An Efficient Rekeying Framework for Multiple Multicast and Broadcast Groups in Mobile WiMAX

Hung-Min Sun[1], Shih-Ying Chang[1], Chi-Yi Kao[1], Chieh Hsing[1], and Chien-Chien Chiu[2]
[1]*Deptepartment of Computer Science, National Tsing Hua University, Taiwan, R.O.C.*
[2]*WiMAX Center of Networks & Multimedia Institute, Institute for Information Industry, Taipei, Taiwan, R.O.C.*
hmsun@cs.nthu.edu.tw, godspeed@is.cs.nthu.edu.tw, and vittorio@nmi.iii.org.tw

Abstract*- IEEE 802.16e is an emerging wireless technology, it is also called mobile WiMAX due to its mobility, which supports seamless services under vehicular speed. Multicast/Broadcast (M&B) in WiMAX is very useful for several applications, such as multimedia services and streaming stock quotes. IEEE 802.16e defines Multicast and Broadcast Rekeying Algorithm (MBRA) to protect M&B group communication; however, MBRA lacks forward secrecy and backward secrecy. According to the properties of mobility and multiple M&B groups, the conventional rekeying schemes which provide forward and backward secrecy will incur another problem, burst rekeying problem, which rekeying procedures are frequently triggered. In this paper, we propose a new framework cooperating with batch rekeying algorithms to reduce the number of triggered rekeying procedures without affecting security. The simulation result shows that we can mitigate the burst rekeying problem to get better performance.*

Keywords: Batching rekeying, communication system security, multicast security, wireless multicast.

1. Introduction

In IEEE 802.16 family, the recent standard for mobile communication, 802.16e (802.16-2005) [4], is an important milestone in wireless communication technologies. Worldwide Interoperability for Microwave Access (WiMAX) [5] is a forum responsible for certifying the products of IEEE 802.16. IEEE 802.16e is also called mobile WiMAX due to its mobility, which supports seamless services under vehicular speed. WiMAX provides wider converge and higher bandwidth than conventional wireless technologies, such as WiFi (IEEE 802.11) [6]. Thus, WiMAX will largely enhance the quality of wireless access network and be helpful for spreading associated wireless applications. Multicast/Broadcast (M&B) service in WiMAX is useful for several applications, such as multimedia services and streaming stock quotes [13] because service providers can efficiently distribute the same contents to the users within a M&B group with low bandwidth consumption.

Most multicast applications require secure mechanisms to protect communication within a group. Three requirements needed for securing group communication are listed as follows [11]. First is group confidentiality. The messages exchanged within a group can not be sniffed by attackers. Only authorized group members can obtain multicast and broadcast messages. Therefore, all messages exchanged within a group should be encrypted by a group key shared by only authorized group members. Second is forward secrecy. If an attacker compromises any subset of old group keys, he still can not obtain any subsequent group keys. This property means that a leaving user can not know any group key that will be used in later sessions. In this case, the group key used in current session should be updated when a user leaves the group. Third is backward secrecy. If an attacker compromises a set of group keys, he can not obtain preceding group keys. This property means that a new joining user can not know the group key used in previous sessions. Similarly, the group key used in current session should be updated when a user joins the group. For convenience, we call the updating operations for forward secrecy and backward secrecy *rekeying*.

Although IEEE 802.16e [4] defines Multicast and Broadcast Rekeying Algorithm (MBRA) to protect M&B group communication, some research [7][16] show that MBRA lacks forward secrecy and backward secrecy because MBRA is periodically triggered without reflecting the changes in group membership.

Many schemes have been proposed, such as LKH [8] , LKH+ [10], OFT [9] and so on, to secure

group communication since secure group communication have been investigated several years. Most schemes which meet the aforementioned security requirements require O(log(n)) messages where n is the number of members in a group to update keys because these schemes update keys via a key tree. Although these proposed schemes can meet aforementioned security requirements, they will incur another problem in the cases of multiple multicast groups which the communication in each group is protected by different group key.

Considering the cases of multiple groups, the rekeying procedure will be triggered frequently. When a user moves from a group to another group, most schemes require two rekeyings. One is for forward secrecy and the other is for backward secrecy. We can infer that the overhead of rekeying will be extremely large when there are multiple large dynamic groups; we call this issue *burst rekeying problem*. To the best of our knowledge, none of researches discuss this issue in Mobile WiMAX.

This paper is organized as follows. Background is described in Section 2. Section 3 states the basic construction of the proposed framework. In Section 4, we present the detailed construction of the proposed framework. In Section 5, we describe the design of the experiments and the simulation result. Finally, we conclude in Section 6.

2. Background

2.1 Mobile WiMAX network architecture

A WiMAX network [2] is composed of two parts, which are handled by different network providers, Network Access Provider (NAP) and Network Service Provider (NSP). NAP builds one or more Access Service Networks (ASN), which provide WiMAX radio access infrastructure for one or more NSPs and radio access functions for Mobile Station (MS) also called Subscriber Station (SS). NSP constructs Connectivity Service Network (CSN), which supplies IP connectivity and WiMAX bandwidth services to MS. ASN can be separated into two parts, one or more Base Stations (BS) and one or more ASN Gateways (ASN-GW). CSN comprises AAA server to execute authentication, access control and accounting functions. Fig. 1 illustrates WiMAX network architecture.

To protect confidentiality of M&B, multicast and broadcast messages are encrypted by a Group Traffic Encryption Key (GTEK). A WiMAX network can be composed of several M&B groups in which each group is protected by an individual GTEK. Besides that, the coverage of a M&B group

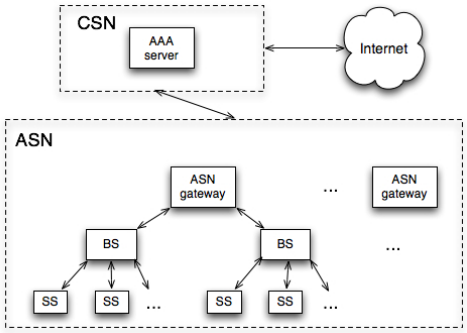

Figure 1 WiMAX network architecture

can comprise one BS or several BSs. More importantly, when MSs frequently move from one M&B group to another, this situation will result in a burst rekeying problem.

2.2 Batch rekeying

Batch rekeying [1], which processes a batch of join and leave requests in a group, is majorly designed for mitigating inefficiency problem in individual rekeying [8], which processes a request at a time. The overhead for processing multiple requests is close to that for processing a single request. An approach [14] can achieve that the messages required for multiple requests is equivalent to that required for a single request by using exclusive key set. Another approach [15] uses Chinese Remainder Theorem (CRT) to optimize the overhead of batch rekeying. Consequently, the overhead of multiple requests can be the same as that for a single request by using batch rekeying.

However, batch rekeying is unsuitable for dynamic groups in most cases since it is hard to obtain multiple requests at the same time. In other words, users rarely leave and join a group at the same time. Therefore, batch rekeying procedures are often triggered periodically for practice.

Our framework does not have the limitation of periodical trigger because our framework can naturally result in the cases of multiple requests as described in Section 3. Thus, our framework can well cooperate with batch rekeying.

3. Basic Construction of the Proposed Framework

If we want to ensure the forward and backward secrecy, the rekeying procedure will be frequently triggered in mobile WiMAX. Note that MBRA does not support forward and backward secrecy. In general, the rekeying overhead for ensuring forward and backward secrecy in a single group would be O($log(n)$) [8][9][10]. Obviously, the cost will be extremely large for multiple groups. Fig. 2

gives an example about rekeying in multiple groups. In this example, we assume that there are only two groups and two MSs move between them. In the previous schemes, both MS *a* and MS *b* trigger 4 rekeying procedures to make total 8 rekeying procedures. More precisely, we assume that *n* is 256 in these two groups. This requires total 8**log*(256) = 64 messages for rekeying.

If many MSs frequently move among multiple groups, the number of triggered rekeying procedures will be extremely large. This overhead may lead to delay in communication which we called burst rekeying problem. In this paper, we propose a framework to address this problem.

A MS has three behaviors. (1) Logging in WiMAX networks. (2) Logging off WiMAX networks. (3) Handover among different groups. Anyway the first two behaviors must trigger rekeying procedures defined in Section 4 we call LocalizedRekeying(*i*) where *i* is group ID. In our framework, however, case 3 does not always require rekeying compared with the previous schemes. We achieve this property by recording two time, log-in time of the MS *m* denoted by T_MS(*m*) and the latest key update time of the group *i* denoted by T_G(*i*), and using batch rekeying algorithms.

In original design, moving from a serving group to a target group will trigger two rekeying procedures. One is triggered in the serving group for forward secrecy and the other is triggered in the target group for backward secrecy. We call them forward update and backward update for convenience. However, our scheme can omit forward update and backward update under some conditions without affecting forward secrecy and backward secrecy.

For forward update, we can delay the time to trigger the rekeying procedure until the MS logs off WiMAX networks, since accessing the multicast contents provided by all groups is legal if the MS still subscribes WiMAX network services. After the MS logs off the network, all groups that the MS knows the latest GTEKs should be triggered the rekeying procedures. Note that not all groups that the MS have ever stayed should be triggered rekeying. Some of these forward updates can be omitted if the GTEKs of these groups have been updated before the MS logs off the network. For example, some MSs log in or log off from these groups. Besides that, we use batch rekeying to make the cost of the forward update close to individual rekeying since the rekeying procedures triggered in this case is to conduct multiple group membership changes.

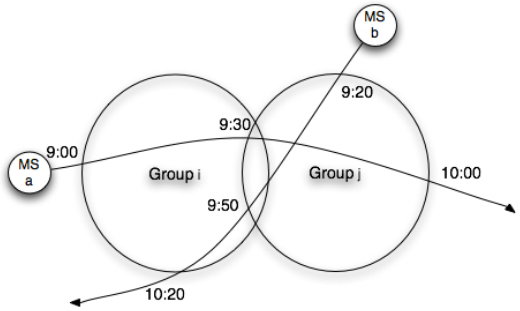

Figure 2 MS *a* moves from group *i* to group *j* and MS *b* moves from group *j* to group *i* at different times.

For backward update, we can omit this update in some situations. If T_MS(*m*) is earlier than T_G(*i*), this means that the MS *m* has the privilege to access the session protected by the latest GTEK in group *i* although the MS *m* was not in group *i* before. Therefore, the group *i* requires no rekeying. The group manager can directly send current GTEK to *m*. Otherwise, if T_MS(*m*) is ≥ T_G(*i*), the rekeying procedure is still required.

Take Fig. 2 as an example, when MS *a* logs in a WiMAX network from group *i* at 9:00 and logs off the WiMAX network from group *j* at 10:00, undoubtedly these two events will trigger 2 rekeying procedures. When MS *a* moves from group *i* to group *j*, forward update can be delayed until MS *a* logs off the WiMAX network. In this case, backward update can be omitted since the joining time 9:00 is earlier than the latest key update time 9:20. Note that we assume that Ms *a* has the privilege to access the session between 9:20 to 9:30 in group *j* because he joined the WiMAX network at 9:00. After MS *a* leaves the WiMAX network, the forward update in group *i* should be triggered. However, this update can be omitted. MS *a* does not know the latest GTEK in group *i* because MS *b* moves from group *j* to group *i* at 9:50 and triggers a batch rekeying. Note that the batch rekeying means that this rekeying is for one member joining (MS *b*) and one member leaving (MS *a*). As a result, total 2 rekeying procedures are triggered by MS *a*. MS *a* and MS *b* will require to trigger total 5 rekeying procedures. Comparing to the previous schemes, we can reduce 8 rekeying procedures to 5 rekeying procedures. The

Table 1
LocalizedRekeying(i) Procedure

***Input**: group ID i*	
1.	Use batch rekeying to update $GTEK_i$ to prevent MSs in GTMSL(*i*) from knowing this new key.
2.	Remove group ID *i* from MSTL(*a*) for all MS *a* in GTMSL(*i*).
3.	Empty GTMSL(*i*).

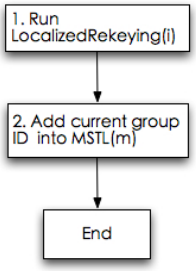

Figure 3 Key update process when MS *m* joins WiMAX network from group *i*.

improvement is significant.

In the proposed framework, we require to know the latest key update time of BSs, login time and logoff time of MSs. Since the recorded time decides the timing of triggering rekeying, time synchronization should be considered. However, our framework does not require strict time synchronization. We think this requirement is achievable for mobile WiMAX.

In summary, we can reduce the number of triggered rekeying procedures without affecting forward secrecy and backward secrecy by the aforementioned ideas.

4. The Proposed Framework

In this section, we describe detailed construction of the proposed framework. Let Group Temporal Mobile Station List GTMSL(*i*) be the list in which the MSs who know the latest GTEK of group *i* are recorded. Let Mobile Station Traversal List MSTL(*m*) be the list in which the groups which the latest GTEKs are known by MS *m* are recorded.

The LocalizedRekeying procedure is defined in Table 1. In step 1, MSs in GTMSL(*i*) have leaved or is leaving group *i,* so we use batch rekeying for multiple leave requests. In step 2, we remove group ID *i* from MSTL(*a*) because MS *a* does not know the latest GTEK anymore. This procedure also reduces the number of forward updates. After executing this procedure, only the MSs which are

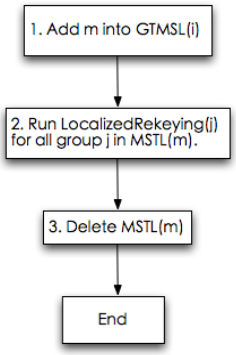

Figure 4 Key update process when MS *m* leaves WiMAX network from group *i*.

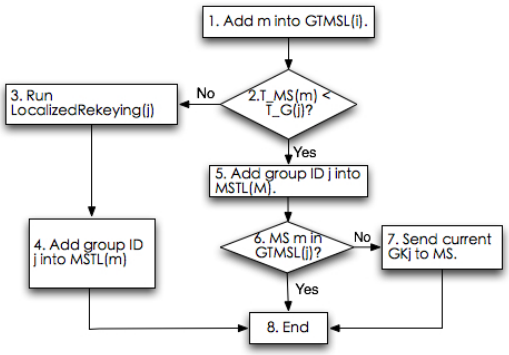

Figure 5 Key update procedure when MS *m* moves from group *i* to group *j*.

currently being in group *i* can know the newly updated GTEK.

The proposed framework processes three cases of MS's behaviors that are illustrated in Fig. 3, Fig. 4 and Fig.5 as follows.

- When MS *m* logs in a WiMAX network from group *i*,

(1) Run LocalizedRekeying procedure for group *i*.
(2) Add *i* into MSTL(*m*) to denote that MS *m* has known the latest updated GTEK of group *i*.

- When MS *m* logs off a WiMAX network from group *i*,

(1) Add *m* into GTMSL(*i*) to let MS *m* not know the latest GTEK after the rekeying procedure is triggered in next step.
(2) Run LocalizedRekeying procedure for all group *j* in MSTL(*m*) because all these groups, which MS *m* knew the latest GTEK should be updated.
(3) Delete MSTL(*m*) to complete the log-off of MS *m*.

- When MS *m* moves from group *i* to group *j*,

(1) Add *m* into GTMSL(*i*) since MS *m* has leaved group *i* and knew the latest GTEK.
(2) If T_MS(*m*) < T_G(*i*), go to step (5). Otherwise, go to step (3).
(3) Run LocalizedRekeying(*j*) since MS *m* is not allowed to access current session of group *j*.
(4) Add group ID *j* into MSTL(*m*) since *m* has joined group *j*. Then, go to step (8).
(5) Add group ID *j* into MSTL(*m*) by the reason same to step (4).
(6) If *m* in GTMSL(j), go to step (8). Otherwise, go to step (7).
(7) Send current GTEK to *m* since he did not know it.
(8) End.

The step (1) records *m* for forward update and the step (2) decides whether backward update is

required. In the step (6), we check whether MS *m* has ever come to group *j* and knew the latest GTEK.

In mobile WiMAX, an entity should be responsible for recording these data and triggering the rekeying procedure in our framework. We think this entity can be ASN-GW or other entities in the higher logical level of ASN network.

5. Experiments

In this section, we will describe how to simulate user actions according to [2][3]. Then, we compare the performance of our scheme with the previous schemes. The result shows that our scheme is better a lot than the previous schemes. Note that the previous schemes denote that triggering rekeying procedures whenever group membership changes.

5.1 Introduction of simulation model

We set up the simulation environment as follows.

(1) Three initial groups in which each group has fifty initial users.
(2) Each group has an upper bound of users. If a group has already reached to this bound, any user can not join into the group.
(3) Each user has three GTEKs at most according to setting (1). If a user has two GTEKs for the same group via handover, the user will keep the latest one.
(4) The ratio of the number of login, logoff, and handover stands for the user behaviors; Furthermore, our simulation model has different simulation values, the selection of the simulation value will be explained in Section 5.2, in the morning, afternoon, and evening, so the simulation values are different in different time periods. For example, the simulation value must be the biggest in the evening in a whole day, because we assume the traffic is the largest in the evening; however, the simulation values still base on the ratio.

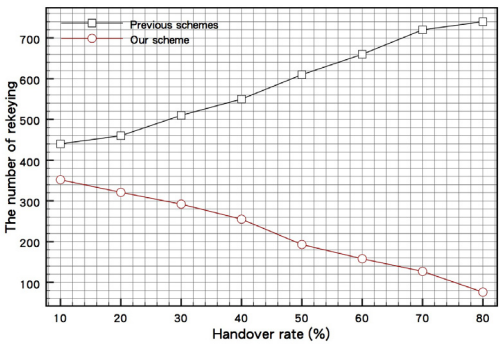

Figure 6 The handover rate versus the number of rekeying for previous schemes and our framework

Besides that, our simulation model not only uses aforementioned settings but cooperates with the Poisson distribution and random techniques[2][3] to simulate user behaviors precisely.

5.2 Simulation flow

In the beginning, we set up our simulation model; at this step, we need to decide the group size, maximum limit of users, and ratio of the number of login, logoff, and handover. After that, we simulate user behaviors step by step as follows:

(1) Choosing an expected value which is the product of lambda and time period of Poisson Distribution for each login, logoff, and handover, which bases on the ratio of the number of login, logoff, and handover, time period, and group size; then, we use this expected value to calculate the value of maximum probability via Poisson Distribution as the simulation value for each login, logoff, and handover in different time periods to simulate user actions.
(2) We randomly choose user and group for login, logoff, and handover to simulate user actions; especially, the handover will be randomly selected to a nearly group.
(3) We respectively choose the simulation value for each login, logoff, and handover in different time periods to simulate user actions. In addition, we assume each time period has five hours.
(4) When we simulate a user to move from a group to another group, our scheme will do some checks mentioned in Section 4; however, the previous schemes do not have these checks.

At the moment, we use Fig. 6 as an example to explain clearly our simulation flow. In the beginning, we set the group size and maximum limit of users for each group. After that, we adjust the ratio of the number of login, logoff, and handover from 4.5:4.5:1 to 1:1:8; the login and logoff rate are the same in every simulation, but the handover rate ascends one in each simulation. According to the ratio, we choose the expected values for every time period in each simulation, then we use the expected values to calculate the simulation values via Poisson distribution. For example, we select the 6:6:1 in the morning as the expected values for login, logoff, and handover times when the ratio is 4.5:4.5:1. Then, we use the expected values to calculate the value of maximum probability via Poisson Distribution as the simulation values, so we may get the 5:5:1 as the simulation values in the morning for login, logoff, and handover times. Finally, we can use the simulation values to simulate user behaviors in the

morning when the ratio is 4.5:4.5:1.

Section 5.3 will show the result of simulations, and our framework is obviously more efficient than the previous schemes when the handover rate is higher than login and logoff. Finally, we will compare the number of triggered rekeying procedures of our framework with that of the previous schemes.

5.3 Performance with different handover rate

In this experiment, we fix the group size and the maximum limit of users. Then, we adjust the ratio of the number of login, logoff, and handover to show our scheme is better a lot than the previous scheme when the handover rate is higher than others. Fig. 6 illustrates the simulation result; the number of triggered rekeying procedures in our scheme is mush less than that in the previous schemes when the handover rate ascends little by little.

6. Conclusions

In this paper, we proposed a new framework to reduce the number of triggered rekeying procedures in multiple M&B groups. In our proposed framework, we can efficiently reduce the number of forward and backward updates by recording some time and using batch rekeying. The experimental result shows that our scheme gets better performance while handover rate gets higher. The additional overhead of the proposed framework is to require an entity to record times and trigger rekeying procedures. In the future, we want to make the simulations more close to the real behaviors of MSs.

Acknowledgements

This study is conducted under the "III Innovative and Wireless Broadband Communications Technology and Application Project" of the Institute for Information Industry which is subsidized by the Ministry of Economy Affairs of the Republic of China.

References

[1] X. S. Li, Y. R. Yang, M. G. Gouda and S. S. Lam, "Batch Rekeying for Secure Group Communications," *ACM WWW10,* pp. 525-534, May 2001.

[2] Y. Sun and K.J.R. Liu, "Hierarchical Group Access Control for Secure Multicast Communications," *IEEE/ACM Transactions on Networking*, vol. 15, pp. 1514-1526, 2007.

[3] Q. Zhang, and Y. Wang, "A centralized key management scheme for hierarchical access control," Proceedings, *IEEE GLOBECOM*, vol. 4, pp. 2067-2071, 2004.

[4] IEEE std. 802.16e-2005, IEEE standard for local and metropolitan area networks, part 16, air interface for fixed and mobile broadband wireless access systems, IEEE Press, Piscataway, NJ, Tech. Rep. 802.16e, 2005.

[5] Wimax end-to-end network systems architecture stage 2-3 release 1.1.0." WiMAX forum, Tech. Rep., 2007.

[6] Wireless LAN medium access control (MAC) and physical layer (PHY) specification," IEEE Press, Piscataway, NJ, Tech. Rep. 802.11, 1997.

[7] S. Xu, C. Huang, and M. Matthews, "Secure multicast in various scenarios of WirelessMAN," *SoutheastCon, 2007. IEEE*, pp. 709–714, 2007.

[8] C. Wong, M. Gouda, and S. Lam, "Secure group communications using key graphs," *IEEE/ACM Transactions on Networking (TON)*, vol. 8, no. 1, pp. 16–30, 2000.

[9] D. McGrew and A. Sherman, "Key establishment in large dynamic groups using one-way function trees," *Manuscript*, vol. 474, 1998.

[10] 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.

[11] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas, "Multicast security: a taxonomy and some efficient constructions," *INFOCOM' 99. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, vol. 2, 1999.

[12] Y. Sun, W. Trappe, and K.J.R. Liu, "A scalable multicast key management scheme for heterogeneous wireless networks," *IEEE/ACM Transactions on Networking (TON)*, Volume 12 , Issue 4, pp. 653-666, IEEE, 2004.

[13] S. Paul, *Multicasting on the Internet and Its Applications*. Boston, MA: Kluwer, 1998.

[14] H.M. Sun, C.M. Chen, and C.Z. Shieh, " Flexible-Pay-Per-Channel: A New Model for Content Access Control in Pay-TV Broadcasting Systems, " IEEE Transactions on Multimedia, accepted, ready to publish, 2008.

[15] X. Zheng, C. T. Huang, and M. Matthews, "Chinese Remainder Theorem Based Group Key Management," *ACM Southeast Regional Conference (ACMSE 2007)*, pp. 266-271, 2007.

[16] S. Xu, C.T. Huang, and M. Matthews, "Secure Multicast in WiMAX," JOURNAL OF NETWORKS, Vol 3, pp. 48-57, 2008.