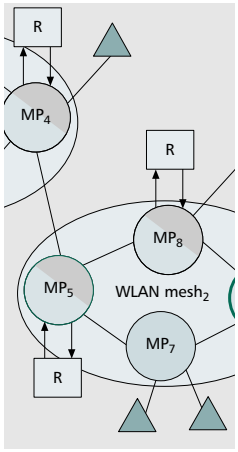
MESH WLAN NETWORKS: CONCEPT AND SYSTEM DESIGN

STEFANO M. FACCIN, NOKIA TECHNOLOGY PLATFORMS
CARL WIJTING AND JARKKO KNECKT, NOKIA RESEARCH CENTER
AMEYA DAMLE, SOUTHERN METHODIST UNIVERSITY



A new paradigm is becoming more and more popular: peer-to-peer communications, where wireless nodes communicate with each other and create ad hoc mesh networks independently of the presence of any wireless infrastructure.

ABSTRACT

In recent years WLAN technology has become the common wireless access technology for mobile computing. Additional to infrastructure access to WLAN networks, peer-to-peer and mesh networking are currently gaining in interest. Mesh networking techniques using WLAN are being standardized in IEEE 802.11s. This article describes use cases, the main technical issues, and a set of potential solutions for mesh network development. Furthermore, an overview of the standardization activities in IEEE 802.11s is presented. The key technical aspects of mesh networks identifed are topology creation, routing, medium access control, security, quality of service, and power efficiency.

INTRODUCTION

Traditional wireless networks are based on the presence of an infrastructure providing wireless access for network connectivity to wireless terminals. This paradigm has reigned for many years in cellular networks, enterprise networks, and a variety of public/private networks. However, a new paradigm is becoming more and more popular: peer-to-peer communications, where wireless nodes communicate with each other and create ad hoc mesh networks independently of the presence of any wireless infrastructure.

The rapid diffusion of IEEE 802.11 (WLAN) access and the increasing demand for WLAN coverage is driving the installation of a very large number of access points (APs). Although the cost of APs is traditionally not very high (in particular, compared to the cost of cellular equipment), the deployment of APs requires connecting the APs through a wired connection (traditionally Ethernet), and this introduces complexity and high costs for deployment in certain locations. Moreover, due to the limited range of coverage of 802.11, APs may need to be moved often in order to accommodate the increasing traffic demands. Therefore, the deployment of APs by interconnecting them through a wireless link, and specifically the creation of mesh networks based on 802.11, has become an indispensable technique for the growth of next-generation wireless networks.

The telecommunication industry has kicked off a series of activities for developing new and efficient solutions for mesh networks. This article describes the use cases, main technical issues, and a set of potential solutions for mesh network development. In particular, we address the efforts undertaken in IEEE 802.11 Task Group s (TGs), which is developing mesh WLAN networks that perform routing at link layer (layer 2).

After an introduction on layer 2 ad hoc networks, the article addresses the key functionality of mesh networks, including routing, security, quality of service (QoS), and power efficiency, providing the reader with an overview of the key aspects of mesh networks.

LAYER 2 MESH NETWORKS

This section describes the main drivers for the development of 802.11 mesh networks and the ongoing activities in IEEE related to mesh networks, and addresses use cases for mesh networks.

MESHED WLAN NETWORKS: IEEE 802.11S

The 802.11 working group in IEEE [1] has recently started working on mesh networks in the task group identified as TGs, which will produce the 802.11s standard for mesh networks. The main target of TGs is to investigate and design mesh networks consisting of different WLAN devices performing routing at link layer. TGs is currently working on the presentation and selection of different proposals, with the target of having one joint proposal during 2006. The standard is aimed for approval in 2008.

Specifically, 802.11 TGs defines an extended service set (ESS) mesh (referred to here as a mesh network) as a collection of WLAN devices interconnected with wireless links that enable automatic topology learning and dynamic path configuration. 802.11 mesh networks will be based on extensions to the IEEE 802.11 MAC standard, based on the definition of a mesh net-

1536-1284/06/$20.00 © 2006 IEEE

work architecture and new protocol mechanisms. The architecture will provide an IEEE 802.11 Wireless Distribution System (DS) that supports both broadcast/multicast and unicast delivery at the MAC layer using radio-aware metrics over self-configuring multihop topologies, thus providing the functional equivalent of a wired DS. In 802.11 the target configuration consists of at least 32 participating devices; larger configurations will also be considered by the standard.

Use Cases

This section introduces different use cases for WLAN networks. The first section focuses on access network scenarios, including 'traditional' WLAN access (ad hoc and infrastructure mode) and extended use cases such as an integrated mode of operation between these modes. The second section introduces the use cases for fully meshed networks, enabling multihop connections between different mesh APs.

Access Network Use Cases — The *Infrastructure Network* use case refers to current, widely used deployment of 802.11. It includes an AP in control of the network, that is, all communication between stations or with the backbone goes via a mesh AP (MAP). Figure 1a shows a typical example of infrastructure mode usage.

For a station, the main aim in this scenario is to configure and establish IP connectivity through a WLAN infrastructure network. Upon entering the coverage area of a MAP, the station scans for beacons; after receiving beacons, it associates with the MAP. Generally, the MAP is a layer 2 device only and a Dynamic Host Configuration Protocol (DHCP) server located deeper inside the service provider's network provides the station's IP address enabling IP connectivity; alternatively, some implementations have a DHCP server running on the MAP. Once connected, all packets destined to other stations in the network or to the Internet are routed through the MAP. Hence, a specific routing algorithm is not required in this scenario. If the station moves into the coverage area of another MAP, then the station needs to reassociate with the new AP. Security in the communication is provided by the new 802.11i standard, while the station and the MAP follow the 802.11e standard to provide quality of service (QoS). Stations connect to the AP using only one channel that is preconfigured by the MAP.

An *Ad Hoc Network* is a network that is formed without the presence of any AP and as a result of dynamic interconnection of stations in a given area. Establishment of IP connectivity using point-to-point links is the main objective in the ad hoc network use case (Fig. 1b). In ad hoc networks the topology is dynamic; therefore, distributed algorithms for beacon transmission are adopted. A station attempting to join an ad hoc network first scans for transmitted beacon messages. If beacons are received, the station will join the network. If the station does not receive a beacon message within a given time, it will initiate a new ad hoc network and start sending beacon messages. Contrary to the infrastructure use case, there is no central controller; therefore, IP addresses are typically applied statically.

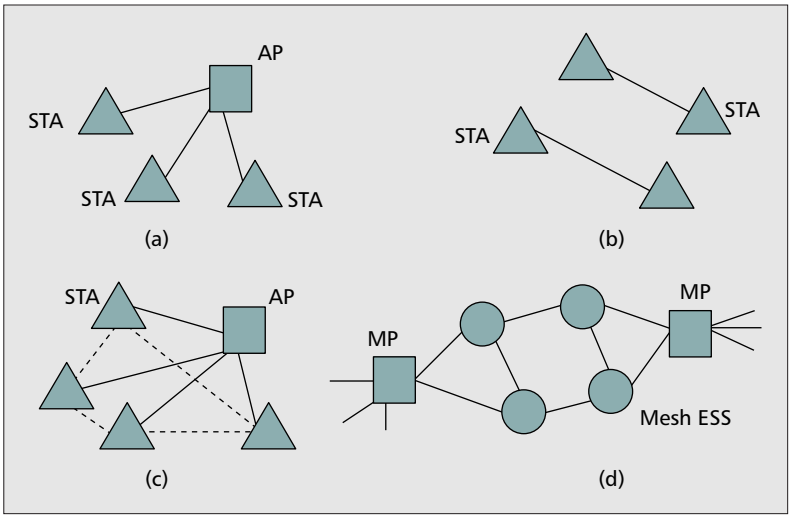


Figure 1. *Illustration of the use cases: a) infrastructure; b) ad hoc; c) mixed mode; d) mesh network.*

Security is traditionally only provided at network layer or above, while 802.11e mechanisms control the QoS mechanisms in the data communication.

The *Mixed Mode* use case allows stations to communicate directly among each other, even if some of them are connected to an AP. Compared to ad hoc networks, this mode allows connectivity to networks beyond the border of the ad hoc network (e.g., the Internet). The Mixed Mode scenario can therefore reap the benefits of both ad hoc and infrastructure modes of operation. Figure 1c illustrates this operation, with point-to-point links between the stations, as well communication via an AP [2].

Several implementations for these scenarios are proposed which try to serve the same objective of configuring and establishing IP connectivity. Some of the options that exist for achieving this goal are as follows: AP-controlled switching between the two modes, dual-mode stack, and an integrated MAC layer.

Use Cases for Mesh Networks — The main purpose of this type of scenario is to configure and establish IP connectivity with a wireless meshed DS. This is achieved through a WLAN network with wireless interconnected mesh points (MPs). Figure 1d depicts the topology for this type of networks. Mesh Points can be either the abovementioned mesh APs (MAPs) or stations with extended functionality calleds mesh STAs (MSTAs).

Within mesh networks, two initialization processes can be distinguished: firstly, a station associating with a MAP and, secondly, a MAP associating with a neighboring node to join the mesh network. The association of a station and MAP is performed in the traditional 802.11 manner. For the association with a neighboring MP, a particular MP needs to obtain an IP address, and perform scanning, neighbor discovery, authentication of the MP, and possibly negotiate channels. It has to be noted that the meaning of the term "association" is extended with respect to the traditional IEEE 802.11 term.

	Static	Low mobility	High mobility
Discovery	Passive/active	Passive/active	Active
Routing	Infrequent updates High steady state performance	Infrequent updates High steady state performance	Frequent updates Low overhead
Security	Infrequent re-authentications, mainly for refresh	Infrequent re-authentications	Frequent re-authentications, mainly due to mobility
QoS	Slow/static mechanisms Long-term reservations	Slow mechanisms	Fast/dynamic mechanisms
Power awareness	Mainly wired connected devices	Mixed devices, wired connected dominant	Many battery-driven devices

Table 1. *Comparison of meshed networking for different types of mobility.*

The resulting topology may involve multihop routing, which will be done at layer 2, based on MAC addresses. Depending on the movement speed of the MPs, the mobility can be classified into three categories of increasing speed: static, low mobility, and high mobility (Table 1). Therefore, the routing algorithm employed over such a network should be able to take into account any of these three cases and their characteristics. In case of low mobility, the steady-state performance should be optimized and incidental updates (e.g., for route discovery) could consume more resources, whereas in the high mobility case, route maintenance and updating speed are important factors.

Security should also be dependent on layer 2 (L2), and should take mobility into consideration. With a static topology, very infrequent authentication can be satisfactory, but with nodes having high mobility very frequent authentication is necessary [3]. QoS should be provided on a link-to-link basis, with an additional mechanism to reserve resources for data flows over multiple hops.

Mesh networks could have topologies ranging in dimension from small to large. Self-configurability is an important feature; however, in the case of smaller networks, the mesh network can also be a managed network.

Instances of Mesh Networks

This section describes two topologies that are used in this article to discuss the main technical aspects of mesh networks. Figure 2 depicts the logical components in a set of interconnected mesh networks, where some MPs act as regular MAPs, whereas others have augmented functionality. A gateway MP performs routing at link layer (L2) or network layer (L3) between interconnected mesh networks, whereas a mesh portal is traditionally an AP connected to the wired DS.

Mesh networks may have a connection to the Internet through a wired DS using a wireless connection between MAPs or STAs, and are referred to as connected mesh networks. Figure 3a shows a typical topology of a mesh network where some MPS are connected to the wired DS, and are called mesh portals. Specifically, Fig. 3a shows a mesh network where MPs are all MAPs, whereas the stations are connected as leaf nodes. In this specific example, the entire mesh network would belong to one IP subnet, as traditionally happens for all the entities connected through one DS.

Figure 3b shows a typical topology of a "free-standing" mesh network, that is, a mesh network where MPs are either MAPs, STAs, or MSTAs, but none of them is connected to the Internet though a wired DS. Such networks are also referred to as meshed ad hoc networks.

Key Functionality of Mesh Networks

This section describes the various key functionality of mesh networks.

Mesh Topology Creation

Upon activation, MPs need to discover mesh networks that are potentially already present, so that they can associate with them. If no networks are detected, the MP needs to be capable of initiating a new one. An important feature from a usability perspective is auto-configuration, that is, the mesh network mechanisms should operate without the need for user intervention.

Two distinctive approaches can be taken toward network discovery: a *passive* approach and an active approach. In the passive approach the network discovery is based on the reception of beacon messages, whereas in the active approach probing messages are sent. The active approach results generally in a shorter response time, thus allowing fast discovery of the topology, whereas the passive approach requires listening to all possible channels, thus leading to a longer discovery process.

The discovery phase, based on initial active or passive scanning, results in basic connectivity between the nodes in the network. After discovering the basic connectivity in the network topology, MPs will form the mesh ESS network by associating with the neighboring nodes. Since all nodes within a mesh ESS operate on the same channel, the number of nodes that can be serviced by one ESS is limited. If, after identifying and associating all nodes within the mesh, the

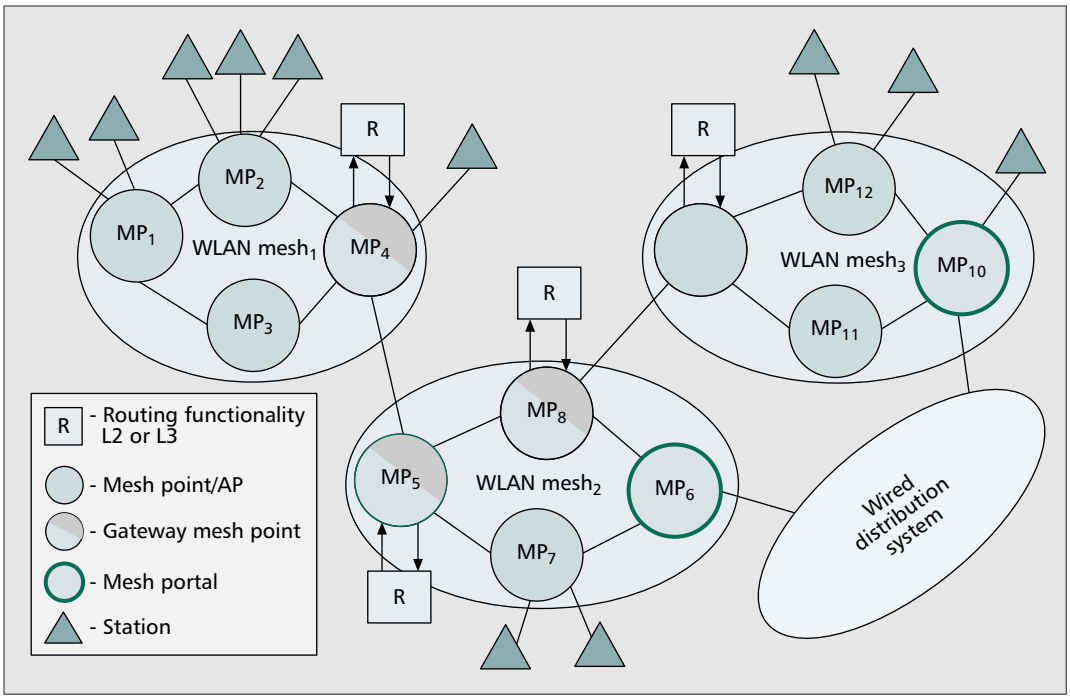


Figure 2. *Functional components of mesh networks.*

The discovery phase, based on initial active or passive scanning, results in basic connectivity between the nodes in the network. After discovering the basic connectivity in the network topology, MPs will form the mesh ESS network by associating with the neighboring nodes.

mesh consists of a large number of nodes, it may be divided into smaller clusters with a limited number of nodes (smaller mesh ESS networks) operating at different channels. This requires some nodes to perform a gateway function interconnecting these smaller ESS mesh networks.

After the initial discovery phase, beacon messages remain to be transmitted periodically and are used for topology maintenance. Based upon received beacon messages, the nodes obtain information about the current state of the topology so that they can refresh their connectivity associations and update them when necessary (for example, due to mobility).

Routing

In an IEEE 802.11 mesh network, routing is essential to allow communication between MPs. This section analyses the issues related to routing in IEEE 802.11 mesh networks and discusses some potential solutions.

IP Layer Routing Protocols in Wireless Ad Hoc Networks — The IETF MANET working group concentrates on standardizing IP (layer 3) routing protocol functionality suitable for wireless ad hoc networks.

Two types of protocols [4] are considered:

- Proactive routing protocols, where nodes periodically exchange routing tables and maintain the entire topology of the network, with each node knowing the shortest path to each node in the network. Destination Sequenced Distance Vector (DSDV) and Optimized Link State Routing (OLSR) are commonly used proactive routing algorithms [3].
- Reactive routing protocol, where routes are established on-demand. Dynamic Source Routing (DSR) and Ad Hoc On-Demand Vector (AODV) [3] are the most commonly used reactive protocols.

Proactive algorithms are useful in small networks because the routing overhead in maintaining the routes is low, and since the network size is small, the memory requirement to store the routing table is also low, thus minimizing the delay due to routing table lookups. On the contrary, reactive algorithms are preferable when the network size is large, since the need to store routes towards all the destinations would impose considerable memory requirement and cause lookup delays. As the routes are created on demand, reactive algorithms are also traditionally preferred for mobile scenarios.

MAC-Layer Routing vs. IP Layer Routing — According to MANET protocols, when a node wants to send data to a destination, it refers to an existing route in its routing table and forwards the packet to the next hop for delivery to the destination. Finding and maintaining routes is a function of the specific routing protocol used. Assuming that a route towards the destination exists, the protocol stack in the node consults the routing table to find the IP address of the next hop, and obtains the MAC address of the next hop through the traditional Address Resolution Protocol (ARP). The node then sends a MAC data frame to the next hop that in turns performs routing for the packet.

Layer 3 routing mechanisms work well when all the intermediate nodes are stations and therefore have IP layer routing functionality. In mesh networks, these mechanisms would not be suitable since mesh networks can be composed of both MSTAs and MAPs. APs are traditionally purely Layer 2 devices, which are incapable of decoding the IP packet, and adding layer 3 functionality to an AP is typically considered not acceptable. The same can be expected of MAPs. Therefore, the layer 3 routing techniques proposed by MANET cannot be directly applied to

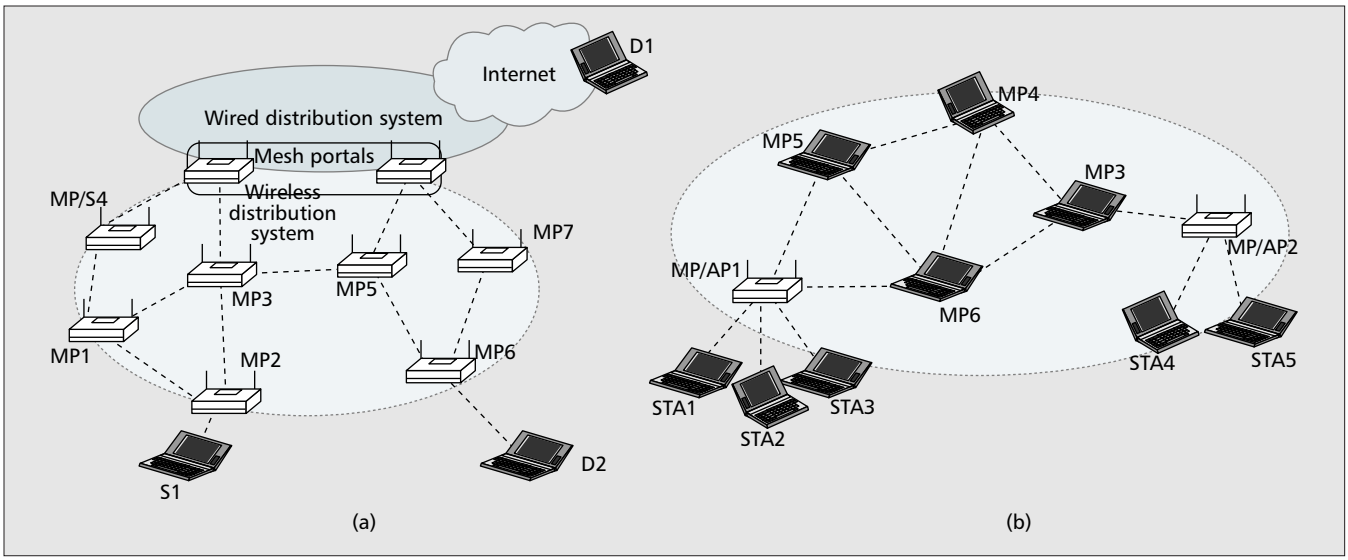


Figure 3. *Examples of mesh network topologies: a) 802.11 connected mesh; b) 802.11 mesh ad hoc.*

mesh networks. Moreover, the routing defined in MANET is done based on a single simple metric of hop count, i.e. a station chooses the path to the destination having the minimum number of hops. In mesh networks, a shortest path metric is not at all useful. In fact, the shortest path may be overloaded from a point of view of wireless bandwidth, or may not satisfy the QoS, latency or security requirements for a given communication. The metric for mesh networks needs to be aware of link conditions, power efficiency factors and other link level aspects in order to route the data to the destination. One may think of making these parameters available to layer 3 routing protocols for use in the path metrics. However, in order to avoid inefficiencies and duplication of functionality, this would require a tight integration of layer 3 and layer 2 functionality, which is difficult to achieve in real-life products and to standardize since, for example, the integration matches the scope of neither IETF nor IEEE 802.11).

Hence, *layer 2 routing* based on MAC addresses is the main solution considered for 802.11 mesh networks. However, routing solutions defined at layer 2 borrow concepts from MANET.

Routing Protocols for Mesh Networks — Routing for mesh networks is performed at the link layer (layer 2) and is based on the following logical scheme:

- Having the destination IP address to which the data has to be sent, the source STA obtains the MAC address of the destination through ARP and looks up the MAC layer routing table to verify if a route exists or needs to be created.
- If a route is known, data frames are forwarded according to the existing route towards the next hop. If a route does not exist, a new route is created.

The size of mesh networks and the level of mobility depend upon the usage scenario. Mesh networks can be very dynamic networks (i.e., MPs are being added/removed frequently). Therefore, the use of any single routing protocol, either proactive or reactive, would not be efficient. A *hybrid protocol* can be used to overcome this issue, where the protocol would be proactive towards MPs in the neighborhood, and reactive towards MPs far away. Alternatively, multiple algorithms can be used simultaneously, where the mesh network is segmented into clusters. Within each cluster a proactive algorithm is used, whereas between clusters a reactive algorithm is used.

As an alternative, mesh networks can use *adaptive routing protocols*, whose behavior is modified dynamically by monitoring the change in the network parameters (e.g., size, dynamicity, mobility, etc.). This would allow using proactive algorithms when a network is contained in size and has low mobility, and adopt reactive algorithms when a network grows in size and/or becomes very mobile. Moreover, the protocol modifies its behavior in real time as the network changes its topology.

Metrics for Mesh Networks Routing — An essential component of the routing solution is the use of metrics to determine the preferred route between source and destination. A conventional metric used to determine the minimum distance between two nodes is the 'hop count'; however, in order to provide efficient routing and support complex mesh networks with different QoS, bandwidth, latency, and security requirements, a *multidimensional metric* capable to capture link conditions must be used. The routing algorithm used to discover routes would include calculation of a multidimensional metric that may include the QoS parameters, power efficiency, security of wireless links and intermediate node, reliability, and so forth. A QoS-aware routing algorithm is needed, for example, to support demanding real-time applications such as voice and video. Security awareness that considers the security of the links and of intermediate nodes is needed, for example, when the use case and applications require a high level of security. Power efficiency is instead

a must when considering mobile devices that rely on battery power.

The multidimensional metric will be used differently from network to network, depending on the specific use case and applications requirements.

Security in Mesh Networks

Threats in Mesh Networks — Security is a key issue in the design of mesh networks. With a wireless DS, it is required that the end user be assured of end-to-end security. Mesh networks can easily be tampered with by a variety of attacks. Security measures should be taken to avoid these threats and make the communication in mesh network reliable.

Confidentiality and integrity: it is essential that data sent by an MP cannot be eavesdropped or modified. In mesh networks, the presence of wireless links and intermediate MPs that can be actual stations requires that encryption and integrity-protection mechanisms are in place both to stop the threats to the radio links and intermediate MPs from eavesdropping and to stop modification of the data being transmitted.

Unauthorized access: only MPs that can be successfully authenticated shall be allowed to join a mesh network. In connected mesh networks (e.g., Fig. 3), authentication can take place due to the interconnection with the wired DS, as in traditional 802.11 networks in infrastructure mode. However, for meshed ad hoc networks no "centralized" authentication entity exists; therefore, alternative solutions must be in place to allow authentication between MPs.

Denial of service (DoS) attacks: in a multihop ad hoc network, a traditional DoS attack is caused by an intermediate node selectively dropping traffic frames, thus causing one or more MPs to not receive any traffic from one or more sources. A DoS attack characteristic of mesh networks is caused by routing misbehavior of an MP, for example, as in the "black hole" [5] where the malicious MP tampers with the routing messages in a network, or spoofs the MAC address of an MP into claiming a "fake" shortest path so as to get all the packets routed to itself, without any intention to route the packets to destination and effectively denying the destination MP from receiving any packets from the source MP. It has to be noted that any MP that authenticated correctly when joining the network may suddenly start misbehaving and causing DoS. Such scenarios are traditionally very difficult to discover and prevent.

The main target of security solutions in mesh networks is to counter the threats described above. Authentication and encryption are described further in the following subsections.

Authentication in Mesh Networks — To prevent unauthorized users from accessing the mesh networks, a robust authentication mechanism must be in place. Each station joining a mesh network must be able to authenticate through 802.11i mechanisms. A main requirement in mesh networks is to minimize modifications to the station's 802.11i functionality in mesh networks. This is achieved by having the station joining the network act as the 802.11i supplicant, and having the MP the station is connecting to act as the authenticator (Figs. 4a and 4b). In connected mesh networks, IEEE 802.1x is used between the station and the MAP, and the Extensible Authentication Protocol (EAP) carries authentication signaling towards the backend infrastructure. In meshed ad hoc networks, the lack of a backend infrastructure requires a distributed approach to authentication in which each MP may have the ability to authenticate stations, or a centralized approach in which one MP is in charge of acting as authentication server for the network. In both cases, authentication is based on security associations distributed with mechanisms outside the scope of IEEE 802.11 (e.g., nodes belonging to an organization may have preconfigured security associations).

Encryption in Mesh Networks — To provide a viable encryption solution while minimizing complexity and overhead, a two-level solution is proposed (Figs. 4c and 4d). At the first level, hop-by-hop encryption is used, in which a source station encrypts traffic at the MAC level using the 802.11i key it shares with an AP. The AP in turns decrypts the traffic and reencrypts is using the 802.11i group key, then forwards it to the next MP. When the traffic reaches the last MP before the destination station, the MP decrypts the traffic and reencrypts it using the 802.11i key the MP shares with the station. In this way, intermediate MPs are not required to decrypt/reencrypt forwarded traffic. With respect to traditional 802.11i, the idea is that all the MPs in a mesh network would share the same group key, which is generated and distributed through a variety of possible mechanisms.

The second level is introduced to avoid intermediate MPs being able to eavesdrop on or tamper with the data (e.g., in particular when the MP is a station). The second level is based either on STA-STA L3 security (outside the scope of IEEE 802.11), or on the introduction of a novel second level of STA-STA encryption at the MAC layer.

Quality of Service

Different applications and traffic types have different requirements in terms of the service level provided by the network. The requirements are met by using QoS mechanisms that aim at providing prioritized access to some traffic types, as well as guaranteed performance bounds for parameters such as packet loss, throughput, delay, and jitter [6].

In the context of mesh networks, two main QoS issues can be identified. Firstly, offering QoS in the presence of a mix of access network traffic and backbone traffic (Fig. 5) requires call admission control (CAC) and a mechanism for differentiating these two types of traffic in order to ensure that both obtain the appropriate service level. Secondly, offering QoS guarantees over multiple hops requires a mechanism above traditional L2 in order to make end-to-end flow-based assignments and guarantee that the allocated service assignments can be granted.

CAC is performed at two interfaces in the

Security is a key issue in the design of mesh networks. Mesh networks can easily be tampered with by a variety of attacks. Security measures should be taken to avoid these threats and make the communication in mesh network reliable.

system. Firstly, it is applied on stations associating with MPs to fairly balance the traffic entering the system and the traffic forwarded further into the system via the mesh network. Secondly, it is applied between MPs to control the system load in the backbone. CAC first determines the available capacity to accept the node based on the ratio between access and backbone traffic, then it accepts traffic flows based on the traffic type (single-hop or multihop).

In mesh networks, the MAC layer may ensure that a minimum guaranteed service level for the backbone inter-MP traffic is available, for example, by means of different interframe spaces for access and backbone traffic, or by means of service-differentiation mechanisms from IEEE 802.11e using enhanced distributed channel access (EDCA). Alternatively, the MP may apply time division of the bandwidth assigned to access and backbone traffic. Further, MPs may perform packet aggregation and instantaneous forwarding of the incoming traffic, based on the service type (e.g., packets with high throughput but loose delay requirements may be aggegated, whereas short, delay-sensitive voice-over-IP packets are forwarded instantaneously with low delay).

In order to support end-to-end QoS guarantees, *flow control* is introduced so that QoS levels can be mapped between the access and backbone traffic. Flow control and CAC are tightly linked, with the former being based on the use of flow identifiers and the latter determining service-level requirements based on packet headers. CAC servers running in different MPs along the path maintain a list of active flows and their service requirements, thus creating service-awareness multiple-hops. As an alternative to the use of packet headers, 802.11e TSPEC signaling may also be used for exchanging the QoS requirements, thus allowing for more precise reservations.

When certain MPs are highly loaded with traffic, *load balancing* can be used to relieve the loaded MPs and move traffic to less loaded MPs, and to avoid delaying traffic and dropping frames due to congestion. Mesh routing mechanisms may be used to optimize the path, for example, by using metrics related to system load.

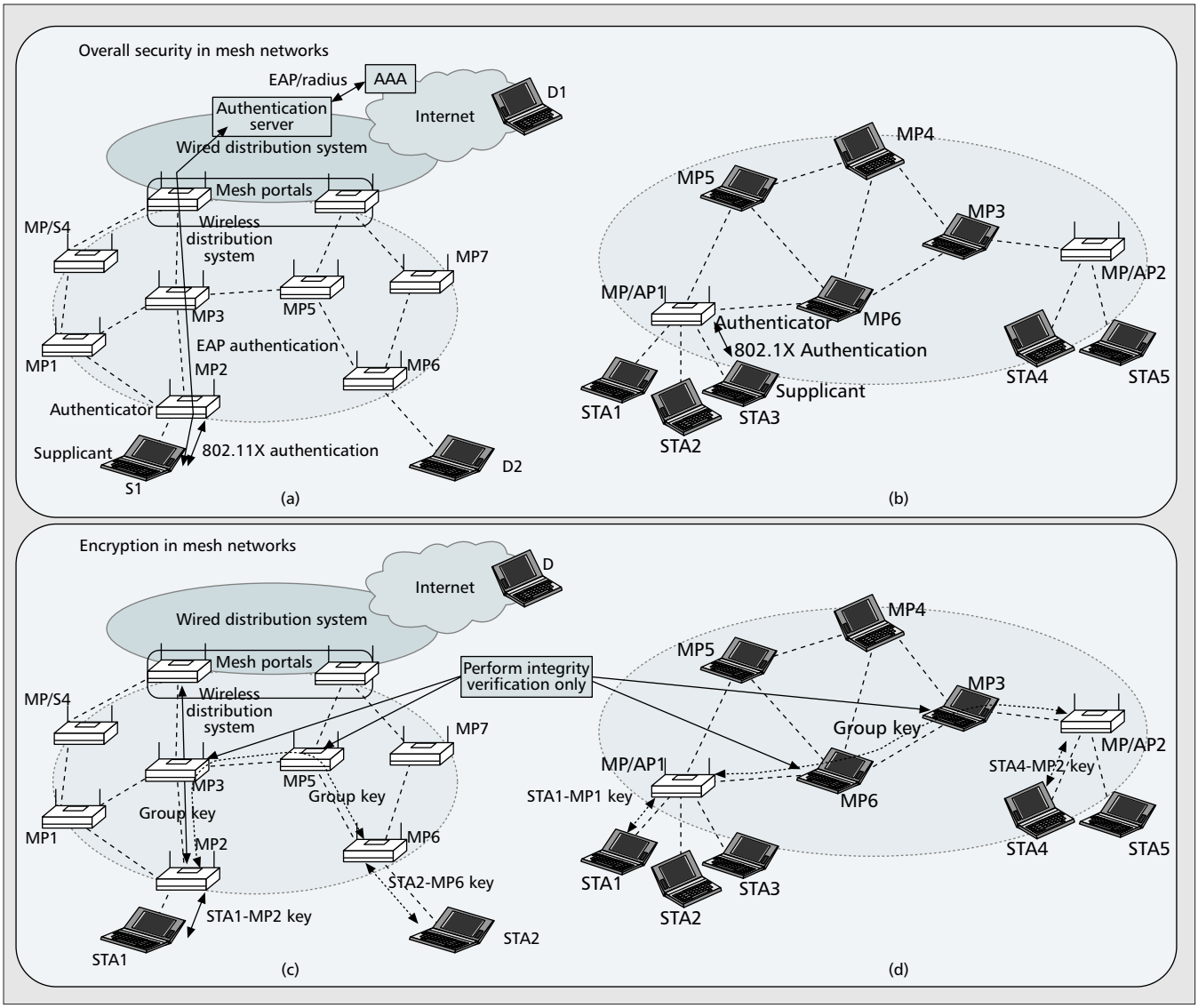


Figure 4. *Security in: a) 802.11 connected mesh network; b) 802.11 mesh ad hoc network; encryption in c) 802.11 connected mesh network; d) 802.11 mesh ad hoc network.*

Power Efficiency

In many cases MPs will be battery-driven devices, which implies that the up-time of the MPs depends on both the battery capacity and the device power consumption. Power-efficiency mechanisms aiming for reduced power consumption and fair distribution of traffic through the network are therefore important for mesh networks.

A straightforward approach towards power saving in multihop networks would be to let inactive MPs enter sleep mode. However, in contrast to traditional stations, MPs may also have a traffic-forwarding function that requires them to receive and transmit data on behalf of other MPs. Therefore, scheduling of wake-up time for MPs is complicated. Another approach is the adaptation of transmit power; however, this may cause topology modifications since the transmission range of MPS changes with the transmission power.

The most promising method for power awareness in mesh networks is power-aware routing, where the network routing paths are optimized for power consumption [7]. In a multidimensional metric as described above, new power-efficiency-related parameters can be introduced. These parameters can vary from simply indicating that a MP is "wire" or "battery" operated, to being more complex, for example, indicating a range of power statuses. Different power parameters in the routing metrics may result in different routes through the network and different optimized values, for example, overall up-time of the network versus up-time of individual nodes.

Conclusions and Future Work

The development of 802.11 mesh networks is at its very inception, and several technical solutions need to be developed. This article has provided an overview of mesh WLAN networks, describing the ongoing work in IEEE 802.11 and identifying key technical aspects of mesh networks: topology creation, routing, security, QoS, and power efficiency. The authors believe that the technical aspects addressed in this article are key for the success of mesh networks, and more attention needs to be devoted to such areas.

References

[1] IEEE 802.11 Std., "Information Technology — Telecommunications and Information Exchange between Systems — Local and Metropolitan Area Networks — Specific Requirements — Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 1999 ed. (Rel. 2003).

[2] J. Chen, S.-H.G. Chan, and S.-C. Liew, "Mixed-Mode WLAN: The Integration of Ad Hoc Mode with Wireless LAN Infrastructure," *IEEE GLOBECOM '03*, vol. 1, 1–5 Dec. 2003, pp. 231–35.

[3] J.Broch *et al.*, "A Performance Comparision of MultiHop wireless Ad Hoc Network Rouring Protocols," *Proc. IEEE MOBICOM*, Dallas, TX, Oct. 1998.

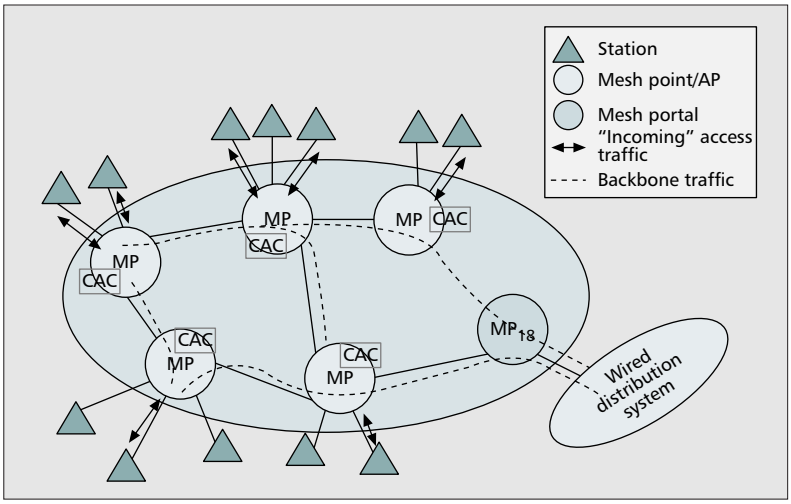


Figure 5. *QoS support in mesh networks.*

[4] S. Corson and J. Macker, "Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," IETF RFC 2501, Jan. 1999.

[5] H. Deng, W. Li, and D. Agrawal, "Routing Security in Wireless Ad Hoc Networks," *IEEE Commun. Mag.*, Oct. 2002.

[6] S. Mangold *et al.*, "IEEE 802.11e Wireless LAN for Quality of Service," *Euro. Wireless 2002*, Florence, Italy, Feb. 25–28, 2002.

[7] Y.-C. Tseng, C.-S. Hsu, and T.-Y. Hsieh, "Power-Saving Protocols for IEEE 802.11-Based Multihop Ad Hoc Networks," *IEEE INFOCOM*, June 2002, vol.1 pp 200–09.

Biographies

Stefano M. Faccin (stefano.faccin@nokia.com) received his M.S. degree in computer science and telecommunications from Politecnico di Torino in 1995. He joined Nokia Research Center in 1998. As research manager, he focuses on noncellular wireless technologies (e.g., IEEE 802.11, 802.16, and 802.21) and IP network architectures for the future Internet. He has 11 years of experience with standardization fora in 3GPP, IETF, and IEEE 802, is Co-Chair of the MIPSHOP WG in IETF, and is Liaison Officer for IEEE 802.11 and 802.21 to 3GPP2. He is the author of several technical papers, and has 11 patents granted and more than 50 pending patent applications.

Carl Wijting received his M.Sc. degree in electrical engineering from Delft University of Technology, The Netherlands in 1998, and his Ph.D. degree in wireless communications from Aalborg University, Denmark in 2004. Since 2004 he has worked for Nokia Research Center as a research engineer in the Radio Technologies Laboratory, where he is involved in research and development of WLAN systems, focusing on mesh networking concepts and multiradio concepts. He has authored and coauthored around 20 international journal and conference papers, and a chapter in the book *WCDMA: Towards IP Mobility and Mobile Internet*.

Jarkko Kneckt received his M.Sc. degree in electrical engineering from Helsinki University of Technology, Finland, in 2002. Since 2000 he has worked at Nokia. At the beginning of 2003 he joined Nokia Research Center, Helsinki, where he is currently a research engineer in the Radio Technologies Laboratory. His research interests include WLAN system performance and networking solutions. He was a Nokia delegate to 802.11e and further continued as a Nokia delegate to 802.11s.

Ameya Damle graduated from Southern Methodist University with an M.S. degree in telecommunications in 2005.