International Journal of Engineering, Mathematical and Physical Sciences
ISSN: 2517-9934
Vol:8, No:9, 2014

Survey of Key Management Algorithms in WiMAX

R. Chithra, B. Kalavathi, J. Christy Lavanya

***Abstract*—**WiMAX is a telecommunications technology and it is specified by the Institute of Electrical and Electronics Engineers Inc., as the IEEE 802.16 standard. The goal of this technology is to provide a wireless data over long distances in a variety of ways. IEEE 802.16 is a recent standard for mobile communication. In this paper, we provide an overview of various key management algorithms to provide security for WiMAX.

***Keywords*—**Broadcast, Rekeying, Scalability, Secrecy, Unicast, WiMAX..

I. Introduction

WiMAX (Worldwide Interoperability for Microwave Access). It is a subset of IEEE 802.16 standard. The main aim of WiMAX is to provide high internet service access to the users of wireless metropolitan area network (wireless MAN). Multicast is one of the most popular service in the network, which provides an efficient large scale content distribution. To provide secure multicast service, WiMAX uses key management concept in the distribution. WiMAX uses the protocol called Privacy Key Management (PKM) protocol to provide secure key distribution between BS (Base Station) and SS (subscriber station). The security factors such as authentication, authorization, key exchange data encryption and decryption is achieved by PKM protocol. For secure Multicast service, WiMAX has various key concepts like MBRA (Multicast and Broadcast Rekeying Algorithm), ELAPSE (Efficient sub Linear Rekeying Algorithm with Perfect Secrecy), SRA (Scalable Rekeying Algorithm), Novel and Efficient Rekeying Scheme, and Efficient Rekeying Scheme depends on Linear Ordering of Receivers (LORE).

II. Overview of Keying Algorithms

A. Multicast and Broadcast Rekeying Algorithm

Multicast and Broadcast Service (MBS) of IEEE 802.16e (Mobile Wireless Network) is an additional feature for broadband wireless standards. Initially MBRA is designed to provide strong authentication between SS and BS. MBRA is used in intra-broadcast service [2]. It allows a BS to distribute the same set of data to more SS simultaneously. For that each SS should be authenticated by BS using Privacy Key Management technique. IEEE 802.16e introduces MBRA as a basic rekeying algorithm to generate, update and distribute two set of keys. That is Group Key Encryption key and Group key Traffic Encryption key as proposed in [1]. Initially SS may get the initial Group key Traffic Encryption key (GTEK), mainly used to encrypt the multicast traffic. This can be done during primary connection management by sending key request and key reply messages. BS consists of two Group key update command messages: One is for GKEK update mode [3] and another for GTEK update mode [3]. These update messages are used to update and distribute traffic keying material regularly. GKEK is used to encrypt the GTEK in GTEK update mode. Then BS can transmit key update command message for GKEK update mode to each SS through primary management connection. This message contains the new GKEK encrypted with the Key Encryption Key (KEK). This key can be derived from Authentication key (AK) [3] during authentication process. In MBRA, messages are transmitted in two ways [3], [5].

BS can transmit KEK (GKEK) to each SS through unicast message which has been encapsulated by KEK of each SS.

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

BS can transmit (GKEK) GTEK to all SS in order to update the GTEK through broadcasting to all SS.

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

In MBRA, BS has to transmit or unicast a new keys to each SS in the network. When the number of SS increases, the unicast messages will also be increased. So the communication overheads will also occur. Hence this method is neither scalable nor efficient. Also it can consequently lead to vulnerable attacks, because it does not address forward secrecy (a member leaving a group cannot able to read any future messages) and backward secrecy (a new member is joining a group will not get any access to previous messages).

B. Efficient sub Linear Rekeying Algorithm with Perfect Secrecy

Efficient sub Linear Rekeying Algorithm with Perfect Secrecy is proposed in [3], [5], [7] to overcome the limitations of MBRA. This method is a tree-based rekeying scheme which solves the issues like scalability, forward and backward secrecy of MBRA. This method is developed using logical key hierarchy structure based on binary tree concept [7].

ELAPSE divides the number of SS into N=log(n,2) sub groups, where n is the number of SS and each sub group maintains a set of hierarchical named sub group KEK's (SGKEK) instead of maintaining single GKEK. All SS maintain the same set of GTEK and each SS in each subgroup

MsR.Chithra, Assistant Professor, is with the Department of Information Technology, K. S. Rangasamy College of Technology, Tamil Nadu India (Mobile: 9994312842 ; e-mail: chithra@ksrct.ac.in).

Dr.B. Kalavathi, Professor, is with the Department of Information Technology, K.S. Rangasamy Institute for Engineering and Technology, Tamil Nadu India.

J. Christy Lavanya, PG Scholar, is with the Department of Information Technology, K. S. Rangasamy College of Technology, Tamil Nadu India (Mobile: 8144754845; e-mail: lavanyasrit06@gmail.com).

saves a setoff SGKEK.

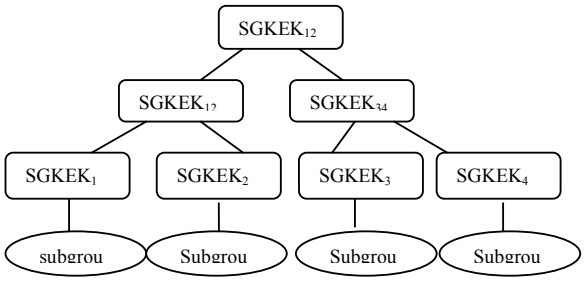

Fig. 1 Group formed based on binary tree concept

By the Fig. 1 SS in subgroup$_1$ stores the group keys SGKEK$_1$, SGKEK$_2$, SGKEK$_{1234}$. The SGKEK$_{1234}$ is similar to GKEK in MBRA. In MBRA, GKEK is not delivered to each BS by unicast message instead it is distributed among the subgroups by broadcast message. There are no member can join or leaves in simple rekeying concept. Therefore every GTEK lifetime define a multicast session. In this, GTEK lifetime or session expires due to time with no membership changes, then BS broadcast a new GTEK encapsulated by SGKEK$_{1234}$to all SS. The broadcast message is

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

1) Member Join Event

When a new SS enters into base station coverage area and subgroup$_2$ has the lowest number of members, then BS assign the newly joined member to the subgroup$_2$. Then BS needs to update the group keys among its members. So that BS unicast message (4) to newly joined SS and all joined SS in the subgroup$_2$. Then Key Encryption Key (KEK) is used to encapsulate the message (4) to each SS and message (4) contains all new group keys from subgroup$_2$ to the root of binary tree.

$$BS \rightarrow \text{SS}_{\text{SG2}}\text{and new SS}\{\text{GTEK}, \text{SGKEK}_{1234}, \text{SGKEK}_{12}, \text{SGKEK}_2\}_{\text{KEK}} \quad (4)$$

BS sends two broadcast message to update the group keys and to provide balanced secrecy.

$$BS \Rightarrow \text{SS}_{\text{SG3}}, \text{SS}_{\text{SG4}}\{\text{GTEK}, \text{SGKEK}_{1234}\}_{\text{SGKEK}_{34}} \quad (5)$$
$$BS \Rightarrow \text{SS}_{\text{SG1}}\{\text{GTEK}, \text{SGKEK}_{1234}, \text{SGKEK}_{12}\}_{\text{SGKEK}_1} \quad (6)$$

2) Member Leaves Event

The group keys needs to be updated when an existing SS leaves from BS coverage area. This process is same as done in the member join event. When one SS of subgroup$_2$ leaves the BS, then the BS should unicast message to all remaining SS in subgroup$_2$. It also sends two broadcast messages to all SS except subgroup$_2$.

$$BS \rightarrow \text{SS}_{\text{SG2}}\{\text{GTEK}, \text{SGKEK}_{1234}, \text{SGKEK}_{12}, \text{SGKEK}_2\}_{\text{KEK}} \quad (7)$$
$$BS \Rightarrow \text{SS}_{\text{SG3}}, \text{SS}_{\text{SG4}}\{\text{GTEK}, \text{SGKEK}_{1234}\}_{\text{SGKEK}_{34}} \quad (8)$$
$$BS \Rightarrow \text{SS}_{\text{SG1}}\{\text{GTEK}, \text{SGKEK}_{1234}, \text{SGKEK}_{12}\}_{\text{SGKEK}_1} \quad (9)$$

ELAPSE leads to poor scalability when the tree depth increases. It consumes more bandwidth when the number of unicast message increased, so the number of transmissions, communication overheads and energy consumption will be more. It leads to storage overheads because BS needs to store more group keys to maintain the subgroup.

C. Efficient Rekeying Scheme Depends on Linear Ordering of Receivers (LORE)

This method is proposed in [4] in order to overcome the security problems of MBRA such as forward and backward secrecy. Also it protects the large group such as Multicast and Broadcast group. This scheme has less communication and storage cost.

LORE consists of three operations:

1) Key Assignment

A group can have n number of users. A central key server (KS) generates two set of keys for each users. (ie)Forward key set (Fset) and Backward key set (Bset). Each key set has n keys to encrypt new group key. KS assigns each user as a U_i (i indicates the order of user among n users).

2) Join Operation

Whenever a user joins a group LORE update a group key GK to increase the backward secrecy.

$$KS \rightarrow \text{G}\{\text{GK}'\}_{\text{GK}} \quad (10)$$
$$KS \rightarrow \text{u}_\text{i}\{\text{GK}'\}_{\text{SK}_\text{i}} \quad (11)$$

U_i cannot know the following group key.

3) Leave Operation

Whenever a user leaves a group LORE update a group key GK to increase the forward secrecy

$$KS \rightarrow \text{G}\{\{\text{GK}'\}\text{f}_{\text{i}+1}\}_{\text{GK}} \quad (12)$$
$$KS \rightarrow \text{G}\{\{\text{GK}'\}\text{b}_{\text{i}-1}\}_{\text{GK}} \quad (13)$$

f_i+1 and b_i+1 is known by all the users but leaving user U_i cannot know the subsequent group key GK'. It requires O(log(n)) messages for join operation. So it lacks collusion protection.

D. Novel and Efficient Rekeying Scheme

This method is proposed in [5] in order to overcome the issues of MBRA and ELAPSE. It is more efficient than MBRA because it reduce communication overheads when numbers of SS increases.

Efficient rekeying scheme depends on three events:

1) Member Join Event

Whenever a new member is joined to BS, then BS should transmit at present GKEK and GTEK to newly joined member. That should be protected by individual key {KEK}.

$$BS \rightarrow \text{SS}\{\text{GKEK}, \text{GTEK}\}\text{KEK} \quad (14)$$

2) Lifetime of Group Key Expires

At this time BS should send a new key to each SS, so that SS can generate a new key by applying one way hash function on present group key.

$$GTEK_{new} = f(GTEK_{old})$$
$$GKEK_{new} = f(GKEK_{old})$$

3) Member Leaves Event

During this time BS broadcast a random number{r} to all SS so that should be protected by old GKEK. By using the random number and old GKEK SS can generate new group key.

$$BS \Rightarrow \text{ all SS}\{\text{r}\}_{\text{GKEK}} \quad (15)$$
$$GTEK_{new} = f(GTEK_{old)}$$

At member leaves event, a SS leaves the group but it is still in the transmission range of BS, they can easily decrypt the broadcast a new group key. So secrecy is not fully achieved.

E. Scalable Rekeying Algorithm

A new method SRA is proposed [7] in order to overcome the issue of scalability is ELAPSE. This method uses a fixed number of subgroups which means the tree has a constant depth. So it provides poor scalability. SRA is implemented using linear list structure to make a complete binary tree for improving the scalability of ELAPSE.

SS	GROUPKEY	L1	L2

Fig. 2 A linear linked list node

SS indicates the number of current SS in the certain subgroup. Group key denotes the subgroup group key. It consists of pointer fields L1 and L2 which indicates the SS of that subgroup and points to the next subgroup. SRA uses log(n,2) to divide the group into subgroup. Where n is the number of SS in the BS. Based on this, number of subgroups can be increased or decreased.

Group key updating or rekeying occurs on three events:
Lifetime expiry of GTEK/GKEK
Member Join Event
Member Leave Event

SRA and ELAPSE perform the same function for the event of lifetime expiry GTEK/GKEK. For the member join/leave event it should add/delete subgroup at particular time to increase or decrease subgroups based on log(n,2)[7]. In complete binary tree aren't node has the index of i, left child has the index of 2i and right child has the index of 2i+1. SRA uses the complete binary tree concept to maintain the subgroups.

1) One Subgroup Creation

When the number of SS in the BS coverage area increases to three members then based on the optimal value log(n,2) one new subgroup should be added. For that, one subgroup is break into 2 subgroups SG1 and SG2 and added separately. Based on complete binary tree parent node has index 1, $subgroup_1$ has index 2 and $subgroup_2$ has index 3. BS unicast new GTEK to all SS and two messages such as $SGKEK_1$ and $SGKEK_2$ to SG1 and SG2 to perform an updating /rekeying process.

$$BS \rightarrow \text{SS}_{\text{SG1}}\{\text{GTEK}, \text{SGKEK}_1\}\text{KEK} \quad (16)$$
$$BS \rightarrow \text{SS}_{\text{SG2}}\{\text{GTEK}, \text{SGKEK}_2\}\text{KEK} \quad (17)$$

As the number of SS increases above 5 then new subgroup is added from left to right child to satisfy the property of complete binary tree. So SS of SG1 is divided into 2 new subgroups as SG11 and SG12.

2) Three Subgroups Creation

After one new subgroup is inserted BS has to update the group keys so it should unicast the message to SG11 and SG12

$$BS \rightarrow \text{SS}_{\text{SG11}}\text{and new SS}\{\text{GTEK}, \text{SGKEK}, \text{SGKEK}_1, \text{SGKEK}_{11}\}\text{KEK} \quad (18)$$
$$BS \rightarrow \text{SS}_{\text{SG12}}\{\text{GTEK}, \text{SGKEK}, \text{SGKEK}_1, \text{SGKEK}_{12}\}\text{KEK} \quad (19)$$

SG2 is divides into two subgroups SG21 and SG22 when the member of SS increases to 11 or less than 11.

In the member leave event, if some of SS leaves from BS coverage area then number of subgroups based on log(n,2) should decreased. When number of SS become less than 12, then SG21and SG22 should join together to form one subgroup (ie) SG_{2b}. Then BS unicast a message to update the group keys

$$BS \rightarrow \text{SS}_{\text{SG2b}}\{\text{GTEK}, \text{SGKEK}, \text{SGKEK}_{2b}\}\text{KEK} \quad (20)$$

TABLE I
COMPARATIVE ANALYSIS OF VARIOUS ALGORITHMS

Scheme	Forward & Backward Secrecy	Scalability	Admin Cost In Bs	Sub-Grouping	Life Time Of Keys
MBRA[2], [5]	Not Supported	Very Weak	Low	No	Short
Xu et al.[2]	Supported	Weak	High	No	Short
J.Brown et al.[5]	Supported	Good	High	Yes	Short
GKDA[1]	Supported	Good	High	Yes	Short
Sun et al.[4]	Supported	Good	High	Yes	Short
G.Kambourakis[6]	Supported	Good	Low	Yes	Long
ELAPSE[3,7]	Supported	Good	High	Yes	Short
SRA[7]	Supported	Very Good	High	Yes	Short

III. Conclusion

In this chapter, we have reviewed and analyzed several algorithms used for mobile WIMAX. Especially multicast and broadcast rekeying algorithm, ELAPSE, SRA etc. we analyzed the algorithms based on several parameters and factors such as scalability, forward and backward secrecy, sub grouping, computational cost etc. From the comparison SRA provides high scalability property under our rekeying algorithm. Because it creates the subgroups dynamically based on existing SS and make a good balance between the numbers of SS in the each subgroup. By processing the rekeying algorithm number of unicast messages is reduced, so it overcomes the transmission overhead.

References

[1] H. Li, G. Fan, J. Qiu, X. Lin, GKDA,"A group-based key distribution algorithm for WiMAX MBS security", in: PCM 2006, in: LNCS, vol. 4261, Springer Verlag, 2006, p. 310318.

[2] S. Xu, C.-T. Huang, and M. M. Matthews, "Secure Multicast in WiMAX," Journal of Networks, vol. 3, pp. 48-57, 2008.

[3] C.-T. Huang, M. Matthews, M. Ginley, X. Zheng, C. Chen, and J. M. Chang, "Efficient and Secure Multicast in WirelessMAN:A Cross-layer Design," Journal of Communications Software and Systems, vol. 3, pp. 199-206, 2007.

[4] H.Sun, S.Chang ,S.Chen, C.Chiu ," An Efficient Rekeying Scheme for Multicast and Broadcast(M & B) in Mobile WiMAX ," in IEEE Asia-Pacific Services Computing Conference,2008.

[5] J. Brown, X. Du, and M. Guizani, "Efficient rekeying algorithms for WiMAX networks," Security and Communication Networks, vol. 2, pp. 392–400, 2009.

[6] G. Kambourakis, E. Konstantinou, and S. Gritzalis, "Revisiting WiMAX MBS security," Computers and Mathematics with Applications, vol. 60, pp. 217-223, 2010.

[7] M. M. G. Sadeghi, B. M. Ali, M. Ma, J. A. Manan, N. K. Noordin, and S. Khatun, "Scalable Rekeying Algorithm in IEEE 802.16e," in 17th Asia-Pacific Conference on Communications (APCC), Sabah, Malaysia, 2011, pp. 726-730.