum: Wireles Universal Serial Bus Specification, Revision 1.0, Mai 2005, http://www.usb.org/developers/wusb/wusb_2007_0214.zip

[ZIBA05] Dusan Zivadinovic, Oliver Bartels, Noch mehr Funk-Techniken auf dem Sprung in die Computer-Welt, c't 2/2005, Seite 128, Februar 2005

G.8 Abkürzungen

4BOK	Quaternary Bi-Orthogonal Keying
AES	Advanced Encryption Standard
BPSK	Binary Phase Shift Keying
BSI	Bundesamt für Sicherheit in der Informationstechnik
CBC	Cipher Block Chaining
CCM	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
CEPT	Conference European Des Administrations Des Postes Et Des Telecommunications
CK	Connection Key
CMOS	Complementary Metal Oxide Semiconductor
CWUSB	Certified Wireless USB
DCM	Dual Carrier Modulation
DoS	Denial of Service
DS-UWB	Direct Sequence UWB
ECMA	European Association for standardizing Information and Communication Systems
EDR	(Bluetooth) Enhanced Data Rate
EIRP	Equivalent Isotropically Radiated Power (Strahlungsleistung bezogen auf eine isotrope Antenne)
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FCS	Frame Check Sequence
FDS	Frequency-domain spreading
FEC	Forward Error Correction
GPS	Global Positioning System
GTK	Group Temporary Key
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
IT	Information Technology
LAN	Local Area Network
LDC	Low Duty Cycle
MBOA	Multiband OFDM Alliance
MB-OFDM	Multiband Orthogonal Frequency Division Multiplex
MIC	Message Integrity Code, Prüfsumme zur Integritätsprüfung
OFDM	Orthogonal Frequency Division Multiplexing
PAN	Personal Area Network
PC	Personal Computer

PMK	Pairwise Master Key, symmetrischer geheimer Schlüssel
PTK	Pairwise Transient Key, symmetrischer temporärer Schüssel
RFC	Request for Comments
SIG	(Bluetooth) Special Interest Group
SFN	Secure Frame Number
TDS	Time-domain spreading
TFC	Time-Frequency Codes
TPC	Transmit Power Control
USB	Universal Serial Bus
UWB	Ultra Wideband
WPAN	Wireless PAN
WLAN	Wireless LAN

G.9 Glossar

Chiprate

Siehe Spreizsequenz

Code-Rate

Die Code-Rate ist ein Maß für die Redundanz, die ein FEC-Code den Nutzdaten hinzufügt und ist definiert als das Verhältnis von Informationsbits am Eingang eines Encoders zu den codierten Bits am Ausgang eines Encoders.

Faltungs-Code

Ein Faltungs-Code ist ein spezieller FEC-Code, der sich insbesondere zur Kanalkodierung für stark störanfällige Übertragungsmedien (z.B. drahtlose und mobile Kommunikationssysteme) eignet.

Forward Error Correction (FEC)

Bei der Vorwärtsfehlerkorrektur kodiert der Sender die zu übertragenden Daten in redundanter Weise, sodass der Empfänger Fehler erkennen und korrigieren kann.

Orthogonal Frequency Division Multiplex (OFDM)

OFDM ist ein Modulationsverfahren, das anstelle eines einzelnen Trägers eine große Zahl von Unterträgern gleichzeitig moduliert und parallel auf den Unterträgern (prinzipiell wie bei einer parallelen Schnittstelle an einem PC) Daten überträgt. Die erreichbaren Datenraten hängen von der Anzahl der für die Datenübertragung verfügbaren Unterträger, von den verwendeten Modulationsverfahren auf den Unterträgern und von der Code-Rate des verwendeten FEC-Code ab. Modulationsverfahren und Code-Rate werden oft dynamisch in Abhängigkeit von der Kanalqualität gewählt. OFDM wird beispielsweise auch bei WLAN verwendet.

Spreizsequenz

Bei Bandspreizverfahren wie Direct Sequence Spread Spectrum Code (DSSS) wird jedes einzelne Bit der zu übertragenden Nachricht mit einer Spreizsequenz multipliziert. Das Ergebnis ist ein Vielfaches der Spreizsequenz, das letztendlich über den Kanal übertragen wird. Hierdurch wird das Nutzdatensignal künstlich aufgeweitet, es entsteht ein gespreiztes Spektrum. Die Nutzbitrate ist damit stets kleiner als die Rate mit der das gespreizte Signal übertragen wird (Chiprate).

H. NFC

Inhaltsverzeichnis des Abschnitts

H.1 Grundlagen und Funktionalität

Near Field Communication (NFC) ist eine Technik zur drahtlosen Kopplung von Geräten. Sie stellt eine Weiterentwicklung der RFID-Technik (Radio Frequency Identification) dar, bei der Daten auf einem Transponder berührungslos gelesen und gespeichert werden können. NFC erweitert die RFID-Technik um die Möglichkeit, zwei gleichberechtigte „intelligente“ Geräte miteinander verbinden zu können, wie beispielsweise bei Bluetooth. Wesentliches Merkmal ist jedoch die Einfachheit, mit der diese Kopplung geschieht. Sobald sich zwei Geräte in gegenseitiger Reichweite befinden, bauen sie in kürzester Zeit eine Verbindung auf. Die Reichweite wurde bei NFC bewusst auf maximal 10 cm bis 20 cm begrenzt, damit der Anwender eine möglichst gute Kontrolle über die Kommunikation behält. Die geringe Reichweite vereinfacht nach Ansicht der Entwickler das Identifizieren der Kommunikationspartner; NFC wird gar eine inhärente Sicherheit zugeschrieben (siehe [NFCABT]).

Die an der Entwicklung und Vermarktung der Technik beteiligten und interessierten Unternehmen haben sich im NFC-Forum zusammengeschlossen. Dabei steht die Anwendung der Technik in sogenannten Consumer-Geräten im Vordergrund. Man verspricht sich von NFC neue Einsatzszenarien für mobile Geräte, wie beispielsweise Mobiltelefone, Digitalkameras oder PDAs. Auch an eine Verwendung von NFC als Vorstufe zu einer anschließenden Kommunikation mittels WLAN oder Bluetooth ist gedacht (siehe [NFCCON]). In diesem Fall übernimmt NFC die Übertragung von Informationen, die zur Konfiguration von Bluetooth oder WLAN benötigt werden. Diese Idee hat inzwischen Eingang in die Bluetooth-Spezifikation 2-1 + EDR gefunden, die ein Verfahren zum Verbindungsaufbau unter Zuhilfenahme von NFC beschreibt (siehe Kapitel B. Bluetooth).

H.1.1 Standards

Eine Standardisierung der OSI-Schichten 1 und 2 (d.h. physikalische Übertragung und Medienzugang) von NFC ist mit den Standards ECMA 340 und ECMA 352 erfolgt (siehe [ECMA340] und [ECMA352][1]). Darüber hinaus werden in den Standards ECMA 356 und ECMA 362 Testmethoden spezifiziert (siehe [ECMA356] und [ECMA362][2]). Spezifikationen zur Unterstützung praktischer und herstellerübergreifender Implementierungen von NFC finden sich beim NFC-Forum, einem Zusammenschluss von Herstellern, Entwicklern und Anwendern dieser Technik. Das NFC-Forum hat unter anderem die nachfolgenden Spezifikationen herausgegeben:

- Logical Link Control Protocol (LLCP): Diese zum Zeitpunkt der Herausgabe dieser Broschüre noch vorläufige Spezifikation (siehe [NFCLLC]) beschreibt ein Verfahren zum verbindungslosen und verbindungsorientierten Datenaustausch zwischen NFC-Tags.

- NFC Data Exchange Format (NDEF, siehe [NFCDEF]): Basis für jeglichen Datenaustausch zwischen NFC-Komponenten ist dieses Datenformat. Es beschreibt den grundsätzlichen Aufbau von Datenblöcken mit Längen- und Typfeldern sowie die Möglichkeit zur Verkettung mehrerer Datenblöcke.

---

1 Diese Standards wurden auch vom internationalen Standardisierungsgremium ISO als Standards ISO/IEC 18092 und ISO/IEC 21481 sowie vom europäischen Standardisierungsgremium ETSI als Standards ETSI EN 302 190 bzw. ETSI TS 102 190 und ETSI TS 102 312 übernommen.

2 Die entsprechenden ISO- und ETSI-Standards sind ISO/IEC DIS 22536 und ISO/IEC DIS 23917 sowie ETSI TS 102 346 und ETSI TS 102 394.

- NFC Record Type Definition (RTD, siehe [NFCRTD]): Hier werden Inhaltstypen und deren Benennung festgelegt. Die Definition orientiert sich an dem in RFC 2141 beschriebenen Format für Uniform Resource Names (URNs, siehe [RFC2141]), die hier in komprimierter Form angegeben werden.

- Definition verschiedener Inhaltstypen, beispielsweise Text oder Verweise auf Ressourcen (sogenannte Uniform Resource Identifier, URIs, siehe [NFCURI]).

- Spezifikation des Betriebs und Managements von vier verschiedenen *Tag*-Typen zur Verwendung in NFC-Anwendungen (siehe [NFCTAG]). Das Spektrum reicht von RFID-*Tags* mit 64 Byte Speicher bis zu *Tags* mit 64 KByte Speicher, auf denen sich mehrere Anwendungen betreiben lassen. In den Spezifikationen wird auf die Speicherverwaltung der *Tags* eingegangen sowie auf entsprechende Befehlsformate.

- NFC Connection Handover (siehe [NFCCON]): Diese Spezifikation beschreibt Datentypen und Nachrichtenformate für die Verwendung von NFC als Vorstufe für das Etablieren anderer drahtloser Datenverbindungen. Es wird insbesondere auf die Verwendung von NFC auf das *Secure Simple Pairing* bei Bluetooth 2.1 + EDR eingegangen.

H.1.2 Funktionsweise

NFC nutzt zur Kommunikation hochfrequente Magnetfelder auf der Frequenz 13,56 MHz. Die Kopplung der Geräte erfolgt induktiv über Spulen. Diese Technik kommt auch bei zahlreichen RFID-Systemen zum Einsatz.

Bei NFC werden die beiden Partner einer Kommunikation als Initiator und Target bezeichnet. Der Initiator beginnt mit der Kommunikation, das Target antwortet darauf. Dabei unterscheidet man zwischen aktivem und passivem Modus. Im aktiven Modus erzeugen Initiator und Target zum Zwecke der Datenübertragung selber jeweils ein Magnetfeld. Im passiven Modus erzeugt nur der Initiator ein Magnetfeld. In diesem Modus entnimmt das Target die für die Informationsübertragung benötigte Energie dem Magnetfeld des Initiators; es benötigt somit keine eigene Stromversorgung. Die Funktionsweise eines Target im passiven Modus gleicht der von RFID-*Tags*. In der Tat besteht Kompatibilität zu RFID-*Tags* nach dem Standard ISO 14443, Teil 1 bis 4 und seinen Ergänzungen (siehe [ISO14443]).

NFC unterstützt gemäß dem aktuellen Standard die drei Übertragungsraten 106, 212 und 424 kbit/s. Die Übertragung erfolgt je nach Kommunikationsmodus auf unterschiedliche Weise:

- Aktiver Modus: Initiator und Target erzeugen abwechselnd ein hochfrequentes Magnetfeld, das zur Datenübertragung amplitudenmoduliert wird. Die Übertragung erfolgt somit in einem Halbduplex-Verfahren. Beide Kommunikationspartner benötigen in diesem Modus eine eigene Energieversorgung.

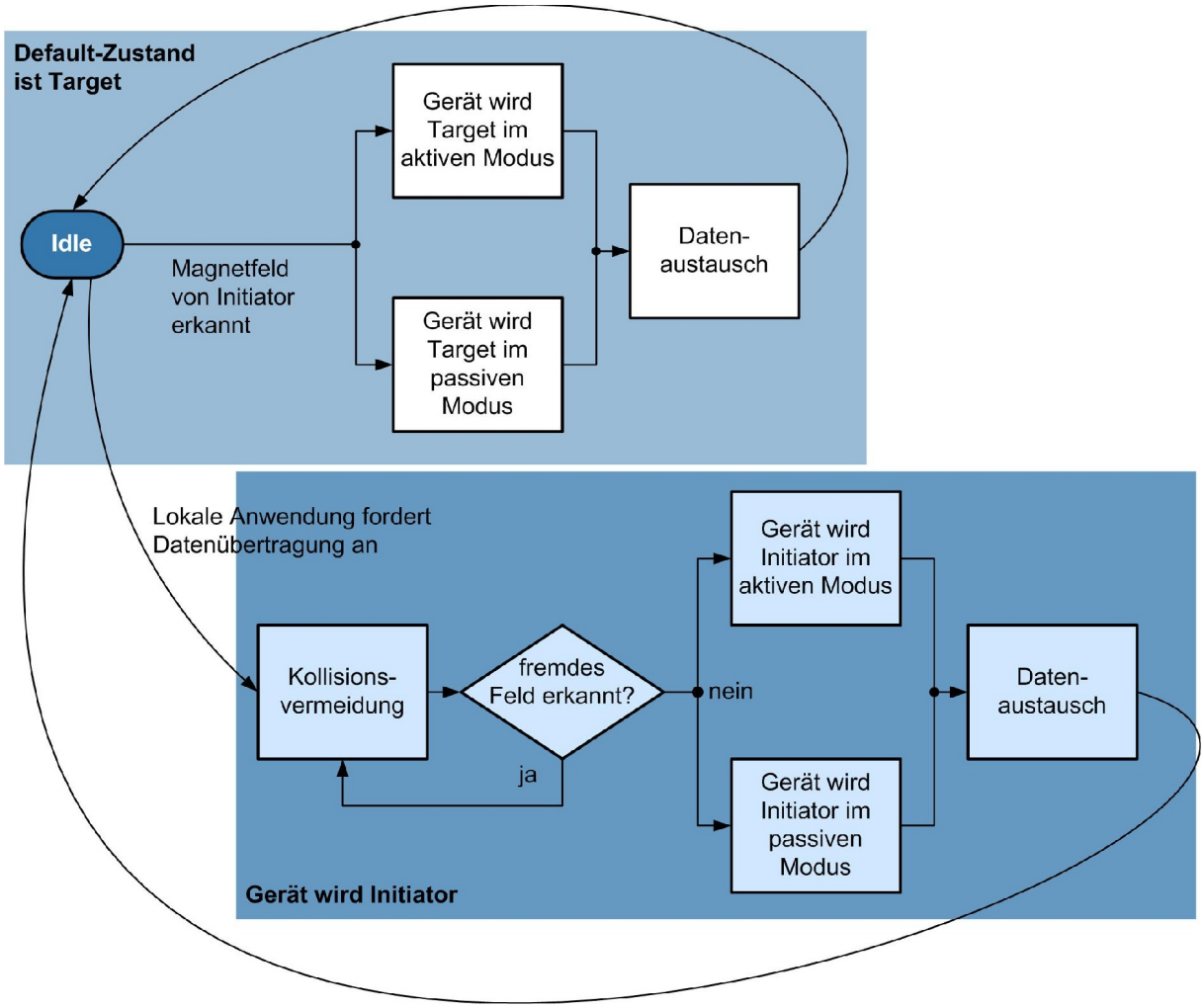
- Passiver Modus: Der Initiator erzeugt ein dauerndes hochfrequentes Magnetfeld, das er zur Datenübertragung amplitudenmoduliert. Das Target sendet seine Daten über eine sogenannte Lastmodulation, indem es dem Magnetfeld des Initiator mehr oder weniger Energie entzieht. Das Target benötigt in diesem Modus keine eigene Energieversorgung und wird stattdessen aus dem Magnetfeld des Initiator gespeist.

Das Medienzugangsverfahren regelt die Kommunikation der NFC-Geräte. Vereinfacht läuft eine Kommunikation immer nach dem folgenden Muster ab:

- Zunächst ist jedes NFC-Gerät ein Target, erzeugt kein Magnetfeld und wartet auf einen Befehl von einem Initiator.

- ► Eine Anwendung, die Daten übertragen will, macht das NFC-Gerät zum Initiator. Sie bestimmt auch, ob aktiver oder passiver Modus und welche Datenrate eingesetzt werden soll.
- ► Der Initiator ermittelt vor Beginn der Sendung, ob andere Magnetfelder existieren. Falls nein, aktiviert er sein eigenes Magnetfeld und aktiviert dadurch das Target.
- ► Die Übertragung eines Befehls durch den Initiator erfolgt entsprechend dem zuvor von der Anwendung gewählten Modus.
- ► Das Target antwortet entsprechend dem vom Initiator vorgegebenen Modus.

Abbildung H-1: Kommunikation bei NFC (vereinfacht)



H.1.3 Anwendungen

Zum Zeitpunkt der Veröffentlichung dieser Broschüre gibt es verschiedene Anwendungen von NFC, die bisher ausnahmslos in Testinstallationen betrieben werden. Wichtigstes Anwendungsfeld ist bisher das bargeldlose Bezahlen von Fahrscheinen im öffentlichen Personenverkehr (ÖPV). Verschiedene Verkehrsbetriebe haben solche Systeme für einen begrenzten Kundenkreis in Betrieb genommen. Es wird auch an einem Industrie-Standard gearbeitet, der ein aus Sicht des Fahrgastes einheitliches System für alle ÖPV-Unternehmen zum Ziel hat (siehe [VDVKA]). Voraussetzung für viele derartige An-

wendungen ist, dass die Kunden ein Mobiltelefon besitzen, das einen NFC-Chip enthält. Derzeit gibt es verschiedene Ideen für die Funktionsweise solcher Anwendungen:

- Der Fahrgast kauft einen Fahrschein für eine bestimmte Strecke vor Antritt der Fahrt an einer Web-Anwendung des Verkehrsbetriebs im Internet. Der Fahrschein wird in Form eines Datensatzes per Kurzmitteilungsdienst an das Mobiltelefon des Fahrgastes übertragen. Der Fahrgast führt das Mobiltelefon während der Reise mit sich. Dieser Fahrscheinentwertung erfolgt wie üblich durch den Kontrolleur, der ein NFC-Lesegerät an das Mobiltelefon des Fahrgastes hält und den Fahrscheindatensatz ausliest. Bei erfolgreicher Kontrolle wird der Fahrscheindatensatz im Mobiltelefon des Fahrgastes als entwertet markiert.

- Der Fahrgast braucht vor Fahrtantritt keinen Fahrschein zu erwerben. Stattdessen führt er ein Mobiltelefon mit NFC-Chip und entsprechender Anwendung mit sich. Bei Fahrtantritt berührt er mit dem Mobiltelefon einen am Bahnsteig oder im Fahrzeug montierten NFC-Chip. Daraufhin überträgt das Mobiltelefon die Information über Ort und Zeit des Fahrtantritts an einen Rechner des Verkehrsbetriebs. Bei Fahrtende geschieht dasselbe noch einmal; der Fahrgast berührt einen NFC-Chip und die Daten über das Fahrtende werden an den Verkehrsbetrieb übermittelt. Daraufhin erfolgt die Abrechnung der Fahrtkosten.

Die genannten Anwendungen erfordern neben dem NFC-Chip im Mobiltelefon auch entsprechende Software, die mit dem NFC-Chip kommuniziert. Entsprechende Entwicklungsunterstützung in Form von SDKs (Software Development Kit) wird von den Herstellern bereitgestellt. Allerdings ist damit die Software-Entwicklung mehr oder weniger an den verwendeten Gerätetyp gebunden, ein Hemmschuh für die schnelle Ausbreitung von NFC-Anwendungen. Daher gibt es inzwischen auch Entwicklungsaktivitäten zur standardisierten Abwicklung von NFC-Anwendungen über die SIM-Karten der Telefone.

Nicht zuletzt gibt es bereits erste Implementierungen des Secure Simple Pairing bei Bluetooth 2.1 + EDR mittels Out-of-Band (OOB), d.h. über NFC.

H.2 Sicherheitsmechanismen bei NFC

Weder die aktuellen Standards noch die Spezifikationen des NFC-Forum beschreiben Sicherheitsmechanismen. Im Gegenteil, der Verzicht auf Sicherheitsmechanismen und auf die damit verbundene Verwaltung entsprechender Parameter soll eine Voraussetzung sein für den unkomplizierten und schnellen Verbindungsaufbau zu jedem gewünschten Kommunikationspartner. Sicherheit entsteht nach Ansicht der Entwickler durch die sehr geringe Reichweite des Verfahrens. Darüber hinaus wird bezüglich Sicherheit auf die auf NFC zu implementierende Anwendung verwiesen. Die Spezifikation [NFCLLC] enthält z.B. den Hinweis, dass das LLCP keinen sicheren Datentransfer bietet und dies von den Protokollen der niedrigeren oder höheren Schichten bewerkstelligt werden kann.

H.3 Gefährdungen beim Einsatz von NFC

Die folgenden Gefährdungen beim Einsatz von NFC sind denkbar.

H.3.1 Fehlende Authentisierung und Verschlüsselung

Es besteht die Gefahr, dass ein Target von einem fremden Initiator angesprochen wird und Daten preisgibt. Weiterhin kann auch bei den geringen Reichweiten eines NFC-Systems nicht ausgeschlossen werden, dass ein Dritter den Dialog zwischen Initiator und Target belauscht (siehe Kapitel H.3.2). Verfahren zur Authentisierung und Verschlüsselung sind im Standard nicht vorgesehen und müssen von den Anwendungen bereitgestellt werden.

H.3.2 Unkontrollierte Ausbreitung der Funkwellen

Die von NFC-Geräten erzeugten hochfrequenten Magnetfelder lassen sich – entsprechende Empfangstechnik vorausgesetzt – in größerer Entfernung wahrnehmen, als von den Erfindern der Technik angenommen. Die erzielbare Entfernung hängt davon ab, ob ein NFC-Gerät den aktiven oder passiven Modus einsetzt (siehe [MEPLÖ07] und [HABRE06]):

- Die im aktiven Modus von beiden Partnern abwechselnd ausgesandten Signale lassen sich in mehreren Metern Entfernung wahrnehmen, möglicherweise sogar in bis zu 10 Metern Abstand.

- Im passiven Modus verwendet das Target eine Lastmodulation des vom Initiator ausgesandten Signals. Das modulierte Signal lässt sich in 10 bis 20 cm Abstand durch den Initiator wahrnehmen. Es ist aber nicht auszuschließen, dass mit entsprechender Empfangstechnik Reichweiten von 1 Meter übertroffen werden.

Die Autoren von [HABRE06] behaupten als Ergebnis einer theoretischen Betrachtung, dass NFC gegen Man-in-the-Middle-Angriffe praktisch immun sei, sofern als Übertragungsrate 106 kbit/s gewählt würde. Dagegen hat der Autor von [HAN05] ein technisches System konstruiert, über das ein RFID-*Tag* Daten mit einem 50 Meter entfernten Leser austauschen konnte. Diese als Relay-Attacke bezeichnete Angriffsart lässt sich prinzipiell auch für NFC denken. Ein Angreifer kann mit dieser Methode eine Kommunikation mit dem NFC-Chip vom Anwender unbemerkt und unerwartet initiieren. Der Angreifer erlangt mit dieser Methode auch alle zwischen Initiator und Target ausgetauschten Daten und wird in die Lage versetzt einen Man-in-the-Middle-Angriff auszuführen.

Die NFC-Technik erschwert somit zwar das Abhören, schließt es aber nicht mit genügend hoher Wahrscheinlichkeit aus. Weiterhin sollen die für NFC vorgesehenen Anwendungen gerade in Umgebungen eingesetzt werden, die sich einer Kontrolle entziehen, z.B. in öffentlichen Verkehrsmitteln. Hier gibt es für einen Angreifer durchaus Möglichkeiten, nahe genug an das Ziel heranzukommen und eine NFC-Kommunikation zu kompromittieren.

H.3.3 Denial of Service (DoS)

Die Kommunikation von NFC-Geräten lässt sich prinzipiell stören. Zum einen ist der Einsatz von Störsendern denkbar, die sich auch mit hohen Sendeleistungen auf einfache Weise beschaffen lassen. Die Antennentechnik ist jedoch mechanisch groß und kann nur schwer unauffällig installiert werden. Es können aber auch speziell programmierte NFC-Geräte als Störsender eingesetzt werden, die in unmittelbarer Nähe der zu störenden Systeme installiert werden, sofern die Umgebung dies unbemerkt zulässt.

H.3.4 Erstellen von Bewegungsprofilen

Prinzipiell lassen sich auf mobilen NFC-Geräten implementierte Anwendungen dazu ausnutzen, Bewegungsprofile ihrer Benutzer zu erstellen.

H.3.5 Schwächen in NFC-basierten Anwendungen

Weitere Gefährdungen können sich aus den auf NFC basierten Anwendungen ergeben. Als Beispiel mag das im Kapitel B. Bluetooth beschriebene Verfahren des Secure Simple Pairing mit dem Modell Out of Band dienen. Seine Sicherheit basiert maßgeblich darauf, dass der im Rahmen der Authentisierung verwendete OOB-Kanal über NFC nicht kompromittiert wird. An Anwendungen, die auf NFC basieren, sind letztlich dieselben Sicherheitsanforderungen zu stellen, die man bei anderen drahtlosen Techniken wie WLAN oder Bluetooth für selbstverständlich hält. Die geringe Reichweite der von NFC abgestrahlten Signale als alleiniges Sicherheitsmerkmal anzusehen, wird nicht als ausreichend angesehen.

H.4 Schutzmaßnahmen beim Einsatz von NFC

Konkrete Schutzmaßnahmen hängen wesentlich von den Anwendungen und Einsatzszenarien ab. Falls möglich, sollten mobile NFC-Geräte jedoch so lange vollständig deaktiviert bleiben, bis sie tatsächlich benötigt werden und sich die Einsatzumgebung vollständig kontrollieren lässt. Dies gilt insbesondere auch für den passiven Modus, bei dem ein Target im Normalfall inaktiv ist, bis es durch das Magnetfeld eines Initiator automatisch aufgeweckt wird. Dieser Aufweckvorgang muss deaktivierbar sein.

Inzwischen existieren am Markt verschiedene Abschirmbehältnisse, die RFID-Tags vor unbefugtem Auslesen schützen sollen. Eine einfache Lösung ist das Einwickeln des entsprechenden Trägers in Aluminiumfolie. Solche Abschirmmaßnahmen haben nicht in allen Fällen einwandfrei funktioniert. Es ist also davon auszugehen, dass sie auch NFC-Komponenten nicht sicher schützen werden.

Die vorgesehenen Anwendungen und damit verbundene Sicherheitsmechanismen sollten vor ihrem Einsatz mit NFC einer Risikoanalyse unterzogen werden. Bei entsprechendem Schutzbedarf ist eine Authentisierung und Verschlüsselung auf Anwendungsebene erforderlich.

H.5 Ausblick

Die Möglichkeit, fast beliebige Geräte ohne vorangehende Konfiguration miteinander kommunizieren zu lassen, wird voraussichtlich zahlreiche neue Anwendungen für mobile Kleingeräte entstehen lassen. So wird das Mobiltelefon zu einer kontaktlosen Smartcard, mit deren Hilfe man elektronische Sperren (etwa in der U-Bahn) überwindet, Eintrittsgelder bei Veranstaltungen bargeldlos entrichtet oder gar an der Supermarktkasse bezahlt. Die über die Möglichkeiten der RFID hinausgehende bidirektionale Kommunikation der NFC-Komponenten erlaubt darüber hinaus neue Anwendungen.

Trotz dieser offensichtlichen Vorteile schreitet die Entwicklung solcher Anwendungen nur langsam voran; verschiedene Konzepte mit gleicher Zielsetzung konkurrieren miteinander – es fehlen Standards auf Anwendungsebene. Dementsprechend mangelt es zum Zeitpunkt der Veröffentlichung dieser Broschüre noch an einer breiten Unterstützung durch die Gerätehersteller. Dieser Trend mag durch die in Deutschland verbreitete Skepsis gegenüber neuartigen Zahlungssystemen noch unterstützt werden.

H.6 Fazit

NFC ist eine einfach zu handhabende Funktechnik, die sich nur auf wenigen Zentimetern einsetzen lässt. Damit verbunden ist zwar ein gewisser Schutz gegen Abhören und Störung, jedoch sind Angriffe auch nicht auszuschließen. Daher ist bei entsprechendem Schutzbedarf eine Absicherung auf Anwendungsebene unumgänglich, da aktuell für die NFC-Kommunikation selbst keine Sicherheitsmechanismen vorgesehen sind. Dem Nutzer der Technik bleibt es letztlich überlassen, im Einzelfall zu prüfen, ob das so erreichte Sicherheitsniveau angemessen ist. Bei einer größeren Palette an Applikationen (von der bei NFC durchaus ausgegangen werden muss) kann ein Anwender hier schnell überfordert werden. Grundsätzlich ist es daher für drahtlose Kommunikationssysteme, und somit auch für NFC, wünschenswert, dass Sicherheitsmechanismen einen integralen Bestandteil der drahtlosen Übertragungsdienste darstellen und zumindest optional aktiviert werden können. Auf diese Weise können Entwickler von NFC-Anwendungen einheitlich auf sichere Kommunikationsmittel zurückgreifen.

H.7 Literatur und Links

Diese Liste stellt nur eine wertungsfreie Auswahl ohne Anspruch auf Vollständigkeit dar.

[ECMA340] ECMA International, Standard ECMA-340, „Near Field Communication Interface and Protocol (NFCIP-1) 2nd edition“, Dezember 2004, verfügbar unter http://www.ecma-international.org/publications/standards/Standard.htm

[ECMA352] ECMA International, Standard ECMA-352, „Near Field Communication Interface and Protocol-2 (NFCIP-2)“, Dezember 2003, verfügbar unter http://www.ecma-international.org/publications/standards/Standard.htm

[ECMA356] ECMA International, Standard ECMA-356, „NFCIP-1 - RF Interface Test Methods“, Juni 2004, verfügbar unter http://www.ecma-international.org/publications/standards/Standard.htm

[ECMA362] ECMA International, Standard ECMA-362, „NFCIP-1 - Protocol Test Methods 2nd edition“, Dezember 2005, verfügbar unter http://www.ecma-international.org/publications/standards/Standard.htm

[HABRE06] Ernst Haselsteiner and Klemens Breitfuß:, „Security in Near Field Communication (NFC)“, Beitrag zur Konferenz RFID Security 2006 der TU Graz, Juli 2006, verfügbar unter http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf

[HAN05] Gerhard Hancke: „A Practical Relay Attack on ISO 14443 Proximity Cards“, University of Cambridge, Computer Laboratory, 2005

[ISO14443] International Organization for Standardization, Standard ISO/IEC 14443 Teile 1 bis 4,
„Part 1: Physical characteristics“, Oktober 2003,
„Part 2: Radio frequency power and signal interface“, März 2006,
„Part 3: Initialization and anticollision“, März 2006,
„Part 4: Transmission protocol“, März 2006

[MEPLÖ07] Milosch Meriac und Henryk Plötz: „Practical RFID Attacks“, Beitrag zum Chaos Communication Camp 2007, August 2007, verfügbar unter http://www.openpcd.org/dl/cccamp2007-practical_rfid.pdf

[NFCDEF] NFC Forum: NFC Data Exchange Format (NDEF), Technical Specification, Juli 2006, verfügbar unter http://www.nfc-forum.org/

[NFCABT] “About Near Field Communication”, Webseite des NFC Forum, http://www.nfc-forum.org/aboutnfc

[NFCCON] NFC Forum: Connection Handover, Technical Specification, November 2008, verfügbar unter http://www.nfc-forum.org/

[NFCLLC] NFC Forum: Logical Link Control Protocol, Candidate Technical Specification, März 2009, verfügbar unter http://www.nfc-forum.org/

[NFCRTD] NFC Forum: NFC Record Type Definition, Technical Specification, Juli 2006, verfügbar unter http://www.nfc-forum.org/

[NFCTAG] NFC Forum:
Type 1 Tag Operation, Technical Specification, Juli 2007,
Type 2 Tag Operation, Technical Specification, Juli 2007,
Type 3 Tag Operation, Technical Specification, August 2007,
Type 4 Tag Operation, Technical Specification, März 2007,
verfügbar unter http://www.nfc-forum.org/

[NFCURI] NFC Forum: URI Record Type Definition, Technical Specification, Juli 2006, verfügbar unter http://www.nfc-forum.org/

[RFC2141] RFC 2141, URN Syntax, IETF Proposed Standard, Mai 1997, http://www.ietf.org/rfc/rfc2141.txt

[VDVKA] Liste der Spezifikationen der VDV-Kernapplikation und diverser Zusatzdokumente, VDV-Kernapplikations GmbH & Co. KG, Juni 2008, verfügbar unter http://www.vdv-ka.org/01/load/liste_0701.pdf

H.8 Abkürzungen

ECMA	European Computer Manufacturers Association
ETSI	European Telecommunications Standards Institute
DoS	Denial of Service
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
LLCP	Logical Link Control Protocol
NDEF	NFC Data Exchange Format
NFC	Near Field Communication
ÖPV	Öffentlichen Personenverkehr
OOB	Out of Band
OSI	Open Systems Interconnection
PDA	Personal Digital Assistant
PIN	Persönliche Identifikationsnummer
RFID	Radio Frequency Identification
RTD	(NFC) Record Type Definition
SDK	Software Development Kit
SIM	Subscriber Identity Module
URI	Uniform Resource Identifier
URN	Uniform Resource Name
WLAN	Wireless Local Area Network

H.9 Glossar

Authentisierung

Verifizierung der Identität einer Instanz, z.B. eines Benutzers oder eines Geräts. Zweck ist oft die anschließende Autorisierung für Zugriffe. Ohne Authentisierung ist im Allgemeinen keine sinnvolle Autorisierung möglich.

Denial of Service (DoS)

Ein Angriff vom Typ Denial of Service hat zum Ziel die Arbeitsfähigkeit des angegriffenen Objekts möglichst stark zu reduzieren. Dies beinhaltet beispielsweise die systematische Überlastung eines Netzknotens durch unsinnigen Verkehr (Dummy Traffic) oder die beabsichtigte Herbeiführung eines Fehlerzustands durch das Einspielen fehlerhafter Nachrichten.

Radio Frequency Identification (RFID)

Methode, um Daten auf einem Transponder berührungslos und ohne Sichtkontakt lesen und speichern zu können. Dieser Transponder kann an Objekten angebracht werden, welche dann anhand der darauf gespeicherten Daten automatisch und schnell identifiziert und lokalisiert werden können.

Smartcard

Plastikkarte mit integriertem Schaltkreis, der in der Lage ist, Daten zu verwalten und über eine Schnittstelle mit einem Lesegerät zu kommunizieren.

Tag

Siehe Transponder

Transponder

Der Transponder – auch als Tag bezeichnet – fungiert als eigentlicher Datenträger. Er kann kontaktlos über Funktechnologie ausgelesen und je nach Technologie auch wieder beschrieben werden. Grundsätzlich setzt sich der Transponder aus einer integrierten Schaltung und einer Sende-/Empfangseinheit zusammen. Auf dem Transponder sind eine Identifikationsnummer und weitere Daten über den Transponder selbst bzw. das Objekt, mit dem dieser verbunden ist, gespeichert.

I. Neuere Entwicklungen

Inhaltsverzeichnis des Abschnitts

Vorbemerkungen

Der Einzug drahtloser Technik wird in den kommenden Jahren weiter zunehmen. Gleichermaßen steigt auch die Anzahl der Standards im Zusammenhang mit einer drahtlosen Übertragung. Im Folgenden wird eine Auswahl von neueren IEEE-Standards näher beleuchtet, namentlich:

- IEEE 802.20 (siehe Kapitel I.1) spezifiziert die Bereitstellung mobiler drahtloser Breitbandzugänge auch für höhere Mobilitätsklassen – nicht nur für die Nutzung durch Fußgänger, sondern z.B. auch für die Nutzung im Auto oder im Zug.

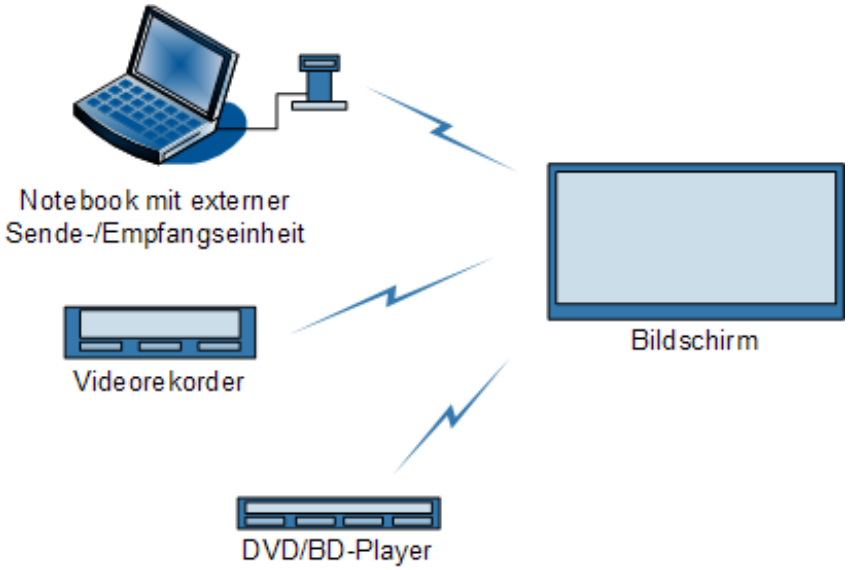
- IEEE 802.21 (siehe Kapitel I.2) standardisiert den Wechsel zwischen unterschiedlichen Netzwerk-Medienzugängen ohne Verlust der Sitzungen auf Nutzerebene. Dies würde beispielsweise einen Wechsel zwischen WLAN, WiMAX und Mobilfunk ermöglichen.

- IEEE 802.22 (siehe Kapitel I.3) ist für die breitbandige Versorgung von Regionen auf Basis des UHF/VHF-Bereiches vorgesehen. Hiermit könnten unter anderem ländliche und dünn besiedelte Regionen mit einem Breitbandzugang versorgt werden. Das Ziel ist damit vergleichbar mit dem von WiMAX, soll jedoch höhere Reichweiten ermöglichen.

Neben den genannten Funktechniken, welche primär eine Stadt oder eine einzelne Region abdecken sowie ggf. eine Mobilität innerhalb dieser Bereiche ermöglichen sollen, geht die Entwicklung insbesondere im Heimbereich vermehrt in Richtung drahtloser Techniken.

Während DECT und WLAN bereits als etablierte Techniken gelten, zählen drahtlose Systeme in der Unterhaltungselektronik, z.B. zur Anbindung von Audio- oder Videosystemen noch zu den neueren Entwicklungen. Das Ziel dieser Systeme ist es, hochauflösende Audio- und Videoübertragungen drahtlos zu gestalten. Die Architektur besteht hierbei aus den Audio-/Video-Quellen (AV-Quellen) wie beispielsweise DVD- oder Blue-ray-Playern (BD-Player), Videorekordern, PCs/Notebooks oder Spielkonsolen (siehe Abbildung I-1) und den AV-Zielen. Diese Zielsysteme sind Bildschirme (z.B. LCD- oder Plasma-Bildschirme) oder Videoprojektoren (Beamer). Sofern die Komponenten die Chipsätze für die drahtlose Übertragung nicht bereits integriert haben, können z.T. externe Sende-/Empfangseinheiten für die Übertragung genutzt werden. Diese sind dann weiterhin mit dem jeweiligen AV-System verkabelt (Quelle und/oder Ziel), wobei die Übertragung zwischen den Einheiten drahtlos erfolgt. Die Verkabelung erfolgt in der Regel per HDMI (High Definition Multimedia Interface), einer digitalen Schnittstelle für die Übertragung von Audio- und Video-Daten.

Abbildung I-1: Wireless-HDMI-Szenario



In diesem Bereich zeigen sich bereits mehr oder weniger verbreitete Ansätze zur Realisierung, welche im Folgenden kurz erläutert werden. Die relevanten Standards hierbei sind:

- Wireless HDMI
- WirelessHD
- WHDI (Wireless Home Digital Interface)
- WiGig

Wireless HDMI ist kein offizieller Standard, sondern bezeichnet ganz allgemein die drahtlose Übertragung von Audio- und Video-Daten zwischen HDMI-kompatiblen Systemen. Neben proprietären Übertragungsprotokollen sind auch IEEE 802.11a/b/g/n (Kapitel A. Funk-LAN (WLAN, IEEE 802.11)) oder UWB (Kapitel G. UWB) für die Übertragung geeignet. Da diese Systeme jedoch nicht die erforderliche Bandbreite für eine unkomprimierte Übertragung von hochauflösenden Video-Daten (HD Video, High Definition Video) bieten, muss hierbei eine Komprimierung (z.B. JPEG2000) eingesetzt werden, welche in der Regel mit einem Qualitätsverlust verbunden ist.

Im Gegensatz zu IEEE-802.11- oder UWB-basierten Systemen ermöglichen die Standards WHDI und WirelessHD eine unkomprimierte Übertragung von Audio-/Video-Daten (AV-Daten). Die WHDI-Spezifikation ist das Ergebnis der WHDI-Interessengruppe (WHDI Special Interest Group, SIG), die Mitte 2008 von einer Hersteller-Gruppe gegründet wurde. Ziel der Spezifikation ist die drahtlose Übertragung von HD Video, Audio und Kontrollsignalen. WHDI ermöglicht laut Herstellerkonsortium eine Videoübertragung mit einer Datenrate von bis zu 3 Gbit/s. Mit dieser Datenrate ist eine Übertragung von HD Video mit einer Auflösung von 1920 x 1080 im Vollbildverfahren (abgekürzt: 1080p) möglich, wobei eine Reichweite von ca. 30 m erzielt werden soll. Betrieben wird WHDI im 5-GHz-Band mit einer Kanalbreite von bis zu 40 MHz. Mittels Spektrum-Management-Funktionen soll ein gleichzeitiger Betrieb von WHDI und z.B. IEEE 802.11a oder IEEE 802.11n ermöglicht werden. Die WHDI-Spezifikation ist nur den Mitgliedern zugänglich, sodass keine Bewertung bezüglich der Sicherheit getroffen werden kann.

Eine weitere Spezifikation für die drahtlose Übertragung von HD Video, Audio und Kontrollsignalen ist WirelessHD. WirelessHD ist – wie WHDI auch – eine Spezifikation eines Herstellerkonsortiums. Im Unterschied zu WHDI operiert WirelessHD im 60-GHz-Band und ermöglicht in der ersten Spezifikation eine Datenrate von bis zu 4 Gbit/s. Theoretisch erlaubt die Technik laut Herstellerkonsortium eine maximale Datenrate von 25 Gbit/s. Ermöglicht wird dies durch den größtenteils ungenutzten 60-

GHz-Bereich, der in manchen Ländern die Nutzung von Kanalbreiten von bis zu 7 GHz erlaubt. In Deutschland steht beispielsweise der Bereich von 59 GHz bis 63 GHz zur Verfügung. Diese Datenrate erlaubt ebenfalls eine unkomprimierte Übertragung der AV-Daten, wobei die Reichweite nicht vergleichbar ist mit der im 5-GHz-Band. Für WirelessHD ist die Reichweite mit ca. 10 m angegeben. Dynamic Beam Forming, also die Wahl des jeweils optimalen Signalpfades, soll die Qualität der Übertragung verbessern. Weitere Details können der öffentlich einsehbaren Übersicht der Spezifikation in Version 1.0 entnommen werden.

Die Sicherheitsmechanismen bei WirelessHD sehen unter anderem eine gegenseitige Authentisierung der Systeme auf Basis eines Public-Key-Verfahrens vor, welches auch für den sicheren Schlüsselaustausch genutzt wird. Hinzu kommt eine Verschlüsselung und Integritätsprüfung der Daten sowie ein Schutz vor Replay-Angriffen. Einzelheiten hierzu sind in der nur für Mitglieder zugänglichen vollständigen Spezifikation enthalten.

Ein weiterer Konkurrent für die drahtlose Übertragung von unkomprimiertem HD Video ist neben WHDI und WirelessHD die WiGig Alliance (Wireless Gigabit Alliance). Die WiGig Alliance wurde im Mai 2009 gegründet. Eine erste Spezifikation des WiGig-Standards soll Ende 2009 den Mitgliedern der WiGig Alliance zur Verfügung stehen, sodass Produkte frühestens 2010 erhältlich sein werden. Technische Details sind bis auf die Nutzung des 60-GHz-Bandes noch nicht verfügbar, dürften jedoch mit denen von WirelessHD vergleichbar sein.

Die genannten Techniken zur drahtlosen Übertragung von AV-Daten befinden sich zur Zeit noch in einer Entwicklungsphase. Zum Teil sind die Standards noch nicht fertiggestellt oder Produkte noch nicht erhältlich, sodass eine erste Bewertung der Sicherheitsmechanismen unmöglich ist. Neben der geringen oder nicht vorhandenen Praxiserfahrung fehlt es weiterhin an wissenschaftlichen Untersuchungen hinsichtlich der IT-Sicherheit solcher Systeme. Im Zweifelsfall sollte auf deren Verwendung verzichtet und eine kabelbasierte Anbindung bevorzugt werden.

I.1 IEEE 802.20 – Mobile Broadband Wireless Access (MBWA)

Die IEEE-802.20-Arbeitsgruppe konzentriert sich auf die Definition einer standardisierten Luftschnittstelle, die für die Nutzung eines Breitbandangebots bei hoher Mobilität und als Basis für die Nutzung von IP-Netzwerken optimiert ist. Sowohl Mobile WiMAX als auch IEEE 802.16m stehen damit prinzipiell in Konkurrenz zu IEEE 802.20.

Seit August 2008 ist der Standard offiziell verabschiedet (siehe [IEEE08-20]).

I.1.1 Grundlagen / Funktionalität gemäß IEEE 802.20

Das Ziel von IEEE 802.20 liegt in der Bereitstellung mobiler drahtloser Breitbandzugänge nicht nur für Fußgänger (Fortbewegung mit ca. 3 km/h), sondern auch für höhere Mobilitätsklassen, wobei Geschwindigkeiten bis zu 250 km/h unterstützt werden sollen. Damit zielt der Standard insbesondere auf die Netzwerknutzung aus Fahrzeugen. Breitbandzugänge für mobile drahtlose Teilnehmer (Mobile Broadband Wireless Access, MBWA) sollen unter allen Bedingungen eine ununterbrochene Konnektivität erlauben, wie man es von kabelbasierten Systemen gewohnt ist.

Im Folgenden werden die Grundlagen und Funktionen von IEEE 802.20 näher beschrieben.

I.1.1.1 Technische Grundlagen

Die IEEE-802.20-Spezifikation beschreibt die grundlegenden technischen Merkmale eines MBWA-Systems, über das drahtlose Dienste für sich mit hoher Geschwindigkeit bewegende Teilnehmer zur Verfügung gestellt werden können.

MBWA ist für IP-basierte[1] Kommunikation optimiert und daher paketorientiert. Über entsprechende Quality-of-Service-Mechanismen (QoS) können auch Echtzeitdienste und IP-basierte Telefonie (Voice over IP, VoIP) unterstützt werden[2]. Mit MBWA-Lösungen auf Basis von IEEE 802.20 soll weltweite Mobilität geboten werden, z.B. unter Nutzung von speziellen Lösungen wie Mobile IP (MIP). Mobile IP ermöglicht einem Teilnehmer, unter seiner ursprünglichen IP-Adresse erreichbar zu bleiben, obwohl er sich vorübergehend in einer fremden IP-Umgebung (Gastnetz) aufhält.

Das Grundmodell von IEEE 802.20 unterscheidet zwischen den folgenden Komponenten (siehe Abbildung I-2):

- Access Terminal (AT)

  Eine Komponente, welche dem Nutzer eine Verbindung zum MBWA Access Network erlaubt. Dieses kann entweder mit bestehenden Systemen verbunden werden, z.B. einem Notebook, oder bereits in Komponenten integriert sein, z.B. in einem PDA.

- Access Nodes (AN)

  Komponenten, die den Access Terminals eine Verbindung mit einem IP-Netzwerk ermöglichen. Speziell im 625k-MC-Modus wird hier auch der Begriff Base Station (BS) anstatt Access Node verwendet.

---

1 wahlweise über IPv4 oder IPv6

2 Es besteht die Möglichkeit, für IP-Netze spezifizierte QoS-Steuerungsmechanismen wie Differentiated Services (DiffServ) und Resource Reservation Protocol (RSVP) geeignet abzubilden.

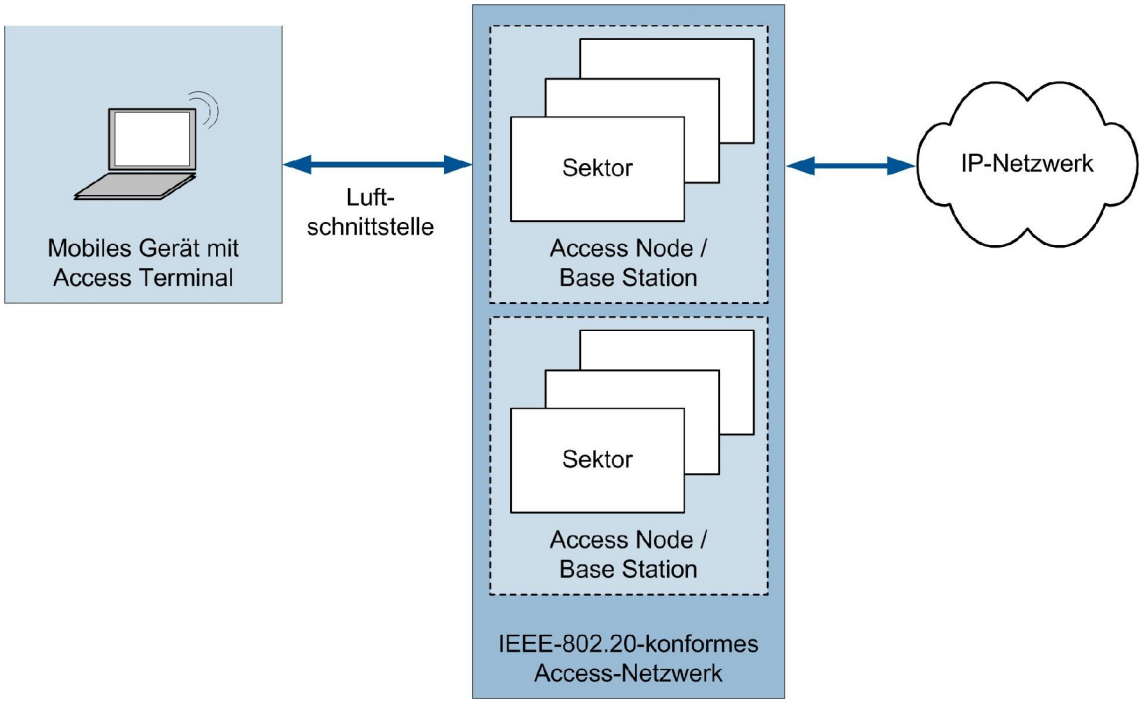
- Access Network

  Das Access Network ist eine Gruppierung von Access Nodes (AN).

- Sektoren

  Physikalische Kanäle zur Kommunikation zwischen AT und AN. Prinzipiell kann eine Basisstation mehrere Kanäle bereitstellen.

Abbildung I-2: IEEE 802.20 – Referenzmodell Netzwerkarchitektur



Implementierungen gemäß IEEE 802.20 arbeiten auf lizenzierten Frequenzen unterhalb 3,5 GHz. Derzeit gibt es zwei Varianten zur Implementierung von MBWA: ein Breitbandverfahren (Wideband Mode) und eine schmalbandige Variante mit Raummultiplexverfahren (625k-MC Mode).

I.1.1.1.1 Wideband Mode

Zur Datenübertragung wird ein breitbandiges Verfahren mit 5, 10 oder 20 MHz Bandbreite verwendet. Die Übertragung wird mittels OFDM (Orthogonal Frequency Division Multiplex) auf sogenannten Unterkanälen durchgeführt, die einen Abstand von je 9,6 kHz aufweisen. Dementsprechend stehen für die Übertragung 512, 1024 oder 2048 Unterkanäle zur Verfügung. Die Symbolrate entspricht genau dem Kanalabstand von 9,6 kHz. Bestimmte Steuerinformationen werden nicht mit dem beschriebenen OFDM-Verfahren versandt, sondern über ein Code-Multiplexverfahren (Code Division Multiple Access, CDMA). Man will damit das Handover zwischen verschiedenen Sektoren vereinfachen, da das AT mittels CDMA gleichzeitig verschiedene Aussendungen auf derselben Frequenz unterscheiden und aufnehmen kann.

Die Modulation erfolgt je nach Qualität des Übertragungsweges mit 2- bis 64-wertigen Verfahren, entsprechend 1 bis 6 Bits pro Symbol. Zur Verbesserung der Robustheit gegen Bitfehler ist die Verwendung eines Faltungs-Code mit Code-Raten 1/3 und 1/5 (Forward Error Correction, FEC) vorgesehen. Dabei wird die Gesamtzahl der versendeten Bits derart vergrößert, dass eine Redundanz entsteht.

Das Medienzugangsverfahren erfolgt entweder zeitschlitzgesteuert (Time Division Duplex, TDD) oder auf Basis eines Frequenzmultiplex-Ansatzes (Frequency Division Duplex, FDD). Beide Verfahren tei-

len ihre Aussendung in kurze „Rahmen“ mit vorgegebener Länge (8 Symbole) auf und ermöglichen so eine Übertragung mit vorhersagbarer Dauer.

AN und AT können jeweils mehrere Antennen einsetzen und ein MIMO-Verfahren (Multiple Input – Multiple Output) anwenden. Dabei wird pro Antenne ein OFDM-Datenstrom auf derselben Frequenz ausgesandt. Da die Signale im Allgemeinen auf mehreren Wegen zum Empfänger gelangen (Mehrwege-Empfang) mischen sich die Symbole zeitversetzt und können, sofern sie auf Seiten des Empfängers ebenfalls von mehreren Antennen empfangen werden, mit Hilfe digitaler Signalverarbeitung wieder getrennt werden. MIMO erlaubt somit eine Vervielfachung der Übertragungsbandbreite ohne zusätzlichen Frequenzverbrauch.

Anhand von Simulationen hat man die im Wideband Mode möglichen Datenraten zu ca. 65 Mbit/s in Richtung des AT und zu ca. 16 Mbit/s in Richtung der Basisstation ermittelt.

I.1.1.1.2 625k-MC-Modus

Der 625k-MC-Modus (625-kHz-spaced MultiCarrier) ist eine Erweiterung der Spezifikation ATIS-0700004.2005 (siehe [ATIS05]). Hier wird ein mit 625 kHz vergleichsweise schmalbandiges Signal eingesetzt, das sich besonders gut für eine gerichtete Übertragung mittels intelligenter Antennengruppen eignet. Durch die Verwendung solcher Richtantennen wird jeder Station ein separater Übertragungsweg bereitgestellt, der sich von den Übertragungswegen zu anderen Stationen lediglich durch die Abstrahlrichtung unterscheidet. Durch dieses sogenannte Raummultiplexverfahren (Space Division Multiple Access, SDMA) wird eine hohe Ausnutzung der zur Verfügung stehenden Frequenzen erreicht. Auf derselben Sendefrequenz können mittels SDMA gleichzeitig mehrere Stationen bedient werden. Das Verfahren ist unter [ATIS05] (hier High Capacity SDMA, HC-SDMA genannt) näher beschrieben.

Im 625k-MC-Modus wird pro Kanal eine Unterteilung in drei Zeitschlitze vorgenommen. Pro Zeitschlitz lässt sich eine Datenrate von 500 kbit/s in Richtung des AT und von 190 kbit/s in Richtung der Basisstation erzielen. Es ist eine Parallelschaltung mehrerer Kanäle vorgesehen, so erreicht man beispielsweise mit 4 Kanälen Downlink-Datenraten von bis zu 2 Mbit/s pro Slot. Die benötigte Bandbreite beträgt dann 2 MHz.

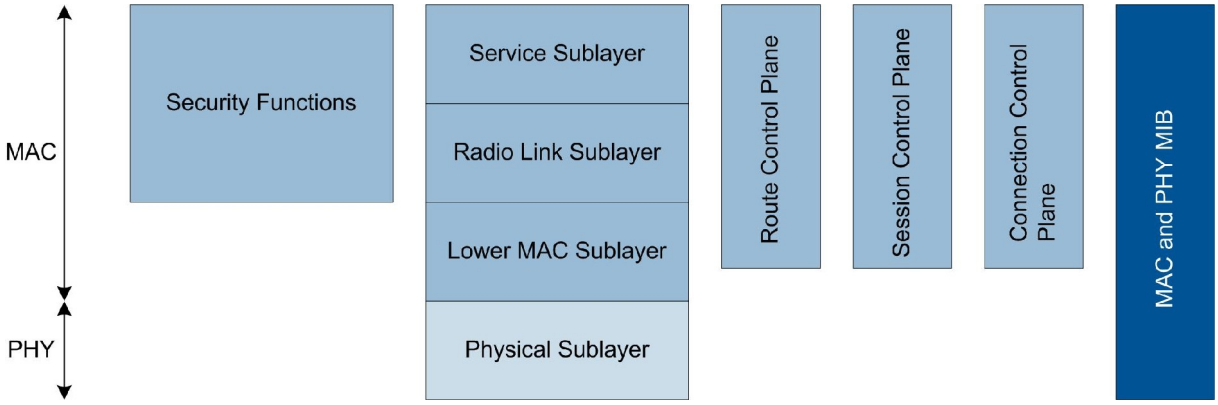
I.1.1.2 Protokollarchitektur

Die MBWA-Architektur gemäß IEEE 802.20 ist hinsichtlich der Protokollarchitektur bewusst mehrschichtig angelegt, obwohl sie sich auf die Layer 1 und 2 beschränkt (siehe Abbildung I-3). Innerhalb jeder Schicht wiederum werden entsprechende Protokolle und Schnittstellen definiert, sodass zukünftige Erweiterungen ohne Änderungen der grundsätzlichen Architektur erfolgen können. Die IEEE-802.20-Dokumente spezifizieren im Einzelnen:

- Security Functions: Hier werden Sicherheitsfunktionen wie Schlüsselaustausch, Verschlüsselung oder Authentisierung von Nachrichten spezifiziert.
- Physical Layer: Hier werden unter anderem die Kanalstruktur, Frequenzen und Modulationsverfahren definiert.
- Lower MAC Sublayer: Hier werden Mechanismen spezifiziert, um Daten über den Physical Layer zu senden bzw. zu empfangen.
- Radio Link Sublayer: Die Protokolle innerhalb des Radio Link Sublayer sind unter anderem für den zuverlässigen Transport, das Multiplexing oder die Aushandlung von QoS-Parametern im Zusammenhang mit dem Transport von Nutzerdaten zuständig.

- Service Sublayer: Hier werden verschiedene Anwendungen bzw. Protokolle bereitgestellt, u.a. für den Transport von Signalisierungsnachrichten, eine Authentisierung mittels EAP (Extensible Authentication Protocol, siehe [RFC3748]) oder die Kompression von Paket-Headern unter Verwendung des RoHC-Protokolls (Robust Header Compression).
- Route Control Plane: Innerhalb der Route Control Plane werden Routen verwaltet.
- Session Control Plane: Protokollaushandlungen und Protokollkonfigurationen werden im Rahmen der Session Control Plane bearbeitet.
- Connection Control Plane: Verbindungsaufbau und Aufrechterhaltung werden innerhalb der Connection Control Plane verwaltet.
- MAC und PHY MIB: Die MIBs stellen Statistiken für den Unicast-Betrieb, z.B. Zugriffsversuche, Anzahl der übertragenen Bytes oder abgewiesene Verbindungen, bereit.

Abbildung I-3: In IEEE 802.20 spezifizierte Schichten für den Unicast-Betrieb



Jeder (Sub-)Layer kann ein oder mehrere Protokolle bzw. Transportmechanismen mit zugehörigen Nachrichten-Formaten und Paket-Headern umfassen.

I.1.2 Sicherheitsmechanismen von IEEE 802.20

In den beiden folgenden Kapiteln werden die Sicherheitsmechanismen von IEEE 802.20, temporäre Adressierung (Kapitel I.1.2.1) und kryptographische Mechanismen (Kapitel I.1.2.2), beschrieben. Der überwiegende Teil der Sicherheitsfunktionen basiert dabei auf Spezifikationen des 3GPP2[3], die zum Teil ergänzt bzw. angepasst wurden (siehe [3GPP2-01] und [3GPP2-02]).

I.1.2.1 Temporäre Adressierung

Ein mit einem Access Network über die IEEE-802.20-Luftschnittstelle verbundenes Gerät besitzt drei Adressen auf Layer 2:

- Universal Access Terminal Identifier (UATI): Ein UATI ist eine temporäre 128-Bit-Adresse, die dem AT vom AN (durch den Session Control Sublayer) zugeordnet wird. Hierüber wird das AT gezielt angesprochen (Unicast-Adresse). Die UATI wird ausdrücklich nicht aus einer Hardware-

[3] Das Third Generation Partnership Project 2 (3GPP2) ist aus einer Initiative der International Telecommunication Union (ITU) hervorgegangen und konzentriert sich auf die Standardisierung und Weiterentwicklung von mobilen Kommunikationssystemen, die spezifisch für den amerikanischen und asiatischen Raum sind.

Adresse abgeleitet. Die UATI dient der systemweiten Identifikation eines Geräts , d.h. gilt sektorenübergreifend und ist netzwerkweit eindeutig.

- MAC ID: Über die 11 Bit lange MAC ID wird ein AT innerhalb eines einzelnen Sektors eindeutig identifiziert und angesprochen. Ein mobiles Gerät erhält somit eine MAC ID je Sektor, in dem es aktiv ist. Eine MAC ID ist nur innerhalb eines Sektors eindeutig. Auch die MAC ID wird unabhängig von der Geräte-Hardware erzeugt.

- Hardware-Adresse gemäß IEEE EUI[4]-48 oder IEEE EUI-64: Diese wird dem AT vom Hersteller im Zuge des Fertigungsvorgangs mitgegeben. Die Hardware-Adresse kann zur Verwaltung von Geräteinformationen durch das Netzwerk mit einem speziellen Befehl ausgelesen werden, dies aber nur über einen verschlüsselten Kanal nach Etablierung der vollen verfügbaren Systemsicherheit.

Die Kommunikation mit einem AT erfolgt somit ausschließlich über temporäre Adressen. Bezüglich der potenziellen Erstellung von Bewegungsprofilen ist dies als ein Sicherheitsmechanismus zu werten.

I.1.2.2 Kryptographische Sicherheitsmechanismen

Als funkbasiertes Verfahren ist IEEE 802.20 der Möglichkeit ausgesetzt, dass unbefugte Dritte unter Verwendung entsprechender Technik die MBWA-Kommunikation mithören bzw. den Versuch unternehmen, sich aktiv in Kommunikationsverbindungen einzuschalten.

Die IEEE-802.20-Spezifikation sieht zur Behandlung dieser Bedrohung innerhalb der Schicht Security Functions vor, die Datenübertragung zu verschlüsseln sowie die Integrität der Übertragungsinhalte zu sichern.

Die vorgesehenen Elemente der Schicht Security Functions sind (siehe Abbildung I-4):

- Key Exchange Protocol: Grundlegendes Protokoll für den Schlüsselaustausch

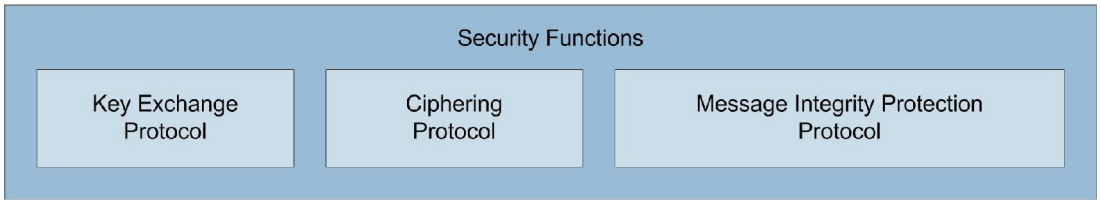
  Hierzu zählen beispielsweise Schlüssel für die Integrationsprüfung und Verschlüsselung der Daten. Diese werden aus einem sogenannten Temporary Security Key (TSKey) abgeleitet. Grundlage für die Erzeugung des TSKey ist ein symmetrischer geheimer Schlüssel (Pairwise Master Key, PMK). Die IEEE-802.20-Spezifikation setzt die Existenz eines solchen PMK bei AT und Access Network voraus. Die Aushandlung des PMK erfolgt beispielsweise mittels EAP.

  Zu den weiteren Funktionen dieses Elements gehören ein Abgleich, ob beide Systeme den gleichen PMK besitzen, sowie ein Schutz gegen Man-in-the-Middle-Angriffe.

- Ciphering Protocol: Verschlüsselung von Paketinhalten auf Basis des Advanced Encryption Standard (AES)

- Message Integrity Protection Protocol: Integritätssicherung für Pakete basierend auf AES-CMAC (Advanced Encryption Standard – Cipher-based Message Authentication Code, siehe [RFC4493])

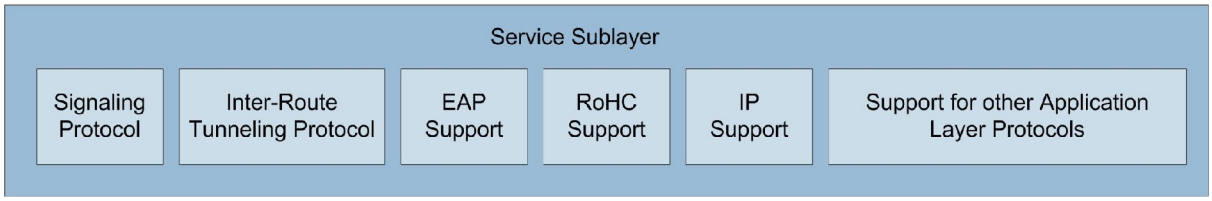
Abbildung I-4: Protokolle innerhalb der Schicht Security Functions



4 EUI = Extended Unique Identifier

Für den Schlüsselaustausch wird auf höhere Protokollschichten verwiesen, wie z.B. EAP im Rahmen des Service Sublayer (siehe Abbildung I-5).

Abbildung I-5: Protokolle innerhalb des Service Sublayer



I.1.3 Gefährdungen bei der Nutzung von IEEE-802.20-Geräten

Zu all den Gefährdungen, denen kabelbasierte Netzwerke ausgesetzt sind (siehe [GSK]), ergeben sich bei der Nutzung von Funknetz-Technik zusätzliche Gefährdungen, die insbesondere auf eventuellen Sicherheitsschwächen der verwendeten Protokolle sowie auf der unkontrollierten Ausbreitung der Funkwellen basieren. Im Folgenden werden Überlegungen zur Gefährdungslage im Vorgriff auf die noch kommende Technik diskutiert.

I.1.3.1 Schwächen im Sicherheitskonzept

Bei den nachfolgenden Betrachtungen handelt es sich zurzeit noch um theoretische Gefährdungen, da entsprechende Produkte fehlen. Inwieweit der Gedanke der Benutzerfreundlichkeit bzw. Minimierung des Herstellungsaufwands und resultierenden Preises womöglich zu unsicheren Produktlösungen führen wird, bleibt abzuwarten.

- Unsichere Voreinstellungen sind nicht grundsätzlich ausgeschlossen.

  Ähnlich wie bei anderen Lösungen zur drahtlosen Kommunikation muss auch im Falle von zukünftigen IEEE-802.20-Implementierungen damit gerechnet werden, dass ab Werk nicht alle im Standard vorgesehenen Sicherheitsmechanismen implementiert und aktiviert sind.

- Unsichere Lösungen der Verwaltung des PMK sind nicht ausgeschlossen.

  Die konkret gewählte Methode zur Aushandlung des PMK wird höheren Protokollschichten zugeordnet und offen gelassen. Die entsprechende Formulierung im Standard kann von Herstellern auch so ausgelegt werden, dass an Stelle automatisierter, abgesicherter Schlüsselverwaltung und -verteilung eine Schlüsseleingabe von Hand, etwa durch den Nutzer eines mobilen Geräts vorgesehen wird, was bekanntlich zu typischen Benutzerfehlern (schwache Schlüssel) führen kann.

I.1.3.2 Unkontrollierte Ausbreitung der Funkwellen

Die Funkwellen der MBWA-Komponenten breiten sich auch über räumliche Grenzen ihres Nutzungsbereichs aus. Dabei kann auch in nicht vom Betreiber kontrollierten Bereichen ein Empfang möglich sein. Je nach Umgebungsbedingungen und Leistungsfähigkeit der verwendeten Empfangsgeräte (z.B. Richtantennen) besteht auch hier noch eine konkrete Abhörgefahr.

I.1.3.3 Bewegungsprofile

Beim Einsatz von Funktechniken lassen sich prinzipiell Bewegungsprofile mobiler Teilnehmer erstellen. MBWA-Lösungen gemäß IEEE802.20 erschweren die Identifikation des beobachteten Geräts da-

durch, dass die benutzten Adressen temporärer Natur sind und in keinem Zusammenhang zur Hardware-gebundenen Adresse stehen.

Ein rein passives Belauschen und Auswerten der IEEE 802.20 Header reicht daher zur Erstellung von Bewegungsprofilen nicht, sondern muss mit anderen Formen der unberechtigten Informationsbeschaffung kombiniert werden, um die temporären Layer-2-Adressen mit einem bestimmten Gerät in Verbindung bringen zu können.

I.1.3.4 Verfügbarkeitsprobleme

Die Verfügbarkeit kann unter anderem durch folgende Ursachen beeinträchtigt werden:

- Störung durch gezielt eingesetzte Störsender (Jammer)
- Denial-of-Service, zum Beispiel Angriffe auf die Energiereserven einzelner Geräte durch Unterbinden der Aktivierung energiesparender Maßnahmen (Beispiel Standby-Modus). Sofern nicht die Authentizität entsprechender Pakete verifiziert wird, sind solche Angriffe prinzipiell denkbar (siehe auch Kapitel D. WiMAX, IEEE 802.16).

I.1.3.5 Implementierungsschwächen

Wird IEEE-802.20-basierte Technik in ausreichendem Umfang angeboten und auch vom Markt angenommen, steigt auch die Wahrscheinlichkeit, dass Fehler in den Implementierungen einzelner Hersteller bekannt werden und schließlich für Angriffe ausgenutzt werden.

Der Nimbus der für potenzielle Angreifer mangels Verbreitung eher uninteressanten Technik wird beizeiten verloren gehen und damit das Risiko der Entwicklung gezielter Angriffsmethoden steigen.

I.1.3.6 Weitere Sicherheitsaspekte

Folgende Aspekte sind ebenfalls zu bedenken:

- Mobile Geräte sind gegenüber stationären Geräten einem höheren Diebstahlrisiko ausgesetzt.
- Das mobile Gerät authentisiert sich gegenüber dem Access Network. Inwieweit eine Authentisierung eines Benutzers gegenüber dem Gerät notwendig ist, entscheidet der Hersteller. Möglicherweise wird in dieser Hinsicht zugunsten der Benutzerfreundlichkeit auf eine Authentisierung verzichtet oder es müssen gesonderte Schritte zur Aktivierung dieser Funktion durchgeführt werden. Bei Abhandenkommen mobiler Geräte sind diese leicht durch unbefugte Dritte zur Kommunikation oder zum Auslesen von lokal gespeicherten Informationen (z.B. des PMK) nutzbar.

I.1.4 Schutzmaßnahmen

Die nachfolgend benannten Schutzmaßnahmen basieren auf den bislang noch theoretischen Gefährdungsbetrachtungen. Eine Ergänzung bzw. Verschärfung kann notwendig werden, sobald entsprechende Implementierungen konkrete Schwachstellen und hierauf abzielende Angriffsformen offenbaren.

IEEE-802.20-Geräte, die mindestens einen Dienst mit Schutzbedarf anbieten, sollten Verschlüsselung und Integritätssicherung unterstützen. Leicht kompromittierbare Formen zum Umgang mit dem PMK sind zu vermeiden. Außerdem müssen die Geräte in geeigneter Weise abgesichert werden. Im Folgenden wird beschrieben, welche Maßnahmen grundsätzlich ergriffen werden können.

Eine Benennung von Restrisiken ist nur bedingt möglich, da mögliche Schwachpunkte wie ungünstige Implementierung durch einen Hersteller oder sorgloser Umgang durch einen Nutzer mangels verfügbarer Produkte noch nicht abschließend bewertet werden können.

I.1.4.1 Absicherung von IEEE-802.20-Geräten

I.1.4.1.1 Gezielte Produktauswahl

Nach Möglichkeit sollten keine Geräte eingesetzt werden, die mit Methoden zur Verwaltung des PMK arbeiten, die sich anderweitig bereits als problematisch herausgestellt haben.

Ab Werk erfolgte schwache Voreinstellungen sollten überschrieben werden können.

I.1.4.1.2 Einspielen von Sicherheitspatches

Von den Geräteherstellern bereitgestellte Sicherheitspatches bzw. eine aktuellere Version der Firmware sollten nach Test und bei Bedarf eingespielt werden.

I.1.4.1.3 Allgemeine Konfiguration

Grundsätzlich ist es empfehlenswert, die vom Hersteller voreingestellte Konfiguration auf Schwachstellen zu überprüfen und nötigenfalls zu ändern. Es ist mit üblichen, bei anderen Lösungen zur drahtlosen Kommunikation bereits zu beobachtenden Schwächen zu rechnen. Diesen sollte nach Möglichkeit gezielt begegnet werden, beispielsweise:

- Eine ab Werk eingestellte automatische Aktivierung möglichst vieler Dienste sollte unterbunden werden. Nicht benötigte Dienste sollten gezielt abgestellt werden.
- Die MBWA-Schnittstellen der Geräte sollten bei Nichtbenutzung deaktiviert werden.
- Falls die Sendeleistung variabel ist, sollte sie so niedrig wie möglich und so hoch wie für die Funktionalität erforderlich eingestellt werden.
- Bei Verlust/Diebstahl eines mobilen (bzw. stationären) Geräts sollte nach Möglichkeit die Löschung aller entsprechenden Schlüssel – inklusive PMK – veranlasst werden.

I.1.4.2 Sicherer Schlüsselaustausch

Es muss berücksichtigt werden, dass bei der Verwendung von EAP der Netzanbieter Freiheiten bei der Wahl der EAP-Methode hat. Speziell passwortbasierte Methoden (z.B. im Rahmen von EAP-TTLS[5]) sind potenziell durch Wörterbuchattacken angreifbar, was bei der Verwendung von schwachen Passwörtern eine Gefährdung darstellen kann. In diesem Fall ist der Netzanbieter für die Absicherung durch z.B. entsprechende Sperrmechanismen verantwortlich.

5 TTLS = Tunneled Transport Layer Security

I.1.4.3 Weitere Schutzmaßnahmen

Generell sind alle Gefährdungen zu berücksichtigen, die für IP-basiert kommunizierende Geräte anfallen (man siehe hierzu insbesondere [GSK]).

Über die genannten Maßnahmen hinaus sollten bei Verfügbarkeit von IEEE-802.20-basierten Geräten – falls dies technisch möglich ist – weitere lokale Schutzmaßnahmen berücksichtigt werden, z.B.

- Zugriffsschutz (materielle Sicherungsmaßnahmen)
- Benutzerauthentisierung
- Virenschutz
- Personal Firewall
- restriktive Datei- und Ressourcenfreigabe auf Betriebssystemebene
- lokale Verschlüsselung

Informationen hierzu findet man in den IT-Grundschutz-Katalogen des BSI (siehe [GSK]). Im Zweifel orientiere man sich am Baustein Allgemeiner Client und wende die zugehörigen Maßnahmen sinngemäß an.

I.1.4.4 Restrisiko

Unabhängig von den beschriebenen Sicherheitsmaßnahmen sind mit der Verwendung zukünftiger IEEE-802.20-Geräte grundsätzlich immer folgende Restrisiken verbunden:

- Das Erstellen von Bewegungsprofilen mobiler Geräte (siehe Kapitel I.1.3.3) kann nicht vollständig verhindert werden, sofern es einem Angreifer gelingt, über unbefugt erlangte Zusatzinformationen einen Zusammenhang zwischen den temporären Adressen (MAC ID, UATI) und dem zugehörigen Gerät herzustellen.
- Die Gefährdung der Verfügbarkeit (siehe Kapitel I.1.3.4) ist nicht vollständig vermeidbar. Zwar erschweren die vorgesehenen Security-Funktionalitäten Angriffe über gezielte Pakete an die Adresse eines IEEE-802.20-Geräts, und bei Verwendung intelligenter Antennentechnik, welche die Richtung des eingehenden Signals berücksichtigt, werden solche Pakete womöglich ausgefiltert. Ein genügend starker Störsender, der die Signale gewollter Kommunikation zwischen AT und Access Network überlagert, ist jedoch als Angriffsform gegen drahtlose Übertragung niemals völlig auszuschalten.

I.1.5 Ausblick

Inwieweit IEEE 802.20 tatsächlich praxisrelevant wird, hängt von verschiedenen Faktoren ab. Je nach angestrebter Nutzungsweise mobiler Geräte stehen verschiedene Alternativen als Konkurrenz im Raum, etwa die mobile Variante von WiMAX (siehe Kapitel D.1.2) oder Mobilfunktechnologien. Eine weite Verbreitung von IEEE 802.20 in den nächsten Jahren darf zumindest skeptisch betrachtet werden.

I.1.6 Fazit

Noch ist MBWA auf Basis von IEEE 802.20 nicht verfügbar, und es können nur die Konzepte und Inhalte der Spezifikation bewertet werden.

Die in IEEE 802.20 spezifizierten Methoden und kryptographischen Algorithmen sind etabliert und mit den vorgesehenen Schlüssellängen nach derzeitigem Stand auch geeignet, um erhöhtem Schutzbedarf zu genügen.

I.2 IEEE 802.21 – Media Independent Handover (MIH)

Ziel der Arbeitsgruppe IEEE 802.21 ist die Spezifikation einer Möglichkeit zum Wechsel zwischen unterschiedlichen Netzwerk-Medienzugängen ohne Verlust der Sitzungen auf Nutzerebene. Ein derartiger medienunabhängiger Netzwechsel (Media Independent Handover, MIH) soll prinzipiell zwischen verschiedenen Lösungen auf Layer 1 / 2 möglich sein, unabhängig davon, ob diese auf IEEE-Standards basieren oder nicht. Hierbei werden insbesondere vertikale Handover adressiert, d.h. Handover zwischen verschiedenen Technologien wie WLAN, WiMAX oder Mobilfunk. Dennoch ist IEEE 802.21 auch für Handover innerhalb einer Technologie geeignet; diese werden auch als horizontale Handover bezeichnet. Ebenso soll ein Wechsel unabhängig davon möglich sein, ob das vernetzte Gerät mobil oder stationär eingesetzt wird.

Der Standard wurde im Januar 2009 veröffentlicht.

I.2.1 Grundlagen

Die grundlegende Aufgabenstellung für die IEEE-802.21-Spezifikation besteht darin, einen nahtlosen Medienwechsel auf Layer 1 / 2 zu erlauben, ohne dass hierdurch der Nutzer eines vernetzten Geräts gezwungen ist, die Verbindungen zu von ihm genutzten Diensten neu zu etablieren.

Es ist nicht notwendig, dass der „nahtlose“ Medienwechsel für den Nutzer unbemerkt vonstatten geht. Jedoch sollen negative Übergangseffekte wie Datenverluste und Pausenzeiten minimiert werden, ohne dass der Nutzer des Geräts eingreifen muss.

Soweit genutzte Anwendungen QoS-Anforderungen aufweisen, soll die Möglichkeit bestehen, auf dasjenige verfügbare Netzwerk zu wechseln, mit dem diesen Anforderungen am ehesten entsprochen werden kann. Die in diesem Sinne notwendigen Funktionalitäten von IEEE 802.21 müssen insbesondere umfassen:

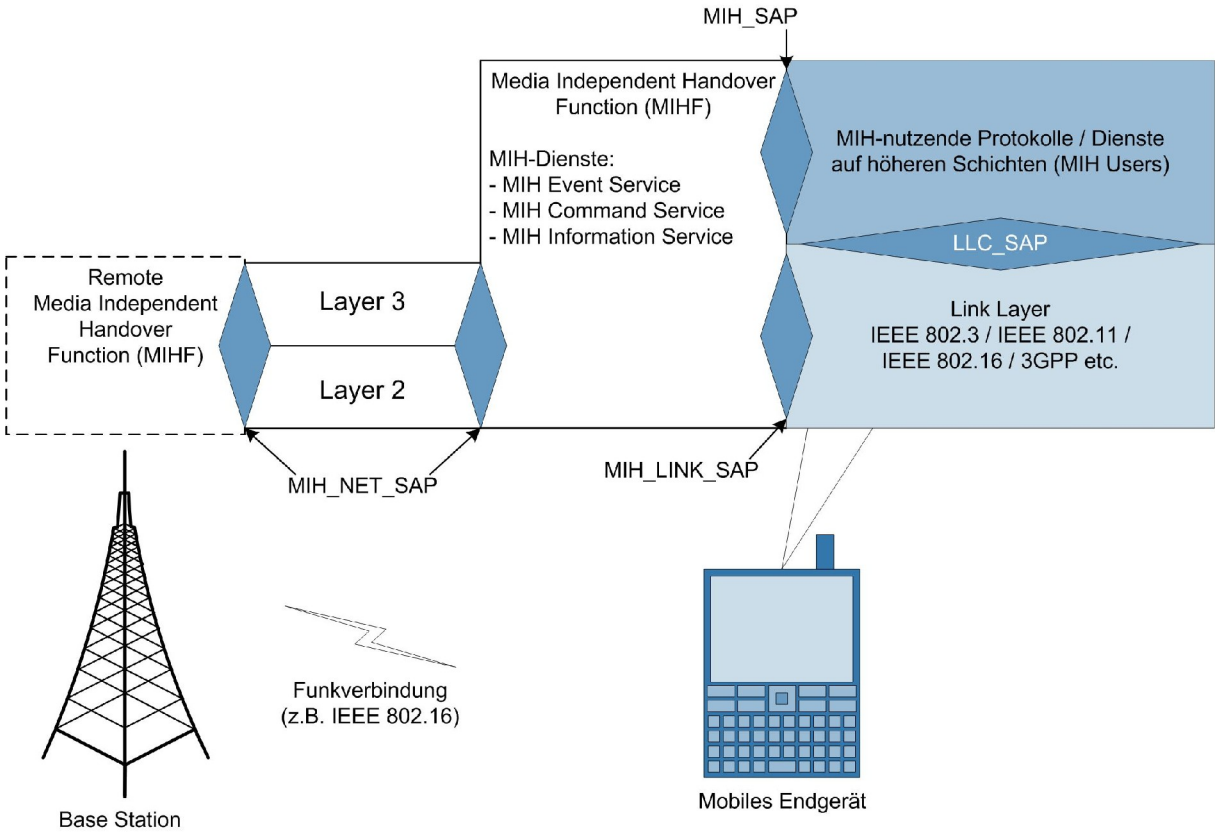
- Ermittlung verfügbarer Netzwerke im Bereich eines zu vernetzenden Geräts
- Gewinnung und Verwaltung von Informationen über die unterstützten Leistungsmerkmale je Netzwerk
- einheitliche Repräsentation verschiedener Layer-1/2-Lösungen gegenüber den höheren Protokollschichten
- Erkennen der Notwendigkeit zum Netzwerkwechsel bei entsprechenden auslösenden Ereignissen

Allerdings ist IEEE 802.21 nicht für das Ausführen des eigentlichen Handover zuständig, sondern allein für das Einholen, Filtern und Weitergeben aller relevanten Informationen. Auch die verantwortliche Instanz für den Handover bzw. die Versorgung mit Informationen ist nicht vorgeschrieben. Der Handover kann sowohl durch den Netzanbieter ausgelöst werden, durch diesen nur in Form von IEEE-802.21-relevanten Daten unterstützt werden oder autark durch das mobile Endgerät erfolgen.

Zur Realisierung dieser Funktionalitäten beschreibt die IEEE-802.21-Spezifikation eine Art Zwischenschicht zwischen physikalischem Netzwerk und dessen Aktivierung (Data Link) und Layer 3 bis 7. Diese Funktionalität wird als Media Independent Handover Function (MIHF) bezeichnet und stellt eine logische Funktion dar, welche über entsprechende Schnittstellen nach unten (Layer 1-2) bzw. oben (Layer 3-7) Schnittstellen bereitstellt (siehe Abbildung I-6). Diese Schnittstellen werden als Service Access Points (SAPs) bezeichnet und können in medienunbhängige und medienabhängige SAPs

unterteilt werden. Der medienunabhängige SAP MIH_SAP dient als Zugriffspunkt für Dienste auf höheren Schichten. Diese MIH-nutzenden Dienste und Protokolle werden bei IEEE 802.21 als MIH Users bezeichnet. Über den medienabhängigen SAP MIH_LINK_SAP erfolgen die Zugriffe auf Layer 1/2 der jeweiligen Technik, wie z.B. IEEE 802.3, IEEE 802.11 oder IEEE 802.16. Der Austausch mit der entsprechenden IEEE-802.21-Infrastruktur, wie z.B. anderen Zugangspunkten erfolgt über den SAP MIH_NET_SAP. Dieser ermöglicht den Austausch von Nachrichten sowohl auf Layer 2 als auch auf Layer 3.

Abbildung I-6: Generelles MIH-Modell bei IEEE 802.21



Die IEEE-802.21-Spezifikation beschreibt Funktionsweise, genutzte Nachrichtentypen und Kommandos in abstrakter Weise, macht aber gezielt keine weiteren Vorgaben für die Implementierung und nennt auch keine Präferenzen in diesem Sinne.

Die im Referenzmodell vorgesehenen IEEE-802.21-Dienste sind wie folgt zu charakterisieren:

- Media Independent Event Services (MIES): Die Spezifikation zu MIES definiert Ereignisse (Events) und Funktionen zur Reaktion auf diese. Ein Ereignis kennzeichnet eine Veränderung der Situation, die eine Revision der derzeitigen Netzwerkwahl nahe legt, diese erforderlich macht bzw. ihren Vollzug abschließt (Link up, Link down, Wechsel bei Leistungsparametern eines Link, Entdecken eines neuen Link, d.h. einer Netzwerk-Alternative, Verschlechterung des Zustands einer Layer-2-Verbindung mit drohendem Verlust, Abreißen einer Layer-2-Verbindung usw.).

- Media Independent Command Services (MICS): Die MICS steuern das Umsetzen von Kommandos, die über die MIH_SAP-Schnittstelle von höheren Protokollen und Diensten entgegen genommen werden. Die Liste der in der Spezifikation vorgesehenen Kommandos umfasst Statusabfragen, das Veranlassen eines Medienwechsels, konfigurierende Eingriffe auf den Data Link Layer und Schritte zur Begleitung des Medienwechsels.

- Media Independent Information Service (MIIS): Der MIIS ist die tragende Komponente der entstehenden Netzarchitekturen. Hier werden alle Informationen zusammengeführt und verwaltet, über die vorhandene Netze und ihre Zustände bzw. Merkmale beschrieben werden und gezielt als Kandidaten für aktive Verbindungen geprüft werden können. So lassen sich beispielsweise Informationen über die Betreiber eines Netzes, Roaming-Vereinbarungen und Kosten ermitteln, aber auch über die von einem Netz zur Verfügung gestellten Sicherheitsmechanismen.

I.2.2 Sicherheitsmechanismen gemäß IEEE 802.21

Sicherheitsmechanismen sind im aktuellen Standard (siehe [IEEE08-21]) nicht vorgesehen und explizit ausgenommen. In diesem Zusammenhang wird auf eine Absicherung im Rahmen der beteiligten Netzwerklösungen verwiesen. Über den Media Independent Information Service können beispielsweise die unterstützten Sicherheitsmechanismen des jeweiligen (potenziellen) Zugangspunktes erfragt werden. Je nach Realisierung der IEEE-802.21-Infrastruktur obliegt es entweder dem Endgerät oder dem Netzanbieter, einen Handover zu veranlassen und auf diese Weise auch eine Bewertung der Sicherheitsmechanismen vorzunehmen.

I.2.3 Gefährdungen bei der Nutzung von IEEE 802.21

Die wesentliche Gefährdung ist über den notwendigen Informationsdienst MIIS gegeben. Gelingt es einem Angreifer, gezielt auf diesen einzuwirken, so kann er wertvolle Hinweise für weiterführende Angriffsschritte erhalten, solche Angriffe durch Manipulation der verwalteten Informationen begünstigen oder über DoS-artige Angriffe die Verfügbarkeit des Informationsdienstes sabotieren und so den Medienwechsel unmöglich machen.

Eine Ursache hierfür liegt im Austausch von Nachrichten, der bereits vor einer Authentisierung zwischen mobilem Endgerät und Zugangspunkt erfolgen kann, bei dem die Pakete somit nicht authentisiert sind und im Klartext übertragen werden. Auf diese Weise können Unbefugte sowohl Informationen sammeln als auch Angriffe vom Typ DoS ausführen.

DoS-Angriffe sind ferner denkbar in einer Weise, dass durch Provokation bestimmter Ereignisse (Events) ein mobiles Gerät immer wieder dazu veranlasst wird, einen Medienwechsel durchzuführen. Eine produktive Nutzung der immer nur kurzzeitig etablierten Links wird dadurch unmöglich gemacht.

Eine weitere Gefährdung stellt der Handover zwischen Zugangspunkten/-netzen mit unterschiedlichen Sicherheitskontexten dar. IEEE 802.21 ist hierbei über den MIIS zuständig für das Einholen der jeweiligen Informationen, z.B. der unterstützten Sicherheitsmechanismen. Es obliegt jedoch dem mobilen Endgerät oder dem Netzanbieter (je nach Umsetzung bzw. Situation), wie er diese Angaben bewertet. Hierbei ist generell zu hinterfragen, wie ein Wechsel von einem sicheren in einen unsicheren Kontext gehandhabt wird und inwiefern der Nutzer diese Entscheidung beeinflussen kann.

I.2.4 Schutzmaßnahmen

Schutzmaßnahmen innerhalb des Geltungsbereichs von IEEE 802.21 sind nicht absehbar. Die dargestellten Gefährdungen müssen auf Ebene der genutzten Netzwerklösungen mit Hilfe von Authentizitätssicherung und Verschlüsselung kritischer Informationen, etwa im Rahmen der MIIS-Nutzung, abgewendet werden.

I.2.5 Ausblick

Es ist davon auszugehen, dass die Nachfrage nach unterbrechungsfreien Diensten auch bei Wechsel des darunter liegenden Transportmediums zunimmt. Dies ist sowohl durch die fortschreitende Mobilität bedingt als auch durch die steigende Anzahl an Schnittstellen in mobilen Endgeräten, wie z.B. Bluetooth, Ethernet, Mobilfunk oder WLAN.

Die Praxisrelevanz von IEEE 802.21 ist von wenigen Einflussgrößen abhängig. Hier kommt es im Wesentlichen darauf an, ob Hersteller einen ausreichend großen Markt sehen und die Vorleistung des Implementierungsaufwands eingehen. Die Akzeptanz auf Kundenseite wiederum wird sicherlich stark davon mitbestimmt werden, ob eine IEEE-802.21-Fähigkeit leicht, im Idealfall ohne Austausch bestehender Installationen von Software auf Layer 2 und 3, d.h. als reine Ergänzung, nachgerüstet werden kann.

I.2.6 Fazit

IEEE 802.21 ist eine reine Verwaltungslösung, mit der Verbindungswechsel über die Grenzen der einzelnen Netzwerktechnik hinaus möglich gemacht werden sollen. Prinzipiell ergeben sich hier keine zusätzlichen Aufgaben zur Absicherung, solange die für die so zusammengeführten Technologiealternativen bereits einzeln formulierten Empfehlungen zu Schutzmaßnahmen umgesetzt werden. Kritisch ist hierbei jedoch der Wechsel zwischen verschiedenen Sicherheitskontexten zu bewerten, insbesondere mit den jeweils unterschiedlich stark ausgeprägten Sicherheitsmechanismen der jeweiligen Technik. Nicht authentisierte Nachrichten im Klartext ermöglichen weiterhin das Ausspähen von Informationen sowie potenziell Angriffe vom Typ DoS.

Hier ist zu beachten, dass die Gewährleistung eines garantierten Mindestsicherheitsniveaus in den entstehenden heterogenen Netzarchitekturen komplizierter wird: Das Sicherheitsniveau wird bestimmt durch die schwächste beteiligte Implementierung bzw. Konfiguration, die ein vernetztes Gerät über IEEE 802.21 auswählen kann.

Sicherheitsanalysen werden komplexer, da Technikwechsel nicht länger auf definierte Übergabepunkte zwischen Netzwerken beschränkt bleiben, sondern im multi-netzwerkfähigen Endgerät selbst entschieden werden.

I.3 IEEE 802.22 – Wireless Regional Area Network (WRAN)

Das Ziel der IEEE-802.22-Arbeitsgruppe ist die drahtlose Versorgung von dünn besiedelten bzw. ländlichen Regionen, bei denen ein Angebot an derzeit aktuellen kabelbasierten Breitband-Zugangsmöglichkeiten wie ADSL eher unwirtschaftlich ist, sodass mit entsprechenden Nachteilen bei der Versorgung solcher Regionen durch Dienstanbieter zu rechnen ist.

Diese regionalen Funknetze (in IEEE 802.22 als Wireless Regional Area Networks, WRANs bezeichnet) operieren in zum Teil bereits genutzten Frequenzbändern, insbesondere des terrestrischen Fernsehens, sodass einer der Kernaspekte die kooperative Nutzung zwischen Primärnutzer (z.B. Fernsehen) und Sekundärnutzer (IEEE 802.22) ist. Hinzu kommt die Koexistenz mit anderen WRAN-Systemen. Entsprechend sind in IEEE 802.22 Mechanismen zur Überwachung der Frequenzbänder und Kommunikation zwischen den Teilnehmern eines WRAN-Systems vorgesehen. Hierfür kommen Cognitive Radios (CRs) zum Einsatz.

Derzeit (Herbst 2009) befindet sich IEEE 802.22 samt den Ergänzungen IEEE 802.22.1 und 802.22.2 noch im Draft-Status. Eine erste systematische Betrachtung der beabsichtigten Inhalte des Standards kann dennoch auf Basis der bisher vorliegenden Dokumente der Arbeitsgruppe erfolgen.

I.3.1 Grundlagen

Gegenstand der Arbeitsgruppe IEEE 802.22 ist die Spezifikation einer Lösung zur regionalen drahtlosen Kommunikation im UHF/VHF-Bereich zwischen 54 und 862 MHz, wobei entsprechende Mechanismen spezifiziert sind, welche eine gemeinsame Nutzung innerhalb dieser Frequenzen vorsehen.

In diesem Zusammenhang ist auch die sogenannte Digitale Dividende von Interesse. Durch die Digitalisierung des Rundfunks, insbesondere Hörfunk und Fernsehen, werden bisher benötigte Frequenzbänder frei und stehen für eine anderweitige Nutzung zur Verfügung. Im Rahmen der Breitbandstrategie des Bundes sollen diese Frequenzen für die Versorgung der Bevölkerung mit breitbandigen Internetanschlüssen insbesondere in ländlichen Regionen genutzt werden. Die Bundesnetzagentur plant die Vergabe des Frequenzbereichs 790 MHz bis 862 MHz noch im Jahr 2009 zu beginnen.

Das WRAN-System stellt generell ein Punkt-zu-Mehrpunkt-Richtfunksystem dar, vergleichbar mit IEEE 802.16 (WiMAX). Im Unterschied zu WiMAX soll IEEE 802.22 jedoch mit einer Basisstation im Idealfall eine Reichweite bis zu 100 km erzielen, wobei 20 km bis 30 km als realistische Werte angesehen werden dürfen.

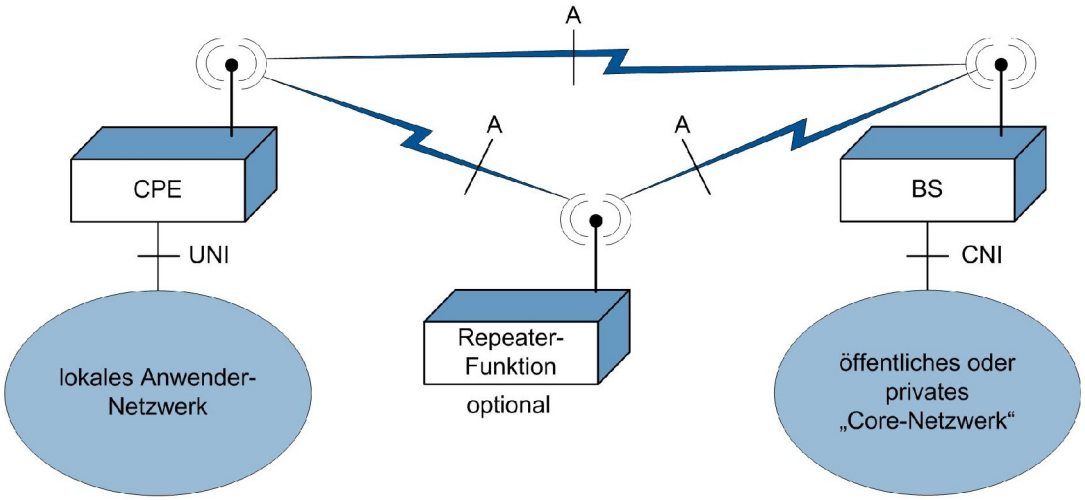
Das WRAN-System wird dabei als Teil der sogenannten Fixed-Wireless-Access-Lösungen (FWA) angesehen, die lokale Netzwerke an eine Gesamtinfrastruktur anschließen. IEEE-802.22-Kundenstationen sind also keine Endgeräte, die über eine Basisstation kommunizieren wie z.B. im WLAN, sondern Punkte, an denen lokale Netze an überregionale Infrastrukturen angebunden werden können.

Für den Endnutzer sollen folgende Datenraten zur Verfügung stehen:

- 1,5 Mbit/s downlink, d.h. von der Basisstation zum Kundengerät (Customer Premises Equipment, CPE)
- 384 kbit/s uplink

Die Grundarchitektur von WRAN nach IEEE 802.22 basiert auf einer Basisstation, die mehrere stationäre Kundenstationen versorgen soll. Die Reichweite dieser Konstellation beträgt ca. 30 km. Über optionale Verstärker-Lösungen (Repeater-Funktion, RF) kann dies ausgeweitet werden (siehe Abbildung I-7).

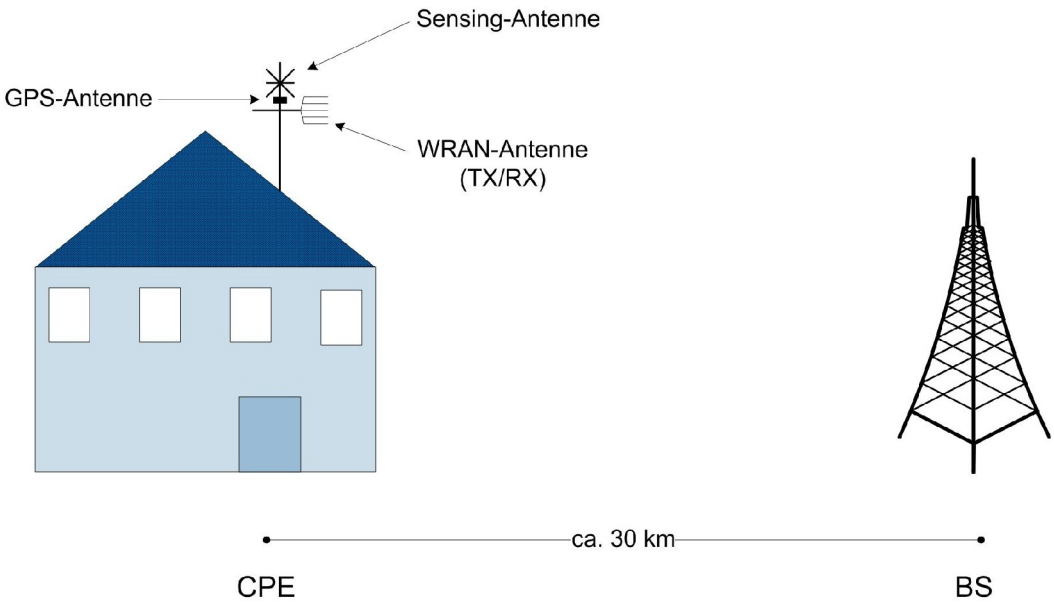
Abbildung I-7: Netzwerkaufbau bei IEEE 802.22



Legende:
A = Air Interface (Luftschnittstelle)
BS = Base Station (Basisstation)
CPE = Customer Premises Equipment (Kundenstation)
CNI = Core Network Interface
UNI = User Network Interface

Eine Kundenstation umfasst eine Außenantenne, für die eine Montage in ca. 10 m Höhe vorgesehen ist, wie z.B. auf dem Dach eines entsprechend hohen Gebäudes (siehe Abbildung I-8) oder in Form eines Antennenmasts.

Abbildung I-8: Typische Kundenanbindung in einem WRAN nach IEEE 802.22



Der IEEE-802.22-Standard wird die drahtlose Kommunikation zwischen Basisstation und Kunden-Station auf physikalischer Ebene (PHY Layer) und MAC Layer regeln. Die Kommunikation ist verbindungslos angelegt (paketbasierte Übertragung).

Der Basisstation obliegt dabei die vollständige Kontrolle der Kommunikation. Sie ist der Master gegenüber den Verstärkern oder Kundenstationen (Slaves). Insbesondere ist es Aufgabe der Basisstation, die Sendeaktivitäten so zu steuern, dass keine Konkurrenz zu TV-Übertragungen oder anderen Funkdiensten entsteht. Eine Kundenstation darf nur senden, wenn sie hierfür ein regelmäßig von der Basisstation gesendetes Freigabesignal erhält. Entdeckt die Basisstation andere Aktivitäten in ihrem Sendebereich, so wechselt sie auf einen noch freien Sendebereich.

In diesem Zusammenhang nimmt das Spektrum-Management eine wesentliche Rolle ein, um eine effiziente und ungestörte Nutzung des Frequenzspektrums zu gewährleisten. Ein Hilfsmittel hierzu sind sogenannte Cognitive Radios (CRs), welche das Frequenzspektrum beobachten, analysieren und dynamisch auf Ereignisse reagieren. Um dies zu ermöglichen, muss ein CR seine eigene Position kennen (z.B. mittels GPS), die Frequenzsituation beurteilen und sich dynamisch an die Frequenzsituation anpassen können.

Die IEEE 802.22-Spezifikation soll u.a. die Anforderungen gemäß Tabelle I-1 erfüllen. Weitere Detailanforderungen können dem Functional-Requirements-Dokument (siehe [IEEE06-1]) entnommen werden.

Tabelle I-1: Anforderungen an WRAN gemäß IEEE 802.22

Anforderungen	zwingend	optional
Unterstützung einer Mischung aus verschiedenen Kommunikationsflüssen wie Datenkommunikation, Voice over IP (VoIP) und Audio-/Video-Anwendungen	X	
Unterstützung von Quality of Service (QoS) zwecks Erfüllung der jeweiligen Anforderungen unterschiedlicher paralleler Kommunikationsflüsse	X	
Unterstützung von IPv4 und IPv6 als Protokoll oberhalb der IEEE-802.22-MAC-Lösung	X	
Unterstützung von VoIP		X
Jitter nicht schlechter als 10 ms (VoIP-tauglich)		X
Unterstützung von QoS-Steuerung über IP Differentiated Services (siehe [RFC2474] und [RFC2475])		X
Konstante Bitrate	X	

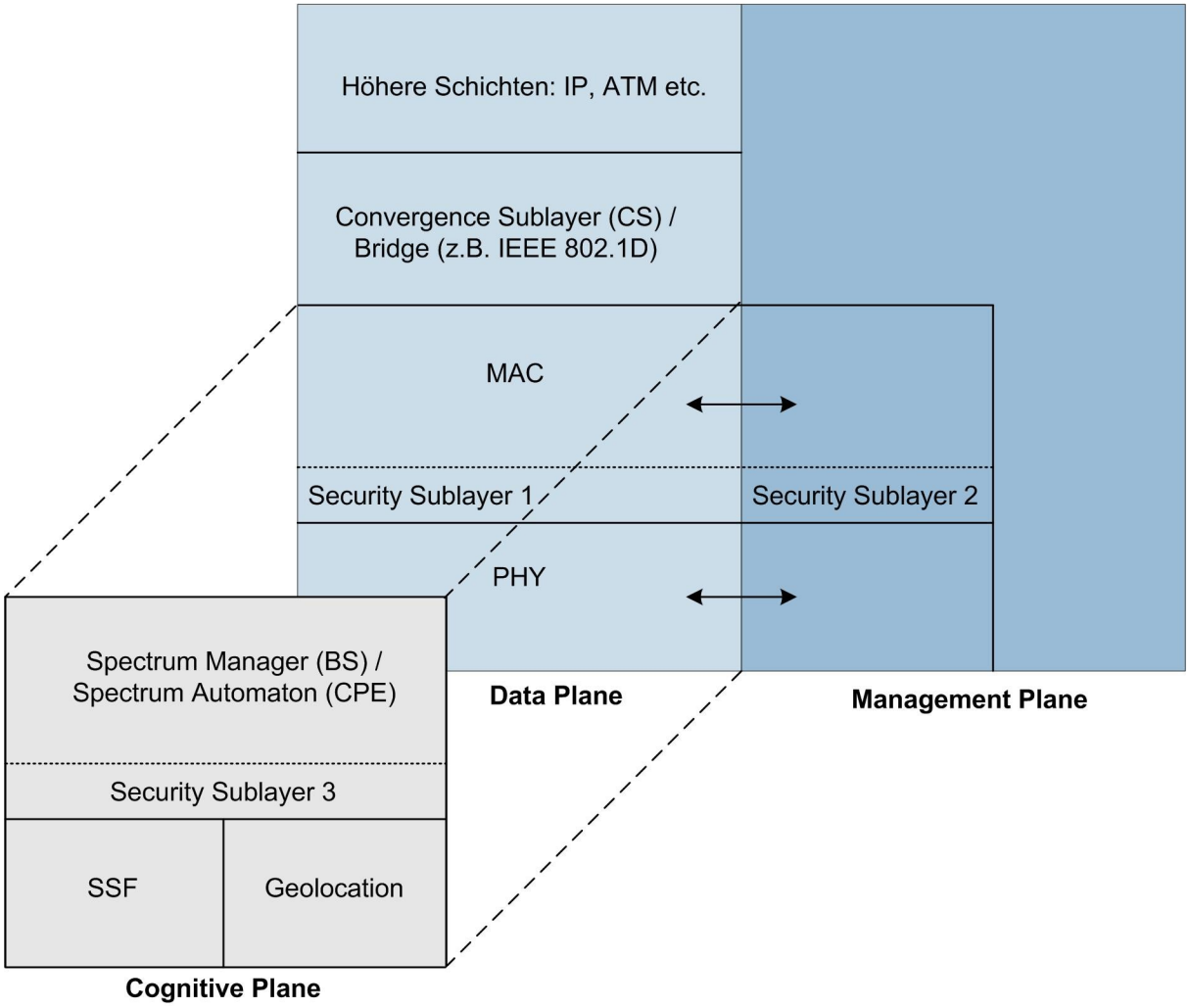
I.3.2 Sicherheitsmechanismen von IEEE 802.22

Die Verantwortlichen der Spezifikation IEEE 802.22 haben das Thema Sicherheit von Beginn an berücksichtigt und konnten die Erfahrungen aus vorangegangen Funkstandards wie IEEE 802.11 oder IEEE 802.16 einfließen lassen. Das Thema Sicherheit sollte insbesondere in Hinblick auf die Besonderheiten von IEEE 802.22 angemessen berücksichtigt werden. Hierzu zählen speziell Cognitive Radios als auch die große Reichweite eines IEEE-802.22-Systems. Geschützt werden sollen neben den Systemen der Endnutzer und des Dienstanbieters speziell die Primärnutzer der Funkfrequenzen wie beispielsweise das terrestrische Fernsehen.

In der Konsequenz ist auch das Sicherheitsmodell unterteilt und adressiert kognitive und nicht-kognitive Aspekte von IEEE 802.22. Die Security Sublayer 1 und 2 adressieren die Nutzdaten sowie die Kontroll- und Management-Nachrichten, während Security Sublayer 3 Cognitive Radios und die Interaktion mit anderen (Teil-)Systemen thematisiert (Abbildung I-9).

Die spezifizierten Sicherheitsmechanismen, namentlich die für den nicht-kognitiven Part, basieren auf IEEE 802.16e (Mobile WiMAX). Hierzu zählen insbesondere die Security Sublayer 1 und 2, welche primär auf PKMv2 (Privacy Key Management) basieren. Bekannt gewordene Schwachstellen des Sicherheitskonzeptes sowie zugehörige Gegenmaßnahmen wurden soweit möglich einbezogen, sodass es an einigen Stellen Abweichungen bezüglich IEEE 802.16e kommt.

Abbildung I-9: Vorgesehene Protokollarchitektur für IEEE 802.22 (vereinfacht)



Für die Security Sublayer 1 und 2 sind zwei Protokolle spezifiziert:

- Das Encapsulation Protocol ermöglicht die Verschlüsselung der Datenpakete zwischen dem CPE und der BS. Hierfür werden sogenannte Cryptographic Suites (Paare von Datenverschlüsselungsmechanismen und Mechanismen zur Integrationsprüfung) und die Regeln für die Anwendung dieser Algorithmen auf die Datenpakete definiert.

- Das Key Management Protocol stellt einen Mechanismus für die sichere Verteilung von Schlüsselmaterial von der BS zum CPE bereit. Hierfür wird das SCM-Protokoll (Security Control Management) genutzt, welches auf dem PKMv2-Protokoll basiert.

Für Cognitive Radios ist der Security Sublayer 3 (siehe Abbildung I-9) spezifiziert. Dieser beinhaltet im Besonderen die Authentisierung von Nachrichten, welche Informationen über die aktuelle Frequenzsituation beinhalten. Hier bestünde andernfalls die Gefahr von DoS-Angriffen, z.B. mittels Replay-Techniken. Die Abtastung und Erfassung der Frequenznutzung bezieht sich sowohl auf die Primärnutzer als auch die Sekundärnutzer der Frequenzbänder, z.B. andere IEEE-802.22-Systeme. Weitere Sicherheitsmechanismen des Security Sublayer 3 sind die Absicherung der GPS-Lokalisierung sowie die Erkennung und Benachrichtigung von fehlerhaften Übertragungen.

I.3.2.1 Security Associations und Schlüsselmaterial

Sämtliche Verbindungen und Datenübertragungen zwischen einer Base Station und dem CPE werden sogenannten Security Associations (SAs) zugeordnet. Eine SA ist ein Satz von Sicherheitsinformationen, die eine Base Station und das CPE teilen, das heißt, alle zugeordneten Verbindungen werden entsprechend der in der SA genannten Sicherheitsmechanismen gesichert. Jede SA hat eine eindeutige Identifikation, den sogenannten SAID (SA Identifier).

Während der Initialisierungsphase muss jede CPE eine primäre SA initiieren. Diese enthält mindestens die zwischen Base Station und CPE genutzte Cryptographic Suite und ggf. darüber hinaus Schlüsselmaterial und Initialisierungsvektoren. Weitere SAs existieren für Multicast- und Broadcast-Verkehr.

Das Schlüsselmaterial für jede SA wird von der Base Station verwaltet und mit Hilfe des Key-Management-Protokolls mit den CPEs synchronisiert. Zu den wichtigsten Schlüsseltypen gehören:

- Authorization Key (AK)

  Der AK wird im Rahmen der Authentisierung zwischen Base Station und Kundenstation generiert und ist eine bestimmte Zeitspanne gültig. Die Kundenstation muss vor Ablauf der Gültigkeitsdauer einen neuen AK anfordern, wenn sie weiterhin mit der Base Station kommunizieren möchte. Jede Kundenstation verfügt für alle ihre SAs nur über einen einzigen AK (bzw. während der Übergangsphase von einem bald ablaufenden zu einem neuen AK temporär über zwei AKs).

- Traffic Encryption Key (TEK)

  Mit dem TEK wird der Datenverkehr zwischen einer Kundenstation und der Base Station verschlüsselt. Eine Kundenstation muss für jede SA einen TEK führen und ist dafür verantwortlich, vor dessen Gültigkeitsablauf einen neuen TEK bei der Base Station anzufordern, der dann mit dem Key Encryption Key verschlüsselt übertragen wird.

- Key Encryption Key (KEK)

  Der KEK wird vom AK abgeleitet und zur Verschlüsselung der TEKs während der Übertragung von der Base Station zur Kundenstation verwendet.

- Group Key Encryption Key (GKEK)

  Der GKEK wird zufällig von der Base Station generiert und der Kundenstation mit dem KEK verschlüsselt übermittelt. Der GKEK dient zur Verschlüsselung der Group Traffic Encryption Keys bei der Übermittlung von der Base Station zu den Kundenstationen.

- Group Traffic Encryption Key (GTEK)

  Der GTEK für Multicast-/Broadcast-Verkehr entspricht dem TEK für Unicast-Verkehr.

- Message Authentication Keys

  Mit Message Authentication Keys werden Management-Nachrichten, z.B. zur Anforderung und Verteilung von TEKs, zwischen der Base Station und den Kundenstationen signiert und verifiziert.

Weitere Details können, sofern hier nicht anders dargestellt, dem Kapitel D. WiMAX, IEEE 802.16 entnommen werden.

I.3.2.2 Key Management Protocol

Das in IEEE 802.22 verwendete Key-Management-Protokoll basiert auf PKMv2 (siehe Kapitel D. WiMAX, IEEE 802.16), enthält jedoch entsprechende Anpassungen und wird unter dem Namen SCM (Security Control Management) geführt.

Zu den Aufgaben des SCM-Protokolls gehören:

- einseitige/gegenseitige Authentisierung
- regelmäßige Reauthentisierung
- Austausch eines Shared Secrets
- Auffrischung des Schlüsselmaterials

SCM unterstützt zwei Verfahren zur Authentisierung:

- RSA-basierte Authentisierung
- ECC-basierte Authentisierung

Das Ergebnis der Authentisierung ist ein Shared Secret zwischen BS und CPE. Von diesem Shared Secret wird weiteres Schlüsselmaterial abgeleitet, z.B. der KEK.

I.3.2.3 Encapsulation Protocol

Über das Encapsulation Protocol werden sogenannte Cryptographic Suites festgelegt, welche die Fähigkeiten der Kundenstation zur Datenverschlüsselung, Integritätsprüfung und Verschlüsselung des Schlüsselmaterials (TEK bzw. GTEK) spezifizieren. Jede Cryptographic Suite hat eine eindeutige Identifikation. Eine Liste dieser Identifikationen wird im Verlauf der Authentisierung von der Kundenstation an die Base Station übermittelt, die dann die erlaubten Identifikationen ermitteln kann. Die Liste der Cryptographic Suites findet sich in Tabelle I-2.

Für die Datenverschlüsselung ist als Verschlüsselungsalgorithmus allein AES im CCM-Modus[6] mit 128-Bit-Schlüssel vorgesehen. Eine Aushandlung möglicher alternativer Verschlüsselungsalgorithmen, abgesehen von dem Verzicht auf Verschlüsselung, ist daher nicht erforderlich. Auch die Integritätsprüfung ist über AES im CCM-Modus mit 128-Bit-Schlüssel möglich.

Grundsätzlich wird nur der MAC PDU Payload verschlüsselt. Der Generic MAC Header und die optionale CRC werden nicht verschlüsselt. Außerdem werden alle MAC-Management-Nachrichten unverschlüsselt übertragen.

Der TEK bzw. GTEK für die Verschlüsselung der Nutzdaten wird bei seiner Übermittlung an die Kundenstation mit AES Key Wrap (128-Bit-Schlüssel) verschlüsselt.

---

6 CCM = Counter with CBC-MAC, CBC-MAC = CBC with Message Authentication Code; CCM ist eine generische Methode für die Verschlüsselung und Integritätsprüfung von Daten, die für die Verwendung einer 128-Bit-Blockchiffrierung (z.B. AES) spezifiziert ist. In Kapitel A. Funk-LAN (WLAN, IEEE 802.11) ist diese Methode kurz beschrieben.

Tabelle I-2: Cryptographic Suites für IEEE 802.22

Cryptographic Suite ID	Beschreibung		
	Datenverschlüsse-lung	Integrationsprüfung	TEK-Verschlüsse-lung
0x00	keine	keine	-
0x01	keine	AES-CCM für Unicast	AES-128 Key Wrap
0x02	AES-CCM	AES-CCM für Unicast	AES-128 Key Wrap
0x03	keine	AES-CCM für Multicast/Broadcast	AES-128 Key Wrap
0x04	AES-CCM	AES-CCM für Multicast/Broadcast	AES-128 Key Wrap
0x05 – 0xFF	reserviert		

I.3.2.4 Sicherheitsmechanismen der Cognitive Plane

Im Unterschied zu anderen Funktechniken wie beispielsweise IEEE 802.16 operiert IEEE 802.22 als Sekundärnutzer in den Lücken eines bereits genutzten Frequenzbandes (White Spaces). Der Primärnutzer ist beispielsweise das terrestrische Fernsehen. Entsprechend sind für den Standard verschiedene Mechanismen zum Schutz des Primärnutzers vorgesehen. Ziel ist es hierbei, die Verfügbarkeit des Primärnutzers nicht zu beeinträchtigen.

Die Cognitive Plane umfasst dabei die Layer 1 und 2 (PHY und MAC) und beinhaltet Funktionen für das Spektrum-Management (Spectrum Manager, Spectrum Automaton) sowie das Abtasten der Frequenzbänder (Spectrum Sensing Function, SSF) und die Lokalisierung (Geolocation). Dies ist in Abbildung I-9 illustriert.

Die Sicherheit für die Cognitive Plane basiert primär auf Collaborative Sensing/Correlation, d.h. mehrere Sensoren (hier CPEs) sammeln Daten (SSF), welche zusammen mit Standortinformationen (Geolocation) als Basis für eine Entscheidung genutzt werden (Spectrum Manager, Spectrum Automaton), z.B. einen Wechsel der Frequenz. Die endgültige Entscheidung obliegt dabei einem zentralen System, in der Regel der BS.

Ein „Werkzeug“ des Collaborative Sensing ist eine gemeinsame Datenbank, in welcher die Primärnutzer gelistet sind. Ob ein empfangenes Signal authentisch ist und tatsächlich einem Primärnutzer zugeordnet werden kann, entscheidet ein Wahlverfahren zwischen den CPEs. Hierfür werden CPEs in einem bestimmten Umkreis befragt (z.B. 4 km), ob diese das Signal ebenfalls erkannt haben. Wird dies von einer festgelegten Mindestanzahl CPEs bestätigt, gilt das Signal als authentisch.

Auf diese Weise schützt Collaborative Sensing nicht nur den Primärnutzer, sondern auch den Sekundärnutzer. Für einen DoS-Angriff genügt es in diesem Fall nicht, nur einem einzelnen CPE gefälschte Informationen zukommen zu lassen, sondern es muss eine Gruppe von CPEs getäuscht werden. Voraussetzung ist ein bereits etablierter Netzzugang und eine ausreichende Anzahl an weiteren CPEs in der jeweiligen Umgebung.

I.3.3 Gefährdungen bei der Nutzung von IEEE 802.22

Dieses Kapitel beschreibt typische Gefährdungen, denen ein WRAN-System nach IEEE 802.22 ausgesetzt sein kann. Da sich IEEE 802.22 noch in der Entwurfsphase befindet, handelt es sich nachfolgend um mögliche Gefährdungen, welche auf den bisher veröffentlichen Teildokumenten basieren, sowie um Kenntnisse in Hinblick auf den Standard IEEE 802.16e, welcher zu weiten Teilen als Grundlage für die Sicherheitsmechanismen innerhalb von IEEE 802.22 diente.

I.3.3.1 Ausfall durch höhere Gewalt

Wie im kabelgebundenen LAN kann es auch in WRAN-basierten Netzen durch Überspannungen zum Ausfall von Komponenten kommen. Außerdem sind Außeninstallationen (z.B. Antennen) durch Blitz und Witterungseinflüsse gefährdet.

I.3.3.2 Unkontrollierte Ausbreitung der Funkwellen

Die Funkwellen der WRAN-Komponenten breiten sich auch über räumliche Grenzen des WRAN-Nutzungsbereichs aus. Aufgrund der genutzten Frequenzen ist die Reichweite hier deutlich höher als bei anderen funkbasierten Systemen wie z.B. IEEE 802.11. Dabei kann auch in nicht vom WRAN-Betreiber kontrollierten Bereichen ein Empfang möglich sein. Je nach Umgebungsbedingungen und Leistungsfähigkeit der verwendeten Empfangsgeräte (z.B. Richtantennen) besteht auch hier noch eine konkrete Abhörgefahr.

I.3.3.3 Bedrohung der Verfügbarkeit

WRANs übertragen Informationen mittels elektromagnetischer Funkwellen. Strahlen andere elektromagnetische Quellen im gleichen Frequenzspektrum Energie ab, können diese die WRAN-Kommunikation stören und im Extremfall den Betrieb des WRAN verhindern. Dies kann unbeabsichtigt durch andere technische Systeme oder aber durch absichtliches Betreiben einer Störquelle (Jammer) als sogenannter Denial-of-Service-Angriff (DoS-Angriff) erfolgen. Eine solche Störquelle kann sich bei ausreichender Sendeleistung auch außerhalb des Bereiches befinden, in dem das WRAN genutzt wird.

I.3.3.4 Gefährdungen im Bereich Cognitive Radio

Die Besonderheit von IEEE 802.22 ist die Verwendung von Cognitive Radios (CRs). Insbesondere in Hinblick auf Sicherheitsaspekte besteht in diesem Bereich noch Forschungsbedarf. Die kooperative Nutzung von Frequenzen durch verschiedene Teilnehmer birgt generell die Gefahr, dass durch Fehlinformationen den CRs ein Primärnutzer vorgetäuscht wird und auf diese Weise ein DoS-Angriff erfolgen kann. IEEE 802.22 sieht hierfür zwar Mechanismen vor, wie beispielsweise Collaborative Sensing (siehe auch Kapitel I.3.2.4). Die Implementierung dieser Funktionalität durch den Dienstanbieter wird zum jetzigen Zeitpunkt jedoch als optional angesehen.

Weitere Details und Gefährdungen im Bereich Cognitive Radio und IEEE 802.22 finden sich beispielsweise in [BIPA08].

I.3.3.5 Physischer Zugangsschutz

Base Station und Kundenstation müssen vor Fremdzugriff geschützt werden. Während die Base Station in der Regel durch den Netzanbieter angebracht und abgesichert wird, besteht für die Kundenstati-

on eine höhere Gefährdung eines unautorisierten Zugriffs. Insbesondere wenn die Kundenstation mehrere Teilnehmer oder Wohnungseinheiten versorgt, stellt dies eine Gefährdung dar.

Speziell der für Public-Key-Verfahren benötigte private Schlüssel muss vor Zugriff geschützt werden. Ein auf diese Weise durchgeführter Identitätsdiebstahl kann für weitere Angriffe missbraucht werden.

I.3.3.6 Schwächen im Sicherheitskonzept

I.3.3.6.1 Übertragung von Management-Nachrichten

Bestimmte Management-Nachrichten sind von einer Datenverschlüsselung und Integritätsprüfung (Cryptographic Suite) im Rahmen einer SA ausgenommen. Dies betrifft die initiale Ortung, Basic-/Primary-, Multicast- und Broadcast-Management-Verbindungen). Aus den abgefangenen Management-Nachrichten kann ein Angreifer Informationen über den Aufbau des Netzes erhalten oder allgemein Angriffe vom Typ DoS ausführen.

Weiterhin besteht eine Gefährdung durch gefälschte Nachrichten im Rahmen der Verbindungsaushandlung von Kundenstation und BS. Ein Angreifer kann beispielsweise die Kommunikation zwischen Kundenstation und BS stören und schwächere Sicherheitsparameter an die BS übermitteln, als durch die legitime Kundenstation theoretisch möglich wären. Dies könnte in der Konsequenz zu einer Klartextübertragung führen.

I.3.3.6.2 Nutzung einer nur einseitigen Authentisierung

Generell ist neben der beidseitigen Authentisierung auch eine einseitige Authentisierung im Standard vorgesehen. Dies bedeutet, dass sich zwar die Kundenstation gegenüber der Base Station authentisieren muss, aber keine Authentisierung der Base Station gegenüber der Kundenstation stattfindet.

Die Kundenstation hat also keine Möglichkeit die Authentizität der Base Station zu überprüfen und kann somit eine falsche Base Station nicht erkennen.

I.3.3.6.3 Verzicht auf Integritätsprüfung und Datenverschlüsselung

Der bisherige Entwurf des Standards bietet die Möglichkeit, auf eine Verschlüsselung und Authentisierung der Datenkommunikation zu verzichten (Cryptographic Suite 0x00, siehe auch Tabelle I-2). In diesem Fall ist keine sichere Kommunikation gewährleistet. Die Entscheidung darüber, welche Cryptographic Suite gewählt wird, obliegt dem Dienstanbieter bzw. der Aushandlung zwischen Kundenstation und Base Station.

I.3.3.6.4 Shared Keys im Multicast-/Broadcast-Betrieb

IEEE 802.22 ist auch für den Multicast- und Broadcast-Betrieb ausgelegt. Der hierfür vorgesehene symmetrische Schlüssel (Group Traffic Encryption Key, GTEK) für die Verschlüsselung und Authentisierung muss allen Teilnehmern bekannt sein und birgt die Gefahr, dass Nachrichten manipuliert werden oder ein Teilnehmer selbstgeneriertes Schlüsselmaterial in Umlauf bringt. Dies würde auch Angriffe vom Typ DoS ermöglichen, da Broadcast-/Multicast-Verkehr der ursprünglichen BS nicht länger entschlüsselt werden könnte. Weitere Details hierzu finden sich im Zusammenhang mit IEEE 802.16e in [DEIN07].

I.3.3.7 Vertrauen in PKI

Bei der Verwendung von Public-Key-Verfahren zur Authentisierung ist der Hersteller in der Pflicht, entsprechende Zertifikate für die Kundenstation entweder im Voraus zu installieren oder dynamisch zu generieren. Insbesondere wenn die Zertifikate vorinstalliert wurden, muss dem Hersteller vertraut werden, dass diese sicher generiert wurden und keine zwei Geräte identisches Schlüsselmaterial besitzen.

I.3.4 Schutzmaßnahmen

Dieses Kapitel beschreibt Schutzmaßnahmen, mit denen ein WRAN-System nach IEEE 802.22 abgesichert werden kann. Da sich IEEE 802.22 noch in der Entwurfsphase befindet, handelt es sich nachfolgend um Schutzmaßnahmen, welche auf den bisher veröffentlichen Teildokumenten basieren sowie Kenntnissen in Hinblick auf den Standard IEEE 802.16e, welcher zu weiten Teilen als Grundlage für die Sicherheitsmechanismen innerhalb von IEEE 802.22 diente.

I.3.4.1 Absicherung der Datenkommunikation

WRANs sollten grundsätzlich mit Datenverschlüsselung und Integritätsprüfung (Cryptographic Suite 0x02 und 0x04 für Unicast- respektive Multicast-/Broadcast-Verkehr) betrieben werden, d.h. die Verwendung von AES im CCM-Modus mit 128-Bit-Schlüssel.

Die Authentisierung zwischen Kundenstation und Base Station sollte beidseitig erfolgen.

Weitere Schutzmaßnahmen gelten für den Anschluss eines Endgeräts an eine Kundenstation. Dies beinhaltet insbesondere die geeignete Trennung des lokalen Systems von dem Funknetz durch den Einsatz von Firewall-Techniken und den Einsatz eines Virenschutzes für die lokal angeschlossenen Systeme.

I.3.4.2 Absicherung der Netzelemente

Netzelemente eines WRAN-Systems sind geeignet zu härten, damit ein erfolgreicher Angriff über die Luftschnittstelle möglichst unwahrscheinlich ist. Dies gilt insbesondere für die Konfiguration der Kundenstationen, denn wenn IEEE 802.22 den Massenmarkt erreichen sollte, besteht gerade hier die Gefahr, dass Voreinstellungen unsicher sind bzw. der Nutzer Fehleinstellungen vornehmen kann.

I.3.5 Ausblick

Generell ist davon auszugehen, dass Funksysteme mit Cognitive Radios in Zukunft eine höhere Relevanz einnehmen werden, da das zur Verfügung stehende Frequenzspektrum begrenzt ist. In der Konsequenz müssen Wege gefunden werden, eine effiziente Nutzung der Frequenzen zu ermöglichen. Eine Lösung stellen hierbei Cognitive Radios dar.

Derzeit ist der Standard IEEE 802.22 noch mitten in der Entwicklung, sodass mit einer Verabschiedung nicht vor 2010 gerechnet werden kann. Inwiefern die Hersteller den Standard aufgreifen und Produkte anbieten, bleibt abzuwarten.

Insgesamt ist eine weite Verbreitung von IEEE 802.22 als Alternative zu DSL in ländlichen Regionen nicht zu erwarten. Als Gründe führten bereits die WiMAX-Anbieter die nicht zu erwartende Rentabilität sowie Konkurrenz aus dem Bereich der Mobilfunk- oder Satelliten-Technik an. Auch existieren be-

reits Produkte auf Basis von Mobilfunktechniken, welche innerhalb der UHF/VHF-Frequenzen operieren. Hinzu kommt die Konkurrenz durch WiMAX, welches bereits mit Produkten aufwarten kann.

Für alle diskutierten neueren Entwicklungen sollte man kritisch im Auge behalten, wie die noch ausstehenden Implementierungen mit dem Thema Sicherheit umgehen. In der Grundanlage gute und bewusst den Aspekt der Sicherheit berücksichtigende Standards können in der Praxis geschwächt werden, wenn die angebotenen Möglichkeiten zur Absicherung nicht konsequent genutzt oder durch Art und Weise der Lösung im Produkt verwässert werden.

I.3.6 Fazit

IEEE 802.22 spezifiziert die Ebenen 1 (Physical Layer) und 2 (MAC Layer) eines drahtlosen Breitbandzugangs im regionalen Bereich (maximal 100 km, typischerweise bis zu ca. 30 km). Die Sicherheitsmechanismen konzentrieren sich daher auf die reine Absicherung der Funkübertragung. Übergeordnete Aspekte wie Teilnehmerauthentisierung oder die Kriterien für die Auswahl einer Cryptographic Suite sind bewusst in den Standards ausgeklammert.

Positiv zu vermerken ist, dass der bisherige Entwurf auf als sicher geltende Verfahren setzt, wie beispielsweise eine gegenseitige Authentisierung mittels Zertifikaten, Datenverschlüsselung und Integrationsprüfung mit AES im CCM-Modus und 128-Bit-Schlüssel sowie weitere Detailverbesserungen. Jedoch ist zunächst der Netzbetreiber gefordert, durch Implementierung geeigneter Mechanismen bzw. Einsatz geeigneter Produkte eine angemessen sichere Infrastruktur zu schaffen, sobald entsprechende Produkte angeboten werden. Der Nutzer hat bei der Absicherung der Systeme einen nur sehr beschränkten Einfluss.

Außerdem sollte der Nutzer, der letztendlich über IEEE 802.22 kommuniziert, im Einzelfall prüfen, ob das angebotene Sicherheitsniveau auch zum Schutzbedarf der über IEEE 802.22 transportierten (bzw. erreichbaren) Daten passt. Ist dies nicht der Fall, muss er selbst weitere Sicherheitsmechanismen umsetzen, wie z.B. Firewall-Systeme, IDS/IPS oder den Einsatz eines VPN im Fall einer LAN-Kopplung.

In Hinblick auf IEEE 802.22 ist speziell das Thema Verfügbarkeit zu berücksichtigen.

I.4 Literatur und Links

Im Wesentlichen sind hier die Veröffentlichungen der zugehörigen IEEE-Arbeitsgruppen zu nennen. Eine vollständige Übersicht der allgemein zugänglichen Beiträge von Mitgliedern der jeweiligen Arbeitsgruppe findet sich unter [IEEE20-C] und [IEEE20-D], [IEEE21] sowie [IEEE22]. Weitere Details zu den kryptographischen Methoden finden sich in den vom Standard referenzierten Dokumenten des 3GPP2 [3GPP2-01] und [3GPP2-02].

Darüber hinaus sind Veröffentlichungen der Hersteller, die Vor-Standard-Implementierungen durchgeführt haben, berücksichtigt.

Die Liste der hier aufgeführten Titel und Links stellt nur eine wertungsfreie Auswahl ohne Anspruch auf Vollständigkeit dar.

[3GPP2-01] 3rd Generation Partnership Project 2, „Common Security Algorithms“ (3GPP2 S.S0078-0), 2002

[3GPP2-02] 3rd Generation Partnership Project 2, „Enhanced Cryptographic Algorithms“ (3GPP2 S.S0055-A), 2005

[ATIS05] High Capacity – Spatial Division Multiple Access (HC-SDMA) radio interface standard (ATIS-0700004-2005) for wireless wideband access, Alliance for Telecommunications Industry Solutions, 2005, http://www.atis.org

[BIPA08] K. Bian und J.-M. Park, „Security Vulnerabilities in IEEE 802.22“, The Fourth International Wireless Internet Conference (WICON 2008), November 2008

[DEIN07] Andreas Deininger et al., „Security Vulnerabilities and Solutions in Mobile WiMAX“, IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.11, 2007

[GSK] Bundesamt für Sicherheit in der Informationstechnik, „IT-Grundschutz-Kataloge“, verfügbar unter https://www.bsi.bund.de/cln_155/DE/Themen/weitereThemen/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

[IEEE06-1] Functional Requirements for the 802.22 WRAN Standard, IEEE, Januar 2006 http://www.ieee802.org/22/Meeting_documents/2006_Jan/22-05-0007-47-0000_RAN_Requirements.doc

[IEEE08-20] IEEE 802.20-2008, „IEEE Standard for Local and metropolitan area networks – Part 20: Air Interface for Mobile Broadband Wireless Access Systems Supporting Vehicular Mobility – Physical and Media Access Control Layer Specification”, 2008, verfügbar unter http://www.ieee802.org

[IEEE08-21] IEEE 802.21-2008, „IEEE Standard for Local and metropolitan area networks – Part 21: Media Independent Handover Services”, IEEE, 2009, verfügbar unter http://www.ieee802.org

[IEEE20-C] IEEE 802.20, „Mobile Broadband Wireless Access (MBWA), Contributions” www.ieee802.org/20/Contributions.html

[IEEE20-D] IEEE 802.20, „Mobile Broadband Wireless Access (MBWA), Working Group Permanent Documents / Working Group Documents” http://www.ieee802.org/20/Documents.htm

[IEEE21] Web-Präsenz der IEEE-802.21-Arbeitsgruppe
http://www.ieee802.org/21/

[IEEE22] Webpräsenz der IEEE-802.22-Arbeitsgruppe
http://www.ieee802.org/22/

[RFC2474] RFC 2474, „Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers“, IETF Proposed Standard, Dezember 1998,
http://www.ietf.org/rfc/rfc2474.txt

[RFC2475] RFC 2475, „An Architecture for Differentiated Services“, IETF Informational, Dezember 1998, http://www.ietf.org/rfc/rfc2475.txt

[RFC3748] RFC 3748, „Extensible Authentication Protocol (EAP)“, IETF Proposed Standard, Juni 2004, http://www.ietf.org/rfc/rfc3748.txt

[RFC4493] RFC 4493, „The AES-CMAC Algorithm”, IETF Informational, Juni 2006,
http://www.ietf.org/rfc/rfc4493.txt

I.5 Abkürzungen

3GPP2	3rd Generation Partnership Project 2
625k-MC	625kiloHertz-spaced MultiCarrier
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
AK	Authorization Key
AN	Access Network
AT	Access Terminal
AV	Audio/Video
BS	Base Station
BSI	Bundesamt für Sicherheit in der Informationstechnik
CBC-MAC	CBC with Message Authentication Code
CCM	Counter with CBC-MAC
CDMA	Code Division Multiple Access
CMAC	Cipher-based Message Authentication Code
CNI	Core Network Interface
CPE	Customer Premises Equipment
CR	Cognitive Radio
CRC	Cyclic Redundancy Check
DECT	Digital Enhanced Cordless Telecommunications
DiffServ	Differentiated Services
DoS	Denial of Service
DSL	Digital Subscriber Line
DVD	Digital Versatile Disc
EAP	Extensible Authentication Protocol
ECC	Elliptic Curve Cryptography
EUI-48	48-Bit Extended Unique Identifier
EUI-64	64-Bit Extended Unique Identifier
FDD	Frequency Division Duplexing
FEC	Forward Error Correction
FWA	Fixed Wireless Access
GKEK	Group Key Encryption Key
GPS	Global Positioning System
GTEK	Group Traffic Encryption Key
HC-SDMA	High Capacity-Space Division Multiple Access
HD	High Definition
HDMI	High Definition Multimedia Interface

IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ID	Identification, Erkennungsnummer
IDS	Intrusion Detection System
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
IT	Information Technology
KEK	Key Encryption Key
LAN	Local Area Network
LCD	Liquid Crystal Display
MAC	Media Access Control
MAN	Metropolitan Area Network
MBWA	Mobile Broadband Wireless Access
MIB	Management Information Base
MIC	Message Integrity Check
MICS	Media Independent Command Services
MIES	Media Independent Event Services
MIH	Media Independent Handover
MIHF	Media Independent Handover Function
MIIS	Media Independent Information Service
MIMO	Multiple Input – Multiple Output
MIP	Mobile IP
OFDMA	Orthogonal Frequency Division Multiple Access
OFDM	Orthogonal Frequency Division Multiplex
PC	Personal Computer
PDA	Personal Digital Assistant
PHY	Physical Layer (IEEE)
PKM	Privacy Key Management
PMK	Pairwise Master Key
QoS	Quality of Service
RF	Repeater-Funktion
RFC	Request for Comments, Veröffentlichung der Internet Engineering Task Force
RoHC	Robust Header Compression
RSA	Rivest, Shamir und Adleman
RSVP	Resource Reservation Protocol
SA	Security Association
SAID	SA Identifier

SAP	Service Access Point
SCM	Security Control Management
SDMA	Space Division Multiple Access
SIG	Special Interest Group
SSF	Spectrum Sensing Function
TSKey	Temporary Security Key
TDD	Time Division Duplex
TEK	Traffic Encryption Key
UATI	Unicast Access Terminal Identifier
UHF	Ultra High Frequency
UWB	Ultra Wideband
UNI	User Network Interface
VHF	Very High Frequency
VoIP	Voice over IP
VPN	Virtual Private Network
WHDI	Wireless Home Digital Interface
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WRAN	Wireless Regional Area Network

I.6 Glossar

Advanced Encryption Standard (AES)

Symmetrisches Verschlüsselungsverfahren mit einer variablen Schlüssellänge von 128, 192 oder 256 Bit

Authentisierung

Verifizierung der Identität einer Instanz, z.B. eines Benutzers oder eines Geräts. Zweck ist oft die anschließende Autorisierung für Zugriffe. Ohne Authentisierung ist im Allgemeinen keine sinnvolle Autorisierung möglich.

Code Division Multiple Access (CDMA)

Beim Code-Multiplexverfahren werden die Daten mehrerer Quellen oder Sender gleichzeitig auf derselben Frequenz übertragen. Die Unterscheidung der Signale erfolgt anhand einer pro Quelle eindeutigen Kodierung mit einer binären Sequenz, deren Bitrate (hier Chiprate genannt) ein Vielfaches der Datenrate beträgt.

Denial of Service (DoS)

Ein Angriff vom Typ Denial of Service hat zum Ziel die Arbeitsfähigkeit des angegriffenen Objekts möglichst stark zu reduzieren. Dies beinhaltet beispielsweise die systematische Überlastung eines Netzknotens durch unsinnigen Verkehr (Dummy Traffic) oder die beabsichtigte Herbeiführung eines Fehlerzustands durch das Einspielen fehlerhafter Nachrichten.

Forward Error Correction (FEC)

Bei der Vorwärtsfehlerkorrektur kodiert der Sender die zu übertragenden Daten in redundanter Weise, sodass der Empfänger Fehler erkennen und korrigieren kann.

Frequency Division Duplexing (FDD)

Die Informationen werden für jede Richtung mit Hilfe einer anderen Trägerfrequenz übertragen. Dadurch wird ermöglicht, dass ein Gerät gleichzeitig senden und empfangen kann.

Message Integrity Check (MIC)

Kryptographischer Integritätsschutzmechanismus

Orthogonal Frequency Division Multiple Access (OFDMA)

Zugangsverfahren, welches das Modulationsverfahren OFDM nutzt, das statt eines einzelnen Signalträgers eine große Zahl von Subträgern gleichzeitig phasen- und amplitudenmoduliert, jedoch um ein Mehrfachzugangsverfahren ergänzt ist. Bei OFDMA können Subträger zu Subchannels zusammengefasst werden, die dann von unterschiedlichen Nutzern verwendet werden können.

Orthogonal Frequency Division Multiplex (OFDM)

OFDM ist ein Modulationsverfahren, das anstelle eines einzelnen Trägers eine große Zahl von Unterträgern gleichzeitig moduliert und parallel auf den Unterträgern (prinzipiell wie bei einer parallelen Schnittstelle an einem PC) Daten überträgt. Die erreichbaren Datenraten hängen von der Anzahl der für die Datenübertragung verfügbaren Unterträger, von den verwendeten Modulationsverfahren auf den Unterträgern und von der Code-Rate des verwendeten FEC-Code ab. Modulationsverfahren und Code-Rate werden oft dynamisch in Abhängigkeit von der Kanalqualität gewählt. OFDM wird u.a. bei WLAN und UWB verwendet.

Service Access Point (SAP)

Schnittstelle zur Interaktion mit einer Kommunikationsschicht. Der Dienstbenutzer (die höhere Schicht) greift nur über den Service Access Point auf den Dienst der niedrigeren Schicht (den Dienstanbieter) zu.

Time Division Duplex (TDD)

Zeitversetzte, in kurze Sequenzen aufgeteilte Übertragung der Daten, bei der Sende- und Empfangskanal die gleiche Frequenz nutzen, jedoch zeitlich voneinander getrennt sind. Die Informationen werden mit Hilfe eines festgelegten Zeitgebers in kurzen Sequenzen zeitversetzt übertragen. Das Umschalten zwischen Sende- und Empfangsmodus geschieht so schnell, dass dem Nutzer die kurzzeitige Unterbrechung des Kanals nicht auffällt.

Ultra High Frequency (UHF)

Frequenzband von 0,3 GHz bis 3 GHz

Very High Frequency (VHF)

Frequenzbereich von 30 MHz bis 300 MHz (Ultrakurzwellen)

J. Alte Techniken

Inhaltsverzeichnis des Abschnitts

Vorbemerkungen

Neben den aktuellen Techniken wie z.B. WLAN und Bluetooth, die zuvor in diesem Dokument ausführlich betrachtet wurden, sind weiterhin Produkte, die auf älteren drahtlosen Techniken basieren, marktverfügbar. Die Auswahl solcher Produkte sollte ebenfalls unter Sicherheitsgesichtspunkten erfolgen, sodass eine Sicherheitsbetrachtung im Rahmen dieses Dokuments erfolgt.

Folgende Techniken sind bereits seit langem verfügbar:

- IrDA (siehe Kapitel J.1) ermöglicht eine Kommunikation über Infrarot-Module mit Peripheriegeräten über sehr kurze bis kurze Distanzen mit Sichtkontakt. Wesentliche Einsatzbereich ist der Datenaustausch zwischen Geräten wie PDA, Mobiltelefon und Kameras untereinander oder mit einem PC.

- Drahtlose Tastaturen, Mäuse und andere Eingabegeräte (siehe Kapitel J.2) sind zurzeit Stand der Technik und werden häufg den kabelbasierten Eingabegeräten vorgezogen. Eine Nutzung von Bluetooth zur Anbindung solcher drahtlosen Endgeräte ist für die Zukunft erkennbar, zum jetzigen Zeitpunkt dominieren jedoch proprietäre Techniken den Markt.

J.1 IrDa

J.1.1 Grundlagen und Funktionalität

Die Infrared Data Association (IrDA), eine 1993 gegründete Non-Profit-Organisation, hat 1994 die erste IrDA-Spezifikation veröffentlicht. In dieser werden die unteren Schichten eines Protokolls für eine Infrarot-Schnittstelle definiert, bei der Infrarotstrahlung (also Licht) als Träger für den Datenaustausch über sehr kurze bis kurze Distanzen verwendet wird. Mittlerweile stellt IrDA auch höhere Protokolle für unterschiedliche Einsatzbereiche zur Verfügung. IrDA wird heute von allen gängigen Betriebssystemen unterstützt, die Kommunikation von Geräten wie PDA, Mobiltelefon und Kameras mit einem PC oder untereinander via Infrarot-Schnittstelle ist in der Praxis etabliert, wird jedoch vermehrt durch eine Kommunikation via Bluetooth abgelöst. Für drahtlose Eingabegeräte wie Tastaturen und Mäuse ist eine Kommunikation über IrDA bereits nicht mehr Stand der Technik, für diese kommen fast ausschließlich Funktechnologien zum Einsatz.

Die Infrarot-Schnittstelle wurde ursprünglich als kabelloser Ersatz der seriellen Schnittstelle konzipiert. Sie arbeitet bidirektional im Halbduplex-Verfahren mit Licht der Wellenlänge von 850 bis 900 Nanometer.

Heute wird grundsätzlich zwischen IrDA Data und IrDA Control unterschieden, wobei letzterem eine wesentlich geringere Bedeutung zukommt. Mit dem Begriff IrDA wird im Allgemeinen das IrDA-Data-Protokoll oder aber die IrDA-Organisation selbst bezeichnet.

J.1.1.1 IrDA Data

Der Standard IrDA Data wurde 1994 veröffentlicht und definiert in seiner ursprünglichen Version 1.0, die auch als Serial Infrared (SIR) bezeichnet wird, eine Datenrate von 2.400 bit/s bis 115,2 kbit/s. In der Version 1.1 wurden 1995 höhere Datenraten von 1,152 Mbit/s (Mid-Infrared = MIR) und 4 Mbit/s (Fast-Infrared = FIR) spezifiziert, wobei die Kompatibilität zu SIR gewährleistet ist.

Die Versionen 1.2 und 1.3 beinhalten Low-Power-Versionen, die mit reduzierter Sendeleistung ebenfalls Datenraten bis zu 115,2 kbit/s (Version 1.2) bzw. 1,152 Mbit/s und 4 Mbit/s (Version 1.3) erreichen. Die 1999 veröffentlichte Version 1.4 bietet durch ratenabhängige Kodierung der Datenbits Datenraten bis 16 Mbit/s (Very Fast Infrared = VFIR, IrSimple Vers. 1.0).

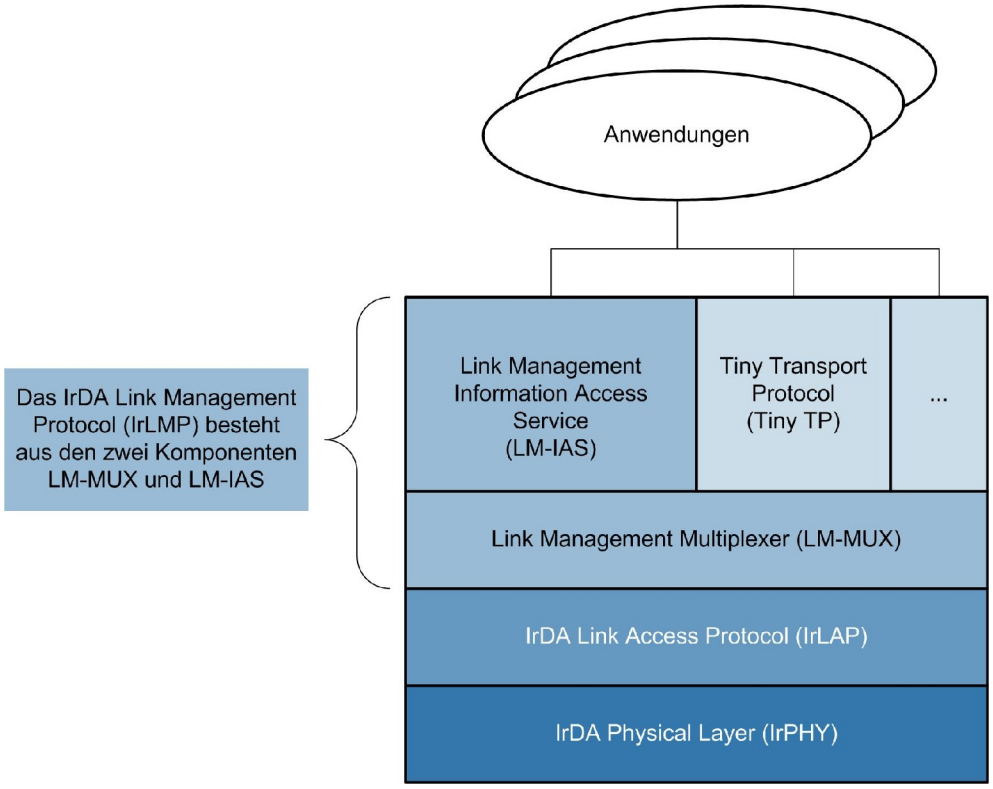
Anfang 2009 veröffentlichte die IrDa-Organisation die Spezifikation von Giga-IR, wodurch Datenübertragungen mit 1 Gbit/s Bandbreite ermöglicht werden. Eine Kompatibilität mit IrSimple ist vorgesehen, d.h. die bisher spezifizierten Geschwindigkeiten von IrDA Data sind ebenfalls nutzbar.

Die Reichweite hängt von der abgestrahlten Leistung ab, sie beträgt in den Low-Power-Betriebsarten 20 Zentimeter, bei normaler Leistungsabgabe 1 bis 2 Meter. Der Abstrahlwinkel beträgt ± 30°.

Um eine Verbindung aufzubauen, müssen zwei Geräte mit ihren Schnittstellen so aufeinander ausgerichtet werden, dass eine direkte Sichtverbindung zustande kommt. Hindernisse und größere Distanzen sind mit IrDA nicht zu überbrücken. Jedoch ergeben sich aus dieser Betriebsart auch Vorteile, da Störungen nur von sehr hellen Lichtquellen oder direkter Sonneneinstrahlung ausgehen.

Die Protokollarchitektur von IrDA Data ist in drei verbindliche und eine Reihe optionale Protokolle unterteilt (siehe Abbildung J-1).

Abbildung J-1: IrDA-Protokoll-Stack



Zu den verbindlichen Protokollen bei IrDa gehören

- Physikalische Bitübertragungsschicht (IrPHY, Version 1.4)

  IrPHY beschreibt die Kommunikation einer Punkt-zu-Punkt-Verbindung, auf der Daten seriell im Halbduplex-Modus bei Sichtverbindung übertragen werden. Die nutzbaren Übertragungsbandbreiten sind 115.2 Kbit/s, 0,576Mbit/s, 1,152 Mbit/s sowie 4 und 16 Mbit/s. Eine Erweiterung mit einer Datenrate von 1 Gbit/s wird in Kürze als Version 1.5 verfügbar sein; die entsprechenden Spezifikationen wurden im April 2009 verabschiedet.

  Details zur physikalischen Übertragungsschicht bei IrDA können der IrDA-Spezifikation entnommen werden, die von der Infrared Data Association bezogen werden kann (siehe [IrDA09]).

- IrDA Link Access Protocol (IrLAP, Version 1.1)

  IrLAP setzt auf der physikalische Bitübertragungsschicht auf und ist für den Verbindungsaufbau zuständig. Es wird zwischen den zwei Betriebszuständen NDM (Normal Disconnected Mode) und NRM (Normal Response Mode) unterschieden. Im nicht verbundenen Modus (NDM) wird nach Signalen möglicher Kommunikationspartner gesucht und gleichzeitig ein Informationssignal mit 9.600 bit/s ausgesendet. Wird ein kommunikationsfähiges Gerät entdeckt, so wird zwischen den zwei Geräten eine Verbindung hergestellt (NRM). Daraufhin werden die jeweiligen Leistungsdaten der Geräte ausgetauscht. Eine Erweiterung des IrLAP um einen Fast-Connect-Modus zum schnelleren Aufbau von Datenverbindungen ist in Arbeit.

  IrLAP sichert die Verbindung mit Hilfe von Fehlerkorrektur (CRC-16 für Datenraten bis 1,152 Mbit/s und CRC-32 für höhere Datenraten) und erneutem Senden von Daten im Bedarfsfall.

  Details zum Verbindungsaufbau in IrDA können der IrDA-Spezifikation entnommen werden, die von der Infrared Data Association bezogen werden kann (siehe [IrDA09]).

- IrDA Link Management Protocol (IrLMP, Version 1.1)

  IrLMP setzt auf IrLAP auf und sorgt als nächst höhere Schicht für Mehrfachzugriff, Kanalbereitstellung für Dienste und das Informationsmanagement. Die Schicht ist unterteilt in Link Management Multiplexer (LM-MUX) und darauf aufsetzend den Link Management Information Access Service (LM-IAS).

Neben diesen verbindlichen Protokollschichten existieren optionale Protokolle, die anwendungsspezifisch den Datenaustausch steuern. So gibt es beispielsweise:

- Das Tiny Transport Protocol (TinyTP, Version 1.1) bietet aufsetzend auf LM-MUX verbesserte Flusskontrolle und Segmentierung.

- Das IrDA Infrared Communications Protocol (IrCOMM, Version 1.0) emuliert serielle RS-232-Schnittstellen (EIA/TIA-232-E) und parallele Centronics-Schnittstellen.

- Das IrDA Local Area Network Access Protocol (IrLAN, Version 1.0) erweitert das Link Management Protocol zur Einbindung von IrDA-Geräten in LANs

- Das IrDA Infrared Mobile Communications Protocol (IrMC, Version 1.1) definiert einen einfachen Datenaustausch zwischen mobilen Geräten, z.B. Visitenkarten, Notizen, Kalendereinträge und Aufgabenlisten; außerdem definiert es eine Anrufkontrolle und Audiodatenübertragung zwischen Mobiltelefonen und Notebooks

- Das IrDA Object Exchange Protocol (IrOBEX, Version 1.4) ermöglicht einen einfachen und schnellen Datenaustausch zwischen mobilen Geräten durch eine Push-and-Pull-Funktion, z.B. für Filetransfer, Bildübertragungen, Übertragung von Status- oder Diagnose-Informationen. IrOBEX ermöglicht auch Verbindungen über einen längeren Zeitraum mit mehreren Datenübertragungen und Idle-Zeiten.

- Die IrDA Infrared Transfer Picture Specification (IrTranP, Version 1.0) spezifiziert Bildübertragungen für digitale Kameras.

- IrDA Infrared for Wrist Watches (IrWW,Version 1.0) stellt ein zeitbasiertes Datenkommunikationsschema für Armbanduhren zur Verfügung.

- IrDA Financial Messaging Point and Pay ((IrFM, Version 1.0) ermöglicht ein digitales Zahlungssystem.

Eine Beschreibung der verschiedenen Protokolle findet sich unter [IrDA09].

J.1.1.2 IrDA Control

IrDA Control (Version 1.0) ist ein Protokoll zur Kommunikation von Peripheriegeräten wie Tastaturen, Mäusen, Joysticks oder Fernbedienungen mit zentralen Hosts, wie z.B. PCs und Fernsehgeräten.

Für diese Infrarotübertragung ist eine andere physikalische Bitübertragungsschicht definiert, mit Datenraten bis 75 kbit/s und Reichweiten bis zu 8 Metern, sodass IrDA Data und IrDA Control zueinander nicht kompatibel sind. Um den Bewegungsraum zwischen Host und Peripheriegerät nicht unnötig einzuschränken, ist in der Spezifikation ein Arbeitswinkel von ± 50° vom Host angegeben.

IrDA Control arbeitet mit einem Zeitschlitzverfahren, sodass ein Host mehrere Peripheriegeräte gleichzeitig ansteuern kann.

Die Protokollarchitektur von IrDA Control umfasst die drei verbindlichen Protokollschichten

- Physical Layer (PHY)
- Media Access Control (MAC)
- Logical Link Control (LLC)

J.1.2 Sicherheitsmechanismen

Im IrDA Standard sind keine Sicherheitsmechanismen gegen ein Mithören des Datenverkehrs spezifiziert. Die Daten werden nur auf Protokollebene gegen Übertragungsfehler mittels CRC gesichert. Sicherheitsmechanismen wie Authentisierung, kryptographischer Integritätsschutz und Verschlüsselung sind nicht vorhanden. Diese müssen auf Applikationsebene implementiert werden.

In gewissem Rahmen wird die Übertragung zumindest bei IrDA Data durch die sehr eingeschränkte Reichweite der Infrarotstrahlen und die benötigte Sichtverbindung geschützt. Bei IrDA Control ist dagegen durch den größeren Streuwinkel und die größere Reichweite mehr Vorsicht geboten.

J.1.3 Gefährdungen

Da im Protokoll keine Authentisierung vorgesehen ist, kann ein beliebiger Partner Daten über die IrDA-Schnittstelle an ein Gerät senden. So nimmt beispielsweise ein Mobiltelefon mit aktivierter IrDA-Schnittstelle SMS-Mitteilungen zum Versand an. An einen PDA oder Laptop können auch Programme über IrDA geschickt werden, die Schadfunktionen enthalten können.

Die Einschränkungen bezüglich des Mithörens der Übertragung durch die geringe Streubreite bei der IrDA-Data-Spezifikation gelten nicht für die IrDA-Control-Spezifikation. Dies ist insbesondere beim Einsatz von Tastaturen mit Infrarotschnittstelle, die auf die IrDA-Control-Spezifikation zurückgreift, zu beachten.

J.1.4 Schutzmaßnahmen

Beim Betrieb von Geräten mit IrDA-Schnittstelle ist darauf zu achten, dass diese nur im Bedarfsfall aktiviert wird: Da im Protokoll keine Authentisierung vorgesehen ist, kann ein beliebiger Partner Daten über die IrDA-Schnittstelle an ein Gerät senden. Außerdem belastet eine eingeschaltete IrDA-Schnittstelle die Batterie bzw. den Akku des mobilen Geräts zusätzlich.

Da die Kopplung nur in einem sehr eingeschränkten Bereich möglich ist, ist ein Mithören der Kommunikation meist ausgeschlossen. Das bestehende geringe Restrisiko aufgrund der Streustrahlung der IrDA-Komponenten kann durch den Einsatz von zusätzlichen Sicherheitsmechanismen (z.B. Authentisierung und Verschlüsselung auf Applikationsebene) oder den Ersatz von IrDA durch kabelbasierte Übertragung weiter minimiert werden.

J.1.5 Ausblick

Die Infrared Data Association hat Anfang 2009 die IrDA-Spezifikation Giga-IR verabschiedet, die den bisherigen Standard IrSimple ergänzt. Dieses Protokoll bietet eine Datenübertragungsrate von 1 Gbit/s. Die Übertragungszeit wird außerdem verkürzt, indem die Latenzzeit beim Verbindungsaufbau der Geräte, d.h. die Zeit bis zwei Geräte aufeinander eingestellt sind und die eigentliche Übertragung beginnen kann, optimiert wurde.

Giga-IR und IrSimple können laut IrDA über ein einfaches Update der bisherigen IrDA-Spezifikationen installiert werden und sind rückwärts kompatibel zu den bisherigen IrDA-Standards, sodass auch eine Kommunikation mit Geräten mit älteren IrDA-Spezifikationen möglich ist.

Durch diese Weiterentwicklung und vor allem die Aussicht auf eine Steigerung der Übertragungsrate auf 1 Gbit/s werden sicherlich in nächster Zeit neue IrDA-Applikationen entwickelt. Jedoch ist zeitgleich ein deutlicher Trend von IrDA-Endgeräten zu Bluetooth-Endgeräten zu erkennen.

J.2 Drahtlose Tastaturen, Mäuse und andere Eingabegeräte

J.2.1 Grundlagen und Funktionalität

Drahtlose Tastaturen und Mäuse sind Peripheriegeräte, die kabellos über Funk- oder selten über Infrarot-Schnittstellen mit einem Empfängermodul kommunizieren, das über einen COM-Port, eine PS2-Schnittstelle oder einen USB-Anschluss mit dem Rechner verbunden ist.

Da keine galvanische Verbindung zum Rechner besteht, müssen kabellose Eingabegeräte über eine eigene Spannungsversorgung in Form von Batterien oder Akkus verfügen. Für eine lange Betriebsdauer ist eine geringe Leistungsaufnahme dieser Geräte unumgänglich. Inzwischen sind Geräte (speziell Mäuse) verfügbar, die ihre Energie drahtlos durch Induktion erhalten. Das Gerät wird dazu einfach auf ein spezielles Pad gelegt, das seinerseits konventionell mit Strom versorgt wird.

Die Betriebsfrequenzen der Systeme liegen ausschließlich in lizenzfreien ISM-Bändern (Industrial, Scientific, and Medical). Funktastaturen und Funkmäuse senden entweder im 27-MHz-Bereich mit zwei Funkkanälen oder mittlerweile vermehrt auch im 2,4-GHz-Bereich mit 8 Funkkanälen.

Die Nutzreichweite der Funksysteme beträgt im 27-MHz-Bereich typischerweise 2 bis 5 Meter und im 2,4-GHz-Bereich ca.10 Meter. Diese genannten Reichweiten hängen extrem von den Umgebungsbedingungen ab, im Gegensatz zu Systemen auf Basis der Infrarot-Technik ist keine direkte Sichtverbindung zwischen Sender und Empfänger notwendig und Wände stellen kein unüberwindliches Hindernis dar. Andere im gleichen ISM-Band sendende Geräte wie z.B. CB-Funkgeräte, Funkspielzeug, funkgesteuerte Antriebe für Garagentore oder WLAN-Verbindungen im 2,4-GHz-Bereich können jedoch den Betrieb der Systeme empfindlich stören und die Reichweite reduzieren. Metallische Hindernisse (Stahlarmierungen, Stahlschränke und Ähnliches) können zum Versagen der Technik führen.

J.2.2 Sicherheitsmechanismen

Durch die erforderliche eigene Stromversorgung über Batterie bzw. Akku ist die Nutzungsdauer von kabellosen Eingabegeräten einschränkt. Wird ein solches Gerät zur Bedienung von Geräten mit hoher Verfügbarkeitsanforderung wie z.B. einem Server zur Überwachung von Netzwerkkomponenten benutzt, so könnte es im Falle einer notwendigen schnellen Bedienung des Geräts bei gleichzeitiger Unterbrechung der Eingabefunktionalität zu folgenschweren Ausfällen kommen.

Ein wesentliches Problem der funkbasierten Eingabegeräte ist die mangelnde Abhörsicherheit. Die ausgesendeten Funksignale können von Dritten empfangen und aufgezeichnet werden. Sind diese Funksignale nicht sicher verschlüsselt, können diese Daten leicht ausgewertet werden. Es gibt auf dem Markt zahlreiche Funktastatursysteme, welche die aus den Tastenanschlägen resultierenden Signale völlig unverschlüsselt – und damit für Dritte abhörbar – übertragen. Hier reicht häufig schon ein zweiter Empfänger vom selben Hersteller aus, um die empfangenen Signale auf einem anderen Rechner sichtbar zu machen.

Hersteller von Funk-Anwendungen geben zur Sicherstellung der garantierten Reichweite Entfernungen an, in denen die Datenübertragung ihrer Geräte fehlerlos funktioniert. Diese Funktionsreichweite ist aber im Falle von Geräten, die nur mit billiger Empfangstechnik ausgestattet sind, meist kleiner als die Entfernung, in der die ausgesendeten Signale mit Hilfe von Richtantennen und hochwertiger Empfängerelektronik noch empfangen, aufgezeichnet und ausgewertet werden können. Unter idealen Bedingungen und mit optimaler Empfängerelektronik können die Signale bis zur doppelten Entfernung noch empfangen werden. Eine Abhörgefährdung in einer größeren Entfernung als die Funktionsreich-

weite kann daher nicht ausgeschlossen werden und stellt insbesondere bei Nutzung des 2,4-GHz-Bereiches mit Funktionsreichweiten von 10 m und Signalreichweiten von bis zu 20 m eine eklatante Gefährdung dar.

Systeme, die auf Basis der Infrarot-Technik kommunizieren, verwenden meistens den IrDA-Standard (siehe Kapitel J.1), der keinerlei Sicherheitsmechanismen unterstützt. Hier wird die benötigte Sichtverbindung zwischen Sender und Empfänger sowie die begrenzte Reichweite als Sicherheitsmerkmal genannt. Das Sicherheitsniveau solcher IrDa-Systeme liegt aufgrund der möglichen Streustrahlung trotzdem unter dem der kabelgebundenen Eingabegeräte.

Mehrere Hersteller bieten funkbasierte Produkte mit proprietären Sicherheitslösungen an. Über die Sicherheit solcher Lösungen kann keine positive Aussage getroffen werden, da die eingesetzten Algorithmen in der Regel von den Herstellern unter Verschluss gehalten werden. Die Qualität solcher Algorithmen scheint jedoch nicht den derzeit üblichen Sicherheitsanforderungen zu entsprechen. Mittlerweile wurde die Kompromittierung von einigen proprietären Algorithmen veröffentlicht. Aufgrund eines extrem einfachen Verschlüsselungsalgorithmus können diese Eingabegeräte unter Nutzung der veröffentlichten Software „von jedermann“ abgehört werden.

Damit baugleiche Geräte nebeneinander betrieben werden können, haben die meisten Hersteller ihre Geräte mit verschiedenen Erkennungsnummern (IDs) ausgerüstet. Hierbei werden verschiedene Prinzipien verwendet, z.B. wird aus einem Pool von IDs ein bestimmter Wert fest für ein Gerät vergeben oder es wird bei einem Batteriewechsel die ID durch die Software erneut zufällig bestimmt.

Auf dem Markt sind vermehrt Produkte erhältlich, die mit Bluetooth-Funktechnik kommunizieren. Bei korrekter Implementierung und Konfiguration der Bluetooth-Sicherheitsmerkmale bieten diese im Allgemeinen einen höheren Schutz als Funksysteme mit proprietärer Technik. Eine Zusammenstellung der Gefährdungen und mögliche Sicherheitsmaßnahmen zum Thema Bluetooth findet man in Kapitel B. Bluetooth.

Abschließend sei erwähnt, dass bei Tastaturen durch die elektromagnetische Abstrahlung der Tastaturmatrix und des Verbindungskabels eine Abhörgefährdung besteht. Dies gilt auch für kabellose Tastaturen. Im Allgemeinen ist die Abhörgefährdung bei kabelgebundenen Tastaturen jedoch wesentlich geringer als bei kabellosen Eingabegeräten.

J.2.3 Ausblick

In näherer Zukunft wird sich die Nutzung von drahtlosen Tastaturen und Mäusen weiter massiv ausbreiten. Auch in sensiblen Bereichen hält die Nutzung von drahtlosen Eingabegeräten verstärkt Einzug, wodurch die aufgezeigten Gefährdungen durch Reichweiten von bis zu ungefähr 10 m eine erhöhte Brisanz erhalten. Jedoch ist ein deutlicher Trend zu Produkten, die auf der Bluetooth-Funktechnik basieren und damit einen höheren Schutz bieten, zu erkennen. Die potenzielle Nutzung von Eingabegeräten, die auf UWB-Funksystemen (Ultra Wideband) basieren, ist zum jetzigen Zeitpunkt unklar, ein Trend in diese Richtung ist nicht erkennbar.

J.3 Fazit

Durch die eingeschränkte Übertragungsreichweite und den relativ geringen Streuwinkel ist bei Infrarotübertragungen immer ein gewisser Grundschutz gegeben. Allerdings muss bei entsprechend höheren Sicherheitsanforderungen auf Sicherheitsmaßnahmen wie Authentisierung, Integritätssicherung und Verschlüsselung auf Applikationsebene zurückgegriffen werden, da die IrDA-Protokolle selbst keine Sicherheitsmaßnahmen bieten. Ist eine solche Sicherung auf Applikationsebene nicht möglich, muss gegebenenfalls auf den Einsatz von IrDA verzichtet werden.

Für die drahtlose Anbindung von Eingabegeräten wie Tastaturen und Mäusen wurde IrDA durch Funktechniken abgelöst.

Zahlreiche Funktastaturen und Funkmäuse senden ihre Informationen ohne Sicherheitsvorkehrungen zu den Rechnern. Ohne großen Aufwand können diese Informationen von Dritten mitgelesen oder gegebenenfalls sogar manipuliert werden. Vom Einsatz solcher Systeme ist aus Sicht der IT-Sicherheit generell abzuraten.

Für Systeme mit proprietären Sicherheitsmaßnahmen, die kein Sicherheitszertifikat aufweisen, geht der Nutzer das Risiko ein, dass die nicht evaluierte Lösung des Herstellers nur eine minimale Sicherheit bietet, die aber bei Weitem nicht ausreicht, um seine Daten effektiv zu schützen. Für einzelne Produkte ist im Internet bereits Software zur Abhörung veröffentlicht.

Drahtlose Systeme, die auf Standards wie Bluetooth basieren und bei denen die Sicherheitsmechanismen korrekt implementiert und aktiviert worden sind, können einen im Vergleich höheren Schutz bieten.

Bei Einsatz von Geräten mit einer Stromversorgung über Batterie bzw. Akku kann die Nutzungsdauer von kabellosen Eingabegeräten eingeschränkt werden. Wird ein solches Gerät zur Bedienung von Geräten mit hoher Verfügbarkeitsanforderung wie z.B. einem Server zur Überwachung von Netzwerkkomponenten benutzt, so könnte es im Falle einer notwendigen schnellen Bedienung des Geräts bei gleichzeitiger Unterbrechung der Eingabefunktionalität zu folgenschweren Ausfällen kommen.

Der Einsatz von Eingabegeräten mit eigener Stromversorgung über Batterie oder Akku sollte an Geräten, die hohen Verfügbarkeitsanforderungen unterliegen und an denen nur unregelmäßig Eingaben per Tastatur oder Maus vorgenommen werden, vermieden werden.

In sensiblen Bereichen sollte man grundsätzlich keine Funktastaturen, Funkmäuse und Infrarot-Produkte einsetzen.

J.4 Literatur und Links

[IrDA09] Homepage der Infrared Data Association, http://www.irda.org

J.5 Abkürzungen

CB(-Funk)	Citizens' Band (Radio)
CRC	Cyclic Redundancy Check
FIR	Fast-Infrared
ID	Identification, Erkennungsnummer
IR	Infrared
IrCOMM	IrDA Infrared Communications Protocol
IrDA	Infrared Data Association
IrFM	IrDA Financial Messaging
IrLAN	IrDA Local Area Network Access Protocol
IrLAP	IrDA Link Access Protocol
IrLMP	IrDA Link Management Protocol
IrMC	IrDA Infrared Mobile Communications Protocol
IrOBEX	IrDA Object Exchange Protocol
IrPHY	IrDA Physikalische Bitübertragungsschicht
IrTran-P	IrDA Infrared Transfer Picture Specification
IrWW	IrDA Infrared for Wrist Watches
ISM	Industrial, Scientific, and Medical
LAN	Local Area Network
LLC	Logical Link Control
LM-IAS	Link Management Information Access Service
LM-MUX	Link Management Multiplexer
MAC	Media Access Control
MIR	Mid-Infrared
NDM	Normal Disconnected Mode
NRM	Normal Response Mode
PC	Personal Computer
PDA	Personal Digital Assistant
PHY	Physical Layer
SIR	Serial Infrared
SMS	Short Message Service
TinyTP	Tiny Transport Protocol
TP	Transport Protocol
USB	Universal Serial Bus
UWB	Ultra Wideband
VFIR	Very Fast Infrared
WLAN	Wireless LAN

J.6 Glossar

Cyclic Redundancy Check (CRC)

Prüfsumme über die zu übertragenden Daten, die in der Nachricht mitgeschickt wird und es dem Empfänger gestattet, Bitfehler, die auf dem Kommunikationskanal entstanden sind, zu erkennen.

Infrared Data Association (IrDA)

Non-Profit-Organisation, die Spezifikationen für Infrarot-Schnittstellen erarbeitet; wird auch als Synonym für das von der Infrared Data Association spezifizierte IrDA Data Protocol verwendet.

IrDA Link Access Protocol (IrLAP)

Für den Verbindungsaufbau zuständige Protokollschicht von IrDA Data

IrDA Link Management Protocol (IrLMP)

Protokollschicht von IrDA Data, die für Mehrfachzugriff, Kanalbereitstellung für Dienste und das Informationsmanagement zuständig ist. IrLMP besteht aus den beiden Komponenten LM-MUX und LM-IAS.

Link Management Information Service (LM-IAS)

Der Link Management Information Service ist der Directory Service eines IrDA-Systems. LM-IAS stellt für ein Applikationselement (Application Entity) die notwendigen Mittel zur Verfügung, um ein entsprechendes Gegenstück (Peer Entity) zu identifizieren und zu lokalisieren.

Link Management Multiplexer (LM-MUX)

Der Link Management Multiplexer gestattet die simultane Nutzung der IrLAP-Verbindung durch mehrere Applikationselemente (Application Entity).