Security Vulnerabilities and Solutions in Mobile WiMAX

Andreas Deininger, Shinsaku Kiyomoto, Jun Kurihara, Toshiaki Tanaka

KDDI R&D Laboratories, 2-1-15, Ohara, Fujimino-shi, Saitama 356-8502, Japan

Summary:
This article shows different security vulnerabilities found in IEEE 802.16e and gives possible solutions to eliminate them. These vulnerabilities are the possibilities to forge key messages in Multi- and Broadcast operation, some unauthenticated messages which are susceptible to forgery and the unencrypted management communication which reveals important management information.

Keywords:
IEEE 802.16e security, multi- and broadcast service, shared key vulnerability, hash chaining solution

1. Introduction to IEEE 802.16e

1.1 General introduction

The development of IEEE 802.16 was started by the IEEE in 2001. After that it was revised several times and ended in the final standard IEEE 802.16-2004 which corresponds to revision D and is often called Fixed WiMAX [1]. It defines Wireless Metropolitan Broadband access for stationary and nomadic use. This means end devices can not move between base stations (BS) but they can enter the network at different locations.
This specification was extended by the development of IEEE 802.16e which supports mobility so mobile stations (MS) can handover between BS while communicating. IEEE 802.16e is often called Mobile WiMAX [2] and is an amendment to the IEEE 802.16-2004 standard. Commercial services of Mobile WiMAX are already planned for several countries.
On the link layer Mobile WiMAX introduces new features like different handover types, power saving methods and multi- and broadcast support. Furthermore IEEE 802.16e eliminates most of the security vulnerabilities discovered in its predecessors [3]. It uses EAP-based mutual authentication, a variety of strong encryption algorithms, nonces and packet numbers to protect against replay attacks and reduced key lifetimes.
First of all some parts of the functionality of Mobile WiMAX are introduced. Afterwards different security vulnerabilities and possible solutions to solve them are presented.

Manuscript received November 5, 2007
Manuscript revised November 20, 2007

1.2 Initial network entry procedure

For initial network entry, a MS has to proceed through several steps. First it has to search for a downlink map message of the BS which is broadcasted periodically. This frame includes information about the initial ranging connection identifier (CID), which is associated with a timeslot in where the initial ranging process can be performed. Access to this common used timeslot is defined as CSMA. The MS then increases its transmission power with each ranging request it sends on the initial ranging slot until it receives a response from BS. This response includes ranging adjustments and the basic and primary management CIDs which reserve particular time intervals for the MS to send and receive management messages. After initial ranging is completed the basic capabilities for the connection are negotiated.
Then the authentication process follows. IEEE 802.16e provides simple RSA-authentication or EAP-based authentication. EAP-based authentication includes higher layer authentication and therefore can be considered as the most secure method. After the authentication process MS and BS have set up a common authorization key (AK).
Then a key encryption key (KEK) is derived from the AK which is used to securely transfer further keys. Also the keys for message authentication in the up- and downlink are derived from AK.
After this, the 3-way TEK-exchange for each data connection is executed. This means MS and BS exchange the keys which are finally used for data traffic encryption. Hereby each message is integrity protected via a MAC digest and the transferred traffic encryption key (TEK) is encrypted by the KEK.
Subsequently each MS must register at BS to be allowed to send data to the network. For managed MSs the registration process additionally sets up a secondary management CID which is needed to manage it.

1.3 Key management

In the 3-way TEK Exchange processed at initial network entry, the MS sets up a security association (SA) for each data communication it wants to establish. Such a security association manages the keys for data encryption (the TEKs), their lifetimes and other security related parameters of this connection. It also includes a TEK state

machine which has the task to periodically refresh keying material when the lifetime of a TEK is going to expire.
To request new keying material the state machine sends a key request to the BS which responds with a key response including a new TEK. This transferred TEK is encrypted by a key encryption key (KEK) which is derived from AK and is globally used to decrypt received keys of all SAs.
To prevent communication disruption each SA simultaneously holds two TEKs. When one TEK expires the second one is used for traffic encryption and a new one is requested.

1.4 Optional sleep mode

To save stations battery capacity and reduce the load on the channel, an optional sleep mode was defined in Mobile WiMAX. It allows the MS to be absent from the serving BS for certain time periods and may power down its transmitter.
Therefore IEEE 802.16e specifies three different sets of power saving classes. Services with common demand properties should be mapped to the same set of power saving class. Each power saving class defines time periods when the MS should be in active state, listening for transmissions, and periods where it is allowed to change to sleep mode. If an MS has different active power saving classes, the overlay of the sleeping periods set in all power saving classes define the final sleeping window. Hence the MS can only change to sleep mode when all applied power saving classes define this time as sleeping time. If at least one connection does not belong to any power saving class, the MS can not change to sleep mode.
When a MS is sleeping it does not communicate with BS and may power down its transmitter. However a MS is able to execute all other processes like e.g. ranging or neighbor measurements which do not require a communication with the serving BS.
When the BS receives data destined to a sleeping MS, this data is buffered and the MS is waked up with a broadcasted Traffic Indication message.

1.5 Multi- and Broadcast service (MBS)

IEEE 802.16e also introduces a service for Multicast and Broadcast communication. This enables the BS to distribute data simultaneously to multiple MSs.
To secure the broadcast communication IEEE 802.16e uses a common group traffic encryption key (GTEK) for traffic en-/decryption. Every group member must know this key. To share the GTEK between MS and BS two algorithms as shown in Figure 1 are used: The mandatory key request/reply mechanism and the optional Multi- and Broadcast rekeying algorithm (MBRA).
In the standard request/reply mechanism a MS has to manage the GTEK update by itself. This means it has to request new keying material if the current key is going to expire. Such a key request triggers a unicast key response from the BS which includes a new key. To ensure an ongoing communication the MS simultaneously holds two keys similar to the TEK key management described above.
An optional alternative to distribute keying material is the Multi- and Broadcast rekeying algorithm (MBRA). Here the keys are managed by the BS. If a key lifetime is going to expire, the BS broadcasts one Key Update Command message to all MSs. This saves a lot of bandwidth as GTEKs are updated very frequently. To encrypt the broadcasted GTEK, a group key encryption key (GKEK) is needed (not shown in Figure 1). This GKEK is updated not very frequently. It is also distributed by a Key Update Command message, but in a unicast way encrypted by the

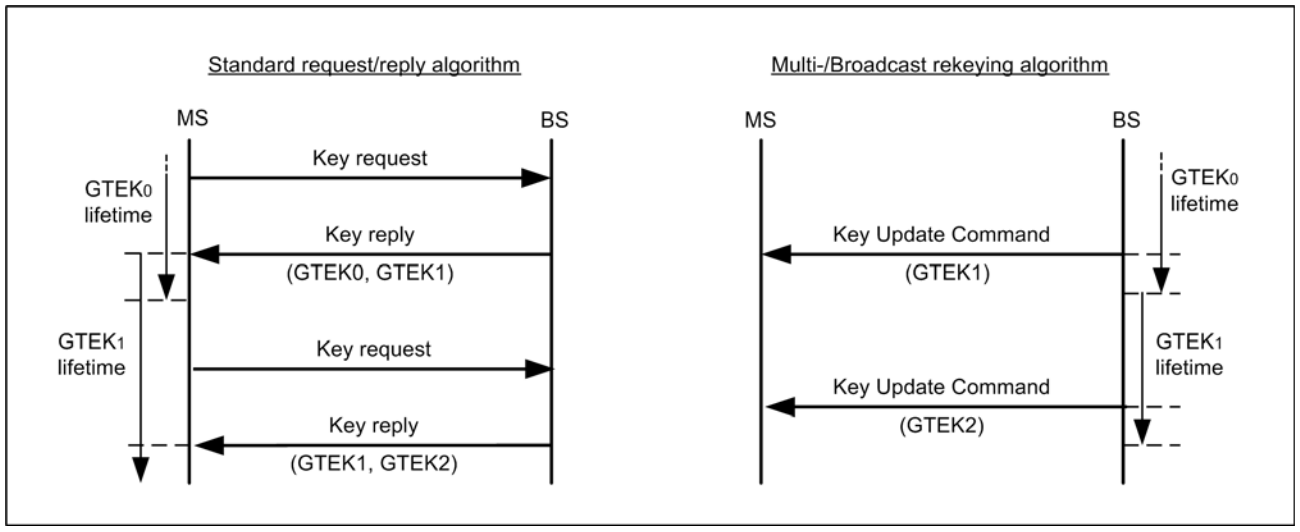


Figure 1 : The standard request/reply mechanism compared with the MBRA

MS-related KEK.
If a MS has not received a new key after a specific time, it requests keying material according to the standard request/reply mechanism. This is also done if the authentication value of a Key Update Command message is not valid.

1.6 Existing Analysis for WiMAX Security

The security of Fixed WiMAX was analyzed in several papers. Especially in [3] a lot of security vulnerabilities are outlined.
With the publication of the Mobile WiMAX amendment, most of these vulnerabilities were solved. The security of IEEE 802.16e was only analyzed by a few papers. [5] examined the 3-way TEK exchange and the authorization process and could not find any security leak. Also [6] analyzed the key management protocol using protocol analyzing software and did not detect any problem.
The multi- and broadcast service was examined by [7] by applying a protocol analyzing tool. He found out that security of the MBS is based on a few parameters which need to be implemented properly for complete protection. It is also pointed out that the interoperation with other protocols could be a security problem if these protocols have lower security characteristics.

2. Vulnerabilities in IEEE 802.16e

This section explains vulnerabilities found in Mobile WiMAX by our analysis. These vulnerabilities are:

- *Unauthenticated messages*
  Mobile WiMAX includes some unauthenticated messages. Their forgery can constrict or even interrupt the communication between mobile station and base station.

- *Unencrypted management communications*
  The complete management communication between mobile station and base station is unencrypted. If an adversary listens to the traffic, he can collect lots of information about both instances.

- *Shared keys in the multi- and broadcast service*
  For symmetric traffic encryption, the multi- and broadcast service in Mobile WiMAX shares keying material with all group members. This introduces the vulnerability that group members can forge messages or even distribute own traffic keying material, thus controlling the multi- and broadcast content.

2.1 Unauthenticated messages

Most of the management messages defined in IEEE 802.16e are integrity protected. This is done by a hash based message authentication code (HMAC) [8] or alternatively by a cipher based message authentication code (CMAC) [9]. However, some messages are not covered by any authentication mechanism. This introduces some vulnerabilities.
First it has to be mentioned that a couple of management messages are sent over the broadcast management connection. Authentication of broadcasted management messages is difficult since there is no common key to generate message digests. Furthermore a common key would not completely protect the integrity of the message as mobile stations sharing the key can forge these messages and generate valid authentication digits.

2.1.1 MOB_TRF-IND

One of these broadcasted and unauthenticated management messages is the Traffic Indication message (MOB_TRF-IND). This message is used by the BS to indicate to a sleeping MS that there is traffic destined to it. Accordingly the MS is waked up from sleep mode.
A unique Sleep ID is assigned to each MS in the base stations range. This sleep ID is a 10 bit value addressing 1023 different MSs. To accelerate message processing, the traffic indication message merges 32 Sleep IDs to one Sleep ID Group. Thus there exist 32 Sleep ID groups containing 32 Sleep IDs each.
If the BS now receives traffic for a sleeping MS, the group ID for this MSs Sleep ID group is set to true. When receiving this message, every MS in the group will check if the traffic is addressed to it by verifying the traffic indication bitmap. This is a 32 bit value that is appended for each Sleep ID group and contains a bit for each individual MS in that group. If the corresponding bit in the traffic indication bitmap is set, the respective MS wakes up and can receive the traffic. All other MSs can continue sleeping after verifying that the Sleep ID group indication bit of their group is set to false.
An adversary could generate this message to frequently wake up MSs and stress their battery. If all bits in the Sleep ID group indication bitmap and all traffic indication bitmaps in this message are set to true, every reachable MSs in sleep mode is forced to wake up.

2.1.2 MOB_NBR-ADV

The neighbor advertisement message (MOB_NBR-ADV) is also not authenticated. The serving BS sends this message to announce the characteristics of neighbor BS to MSs seeking for handover possibilities.
An adversary is able to keep back individual BSs by omitting information about their existence when he forges this message. This prevents MSs to handover to BSs which might have better characteristics as their serving BS. He can also distribute wrong data about neighbor BSs or announce non existing BSs.

2.1.3 FPC

The broadcasted Fast Power Control message (FPC) is also not covered by any authentication mechanism. An FPC message is sent by the BS to one or multiple MS to adjust their transmitting power. By misusing this message it is possible to reduce the transmitting power of all reachable MSs to a minimum so that it is to low to be recognized by the BS. Thus, recursive power adjustments are necessary for the MS until the transmission power is strong enough to reach the BS again. Due to CSMA, the suddenly triggered cumulated power adjustment messages result in many uplink bandwidth requests. This causes collisions in uplink bandwidth request contention slots of the MSs and delays the time until each MS once again has the correct transmission power and can communicate with the BS.
Another misuse of the message is to set the transmitting power of all MSs to the maximum with the intention to stress their batteries.

2.1.4 MSC-REQ

An unauthenticated unicast message is the Multicast Assignment Request message (MSC-REQ). When sending this message the BS can remove a MS from a multicast polling group. A MS which receives such a remove message deletes itself from the polling group and subsequently sends a response back to the BS. This conversation is done using the primary management connection between BS and MS.
A polling group is a group of MS which can get bandwidth from the BS via a polling mechanism. The BS therefore allocates an uplink transmission opportunity for each MS in the polling group. Then MSs can request uplink bandwidth using this transmission opportunity.
As there is no authentication for this message an attacker can easily remove MSs from polling groups. If a MS is removed from a polling group, it has to use the mandatory contention based bandwidth allocation algorithm which results in a greater uplink delay.

2.1.5 DBPC-REQ

The Downlink Burst Profile Change Request message (DBPC-REQ) is a further unicast message with no integrity protection. When the distance between BS and MS varies or the communication characteristics are changing due to another reason, the BS sends this message to change the MSs burst profile to a more robust or a more effective one. The intention in misusing this message can be to temporarily break the communication between MS and BS by changing MSs burst profile so that it is not possible for the MS to demodulate the data received from the BS.

2.1.6 PMC-REQ

Every MS is working whether in open- or closed loop power control mode. The power control mode of a MS can be changed by the MS itself by sending a Power Control Mode Change Request (PMC_REQ) to BS. The BS then answers with the power control mode change response (PMC_RSP). This message can also be sent by the BS in unsolicited manner to change MSs power control mode. It also includes the power adjustment value that should be set up by the MS.
The PMC_REQ message can be used by an adversary to request a change of a MSs power control mode. The message is accepted as if it came from the MS.
Another vulnerability is the forgery of the Power Control Mode Change Response (PMC_RSP) message sent from the BS. With this message an adversary can directly change the power control mode of the MS and also adjust its transmission power with the intention to disrupt the communication.

2.1.7 MOB_ASC-REP

The association result report (MOB_ASC-REP) is another not authenticated message. When MS and BS are keeping association level 2, the BS does not directly have to answer a Ranging Request. Instead it is sending the Ranging Response over the backbone to the serving BS of the requesting MS. The serving BS collects all Ranging Responses of neighboring BSs and merges them to one association report message. This aggregated message is transmitted to the MS via the basic management connection.
The ranging response message itself is integrity protected in most cases but the association report message is never. An adversary can change arbitrary response data in the message like time or power adjustments. Furthermore the message includes the service prediction of the BS which advertises the services the BS can offer to the MS. Here an adversary could forge the message in a way that it looks like no services are available for the requesting MS.

2.1.8 RNG-REQ

For the Ranging Request (RNG-REQ) message the standard does not explicitly define when an authentication digest shall be appended. Here it should be stated that this message must always be covered by a digest when an Authentication Key (AK) is available. For initial network entry no authentication key is available but in most other cases an AK exists and the message can be protected.

Besides there are other non-authenticated messages but a forgery of their carried information can be considered as less dangerous for the operability of the protocol.

2.2 Unencrypted management communication

The topic of unencrypted messages has already been discussed in some papers for Fixed WiMAX. In Mobile WiMAX management messages are still sent in the clear. The consequential risk shall be outlined in this section.

When a MS performs initial network entry it negotiates communication parameters and settings with the BS. Here a lot of information is exchanged like security negotiation parameters, configuration settings, mobility parameters, power settings, vendor information, MSs capabilities etc. Currently the complete management message exchange in the network entry process is unencrypted and the above mentioned information can be accessed just by listening on the channel.

After initial network entry, the management communication over the basic and primary management connections remains unencrypted. As most of the management messages are sent on these connections, nearly all management information exchanged between MS and BS can be accessed by a listening adversary. The only messages which are encrypted are key transfer messages. But in this case only the transferred key is encrypted, all other information is still sent in the clear.

An adversary collecting management information can create detailed profiles about MSs including capabilities of devices, security settings, associations with base stations and all other information described above. Using the data offered in power reports, registration, ranging and handover messages, a listening adversary is able to determine the movement and approximate position of the MS as well. Monitoring the MAC address sent in ranging or registration messages reveals the mapping of CID and MAC address, making it possible to clearly relate the collected information to user equipment.

2.3 Shared keys in Multi- and Broadcast Service

The Multi- and Broadcast service offers the possibility to distribute data to multiple MS with one single message. This saves cost and bandwidth.

Broadcasted messages in IEEE 802.16e are encrypted symmetrically with a shared key. Every member in the group has the key and thus can decrypt the traffic. Also message authentication is based on the same shared key. This algorithm contains the vulnerability that every group member, besides decrypting and verifying broadcast messages, can also encrypt and authenticate messages as if they originate from the ‘real’ BS.

Another aspect which is much more problematic is the distribution of the traffic encryption keys (GTEKs) when the optional Multi- and Broadcast Rekeying Algorithm (MBRA) is used. To transfer a GTEK to all group members it is broadcasted but encrypted with the key encryption key (GKEK). Due to broadcasting, the GKEK must also be a shared key and every group member knows it. Thus an adversary group member can use it to generate valid encrypted and authenticated GTEK key update command messages and distribute an own GTEK.

Every group member would establish the adversary’s key as a valid next GTEK. Subsequently all traffic sent by the ‘real’ BS can no longer be decrypted by the MS. From a MSs point of view only traffic from the adversary is valid.

To force MSs to establish the adversary’s key, there are several possibilities. If the implementation does not work properly, the key from the latter of two subsequently sent GTEK update command messages may overwrite the former one. Hence the adversary just has to send its GTEK update command message after the BS broadcasted a key update message.

If the implementation follows the standard, the keys of both messages are accepted. To be sure the MS will not establish the ‘real’ BSs key, an adversary could forge some part of the BSs GTEK update command message. Such a changed message would not be verified as correct and discarded by the MSs. After this the adversary can send its own GTEK update command message which will be accepted.

In a unicast connection this different keying material at the mobile station would be detected as the base station cannot decrypt data sent by the mobile station. This results in a TEK invalid message destined to the MS which subsequently refreshes its keying material. Since the MBS is only unidirectional, the BS cannot detect that MS has different GTEKs.

3. Solutions suggested

3.1 Unauthenticated messages

Non-authenticated management messages sent on the primary or basic management connection can easily be authenticated using a HMAC or CMAC digit. It has to be decided if this authentication, which additionally needs up to 168 bit, is acceptable. Most messages are very short so that an appended digit would boost the message to a multiple of its original size. Due to this fact a tradeoff between the security and the effectiveness of the protocol has to be found.

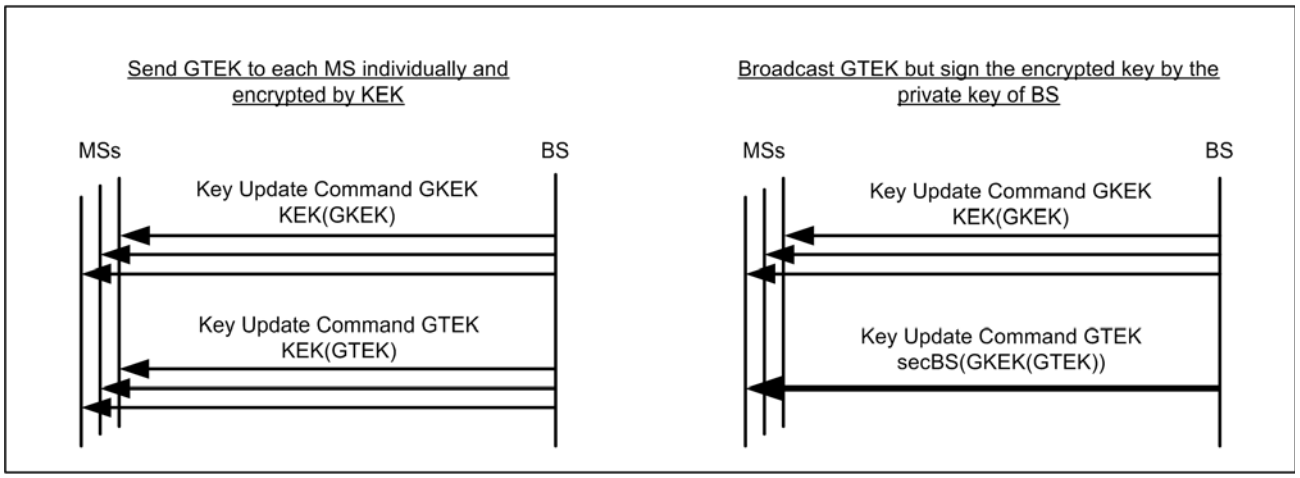


Figure 2 : Possible solutions to transmit GTEK in a secure way

One way for such a tradeoff is to authenticate all messages which can have serious effects if they are forged. In addition to the management messages which already are protected by an authentication digit, this includes all messages presented in section 2.1. Other management messages can remain unauthenticated. To hold down the overall message size, the CMAC or the Short HMAC tuple should be used as it has a much lower size as the full HMAC.
HMAC is based on the SHA-1 algorithm so a MAC size of 128 bit is achieved. For the Short HMAC this value is truncated to 64 bit. With all other needed parameters (i.e. packet number, key sequence number and reserved fields) this results in a Short HMAC digest of 104 bit.
CMAC uses AES128 which also results in a 128 bit value. For the finally used CMAC this value is truncated to 64 bit. With all additional information the complete CMAC digest is also 104 bit in total.

Broadcasted messages have the problem that their authentication is not completely secure when a symmetric key is used since this key must be shared by all group members. This offers the possibility that messages can be forged by every group member. However, a symmetric solution can be processed very fast and protects against message forgery from outside a group. It is a possibility to significantly increase the security without complete protection but low requirements.
Another possibility would be the use of asymmetric cryptography. Broadcasted messages in this case are authenticated by a signature created with the private key of the base station. For mobile stations this requires to verify this asymmetric signature with the known public key when they receive such broadcasted management messages. However, this solution has the big drawback that it needs much time to be performed and the asymmetric keys must be managed. Additionally authentication takes place very often and thus increases the requirements.

3.2 Unencrypted management communication

To protect the management traffic from being read by an adversary, all management communication should be encrypted. This encryption can apply directly after both sides have established a common key (i.e. the authorization key AK).
Such a common key is established after the authentication process hence the following TEK exchange and registration process as well as all subsequent management communication can be encrypted. To avoid the AK of being updated too often, either a security association for each management connection could be established (i.e. primary and basic CID), or a global management security association for both management connections would also be adequate.
Encrypting the management payload of a message does not introduce any overhead to the connection. It just requires encryption and decryption of the message. As it is possible to use a symmetric key, decryption can be processed very fast.
Such a solution conceals confidential management information, protects against unwanted listening and does not disclose management data to create profiles.
In [4], one possible solution is presented to encrypt management information early in the initial network entry process.

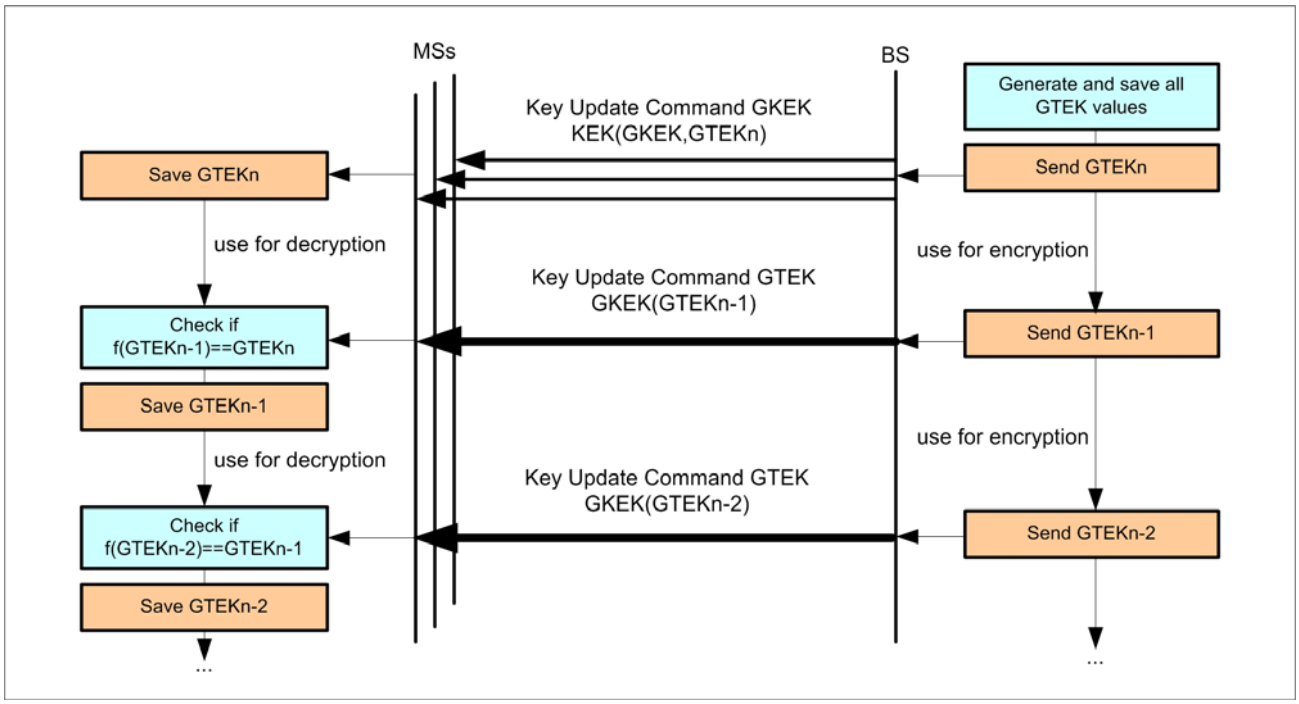


Figure 4 : Avoiding key forgery by a GTEK hash chain

3.3 Shared keys in Multi- and Broadcast Service

Secure encryption of the data transferred via the MBS is difficult. A shared key can not be used as every group member can forge messages when having the current symmetric keys.
But what can be avoided is the distribution of forged key update command messages allowing an adversary to take control over the data content on a MBS connection.
One possibility to achieve this is to avoid broadcasted key updates. Instead the GTEK update command message could be sent to each MS in a unicast way like the GKEK update command message. The key should then be encrypted with the MS-related KEK which is only known by this individual MS.
Compared with the Request/Reply algorithm this still saves half of the bandwidth as no request message is necessary. The BS sends the GTEK update command message by itself when the current key's lifetime is going to expire. The left side of Figure 2 shows this solution in comparison to the GKEK update command message which works the same way.
Another solution is the use of public key cryptography. Here the GTEK update command message remains broadcasted and encrypted with the shared key GKEK but is additionally signed by an asymmetric signature. MSs receiving a GTEK update command message can verify the signature of the BS and subsequently decrypt the GTEK with the shared GKEK. The right hand side of Figure 2 shows this method together with the unicasted GKEK update command message.

A third possibility is to generate GTEKs as part of a hash chain. Here the BS first generates a random number which represents the initial key $GTEK_0$. Then the other GTEKs are generated by applying a one way hash function to the previous GTEKs respectively. This is iterated n times.

$$\begin{aligned} GTEK_0 &= random() \\ GTEK_1 &= f(GTEK_0) \\ GTEK_2 &= f(GTEK_1) \\ &\vdots \\ GTEK_n &= f(GTEK_{n-1}) \end{aligned}$$

This hash chain allows to verify each GTEK by applying the same one way function to the previous one. To achieve this chained authentication the last GTEK has to be distributed to each MS in a secure way as it is the only key in the chain which can not be authenticated by another one. One possibility is to distribute $GTEK_n$ in the GKEK update command message which is a unicast message and encrypted by a MS related key.

Table 1: Comparison of the proposed key vulnerability solutions

	Exclusive unicasting	Asymmetric signature	Hash chain authentication
Introduced traffic (n = group size)	O(n)	O(1)	O(1)
Computing requirements mobile station	low	high	low
Computing requirements base station	low	high	low
Period without forward secrecy	short	short	long

If a MS receives a new GTEK via a broadcasted GTEK update command message it can verify its integrity by applying the one way hash function *f* to it. If the authentication is positive, the current GTEK can be overwritten and the received one is established. If the authentication fails, the MS discards the message and requests a new GTEK via the unicast Request/Reply mechanism. Figure 3 shows this behavior.

To apply this algorithm, the key GKEK update command message has to be capable of transporting GKEK and GTEK keys together. The design of the key update command message already includes both keys so only a little modification is necessary here. Additionally the GTEK state machine at BS must generate the GTEK hash chain and store all the keys. The GTEK state machine at MS must add the functionality to authenticate GTEK keys by calculating the hash function and comparing it to the previous key.
A drawback of this algorithm is that it has a reduced forward secrecy. This means a MS, joining the group, can decrypt all broadcasted data since the last hash chain generation. If forward secrecy is crucial, the hash chain has to be regenerated each time a MS enters the group.

To compare these different solutions their characteristics are contrasted to each other in Table 1.
First the introduced traffic of each solution shall be discussed. To distribute the key in unicast behavior needs one key update per mobile station. This means the introduced traffic directly corresponds to the group size n. When using an asymmetric signature or a hash chain to authenticate the GTEK transfer, only one message is needed to update the keys of all mobile stations due to broadcasting. Thus the introduced traffic in these solutions is constant and does not depend on the number of members in the group.
Another important fact is the computing requirements of the different algorithms for the mobile stations and the base station. Especially the mobile stations should not be occupied with complicated calculations to save battery power.
For exclusive unicasting the mobile stations just have to verify the HMAC and save the keys. Hence, the required computing power is very low. Also the use of a hash chain does not require much computation. Here the mobile station has to calculate the hash function of the received key and compare it with the saved key.
For both solutions the requirements for the base station are also very low. For exclusive unicasting, new keys are generated randomly, for the hash chain they are subsequently calculated with a hash function. When an asymmetric signature is used, the computational needs are much higher. In own laboratory measurements it was determined that the time to verify an asymmetric signature is about 20 times higher than verifying with a HMAC digit. Also the requirements for the base station to create the asymmetric signature with it's private key is about 900 times higher compared with the creation of a HMAC digit. However, the base station can be assumed to have much more computing power and an asymmetric signature has to be created only once per GTEK update of all mobile stations.
Finally the forward secrecy of the solutions shall be analyzed. All solutions and also the currently defined MBRA can not provide forward secrecy. Every algorithm has a period in which previously sent data can be decrypted by a mobile station which joins the group. For exclusive unicasting and the asymmetric solution this period is one GTEK lifetime. This means that a mobile station that joins the group can decrypt all the traffic that was encrypted with the currently used GTEK. When authentication is based on a hash chain, this period lasts for the lifetime of one complete hash chain. Due to the direct concatenation of the keys with a known one way hash function, a mobile station which joins the group can easily calculate all previous GTEKs in the current hash chain.

4. Conclusion

In this paper, we showed different security vulnerabilities found in IEEE 802.16e and gave possible solutions to eliminate them.
When all proposed changes are applied, the security of Mobile WiMAX can be significantly increased.
Encrypting the management communication solves the vulnerability which existed since the first version of the standard. With applied encryption an adversary is no longer able to collect management information about mobile devices.
Some messages were found which carry sensitive information without any authentication. If they are forged this can be dangerous for system operation. If the message authentication is extended to these messages as proposed, they are protected against forgery.
To prevent a key misuse in the multi- and broadcast rekeying algorithm three different solutions were presented based on unicasting, asymmetric cryptography and hash chaining. Generating traffic encryption keys in a hash chain is a fast solution that does not introduce much overhead. Unfortunately it has a long period without forward secrecy. Thus if forward secrecy is important one of the other algorithms might be appropriate.

References

[1] IEEE Std. 802.16-2004, IEEE Standard for Local and Metropolitan Area Networks, part 16, Air Interface for Fixed Broadband Wireless Access Systems, IEEE Press, 2004.

[2] 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, 2006.

[3] Johnston D., Walker J.: Overview of IEEE 802.16 Security, IEEE Computer Society, 2004.

[4] Taeshik Shon, Wook Choi: An Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions, First International Conference, NBiS 2007, LNCS, Vol. 4650, pp. 88-97, 2007

[5] Datta A., He C., Mitchell J.C., Roy A., Sundararajan M.: 802.16e Notes, Electrical Engineering and Computer Science Departments, Stanford University, CA, USA, 2005, available at http://www.iab.org/liaisons/ieee/EAP/802.16eNotes.pdf

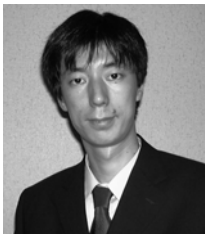
[6] Yuksel E.: Analysis of the PKMv2 Protocol in IEEE 802.16e-2005 Using Static Analysis Informatics and Mathematical Modeling, Technical University Denmark, DTU, 2007, available at http://www2.imm.dtu.dk/pubdb/views/publication_details.php?id=5159

[7] Ju-Yi Kuo: Analysis of 802.16e Multicast/Broadcast group privacy rekeying protocol, Stanford University, CA, USA, 2006, available at http://www.stanford.edu/class/cs259/projects/project01/01-Writeup.pdf

[8] Krawczyk H., Ballare M., Canetti R.: HMAC: Key-Hashing for Message Authentication, RFC 2104, http://www.ietf.org/rfc/rfc2104.txt, IETF, 1997.

[9] Dworkin M.: Recommendation for Block Cipher Modes of Operation: The CMAC mode for authentication, NIST special publication 800-38B, National Institute of Standards and Technology (NIST), MD, USA, 2005.

Andreas Deininger is studying Mechatronics at the University of Stuttgart, Germany. During his studies he specialized in Communication- and Control Engineering. Currently he is doing an internship in the Information Security Lab. of KDDI R & D Laboratories Inc. with the focus on WiMAX security.



Shinsaku Kiyomoto received his B.E. in Engineering Sciences, and M.E. in Materials Science, from Tsukuba University, Japan, in 1998 and 2000 respectively. He joined KDD (now KDDI) and has been engaged in the research on stream cipher, cryptographic protocol, and mobile security. He is currently a researcher of the Information Security Lab. in KDDI R & D Laboratories Inc. He received his doctorate of engineering from Kyushu University in 2006. He received the Young Engineer Award from IEICE in 2004. He is a member of JPS, IEICE, and IPSJ.

Jun Kurihara received the B.E., Department of Computer Science, and M.E., Department of Communications and Integrated Systems, from Tokyo Institute of Technology, Japan, in 2004 and 2006 respectively. He joined KDDI and has been engaged in the research on stream cipher, cryptanalysis, and secret sharing scheme. He is currently a researcher of the Information Security Lab. in KDDI R&D Laboratories Inc. He is a member of IEICE.

Toshiaki Tanaka received B.E. and M.E. degrees in communication engineering from Osaka University, Japan, in 1984 and 1986 respectively. He joined KDD (now KDDI) and has been engaged in the research on cryptographic protocol, mobile security, digital rights management, and intrusion detection. He is currently a senior manager of the Information Security Lab. in KDDI R & D Laboratories Inc. He received his doctorate of engineering from Kyushu University in 2007. He is a member of IEICE and IPSJ.