Efficient and Secure Multicast in WirelessMAN

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

***Abstract*—Multicast delivery of data is a powerful mechanism that has strong potential in next generation networks. The increased efficiency over unicast is a definite advantage, but the use of multicast poses many security risks. Effectively adding security measures to a multicast service is an intriguing problem, especially when the service is deployed in a wireless setting. Next generation IEEE 802.16 standard WirelessMAN networks are a perfect example of this problem, and the latest draft specification of the standard includes a secure protocol solution called Multicast and Broadcast Rekeying Algorithm (MBRA). In this paper, we expose the security problems of MBRA, including non-scalability and omission of backward and forward secrecy, and propose a new approach, ELAPSE, to address these problems. We analyze the security property of ELAPSE and use Qualnet simulations to show its efficiency.**

***Index Terms*—802.16 WirelessMAN, Privacy and Key Management (PKM) Protocol, Multicast and Broadcast Rekeying Algorithm (MBRA)**

I. 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 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 subscriber stations (SS).

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 ingredient 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; performance being measured by communication complexity, center (server) space complexity, and user (member) space 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 these protocols are detailed and ELAPSE (Efficient sub-Linear rekeying Algorithm with Perfect Secrecy), a derivative of the Logical Key Hierarchy is proposed. ELAPSE overcomes the lack of backward and forward secrecy of the 802.16 MBRA and operates more efficiently overall. The rest of the paper is organized as follows. In Section II, we review the IEEE 802.16e solution to secure multicast rekeying, with its weaknesses emphasized. In Section III, related works on other approaches to secure multicast are described, and a complete description of our approach, ELAPSE, follows in Section IV. In Section V, ELAPSE is evaluated for its efficiency using the network simulator Qualnet, and then conclusions are made in Section VI.

II. Current 802.16e Standard

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. The Multicast and Broadcast Rekeying Algorithm (MBRA) is used to refresh traffic keying material for the multicast service of IEEE 802.16. Prior to receiving multicast service, an SS must regsiter and authenticate with a base station (BS), during which the BS decides the level of service to be authorized. By use of 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. A Secondary Management Connection is used to transfer delay-tolerant, standards-based messages within IP datagrams 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, and 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, 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 that is appropriate for a specified SAID. Before proceeding with the details of the current standard, let us briefly discuss a trivial solution for securing multicast traffic.

A. A Trivial Solution

In this trivial solution, multicast traffic is sent from the BS to all SS encrypted using a single group wide session key, or Group Traffic Encryption Key (GTEK). It is assumed that all SS have the current key ready to decrypt the multicast data. When a new SS wishes to join the group, an individual request is sent to the BS for the GTEK. The BS responds to the new SS with a new GTEK, and then also sends the updated GTEK to all existing SS individually (all individual exchanges are encrypted with keys established through a previous authentication mechanism). When a member wishes to leave the group, the BS must again send a new GTEK to all other SS individually. Although offering strong backward and forward secrecy, this trivial solution has many problems, most importantly not being scalable due to the many unicast key exchanges.

B. 802.16 Standard

The IEEE 802.16 standard offers some improvement to this trivial solution. A lifetime is specified for the GTEK and thus the GTEK will expire after a certain amount of time. To ensure timely delivery of new GTEKs before expiration of the current one, the use of a Group Key Encryption Key (GKEK) is specified. The GKEK has a lifetime that parallels the lifetime of the corresponding GTEK. By using this GKEK to encrypt the GTEK, new GTEKs can be broadcast to all SS.

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 (1) 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 Authorization Key (AK) established during authentication. Then, the BS transmits the (2) 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.

$$\text{BS} \rightarrow \text{SS} : \{\text{GKEK}\}_{\text{KEK}} \quad (1)$$

$$\text{BS} \Rightarrow \text{all SS} : \{\text{GTEK}\}_{\text{GKEK}} \quad (2)$$

where $\rightarrow$ stands for a unicast message and $\Rightarrow$ stands for a broadcast message.

There are still two problems with this protocol. Firstly, this protocol is not scalable as it still needs to unicast to each SS. It can be generalized, especially in a potentially large network such as a WirelessMAN, that any rekeying scheme depending on unicast methods is not scalable. 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, 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 a leaving SS from receiving the next GKEK and decrypting the next GTEK.

Note that the lifetimes of GTEKs as specified by the IEEE 802.16 standard are an important security consideration. Currently, the range is specified to be 0.5 hours minimum, 12 hours by default, and 7 days maximum [2]. This lifetime has great leverage on the relationship between scalability and forward/backward secrecy provided by the standard. A long enough lifetime needs to be maintained to allow a BS enough time to individually update the GKEK so the new GTEK can be broadcast. However, longer GTEK lifetimes imply much greater lapses in backward/forward secrecy on member join/leave events, respectively, as there will be more messages encrypted using the given GTEK.

III. 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. Some 802.16 group members also published a book [5] in 2006, which provides a detailed overview of the standard and explains the rationale behind development decisions. The authors of [6] review the standard, analyze the security provided by the standard, and discuss the requirement of mutual authentication between SS and BS. In [7] the PKM protocol is discussed in detail, more attacks on the versions of the PKM protocols listed in [3] and [5] are discovered, and revisions of PKM protocols are proposed. In [8], another attack on PKM version 2 in [2] is

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

There is a report [9] which analyzes the IEEE 802.16 MBRA, which especially focuses on replay attacks against the MBRA, similar to the attacks listed in [6], [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. [10] and [11] are the first few works dealing with secure multicast, in which straightforward, yet not scalable methods, are described. The Iolus approach detailed in [12] is a distributed method in which a hierarchy of agents are 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. However, Iolus may not be directly applicable to the 802.16 environment in which there is only one server (BS) and a number of clients (SS), and may not make the best use of the property of 802.16 that every SS within the radio range of BS can receive the multicast messages in one hop. Kronos [17], 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 [13] and [14], which provide O(log n) communication complexity, where n is the number of group members. There are three schemas in the Versa-key framework [15], 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 LKH+. In [16] a hybrid system is proposed that integrates LKH with a simple flat schema, providing a family of key management algorithms according to the number of members in each subgroup. Each subgroup is then organized as a leaf in the LKH tree. By dividing the group into subgroups with O(log n) members, the algorithm exhibits only O(n/log n) center space complexity. The authors of [16] claim it is the first rekeying algorithm to require only sublinear space at the server.

In this paper, ELAPSE, an alternative to the IEEE802.16 MBRA is proposed. ELAPSE is a more efficient alternative that provides complete backward and forward secrecy to communications, and integrates the advantages of the approaches presented in [16] and [17] to achieve better efficiency.

IV. ELAPSE

We have established that MBRA published in the latest 802.16 standard is insufficient. As mentioned, the MBRA offers only modest improvements over a trivial solution. A proper solution should maintain backward secrecy and forward secrecy. From these goals, an improved MBRA must re-key on member joins, on member leaves, and periodically if there is no member join or member leave. Also, an improved MBRA must be scalable so that its complexity is less than O(n) with respect to the size of the group.

The focus of the approach presented here will be sub-grouping SS so that the GKEK will not be maintained via unicasting to individual SS, but via broadcasting to sub-groups. For every cell of a BS and many SS in a multicast application, the SS will be sub-grouped into $N = 2^k$ sub-groups, with each sub-group maintaining k keys. The exact value of N is to be determined by the implementer to offer the best performance for a given application. For example, an application that averages 600 SS may pick a value of N = 8 sub-groups, each sub-group averaging 75 members and maintaining k = 3 keys. When a new SS requests keying material, it will be grouped into the sub-group with the lowest member count. This is done to keep the sub-groups balanced in size. Otherwise, one sub-group may become very large with respect to the others, and the efficiency of re-keying drops significantly.

Each sub-group maintains a hierarchy of sub-group KEKs (SGKEK) instead of a single GKEK. According to a binary tree hierarchy, each SS within a sub-group will store k SGKEKs. The following figure shows the case for N = 4. In the figure, note that sub-group 1 stores $SGKEK_1$, $SGKEK_{12}$, and $SGKEK_{1234}$, and that $SGKEK_{1234}$ will function as the traditional GKEK did. Also, all future examples will be made with reference to Fig. 1.

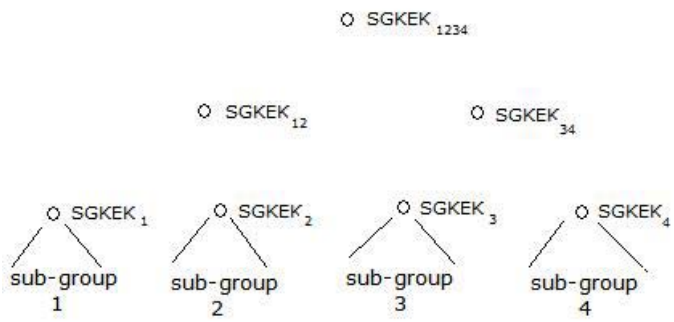

Fig. 1 Basic key hierarchy with 4 sub-groups

In the simplest case of re-keying, there are no member joins or leaves. For reference, every GTEK lifetime shall define a multicast session. In this case the GTEK, or session, expires due to time with no membership changes. The lifetime of the GTEK remains the same as it is in the 802.16 standard. In this case only one message needs to be sent.

$$BS \Rightarrow \text{all SS} : \{GTEK\}_{SGKEK^{1234}} \quad (3)$$

The next case shall be re-keying due to a member join. The member join starts off as it does in the original specification with a key request sent from SS to BS, and a key reply sent from BS to SS. However, the key reply is modified to include a new hierarchy of SGKEKs. So for example when a new SS joins and sub-group 2 is currently the sub-group with the lowest number of members, the key reply is like message (4), with all keys being not current, but updated versions.

$$BS \rightarrow SS : \{SGKEK_{1234}, SGKEK_{12}, SGKEK_{2}\}_{KEK} \quad (4)$$

Message (4) is delivered to all existing SS inside sub-group 2 via unicast as well. While (4) is being delivered, the BS re-keys all existing SS with new versions of appropriate keys in parallel. Continuing with the same situation of a SS joining sub-group 2, (5) and (6) would be delivered to re-key all SS not in sub-group 2.

$$BS \Rightarrow SS_{SG3}, SS_{SG4} : \{SGKEK_{1234}\}_{SGKEK34} \quad (5)$$
$$BS \Rightarrow SS_{SG1} : \{SGKEK_{1234}, SGKEK_{12}\}_{SGKEK1} \quad (6)$$

where SS_{SGi} means the collection of SS within sub-group i.

The updated GTEK is not included in these messages for a performance reason. If during the updates, more SS attempt to join, the situation has not changed. We will refer to this situation as a multi-join. To maintain efficiency, all joining SS in a multi-join event will be placed into the same sub-group, which was the sub-group with lowest number of members at the start of the event, regardless if adding all the joining SS results in the sub-group not being the smallest anymore. The only addition in the case of a multi-join instead of a single join would be another message (4) to each additional SS joining the service. At the conclusion of all SGKEK updates during a join or multi-join, the new GTEK is broadcast to all SS with message (7).

$$BS \Rightarrow \text{all SS} : \{GTEK\}_{SGKEK1234} \quad (7)$$

On a member leaving the multicast service, re-keying proceeds almost exactly as a complete re-keying does for a join situation. If a member from group 2 were to leave, (4b) would be unicast to all remaining SS in sub-group 2. Next, (5b) and (6b) would be broadcast to the respective members not in sub-group 2. The difference between join and leaves is that with a leave there is no benefit of delaying the new GTEK broadcast until the end of the entire re-keying process. Once a SS receives updated SGKEK material, it will definitely be able to decrypt the next GTEK. Therefore, if an SS that has already received new SGKEK material in the middle of another leave process decides to leave as well, no re-keying can be combined and another re-keying process must commence. In this event messages (4b), (5b), and (6b) are sent by the BS; they are identical to their counterparts except for the inclusion of the newest GTEK.

$$BS \rightarrow SS:\{SGKEK_{1234}, SGKEK_{12}, SGKEK_{2}, GTEK\}_{KEK} \quad (4b)$$
$$BS \Rightarrow SS_{SG3}, SS_{SG4} : \{SGKEK_{1234}, GTEK\}_{SGKEK34} \quad (5b)$$
$$BS \Rightarrow SS_{SG1} : \{SGKEK_{1234}, SGKEK_{12}, GTEK\}_{SGKEK1} \quad (6b)$$

V. Evaluation

In the previous sections, we have shown that the MBRA in 802.16e does not provide backward or forward secrecy, and discussed how our ELAPSE approach ensures complete backward and forward secrecy by rekeying on member joins and member leaves. Next, we use theoretical analysis and empirical simulations to evaluate the performance of ELAPSE compared to MBRA.

A. Efficiency Analysis

To evaluate the efficiency of ELAPSE, its communication and space complexity will be compared to other mulitcast approaches. In the simple flat schema, such as the MBRA in 802.16, the server (group manager) should send rekeying messages to each group member respectively, with the new group key (GTEK in 802.16) encrypted with its secrete key (AK) shared with server (BS). Thus the communication complexity is O(n), server space complexity is O(1) (disregarding the individual AKs, which are created during authentication), and member space complexity is O(1). In the LKH schema the communication complexity is O(log n) for the rekeying procedure; the server space complexity is O(n) and member space is O(log n). For the hybrid schema, the communication complexity falls in between the simple schema and LKH schema, i.e., between O(n) and O(log n); the server space falls in between O(1) and O(n) and the member space falls in-between O(1) and O(log n). The exact complexity is determined by the number of subgroups, and the ranges of these complexities illustrate the tradeoffs associated with this choice.

When the number of subgroups increases (from 1 to n), it can be generalized that the communication complexity decreases (from O(n) to O(log n)), while the server space complexity increases (from O(1) to O(n)) and the member space complexity also increases (from O(1) to O(log n)). The authors in [16] find a (perhaps) optimal balance among these tradeoffs by dividing the group into subgroups with O(log n) members each. With this many sub-groups the communication complexity is still O(log n), the same degree as in LKH schema, while the server space complexity is down to O(n/log n), and the member space is O(log n). ELAPSE, due to its similar use of sub-grouping, exhibits the same communication and space complexities.

B. Simulation Results

To compare the performance, we simulate both ELAPSE and the 802.16 MBRA using Qualnet. Due to the unfinished nature of the 802.16 standard, many execution parameters such as a key request time out, GTEK lifetime, etc. are not completely defined and were chosen arbitrarily by the authors. The values chosen were within reasonable range such that no generality is lost.

Two simulation runs were executed for the MBRA and three variants of ELAPSE, using 2, 4, or 8 sub-groups respectively. The first simulation run was 100 seconds long, and the second was 1000 seconds. 16 SS nodes were simulated with 1 BS delivering one multicast session, and the SS randomly joined and left the session over the entire course of a simulation run. To ensure fairness, the same random number seed, implying the same join and leave pattern for the SS, was used for all the algorithms on the same run. Using the BS as point of reference for collecting statistics, the total number of messages sent from the BS was used to gauge efficiency.

Messages were tallied as unicast or multicast. Broadcast messages such as broadcast GTEK update mode messages were counted as multicast. Counting messages with the 802.16 was straightforward, as key response messages sent on

join and leave, and GKEK update mode messages were counted as unicast. The broadcast GTEK update mode message was counted as multicast. For ELAPSE, all key response messages within the sub-group of the joining/leaving node were counted as unicast. The other messages, SGKEK and GTEK updates, were counted as multicast.

A point about the implementation of the 802.16 MBRA must be made with respect to SS join and leave events. In the current standard, there is no explicit behavior defined, so we will assume the BS rekeys the entire group every join and leave. If it is to be assumed that no rekeying is performed on member join and leaves and only on GTEK expiration, the number of messages sent would be drastically lower (equal to the number of join events that occurred during simulation). However, there would be lapses in secrecy on every join (and leave) equivalent to the amount of data sent before (and after). For these reasons, rekeying on SS joining and leaving was included with the 802.16 MBRA simulation so that all algorithms could be compared strictly in terms of efficiency, with the requirement that the algorithm ensures perfect backward and forward secrecy.

Figure 2 shows the results of the 100 second long simulation runs of the different algorithms. To effectively compare the variants of ELAPSE, the number of unicast and multicast messages were totaled together. Using this total, ELAPSE and the 802.16 MBRA can be compared equally. For the MBRA simulation, the BS delivered 1017 messages. The three variants of ELAPSE using 2, 4, and 8 sub-groups delivered 675, 538, and 524 messages, respectively. For the 1000 second simulation, whose results are shown in Figure 3, a longer GTEK lifetime and less aggressive join/leave behavior was chosen compared to the 100 second simulation. The BS running ELAPSE variants in the simulator sent 774, 585, and 566 messages, respectively. The BS running 802.16 MBRA sent 1204 messages.

From the above simulation results, it is clear that the ELAPSE variants outperformed the 802.16 MBRA. However, as stated earlier there is increased state required with such a hierarchical approach. When using ELAPSE with 2 sub-groups, each SS must maintain 1 extra key, and the BS must maintain 2 extra keys. For 4 sub-groups, it becomes 2 extra keys and 6 extra keys, and when using 8 sub-groups the total is 3 extra keys and 14 extra keys at the SS and BS respectively.

It is well known that the increased communication efficiency comes at a cost of increased state, so based on the theoretical efficiency discussed above, when there are at most 16 SS, using ELAPSE with 4 sub-groups is the optimal choice. This is because the optimal number of sub-groups is achieved when each sub-group contains O(log n) members. With a maximum of 16 SS at a time, we have $\log_2(16) = 4$, which is the optimal choice. Similarly, the server space requirement increases by 6 keys to O(n) = 7 keys (excluding the GTEK and AK), and the member space requirement becomes O(log n) =3 keys.

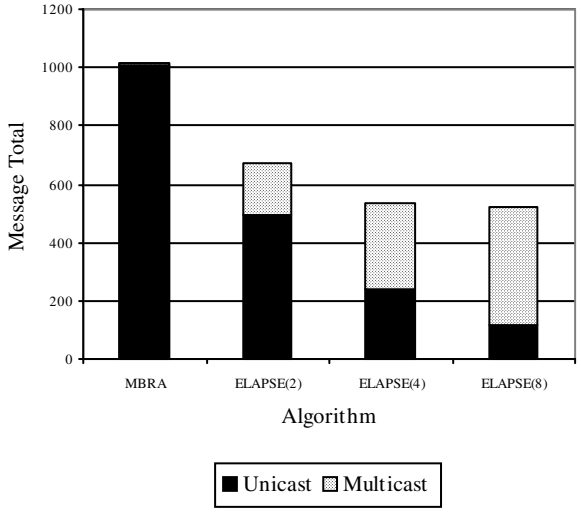

Fig. 2 Messages sent from BS - 100 second simulation

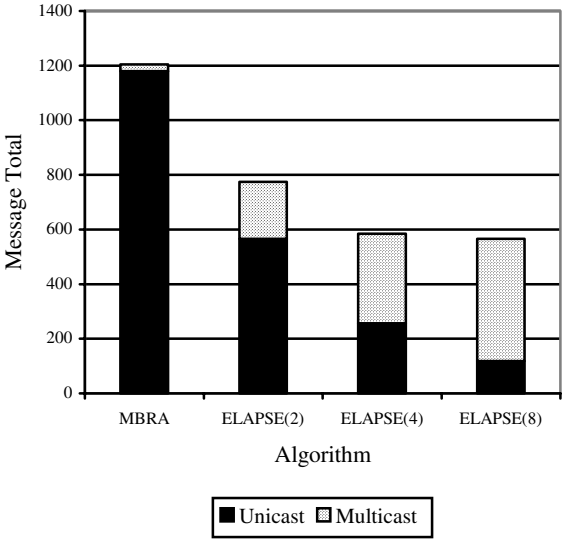

Fig. 3 Messages sent from BS – 1000 second simulation

VI. Concluding Remarks

In this paper we have reviewed the challenges of secure multicast, and analyzed the MBRA of IEEE 802.16e, as it is a noteworthy example of these challenges emerging in next generation networks. While the algorithm at present is in the draft stage, it does have notable weaknesses. In terms of security, it is an incomplete solution by not guaranteeing secrecy of messages before and after member joins and leaves, respectively. As for distributing keying material, it is inefficient, and does not take advantage of the recent research demonstrating the effectiveness of hierarchical approaches. The approach presented in this paper, ELAPSE, provides backward and forward secrecy and outperforms the 802.16 MBRA in simulation. This does come at a cost of increased server and member space requirement, but this tradeoff is a

matter of heightened requirements on the hardware that is to actually implement the 802.16 standard. Given the rapidly decreasing cost of client side hardware and the substantial requirements already in place on the server hardware, we believe the increased space requirement is reasonable and acceptable.

In the future work, we will continue to implement a prototype of ELAPSE and extend the scale of the experiments in order to evaluate the performance and determine the appropriate values of other parameters of ELAPSE in a large network. Moreover, we will investigate a dynamic subgrouping approach in which the number of subgroups will dynamically change according to the recent maximum number of members in the multicast service.

ACKNOWLEDGEMENT

The authors would like to thank Naveen Santhapuri, also from the University of South Carolina, for his assistance with Qualnet and extending its use for specialized wireless network simulations.

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, 2005.

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

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

[5] 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.

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

[7] S. Xu, M. Matthews, and C. T. Huang, "Security Issues in Privacy and Key Management Protocols of IEEE 802.16", Proceedings of the 44th ACM Southeast Conference (ACMSE 2006), March 2006.

[8] S. Xu, and C. T. Huang, "Attacks on PKM protocols in IEEE 802.16 and its later versions", ISWC06, September 2006.

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

[10] A. Ballardie, "Scalable Multicst Key disribution", RFC 1949, 1996.

[11] H. Harney, and C. Muckenhirn, "Group Key Management Protocol Specification", RFC 2093, 1997.

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

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

[14] 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.

[15] 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.

[16] R. Canetti, T. Malkin, and K. Nissim, "Efficient communication-storage tradeoffs for multicast encryption," in Advances in Cryptology-EUROCRYPT'99, 1999.

[17] 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.