Secure Multicast in Various Scenarios of WirelessMAN

Sen Xu, Chin-Tser Huang, Manton Matthews
Department of Computer Science and Engineering
University of South Carolina
Columbia, SC 29208
{xu4, huangct, matthews}@cse.sc.edu

Abstract

Multicast enables efficient large-scale content distribution and has become more and more popular in network service. Security is a critical issue for multicast because many applications require access control and privacy. This issue is more sensitive to wireless network, which is lack of physical boundaries. IEEE 802.16 is the standard for next generation wireless network, which aims to provide the last mile access for Wireless Metropolitan Area Network (WirelessMAN). Multicast is also supported in IEEE 802.16, and a Multicast and Broadcast Rekeying Algorithm (MBRA) is proposed as an optional function for secure multicast. However, this algorithm does not provide backward and forward secrecy, and is not scalable to large group. This paper reviews the above two deficiencies of MBRA and proposes a new algorithm to address them. We also propose algorithms for secure multicast in different scenarios of WirelessMAN besides its basic scheme.

1. Introduction

There are many emerging applications that depend on secure group communications, which require the privacy of participants and access control at the multicast server. On the other hand, scalability is another critical concern for the multicast service underlying these applications due to the possible large number of group members. In the domain of wired networks, efficient and secure multicast is a widely studied problem and several popular protocols have been proposed. This is not necessarily true for the domain of wireless networks, where attention has been less significant.

Wireless networks have become more and more pervasive due to their many advantages. The IEEE 802.16 standard [1] aims to provide broadband wireless access (BWA) for Metropolitan Area Networks (MAN) and the recently released IEEE 802.16e [2] adds mobility features and some other functions including multicast. Multicast in Wireless Metropolitan Area Networks (WirelessMAN) is a promising service, suitable for many applications, such as stock option bidding, pay per view TV broadcasting, video conferencing, etc., for both fixed and mobile subscribers.

The challenge of a secure multicast service, such as the one in IEEE 802.16, is to provide an efficient method for controlling access to the group and its communications. Encryption of group messages and selective distribution of the keys used for encryption is the primary method for ensuring the security. For a dynamic group in which membership changes frequently, the rekeying algorithm employed by the service is a critical factor of the overall service efficiency. This algorithm should guarantee forward secrecy, which prevents a leaving member from accessing future communications; and backward secrecy, which prevents a joining member from accessing former communications. On the other hand, a rekeying algorithm should be efficient as well. That means it should be scalable to a large group and exhibit good performance during key distribution, which is usually measured by communication complexity, server storage complexity, and user storage complexity.

This paper reviews the Privacy and Key Management (PKM) protocol (with respect to the multicast setting) and the Multicast and Broadcast Rekeying Algorithm (MBRA) in IEEE 802.16e. The weaknesses of MBRA are detailed and more efficient and secure modifications are brought up. MBRA is in fact for intra-BS multicast only. We propose Adaptive Inter-BS Multicast Protocol, which is derived from some related works. The rest of the paper is organized as follows. In Section 2, related works on both IEEE 802.16 protocols and on secure multicast protocols are introduced. Section 3 analyzes and modifies the MBRA for Intra-BS multicast. In Section 4, we analyze some currently available rekeying algorithms and propose Adaptive Inter-BS Multicast Protocol. We also propose an efficient rekeying algorithm for handover in Section 5. Finally, we conclude in Section 6.

2. Related Works

Since the first version of the IEEE 802.16 standard [3] was released in 2002, a few articles and books have been published. In [4], the chair of the standard gives a technical overview of IEEE 802.16, which is extended later as [5]. Some 802.16 group members also publish a book [6] in 2006, which provides a detailed overview of the standard and explains the rationale behind development decisions. The authors of [7] review the standard, analyze the security provided by the standard, and discuss the requirement of mutual authentication between Subscriber Station (SS) and Base Station (BS). In [8] the PKM protocol is discussed in detail, more attacks on the versions of the PKM protocols listed in [3] and [7] are discovered, and revisions of PKM protocols are proposed. In [9], another attack on PKM

version 2 (PKMv2) in [2] is detailed. However, none of these publications cover the MBRA version released in earlier 2006 [2].

There is a report [10] which analyzes the IEEE 802.16 MBRA, which especially focuses on replay attacks against the MBRA (in fact, the attacks it brings up are based on assumptions that some attributes in the key management messages are missing), similar to the attacks listed in [7] and [8]. However, it does not cover the backward and forward secrecy afforded to communications before/after rekeying, or the efficiency of the MBRA, both of which are paramount to a desirable, secure rekeying algorithm.

More generally, secure multicast has been a popular topic in the past ten years, and many protocols have been proposed. [11], [12], [13] and [14] are the first few works dealing with secure multicast, in which straightforward, yet not scalable methods, are described. The Iolus approach detailed in [15] is a distributed method in which a hierarchy of agents is used as subgroup controllers. Using Iolus, scalability is ensured because member changes in one subgroup do not affect other subgroups. It also provides other promising features such as fault-tolerance. Kronos [16] takes a unique periodical rekeying approach that rekeys the group only at specified time intervals. Customary rekeying upon member changes are delayed until the next rekeying interval, therefore the number of rekeying is reduced.

Logical Key Hierarchy (LKH) tree algorithms are proposed in [17] and [18], which provide O(log n) communication complexity, where n is the number of group members. There are three schemes in the Versa-key framework [19], one of which is a centralized tree-based management scheme. It applies a one-way function to update a key tree upon members joining, and thus is also referred to as LHK+. One-way Function Tree is proposed in [20], which reduce half of the rekeying messages comparing to LKH. A similar scheme is One-way Function Chain Tree [21]. Adaptive Rekeying scheme is proposed in [22], which can employ different level of complementary keys according to application requirements.

In this paper, different solutions are proposed according to various scenarios of IEEE 802.16 multicast. Some popular rekeying algorithms are directly applied in Intra-BS multicast. Some novel schemes are proposed in handover and Inter-BS multicast. Our Adaptive Inter-BS Multicast Protocol integrates the advantages of the approaches presented in [14], [15] and [22] to achieve better efficiency.

3. Intra-BS Multicast

3.1. IEEE 802.16 PKM protocols and MBRA

Prior to receiving multicast service, a Subscriber Station (SS) must initiate and authenticate with a base station (BS), during which the BS decides the level of service to be authorized. By using the ranging procedure on the Initial Ranging or Basic Connection, an SS establishes a Primary Management Connection with a BS that is used to exchange MAC management messages. If the SS is to be managed, a Secondary Management Connection is established between the SS and BS. The Secondary Management Connection is used to transfer delay-tolerant, standard-based messages in IP datagram such as DHCP, TFTP, and SNMP.

The Privacy Key Management messages are exchanged through the Primary Management Connection, with the exception that PKMv2 Group-Key-Update-Command is transferred over the Broadcast Connection. The Privacy and Key Management (PKM) protocol is applied in the IEEE 802.16 security sublayer within the 802.16 MAC layer and performs two functions. First, the PKM protocol provides secure distribution of keying material from a BS to SS. Second, the protocol enables a BS to enforce access control over network services. A brief summary of a PKM protocol run between an SS and BS is as follows. The SS initiates the protocol and first authenticates with a BS (PKMv2 also provides mutual authentication), establishing a shared secret — an Authentication Key (AK). The BS will also send a Secure Association Identifier (SAID) list that the SS is entitled to access, which indicates the services explicitly authorized to the SS. Then by a Key-REQ message from SS to BS and Key-RSP message from BS to SS, the SS receives the keying material corresponding to a specified SAID.

The Multicast and Broadcast Service in IEEE 802.16 is an efficient and power saving mechanism, which also provides subscribers with strong protection from theft of service by encrypting broadcast connections between an SS and BS. MBRA is used to refresh traffic keying material for the multicast service of IEEE 802.16.

An SS may get the initial Group Traffic Encryption Key (GTEK), which is used to encrypt the multicast traffic, by Key Request and Key Reply messages over the Primary Management Connection. A BS updates and distributes the traffic keying material periodically by sending two Group Key Update Command messages: for the GKEK update mode and for the GTEK update mode. The Group Key Encryption Key (GKEK) is used to encrypt the GTEK in GTEK update mode. Intermittently, a BS transmits the Key Update Command message for GKEK update mode to each SS through its Primary Management Connection. This message contains the new GKEK encrypted with the Key Encryption Key (KEK), which is derived from the AK established during authentication. Then, the BS transmits the Key Update Command message for GTEK update mode through the Broadcast Connection, which contains the new GTEK encrypted with the corresponding GKEK. The protocol can be specified as follows:

Message 1. BS $\rightarrow$ SSs : KEK (GKEK)
Message 2. BS $\Rightarrow$ {SS} : GKEK (GTEK)

Figure 1. MBRA Group Key Update Commands

In Figure 1, "$\rightarrow$" stands for a unicast message and "$\Rightarrow$" stands for a broadcast message.

3.2. Analysis and Modification of MBRA

There are two problems with this protocol. Firstly, this protocol is not scalable as BS still needs to unicast to each SS. Secondly, this protocol does not address the issue of backward and forward secrecy. In the case of member joining, when a new member receives the current GTEK by Key Request and Key Reply messages, it can decrypt all previous messages that were multicast during the lifetime of the same GTEK. In the case of member leaving, there is nothing in this protocol that prevents the leaving SS from receiving the future traffic encrypted by the current GTEK which it possesses of.

In fact, this algorithm is similar to the Group Key Management Protocol (GKMP) [12, 13], which does not provide solution for keeping the forward secrecy except creating an entirely new group without the leaving member. This scheme is thus inherently not scalable to large dynamic group. By sending GKEK to each SS intermittently, it relieves the BS from having to refresh traffic key material in a very short period of time, but the overall computation of BS and communication messages remain the same, which is linear to group size.

There is no specification about the lifetime of GKEK in [2]. However, a recommendation to IEEE 802.16 [24], which originally proposes the MBRA, states that the lifetime of GKEK should be the same as GTEK. In page 313, the standard [2] also states that BS shall distribute updated traffic keying material by sending two Key Update Command messages before old GTEK is expired. In fact, both of the two messages are necessary in order to provide backward/forward secrecy upon member changes. In this case, the usage of GKEK is not necessary at all. We modify MBRA as follows with only the usage of GTEK:

Message 1. BS $\rightarrow$ SSs : KEK (GTEK)
Message 2. BS $\Rightarrow$ {SS} : update notice

Figure 2. Revised MBRA for Intra-BS Multicast

By sending GTEK to SS intermittently, our modified scheme still keeps the benefit of reducing the BS's load for key refreshment. However, we only need to send an update notice in plaintext (with BS's signature if message authentication is necessary, which may also be required in MBRA), thus saving both BS and SS encryption/decryption as well as key storage.

There is some ambiguity in the MBRA of [2]. In page 315, it also states that BS distributes updated GTEK by using two messages when the GKEK has been changed, or by using one (the second) message otherwise. In this case, the lifetime of GKEK should be several times longer than that of GTEK in order to encrypt and distribute more than one GTEK. This kind of rekeying occurs only due to expiration of GTEK. Our modified scheme still gives better performance in this case. BS should add the key index (0 if the GTEK is first distributed by Message 1) in the update notice by Message 2, and each group member only need to update the session key by certain one-way hash function. Meanwhile, the security of group multicast will not be hurt in our modified scheme comparing to MBRA. That is because the omitted GKEK does not provide group control at all by sending Message 2 alone; it is only used to broadcast the GTEK to current group members.

In summary, our modified scheme works as follows: If GTEK is first distributed by Key Update Command messages (including rekeying upon member leave), both Message 1 and Message 2 need to be sent, and the key index in Message 2 is set to 0. If rekeying happens upon member join, only Message 2 need to be sent, with one greater index than previous one, each group member will update the GTEK according to the index using agreed one-way hash function; meanwhile, BS sends this updated GTEK to the new member by unicast (through Primary Management Connection encrypted by KEK). If rekeying occurs due to session key expired, only Message 2 need to broadcast, with one greater index to notify group members to update the GTEK by agreed one-way hash function.

The authors of [23] bring up the chaining problem which exists in its previous proposal [24]. In [24], the authors use the old GTEK to encrypt the new GTEK upon update. Thus they claim, if an SS knowing the current GTEK attempts to delete the specific service (in fact, the member leave case), that SS can continuously decode the newly updated GTEK and be served with multicast service. Therefore, they propose to use GKEK to encrypt the new GTEK. It seems our modified scheme has the same problem also. However, we classify the above case as rekeying upon member leave, in which both Message 1 and Message 2 need to be sent, thus guarantees the backward secrecy to the multicast group. On the other hand, in MBRA of [2], if only Message 2 is sent in this situation as they proposed, the using of GKEK will not provide any more security, because the leaving SS knows not only the old GTEK, but also the GKEK, thus the SS is still able to decrypt the new GTEK and get the multicast service.

In fact, the lifetime of TEK is 30 minutes minimum, 12 hours by default, and 7 days maximum. Such a long time can not guarantee the security of traffic in a group with frequent member changes. If the lifetime of GTEK can be set short enough, the periodical rekeying scheme is still a possible solution for secure inter-BS multicast, such as Kronos [16].

Hierarchy tree key management protocols, such as [17]-[22] are also possible choices for Intra-BS multicast. This kind of scheme mitigates the work load of BS (O(log n) comparing O(n) in the basic scheme), thus is scalable to large group. The trade off is, the SSs have to store and encrypt/decrypt more keys (O(log n) comparing O(1) in the basic scheme).

4. Inter-BS Multicast

IEEE 802.16 does not provide key management scheme for Inter-BS multicast, possibly because exchanging messages among BSs (through the backhaul) is beyond the scope of the standard, or they want to leave this management for protocols in higher layer. However, the key distribution of high layer protocol may require different key encryption scheme, which will result in redundant work for both BSs and SSs. Besides, the group management, such as member authentication, still requires BS to communicate with the group manager or AAA (Authentication, Authorization, and Accounting) servers on backbone. Moreover, the handover procedure also needs the cooperation among BSs. Designing an Inter-BS Protocol will serve these functions, similar to the Inter-AP (Access Point) Protocol for IEEE 802.11, which is in fact a recommendation known as IEEE 802.11F.

4.1. Some Currently Available Algorithms

Without changing the Intra-BS multicast protocols, the Iolus [15] could be used for Inter-BS multicast. Iolus is a kind of cluster scheme, using a secure distribution tree (SDT) composed of a number of smaller secure multicast subgroups. The group manager (Group Security Controller - GSC in [15]) manages the top-level subgroup and the cluster headers (Group Security Intermediaries - GSI in [15] and the BS in WirelessMAN) manage each of the other subgroups. Each GSI just relays the traffic from its parent in SDT to its children, decrypting and re-encrypting packages by corresponding subgroup keys. However, Iolus has its own drawbacks. Although it is scalable, this scheme affects the data path. The GSI may become the bottleneck, because it needs to translate the data by decrypting and encrypting, and relay it to the next GSI; besides it also needs to manage the subgroup. Therefore, the delay for the subgroups which are far from the GSC may become substantial. Moreover, the single point failure problem still exits, because the failure in higher level GSI will disconnect all its sublevel groups.

Intra-domain Group Key Management Protocol (IGKMP) [14] is another possible solution for Inter-BS multicast. In IGKMP, a Domain Key Distributor (DKD) entity is defined for key management, and the domain is divided into a number of administratively-scoped areas, which are administrated by Area Key Distributors (AKD). A domain-wide multicast key (MKey, which corresponds to GTEK in IEEE 802.16) is used to encrypt multicast data. The DKD and AKDs form the All-KD-group, by which the DKD transfers the MKey to each AKD. Each AKD and the group members in its area form the Area-Control-group, through which AKD relays the MKey to its members. With a domain-wide MKey, the AKDs do not need translate multicast data any more, and all the AKDs are in the same level in the All-KD-group, thus mitigates the delay problems in Iolus. However, also due to the usage of domain-wide MKey, the member changes in one Area-Control-group will require the update of MKey, thus affects all other subgroups. This is referred to in [15] as 1- affects-n type problem, which weakens the scalability.

4.2. Adaptive Inter-BS Multicast Protocol

We adapt Iolus and IGKMP, and propose Adaptive Inter-BS Multicast Protocol to fit Inter-BS multicast environment. Instead of forming SDT as in [15], we divide the group infrastructure into two parts: the backbone and the wireless connections (between BSs and SSs). The group manager and BSs form the top level of multicast group like All-KD-group in [14]; we call it the backbone group. Different multicast protocols can be applied within backbone group such as hierarchy key tree. The BSs then multicast the traffic they received and decrypted from group manager to their subgroup members. By this hierarchy, communication in backbone and in wireless network will not be confused and the Intra-BS multicast will not be affected regardless of the backbone multicast scheme. Each Intra-BS multicast can even apply different schemes respectively. Furthermore, the scheme could be optimized, as in [15], by re-encrypting the traffic session key instead of re-encrypting the multicast data directly, which will save the huge amount of encryption/decryption of the traffic.

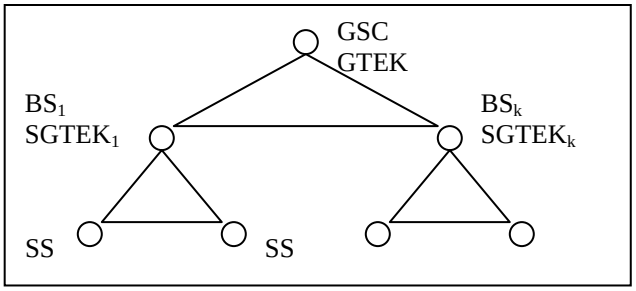

Figure 3 Adaptive Inter-BS Multicast

Our Inter-BS Multicast Protocol adopts the backbone group, thus alleviates the traffic delay due to multiple translations and relays; it also mitigates the single point failure problem in Iolus. On the other hand, because each subgroup has its own GTEK, membership changes in one subgroup will not affect other parts in the group, thus guarantees the scalability to large dynamic group. Moreover, because each BS can adopt its own rekeying scheme, this protocol can take advantage of various popular rekeying algorithms according to the member behavior and terrain environment within the BS. We can further adopt Adaptive Rekeying Scheme [22], which assigns different level and number of keys to each group member. This scheme is suitable to BSs which host both fixed and mobile SSs. Because mobile SSs are more likely to leave the group which will result in rekeying, the BS can group these SSs into one subtree, and allocate complementary key corresponding to the root of that subtree, which is known by all other subroots but not by itself. When a mobile SS

leaves the group, the BS needs to send only one message encrypted by that complementary key to update GTEK to other parts within the BS. On the other hand, BS can also allocate more keys to the members of that subtree, which will reduce the number of messages to update GTEK to the remaining members of that subtree. Moreover, Adaptive Rekeying can also be applied to the backbone group, which may be extended to a hybrid of wireless and wired subgroup headers. That is, there could be both wireless and wired group members within the multicast group.

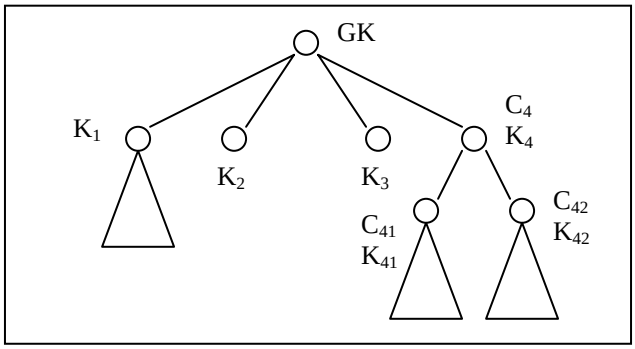

Figure 4. Adaptive Rekeying for Mobile Environment

In Figure 4, GK is group key associated with the root, i.e., the group controller. K_1, K_2, K_3, and K_4 are logic keys as in LHK associating with sub-roots (we will use the logic keys to denote their associated notes as well), while C_4 is the complementary key associating with sub-root K_4 (known to K_1, K_2, K_3, but not K_4). C_4 is assigned here because K_4 is the sub-header that hosts wireless or mobile subscribers. K_{41}, K_{42} are children of K_4 and C_{41}, C_{42} are the corresponding complementary keys. More keys are assigned at this level to facilitate rekeying due to its high dynamic. For example, if a member in sub-tree K_{41} leaves, we only need to send the following messages to update the group key to remaining members:

Message 1. BS $\Rightarrow$ {SS in K_1, K_2, K_3} : C_4 (GK)
Message 2. BS $\Rightarrow$ {SS in K_{42}} : C_{41} (GK)
Message 3. BS $\rightarrow$ SSs in K_{41}: KEK (GK, C_{42})

Figure 5. Adaptive Rekeying update messages

In fact, Figure 5 only shows rekeying in one BS, and all encrypted keys in the updated messages are new version. Message 3 is sent to the remaining SSs in K_{41}, and should be replaced with certain adopted rekeying scheme such as LHK. If extended to backbone group, the leaves will denote sub-headers such as BS instead of SS. By adaptive rekeying scheme, much less messages are needed to update group key while at the cost of only a few additional complementary keys.

Cluster scheme requires the trust on cluster heads (BSs). If the group manager does not want the BSs, which may be manufactured by different vendors, to access the multicast data, it could employ two-tier key scheme which divides the keys into GTEK and subgroup control key (SGCK). Only group members have access to GTEK and BSs distribute only SGCK to handle membership control at subgroup level. This is what [25] defines as semi-trusted systems, which is derived from dual-encryption [26].

5. Efficient Multicast during Handover

IEEE 802.16e adds mobility to WirelessMAN, thus secure and efficient handover becomes critical for mobile WirelessMAN. Besides the ordinary join/leave of group members, the exit/enter will cause many additional rekeys. That is because, when the handover member exits from the Service BS (SBS) and enters the Target BS (TBS), both SBS and TBS need to update their subgroup TEK (SGTEK) due to the intra-BS subgroup member changes. The range of BS is up to 15km, and the mobile speed support is up to 150km/h. That means, even if the vehicle travels from exactly one end of the SBS cell to the other end via the diameter, it will only take about 12 minutes. Besides, the BS can not cover such long range in reality due to the deployment issues such as power and terrains, and some overlap should be provided to ensure smooth handover while cars on highway always drive above 120km/h. Therefore, handover will take place very often for high-speed vehicles, causing many unnecessary group rekeys. That is because the Mobile SS (MSS) is still in the group and should be allowed to access the multicast session, which usually lasts at least half an hour such as TV plays, video conference, etc.

We propose a Delayed Feedback Rekeying Algorithm (DFRA) for MBS during handover to solve the problem above. When the MSS begins handover and exits the SBS, the SBS will not update the SGTEK immediately, because the MSS is still in the top-level multicast group and is allowed to access the multicast traffic, thus the forward secrecy is not a concern at this time. Nevertheless, the SBS needs to make a record for this MSS (in its past handover subgroup member list - PHSML). After the MSS enters the TBS, however, the TBS needs to update its SGTEK in order to provide backward secrecy. That is because the TBS does not know when the MSS joins the multicast group and from which point it is allowed to access the multicast traffic (unless its first SBS makes a record for this which will be passed on to later TBSs). Fortunately, this will not cause much trouble, because it is easy for rekeying upon member join. The TBS only needs to notify its current subgroup members through broadcast connection to update the subgroup key by one greater index using certain one-way hash function, meanwhile sends this updated key to MSS by unicast (through its Primary Management Connection encrypted by KEK). Also, the TBS needs to maintain a current handover subgroup member list (CHSML), to record the SBS from which the MSS switched. If the MSS leaves the multicast group due to certain reasons, the TBS needs to perform subgroup key update upon member leave using certain Intra-BS multicast protocol. Meanwhile, the TBS needs to notify the MSS'

previous SBS according to its entry in local CHSML, in order to make sure this MSS can not access the multicast traffic from that SBS either. If the SBS has already updated its subgroup key upon member leave, or periodically rekeyed due to SGTEK expiration, it will reset the entries for those MSSs in PHSML. Therefore, the SBS need not perform key update, because the MSS is not in the list anymore and is not able to access current subgroup multicast traffic due to key updated already. Otherwise, the SBS should perform subgroup key update upon member leave to ensure backward secrecy. Anyhow, SBS should notify the MSS' previous SBS according to its CHSML as what the TBS did to it, and so on, to ensure all the BSs which have ever served this MSS expel it from accessing multicast traffic.

DFRA could obviate most of the rekeys due to member handover, while still keeping backward and forward secrecy for the multicast group. Moreover, it also solves the ping-pong problem caused by members hovering among adjacent BSs.

6. Conclusion and Future Work

This paper discusses the MBRA in IEEE 802.16 and modifies it as a more efficient algorithm for secure multicast in Intra-BS. We also apply different protocols to Intra-BS and Inter-BS. We propose Adaptive Inter-BS Multicast Protocol which takes advantages of several popular efficient and secure multicast protocols. It not only guarantees backward and backward secrecy, but also alleviates the drawbacks of those popular protocols such as delay of traffic and lack of scalability. It is also adaptive to member behavior, thus suitable for BS whose service is for both fixed and mobile SSs. Moreover, it can be extended to hybrid network with both wired and wireless subscribers in the same multicast group. Finally, we propose DFRA for efficient and secure multicast during handover. For future work, we will finish the data structure and design for these multicast protocols in WirelessMAN, and implement and simulate with QUALNET.

7. References

[1] IEEE Std 802.16-2004: *Air Interface for Fixed Broadband Wireless Access Systems*, 2004.

[2] IEEE Std 802.16e: *Air Interface for Fixed and Mobile Broadband Wireless Access Systems*, 2006.

[3] IEEE Std 802.16-2001: *Air Interface for Fixed Broadband Wireless Access Systems*, 2002.

[4] R. Marks, "A technical Overview of the WirelessMAN Air Interface for Broadband Wireless Access", *IEEE C802.16-02/05*, 2002.

[5] C. Eklund, K. L. Stanwood, S. Wang, R. B. Marks, "IEEE Standard 802.16: A Technical Overview of the WirelessMAN (TM) Air Interface for Broadband Wireless Access", *IEEE Communications Magazine*, June 01, 2002

[6] C. Eklund, R. B. Marks, S. Ponnuswamy, K. L. Stanwood, N. J. M. V. Waes, *WirelessMAN: inside the IEEE 802.16 Standard for Wireless Metropolitan Networks*, Standards Informatin Network, IEEE Press, 2006.

[7] D. Johnston, and J. Walker, "Overview of IEEE 802.16 Security", *IEEE Security & Privacy*, 2004.

[8] S. Xu, M. Matthews, and C.-T. Huang, "Security Issues in Privacy and Key Management Protocols of IEEE 802.16", *Proc. the 44th ACM Southeast Conference (ACMSE'06)*, March 2006.

[9] S. Xu and C.-T. Huang, "Attacks on PKM protocols in IEEE 802.16 and its later versions", *Proc. ISWCS'06*, September 2006.

[10] J. Y. Kuo, "Analysis of 802.16e Multicast/Broadcast group privacy rekeying protocol", *CS 259 Final Project Report*, Stanford University, March 2006.

[11] A. Ballardie, *Scalable Multicst Key Disribution*, 1996. RFC 1949.

[12] H. Harney and C. Muckenhirn, *Group Key Management Protocol (GKMP) Architecture*, July 1997. RFC 2093.

[13] H. Harney and C. Muckenhirn, *Group Key Management Protocol (GKMP) Specification*, July 1997. RFC 2094.

[14] T. Hardjono, B. Cain, and I. Monga, *Intra-domain Group Key Management for Multicast Security*, IETF Internet draft, November 1998.

[15] S. Mittra, "Iolus: A Framework for Scalable Secure Multicasting", *Proc. ACM SIGCOMM'97*, 1997.

[16] S. Setia, S. Koussih, S. Jajodia, and E. Harder, "Kronos: A Scalable Group Re-Keying Approach for Secure Multicast", *Proc. of IEEE Symposium on Security and Privacy*, 2000.

[17] D. M. Wallner, E. J. Harder, and R. C. Agee, *Key Management for Multicast: Issues and Architectures*, June 1999. RFC 2627.

[18] C. K. Wong, M. Gouda, and S. S. Lam, "Secure group Communications Using Key Graphs", *IEEE/ACM Transaction on Networking, Vol. 8, No. 1*, Feb 2000.

[19] M. Waldvogel, G. Caronni, D. Sun, N. Weiler, and B. Plattner, "The VersaKey framework: Versatile Group Key Management", *IEEE Journal on Selected Areas in Communications, Vol. 17, No. 9*, 1999.

[20] A. T. Sherman and D. A. McGrew, "Key establishment in large dynamic groups using one-way function trees", *IEEE Transctions on Software Engineeering, Vol. 29, No. 5*, May 2003.

[21] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas, "Multicast security: A taxonomy and some efficient constructions", *Proc. of the IEEE INFOCOM, Vol. 2*, 1999.

[22] S. Kulkarni and B. Bruhadeshwar, "Adaptive rekeying for secure multicast", *IEICE TRANS. COMMUN., Vol. E85-A, No. 10*, October 2003.

[23] S. Cho, S. C. Chang, C. Yong, "MBRA (Multicast & Broadcast Rekeying Algorithm) for PKMv2", *IEEE C802.16e-04/139*, June 2004.

[24] S. Cho, A. S. Park, C. Yoon, S. C. Chang, K. S. Kim, "A Key Mangement Method for the Multicast Service", *IEEE C802.16e-04/23*, March 2004.

[25] D. Bruschi and E. Rosti, "Secure Multicast in Wireless Network of Miblie Hosts: Protocols and Issues", *Mobile Networks and Applications, VOL. 7*, 2002.

[26] L. Dondeti, S. Mukherjee, and A. Samal, "Scalable secure one-to-many group communication using dual encryption", *Computer Communication, Vol. 23, No. 17*, November 1999.