International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Issue 11, Volume 1 (November 2014) www.ijirae.com

KEY MANAGEMENT STUDY OF SECURE COMMUNICATION IN WIRELESS NETWORKS

R.LalithKumar
Research Scholar/CS
Bharathiyar University, Coimbatore

Dr.A.Arul Lawrence S.K
Professor & Head /CSE
Bangalore -32

Abstract – The need for multicast functionality has introduced new challenges, particularly with respect to provision of secure environments for such applications. Consequently, the security aspects and security objectives achieved in unicast as well as in broadcast environments should also be deployed and achieved in multicast environments. In the security issues in group communication identified several issues specific to this type of environment. Our main interest is in the management of keying material, in particular the distribution and updating of cryptographic keys, which is crucial to ensure the security of any multicast group communication. I will discuss Group Key Management Frameworks (GKMFS).

Keywords – Multicast , GKMFS, Unicast, anycast

1. INTRODUCTION TO MULTICAST AND GROUP COMMUNICATION

Progress has been slow since initial deployment, especially compared to the likes of the World Wide Web (WWW) and the Hypertext Transfer Protocol (HTTP). The reason for this is because multicast features require additional intelligence in the network which introduces nontrivial amounts of state and complexity in both core and edge routers (Gong and Shacham, 1995). However, multicast communication is becoming increasingly important and is a subject of great research interest. Before we proceed further, it is necessary for us to clarify some basic terminology that we will use throughout this thesis. In the following sections, we explain the differences between *multicast*, *broadcast* and *unicast*. We also demonstrate the advantages that multicast offers for enabling group communication.

1.2 Unicast vs Multicast

Unicast is communication between a single sender and a single receiver over a network. The term exists in contradistinction to multicast, communication between a single sender and multiple receivers, and anycast, communication between any sender and the nearest of a group of receivers in a network. An earlier term, point-to-point communication, is similar in meaning to unicast. The new Internet Protocol version 6 (IPv6) supports unicast as well as anycast and multicast.

Extrapolating from definitions in (Deering, 1989), (Miller, 1999), (Ammer, 2000), (Wittmann and Zitterbart, 2001), (Goyeneche, 2004) and (Ciscosystem, 2006), the term *multicast* can be defined as, a*n internetwork function that allows data to be delivered to a specific group of nodes (or recipients) by a single transmission.* From a data sender point of view, *multicasting* allows data to be sent from the source (which is the *sender*) only once, and the network will make copies of data and transmit the data to multiple destinations (which are known as the *recipients* of the multicast data) which have been determined prior to transmission. This special feature enables data to be efficiently sent to a group of recipients, and is therefore attractive for group-based application services such as video conferencing, as well as data delivery services such as stock quote, news or weather updates. Multicast is much more efficient then traditional *unicast* methods, which only transmit data to one intended recipient.

We illustrate an example of unicast versus multicast data communication in *Figure1.* The left figure shows *unicast* data communication, while the right figure shows *multicast* data communication. From *Figure 1*, *unicast* and *multicast* data transmissions are indicated with bold arrows. Based on one -to-many relationship ,it shows a single sender (S) sending data to a group of receivers (R).

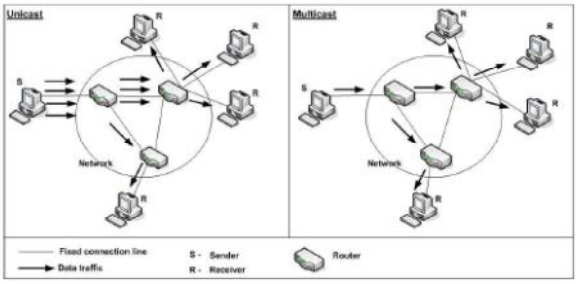


Figure 1: An example of Unicast vs. Multicast communication.

If group communication is to be accomplished via conventional data communication based on unicast, as shown on the above of *Figure 1*, data to all group members needs to be sent across the network separately. Thus, in order to transmit to n recipients (group members), n pieces of data need to be transmitted. As illustrated on the right however, multicast allows a sender of data to transmit only one copy of the data to n recipients. This is achieved when a router (with a built-in multicast function at the network level) makes copies of the data and transmits it to the intended recipients via the nearest routers. End routers (closest to the recipients) will then complete the transmission, and send the data to the intended recipients.

1.3 Multicast vs Broadcast

A closely related concept to multicast is *broadcast*. Commonly used in radio and TV transmission, broadcast is easily understood as a way to transmit data or messages to all recipient nodes in a network. Both broadcast and multicast allow data to be transmitted to more than one recipient at a time. However, in regards to group communication, multicast offers a better solution than broadcast in several aspects (Gong and Shacham, 1995), (Huitema, 1995), (Reid, 1997), (Almeroth, 2000), (Comer, 2001), (Hardjono and Dondeti, 2003) and (Perrig and Tygar, 2003):

• *Host coverage.* Broadcast includes everyone (all hosts) in the network.

This is due to its indiscriminate transmission which can be received by anyone having the correct equipment in place. For example:

(i) Houses with a specific dish can receive satellite channels cast by a satellite station.
(ii) Computers connected to an Ethernet can receive messages cast by the network.

On the other hand, multicast data is not sent to all hosts, but is rather targeted to a predetermined group of hosts which have specific network addresses.

- *Internet Protocol (IP) context*. Broadcast is usually designated by a single address assigned to all stations in the network (such as an Ethernet packet with a MAC address that can be received by all stations) (Reid, 1997). On the other hand, multicast offers more restricted access with an IP multicast address (Deering, 1989) designating a certain group of hosts in such a way that any transmission from one host in the group is received by all other hosts within the group.
- *From a recipient's context*. With broadcast, all recipients will act upon the received message, whereas with multicast only those recipients that have been configured to respond to the destination address in the message will do so. Thus, multicast saves network resources (such as the CPU time) by allowing only the intended group of recipients to further process the message received.

1.4 Group Communication vs Multicast Communication

Throughout this thesis, the terms *group* and *multicast group* carry the same meaning and will be used interchangeably. Informed by various sources such as those in (Deering, 1989), (Forman and Zahorjan, 1994), (Gong and Shacham, 1995), (Chlamtac and Redi, 1998), (Canetti et al., 1999), (Diot et al., 2000), (Hardjono and Tsudik, 2000), (Bruschi and Rosti, 2002), (Hardjono and Dondeti, 2003) and (Baugher et al., 2005), we will avoid formal definitions and interchange the terms *multicast communication, group communication* and *multicast group communication*.

This approach is also supported by the following sources gathered from the *American Heritage* Dictionary of the English Language as well as from the *Cisco* Internetworking Terms and Acronyms (Ammer, 2000) and (Ciscosystem, 2006), where both terms carry similar meanings, as follows:

- *Multicast communication* (Ciscosystem, 2006). A single communication (like an audio, a video or packets) made and copied by the network and sent across a network to a specific subset of network address.
- *Group communication* (Ammer, 2000). A communication that occurs in an assemblage of persons or objects, all interconnected and capable of communicating with each other, in ways that are securely isolated from all other users on the network.

2. MULTICAST ENVIRONMENTS

The popularity of multicast has grown considerably with the wide use of the Internet, as well as the increasing demand for group-based applications such as online forums, Pay Per View Channels (PPVC), various information dissemination services (such as news, weather, or share prices updates), as well as multimedia conferences including video and audio conferencing. While many internet applications use the conventional *point-to-point* or unicast transmission, *one-to-multipoint* or one-to-many transmission was limited to local network applications. Thus, multicast transmission is becoming more popular as the demand for these new group applications increases.

The original protocol that allowed the transmission of data on the internet is the *Internet Protocol* (IP), which supports unicast communication. This extension is known as *IP multicast*. IP multicast is defined as a transmission of an IP datagram to a group of hosts, identified by a single IP destination address (Deering, 1989).

This address must be one of the special addresses designated for the purpose of multicast communication. *Table 1* gives the allocation of multicast addresses in IPv4 (IP version 4), while *Table 2* gives the IPv6 (IP version 6) version of multicast address allocation. While an IP multicast group is identified by a class D IPv4 address which ranges from 224.0.0.0 to 239.255.255.255, in IPv6 multicast addresses always begin with 1111 1111 (binary), or FF (hex). This set of addresses can be used for defining different multicast groups (except for several designated addresses which are reserved and will never be used). Just like conventional communications that are based on unicast, IP multicast is an unreliable, unordered, and best-effort datagram service.

Table 1: Multicast address range in IPv4.

Address Classes	IP Address Allocation (32-bit address range)	
	In binary prefix	In decimal range
A	0.....	0.0.0.0 – 127.255.255.255
B	10.....	128.0.0.0 – 191.255.255.255
C	110.....	192.0.0.0 – 223.255.255.255
D (Multicast)	1110.....	224.0.0.0 – 239.255.255.255
E	11110.....	240.0.0.0 – 247.255.255.255

In other words, it does not guarantee that a datagram will arrive at all the destination group nodes, and it is possible that the order of receiving the datagram at the end nodes may change during transmission. In this early age of multicast technology, when multicast functionality has not yet been widely integrated into traditional network routers, an experimental multicast network called *multicast bone* (MBONE) (Savetz et al., 1998), (Goyeneche, 2004), (Devereaux-Weber, 2006) was constructed as a test bed to realize multicast communication.

Table 2: Multicast address prefix in IPv6.

Address Allocation	Format Prefix (FP) (from 128-bit address space)	
	In binary	In hexadecimal
Reserved	0000 0000.....	00::
Global unicast addresses	001.....	001::
Link-local unicast addresses	1111 1110 10....	FE80::
Site-local unicast addresses	1111 1110 11....	FEC0::
Multicast addresses	1111 1111.....	FF::

These tunnels are particularly useful in many conventional unicast networks where many network routers are not multicast capable. For this to work, both end routers (nearest to a group of multicast hosts) need to be multicast capable routers, and IP packets that are addressed to a multicast group are tunnelled between these multicast routers. We illustrate a multicast communication over a unicast network in *Figure 2*, showing a set of multicast hosts wishing to form a group communication over a unicast network and *Figure.1.3* depicting the tunnelling of IP datagrams that occurs between these multicast hosts. *Figure 2* illustrates communication that occurs between several multicast hosts over a traditional unicast network. This is supported by multicast routers (MR) at both ends of multicast hosts.

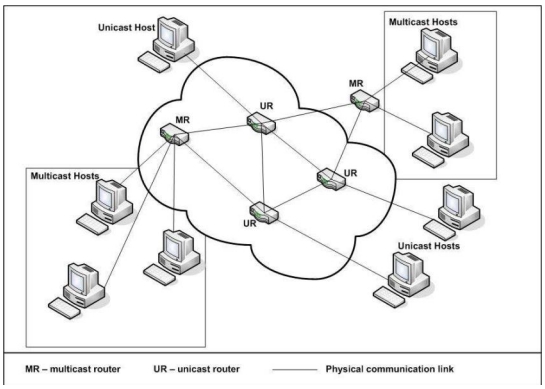
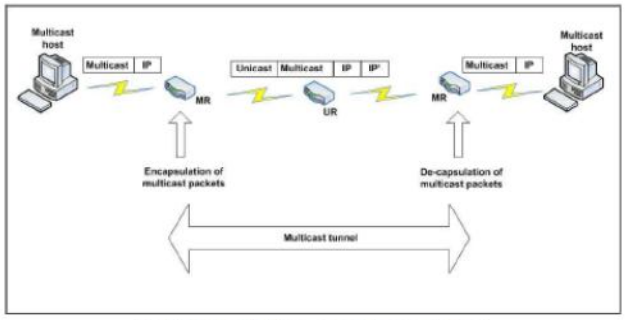


Figure:2. A set of multicast hosts forming a group communication over a unicast network.



(b) Tunneling of IP datagrams that occurs from *(a)*.

Figure 3: An illustration of a multicast communication over a unicast network.

Figure 4 illustrates two multicast hosts communicating with one another over a unicast network via a *multicast tunnel*. This is achieved as follows. At the receiving host, when the datagrams reach the multicast router, the same datagrams will go through a de-capsulation process to recover the original multicast IP datagrams, before being transmitted to the host. This process of encapsulation and de-capsulation creates a *multicast tunnel* between multicast hosts for enabling multicast communication over a traditional unicast network.

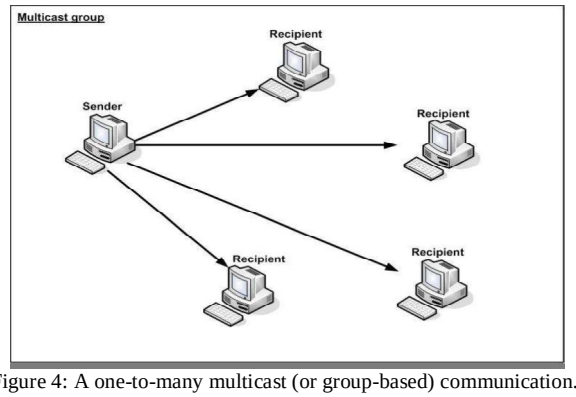


Figure 4: A one-to-many multicast (or group-based) communication.

3. MULTICAST APPLICATIONS

We have now presented an overview of multicast, including the terms that we will use throughout this thesis. We have also demonstrated that multicast technology is more efficient than broadcast and unicast when enabling group communication. In this section, we look at different types of multicast application, as well as several instances of group-based applications that could utilize multicast technology. The main types of multicast application can be divided into two categories, which are *one-to-many* and *many-to-many relationships* (Harney and Muckenhirn, 1997), (Hardjono et al., 2000a), (Wittmann and Zitterbart, 2001). Each of these determines the relationship between the *sender* (S) and the *recipients* (R) of multicast data.

3.1 One-to-Many Relationships

One-to-many relationships correspond to *one-Sender* to *many-Recipients*. In this case, there is one entity that is the sender of the group, while one or more entities will be the recipients of the group communication. *Figure 3* illustrates this type of relationship within a multicast group in the one to many relationship, where there is one entity that acts as the sole sender of the multicast data, while the others are the recipients.

Amongst the examples of such group communications are the following:

- *Data distribution.* Push technologies such as stock quote services, weather or news data, updating of sales information or, price list to all branches, as well as advertisement dissemination based on consumer habits or place of residence.
- *Streamed data delivery*. Widely referred to as broadcasting, such as TV broadcasting as well as Pay Per View (PPV) channels.
- • *Software distribution.* Software upgrades in a company, as well as the distribution of updates by software manufacturers of their products over the Internet.

3.2 Many-to-Many Relationships

In this type of relationship, many-to-many corres-ponds to *many-Senders* to *many-Recipients.* In this case, there are one or more entities that will be the sender (s) and/or the recipients of the multicast group. Thus, an entity can be a sender, a recipient, or both. *Figure 5* shows a multicast group with two entities, while *Figure 6* illustrates that every entity within a multicast group can potentially be both the sender and the recipient of data. Amongst the examples of such group communications are:

- *Audio/video and Teleconferencing*. Also referred to as *Computer-Supported Cooperative Work* (CSCW), group members that are located in different sites will share *white board tools* designed for coordination between members.

- *Distance Learning.* For example teleteaching, which refers to a scenario in which a student in one place is able to participate in a class somewhere else. This requires group communication between those teaching and those learning, since questions have to be asked and solutions need to be discussed. Another example is virtual classrooms, where course participants use the Internet to obtain teaching materials, deliver their assignments, as well as receive feedback from course instructors. Similarly, the instructor distributes papers to the virtual class and assignments are collected from the course participants.

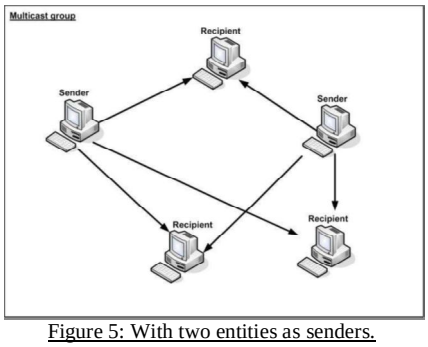


Figure 5: With two entities as senders.

In these applications, very simple group communication mechanisms are implemented in the applications themselves, but not supported by the communication system that underlies them. While this seems to outdate the need for a multicast function, its implementation and performance are very simple.

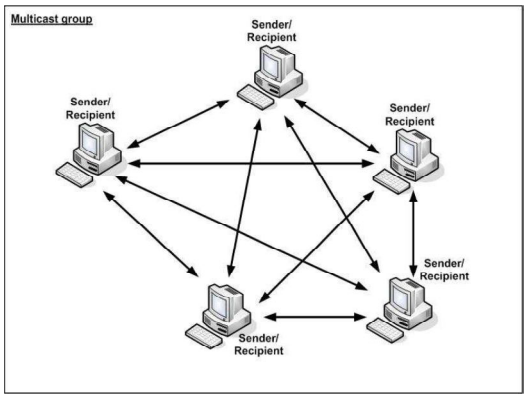


Figure 6: Many-to-many multicast (or group-based) communications

One example is Electronic Mail Systems that allow you to send the same message to groups of recipients, who are normally specified through mailing lists. Other examples are the distribution of news, chatting on the Internet as well as game servers that allow web users to play games like Backgammon, Chess and Life together on the Internet.

4. SECURITY ACTIVITIES AND STANDARDS

The first reference to multicast can be found in the PhD dissertation by Deering in the late 1980s, which was proposed as an Internet Standard in (Deering, 1989). Since then, multicast has become part of the research area of the *Internet Engineering Task Force* (IETF) (IETF, 2007), in particular proposing security solutions for group-based communication such as those in (Deering, 1989), (Ballardie, 1996), (Harney and Muckenhirn, 1997), (Wallner et al., 1999), (Hardjono et al., 2000a), (Hardjono et al., 2000b), (Baugher et al., 2003), (Hardjono and Weis, 2004) and (Baugher et al., 2005).

This *Secure Multicast Research Group* (SMuG) (SMuG, 2007) was formed to discuss issues related to multicast security, as well as to investigate standards for secure multicast. SMuG's main intentions were to focus on the security problems relating to IP multicast, with the aim of providing common solutions for a variety of applications. The results obtained were presented to the IETF for potential standardization. In order to expand its research scope, SMuG was replaced by *The Group Security Research Group* (GSEC) (GSEC, 2007), which was another short-lived research group of the IRTF. With GSEC no longer active, theWorking Group (WG) that is currently active in research on multicast, as well as group communication security, is known as *Multicast Security* (MSEC) (MSEC, 2007). Three main problem areas have been defined by MSEC as the central research areas concerning secure multicast by IETF (IETF, 2007). They are:

- *Multicast data handling.* This covers problems pertaining to the treatment of multicast data by the entities involved in the communication, such as encryption algorithms, as well as data integrity techniques.

- *Management of keying material*. This is concerned with the management of all keying material of a multicast group, including distribution and updating (or re-keying) of all cryptographic keys as well as other security parameters related to the keys (such as information on key expiration periods, or key usage).
- *Multicast security policies.* This area is concerned with all aspects of multicast group security policies, including creation, translation and representation of policy of a multicast group. It is important that group policy is managed properly since policies may be expressed in different ways, they may exist at different levels and they may be interpreted differently according to the context in which they are specified and implemented. For example, policy negotiation and translation (if necessary) should be performed as part of a host joining a multicast group. Otherwise, it is meaningless as new members will not be able to participate in the group communication due to incorrect or inappropriate policies. Published works in these problem areas can be found in (MSEC, 2007) and (GSEC, 2007). These problem areas are equally important and ought to receive equal treatment in order to accomplish secure group communication. While some genuinely new solutions are required, some of these problems can also be addressed by adapting accomplishments in traditional unicast environments. Our interest in particular concerns with security issues that are specific to multicast group communication. We look at this in the following section.

5. SECURITY RESEARCH ISSUES SPECIFIC TO GROUP COMMUNICATION

In this section, we present the main security issues pertaining to group communication. Like unicast, provision of security services for multicast group communications is concerned with *confidentiality, integrity, authenticity* as well as *availability* of group communications.

As in unicast, an adversary may carry out both passive and active attacks against a multicast communication, such as:

- *Eavesdropping on confidential communication,*
- *Disrupting a group session,*
- *Blocking data transmission,*
- *Injecting false data traffic,*
- *Masquerading to join a group session,*
- *Initiating a bogus group session, or*
- *Colluding members exchanging information in order to gain unauthorized access to data which may contain cryptographic key and other group related information.*

Thus, it is crucial to provide a secure data exchange between group members, which includes use of mechanisms or methods to:

- *Establish the identity of the originator of a message.*
- *Protect transmitted data, including cryptographic keys, from unauthorized disclosure and modification.*
- *Control group member's access to data.*
- *Enable any member to verify the nature of the session in which he participated. With no regard to the order of importance, we address the main issues concerned with the provision of security for group (multicast) communication in the following sections.*

5.1. Group Membership Policies

Multicast capability of sending data only to a specific group of hosts (group members) requires some additional processing to restrict access to the specific group. This processing includes the management of group membership. The status of group membership of a multicast group is determined by the group membership policy. This is defined during the creation of a multicast group.

The policy of group membership can be categorized into two types, as follows (Gong and Shacham, 1995), (Bruschi and Rosti, 2002), (Hardjono and Dondeti, 2003):

- *Static policy*. Often referred to as *closed* membership, group membership with a static policy offers a restricted approach to allowing hosts to take part in a multicast group. In this case, group membership of a multicast group is predetermined prior to the commencement of a group communication and all group members belong to a certain multicast group throughout its lifetime. For example, a video conferencing facility for a global organization might have a predefined group of hosts corresponding to its multiple branch sites.
- *Dynamic policy*. Also referred to as *open* membership, a dynamic policy allows any hosts to join (or leave) a multicast group at any time throughout the lifetime of the multicast group. It is essential to define this group membership policy because it determines the entire set of procedures for a particular multicast group communication.

5.2 Key Management

Key management for multicast communication is generally more complex than for unicast environments. In a secure environment, presuming that a request to establish a multicast session amongst a group of hosts is granted, a common group key needs to be distributed to each of the group members prior to the start of the group session.
In secure group communication, specific problems for managing the keying material can be divided into two approaches depending on the group membership policy in place, as follows (Caronni et al., 1996), (Mittra, 1997), (Waldvogel et al., 1999), (Hardjono et al., 2000a), (Noubir et al., 2002) and (Hardjono and Dondeti, 2003):

- *Static approach.* Due to its fixed membership policy, the static approach requires almost no change (or update) in keying material throughout the lifetime of a multicast group except for periodic re-keying. This implies that a new multicast group will need to be created to cope with new members joining the multicast group.
- *Dynamic approach*. The dynamic approach, where any hosts can join (and leave) a multicast group at any time, potentially requires that cryptographic keys be updated whenever there is a change in group membership. The precise need for updating the keys is primarily determined by whether the following services are required:
- *Backward secrecy*. This ensures that past communications, including group keys and their related information, are inaccessible to newly joined members. For provision of backward secrecy, group keying material has to be updated whenever a new join to the group occurs.
- *Forward secrecy*. This ensures that future communications remain inaccessible to departed members. For provision of forward secrecy, re-keying of keying material has to occur whenever an existing member leaves the multicast group. One of the main challenges in key management for group communication is the distribution of the keys needed by group members of a multicast group. In particular, it is important to ensure that each group member gets keys for the right group sessions.

5.3 Group Security and Authentication

In secure multicast environments, provision of security services such as entity authentication, data confidentiality and data integrity are required. However, secure multicast group communication has some specific requirements in these areas (Gong and Shacham, 1995), (Canetti et al., 1999), (Hardjono and Tsudik, 2000), (Almeroth, 2000), (Pessi, 2003) and (Hardjono and Dondeti, 2003):

As hosts may wish to join specific groups, and different groups may have their own security requirements (for example, concerning who can join), it is imperative that:

- ❖ Group managers verify that the service provided by a multicast group is accessible only to authorized group members.
- ❖ Group members verify that the service they participate in is provided by a genuine source.
- ❖ Both (group managers and group members) verify each other's identities. Different policies (static or dynamic) may require different needs for managing group keys (due to *joins* and *leaves*). In a dynamic policy, if backward and forward secrecy are required then re-keying of group keys will have to occur whenever there is a change in group membership.

5.4. Scalability

In general, the term *scalability* refers to the ability of a framework (or mechanisms within a framework) to be extended to cover a larger group of hosts over a wider physical region without too much delay and deterioration in the level of service provided. In the context of secure group communication, the need for scalability primarily affects the management of keying material. While the problem of hosts joining seems to be straightforward (if the provision of backward secrecy is not necessary) and distribution of new cryptographic keys can be supported by the old cryptographic keys, group members leaving poses a much more difficult scalability problem. If the provision of forward secrecy is necessary, new keying material must be sent to the remaining group members in a way that excludes the leaving member.

6. SUMMARY

The need for multicast functionality has introduced new challenges, particularly with respect to provision of secure environments for such applications. Consequently, the security aspects and security objectives achieved in *unicast* as well as in *broadcast* environments should also be deployed and achieved in multicast environments. In the security issues in group communication identified several issues specific to this type of environment. Our main interest is in the management of keying material, in particular the distribution and updating of cryptographic keys, which is crucial to ensure the security of any multicast group communication. we will discuss Group Key Management Frameworks (GKMFS).

7. REFERENCE

[1]. Almeroth, K. C. (2000). The Evolution of Multicast: From the MBone to Inter-Domain Multicast to Internet2 Deployment. *Network IEEE*, 14(1):10–20.
[2]. Ammer, C. (2000). *The American Heritage Dictionary of the English Language, Fourth Edition*. Houghton Mifflin Company.
[3]. Apple (2007). iPhone: Internet in Your Pocket, published by Apple Inc. http://www.apple.com/iphone/.
[4]. Ballardie, A. (1996). *Scalable multicast key distribution*. RFC 1949.
[5]. Baugher, M., Canetti, R., Dondeti, L., and Lindholm, F. (2003). *Group Key Management Architecture*. Internet Draft IETF MSEC WG. http://www2.tools.ietf.org/html/draft-ietf-msec-gkmarch-04.
[6]. Baugher, M., Canetti, R., Dondeti, L., and Lindholm, F. (2005). *Multicast Security (MSEC) Group Key Management Architecture*. RFC 4046.
[7]. Bruschi, D. and Rosti, E. (2002). Secure multicast in wireless networks of mobile hosts: Protocols and issues. *Mobile Networks and Applications*, 7(6):503–511.

[8]. BS (1997). *Information technology - Security techniques - Entity authentication- Part 1: General (BS ISO/IEC 9798-1)*. British Standards.
[9]. BS (2002). *Information technology - Security techniques - Time-stamping services - Part 1 (BS ISO/IEC 18014-1)*. British Standards.
[10]. Canetti, R., Garay, J., Itkis, G., Micciancio, D., Naor, M., and Pinkas, B. (1999). Multicast security: A taxonomy and some efficient constructions. In *Proceeding of IEEE Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOMM)'99*. http://citeseer.ist.psu.edu/canetti99multicast.html.
[11]. Caronni, G., Lubich, H., Aziz, A., Markson, T., and Skrenta, R. (1996). SKIP: Securing the internet. In *Proceedings of WET ICE '96 Fifth Workshop on Enabling Technologies*, pages 62–67. http://citeseer.ist.psu.edu/caronni96skip.html.
[12]. Casner, S. and Deering, S. (1992). First IETF Internet Audiocast. *SIGCOMM Computer Communication Review*, 22(3):92–97. http://citeseer.ist.psu.edu/casner92first.html.
[13]. Chlamtac, I. and Redi, J. (1998). *Mobile Computing: Challenges and Potential*. Encyclopedia of Computer Science, 4th Edition, International Thomson Publishing.

