Notice of Violation of IEEE Publication Principles

"Security Issues in Mobile WiMAX (IEEE 802.16e)"
by Frank A. Ibikunle
in the Proceedings of the Mobile WiMAX Symposium (MWS 2009)
July 2009, pp. 117-122

After careful and considered review of the content and authorship of this paper by a duly constituted expert committee, this paper has been found to be in violation of IEEE's Publication Principles.

This paper contains significant portions of original text from the paper cited below. The original text was copied with insufficient attribution (including appropriate references to the original author(s) and/or paper title) and without permission.

Due to the nature of this violation, reasonable effort should be made to remove all past references to this paper, and future references should be made to the following article:

"Security Vulnerabilities and Solutions in Mobile WiMAX"
by Andreas Deininger,Shinsaku Kiyomoto, Jun Kurihara, Toshiaki Tanaka
International Journal of Computer Science and Network Security, Vol 7, No 11
November 2007

2009 IEEE Mobile WiMAX Symposium

Security Issues in Mobile WiMAX (IEEE 802.16e)

Frank, A Ibikunle
Covenant University, Electrical and Information Engineering Department, Ota.
faibikunle2@yahoo.co.uk

Abstract

The IEEE 802.16 standard, commonly known as WiMAX, is the latest technology that has promised to offer broadband wireless access over long distance. Since 2001, WiMAX has evolved from 802.16 to 802.16d standard for fixed wireless access and to the new IEEE 802.16e (Mobile WiMAX) standard with mobility support. Meanwhile, its security is becoming a critical issue with the proliferation of wireless threats. Though incorporating some security methods, IEEE 802.16e is still vulnerable to malicious attacks. In this paper, we analyze the security of Mobile WiMAX, point out several potential security threats and vulnerabilities. We propose some possible security improvements and solutions to eliminate the vulnerabilities.

Keywords: Mobile WiMAX, multicast and broadcast service, security vulnerability, hash chaining, authentication

1. Introduction

As much as the wireless networks have brought about major development in the way the information is shared between individual-to-individual, individual-to-business and business-to-business scenarios, they still face challenges, which are yet to be solved. We define security as protection of data being transmitted over a wireless networks. It is important to understand the full range of problems that security systems need to address. These needs are confidentiality, integrity and authentication (CIA), and are defined as follows: *Confidentiality*- Allowing only that the intended legitimate recipients to read encrypted messages (information). *Integrity*- is referred to as ensuring that another party has not altered messages after it has been sent. *Authentication*- This is making sure that parties sending messages or receiving messages are who they say they are, and have the right to undertake such actions. On wired networks it has been exhaustively researched and there are many mechanisms available to provide confidentiality, integrity and authentication of information (CIA). Virtual Private Networks (VPNs), Internet Protocol Security (IPSec), Intrusion Detection Systems (IDS) and firewalls are just examples among various security mechanisms that have been proposed to address security issues in wired networks. The major problem when securing the wireless signal is in its mode of transmission [1]. The wireless signal is transmitted through electromagnetic waves, which cannot be physically contained. Being communicated through the air makes them easy to intercept by anyone with the right equipment. WiMAX builds on the experience of security problems of 802.11 wireless networks and was developed to solve most of the wireless LAN shortcomings especially security, and also quality of service, high-speed data rates and long distance connectivity coverage [2]. WiMAX, as a new technology seems not to have fully solved the security flaws of wireless LAN. Confidentiality, in wireless networks is a fundamental concern for a secured transmission. The intended recipient should only receive the information transmitted. The message authentication provides integrity to both the message sender and receiver. The wireless link should always be available and not be susceptible to malicious attacks, which rob the end-user of availability (denial of service attacks) [3]. There are many attacks, which can be launched to compromise authentication mechanisms or protocols. Two common attacks that are especially effective against wireless networks are the message replay attack and the man in the middle attack.

The paper is organized as follows. Section II gives the literature review of Mobile WiMAX Security (IEEE 802.16e). In section III, the Mobile WiMAX standard and parts of the functionality of Mobile WiMAX are introduced. Section IV describes different security vulnerabilities of the technology. Section V presents possible solutions to solve the security threats. While, the paper ended with a conclusion.

2. Literature Review of WiMAX Security

The security of Fixed WiMAX was analyzed in several papers, especially in [6] where 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, such as in [7] that examined the 3-way TEK exchange and the authorization process and could not find any security leak. Also [8] analyzed the key management protocol using protocol analyzing software and did not detect any problem. The multicast and broadcast service was examined in [9], 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.

3. Mobile WiMAX (IEEE 802.16e)

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 is often called Fixed WiMAX [4]. This standard defines Wireless Metropolitan Broadband access for stationary and nomadic use. This means end devices can not move between base stations (BS) but they

978-0-7695-3719-1/09 $25.00 © 2009 IEEE
DOI 10.1109/MWS.2009.50

can enter the network at different locations. This specification was extended by the development of IEEE 802.16e which is known as Mobile WiMAX [5]. This standard supports mobility so that mobile stations (MS) can handover between BS while communicating. On the link layer, Mobile WiMAX introduces new features like different handover types, power saving methods and multicast and broadcast support. Furthermore IEEE 802.16e eliminates most of the security vulnerabilities discovered in its predecessors [6]. It uses EAP-based mutual authentication, a variety of strong encryption algorithms and packet numbers to protect against replay attacks and reduced key lifetimes.

3.1 Initial network entry procedure

For initial network entry, a MS has to pass some steps. The first step is 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 by standard random access channel. 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, the MS and BS 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 uplink 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. Here, 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.

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 may wants to establish. Such a security association manages the keys for data encryption (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 [6].

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. However, an MS is able to execute all other processes like 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.

Multicast and Broadcast Service (MBS): IEEE 802.16e also introduces a service for Multicast and

Broadcast communications. This enables the BS to distribute data simultaneously to multiple MSs. To secure the broadcast communications, the IEEE 802.16e uses a common group traffic-encryption key (GTEK) for traffic encryption/decryption. Every group member must know this key. To share the GTEK between MS and BS, two algorithms are used: The mandatory key request/reply mechanism and the optional Multicast 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 Multicast 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.

4. Security Flaws in IEEE 802.16e

This section explains the flaws found in Mobile WiMAX. These flaws are analyzed as follows:

4.1 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) [11], or alternatively by a cipher based message authentication code (CMAC) [12]. However, some messages are not covered by any authentication mechanism. This introduces some vulnerability. Also, 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.

4.1.1 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 woken 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.

4.1.2 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 serving BS. He can also distribute wrong data about neighbor BSs or announce non existing BSs.

4.1.3 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.

4.1.4 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.

4.1.5 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 MS 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. Another flaw 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.

4.1.6 PMC-REQ

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 too 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.

4.1.7 MOB_ASC-REP

The Association Result Report (MOB_ASC-REP) is another un-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.

4.1.8 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 aforgery of their carried information can be considered as less dangerous for the operability of the protocol.

4.2 Unencrypted management communication

In Mobile WiMAX management messages are still sent in the clear. 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 and MS 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. 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.

4.3 Shared keys in Multicast and Broadcast Service

The Multicast 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 Multicast 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. 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 result 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.

5. The Solutions Proffered to the Vulnerabilities

In this section, we propose some solutions to improving and strengthening Mobile WiMAX (IEEE 802.16e) security.

5.1 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 168bits 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. 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 are already protected by an authentication digit (including all messages presented in section 4.1), other management messages can remain unauthenticated. To hold down the overall message size, the CMAC or the Short HMAC should be used, as it has 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 a problem when their authentication is not completely secure if 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 possible to significantly increase the security without complete protection but with 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 a big drawback, that is, 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.

5.2 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. 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. Another possible solution is to encrypt management information early in the initial network entry process as done in [13].

5.3 Shared keys in Multicast and Broadcast Services

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 1 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. MS 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 1 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.

$\text{GTEK}_0 = \text{random}()$
$\text{GTEK}_1 = f(\text{GTEK}_0)$
$\text{GTEK}_2 = f(\text{GTEK}_1)$
.
$\text{GTEK}_n = f(\text{GTEK}_{n-1})$

This hash chain allows for the verification of 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. 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, the behavior of which is exhibited in Figure 2.

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 given in section 5.3, their characteristics are contrasted with each other in Table 1. Detail explanation of the comparison is given in [13]

Table 1. Comparison of proposed solutions in section 5.3

Characteristics	**Exclusive unicasting**	**Asymmetri c signature**	**Hash chain authentication**
Introduced traffic (n=group size)	0 (n)	0(1)	0(1)
Computing requirements mobile station	low	high	low

Computing requirements base station	low	high	low
Period without forward secrecy	short	short	long

6. Conclusion

IEEE 802.16 is an emerging standard for broadband wireless communications that is receiving a lot of attention from service provider and hardware producers as an alternative to wired broadband access or promising technology to offer broadband wireless access over long distance.

In this paper, we describe different security vulnerabilities found in IEEE 802.16e, such as: Unauthenticated messages which their forgery could constrict or even interrupt the communication between mobile station and base station; Unencrypted management communications between mobile station and base station which if an adversary listens to the traffic, he can collect lots of information about both instances; and lastly, shared keys in the multicast and broadcast service in Mobile WiMAX that can cause group members to forge messages or even distribute own traffic keying material, thus controlling the multicast and broadcast content. We went further to proffered possible solutions to eliminate them. When all proposed changes are applied, the security of Mobile WiMAX can be significantly increased.

References

[1] Griffin "Creating a Secure Network for Your Business", White-Paper, 2005. accessed on 24 June 2006, http://www.aometrosystems.com/whitepaper.htm

[2] Westech Communication Inc (2005), *Can WiMAX Address Your Application*, White Paper, accessed on 3 October 2006,

[3] S. Xu, M. Mathews, and C.T. Huang, Security issues in privacy and key management protocols of IEEE 802.16, in *Proceedings of ACM SE'06*, Melbourne, FL, March 2006.

[4] 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.

[5] 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.

[6] D. Johnston and J. Walker, "Overview of IEEE 802.16 security", *IEEE Security and Privacy*, pp. 40–48, May/June 2004.

[7] 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,

[8] Yuksel E. "Analysis of the PKMv2 Protocol in IEEE 802.16e-2005 Using Static Analysis Informatics and Mathematical Modeling", Technical University, Denmark, DTU, 2007.

[9] Ju-Yi Kuo, "Analysis of 802.16e Multicast/Broadcast group privacy rekeying protocol", Stanford University, CA, USA, 2006,

[10] M. Barbeau, "WiMAX/802.16 threat analysis", in *Proceedings of ACM Q2SWinet'05*, Montreal, Quebec, Canada, October, 2005.

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

[12] 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.

[13] 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.

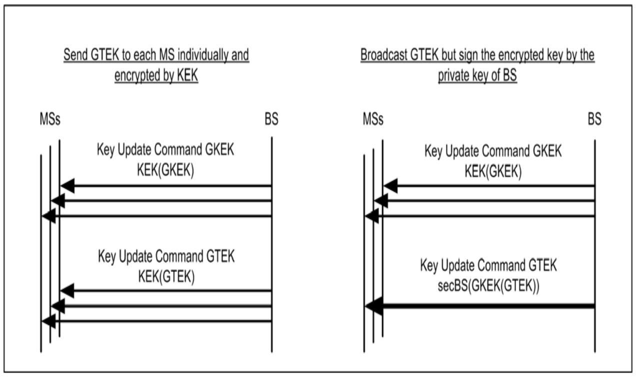
Send GTEK to each MS individually and encrypted by KEK
Broadcast GTEK but sign the encrypted key by the private key of BS
MSs
BS
MSs
BS
Key Update Command GKEK KEK(GKEK)
Key Update Command GKEK KEK(GKEK)
Key Update Command GTEK KEK(GTEK)
Key Update Command GTEK secBS(GKEK(GTEK))

Figure 1. Possible solutions to transmit GTEK in a secure way

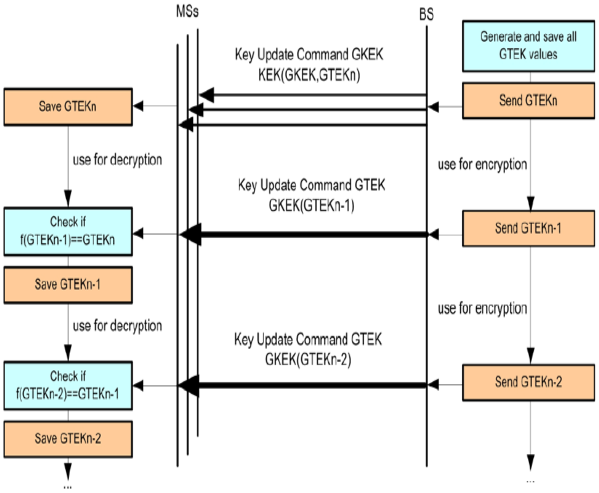
MSs
BS
Generate and save all GTEK values
Key Update Command GKEK KEK(GKEK,GTEKn)
Save GTEKn
Send GTEKn
use for decryption
use for encryption
Key Update Command GTEK GKEK(GTEKn-1)
Check if f(GTEKn-1)==GTEKn
Send GTEKn-1
Save GTEKn-1
use for decryption
use for encryption
Key Update Command GTEK GKEK(GTEKn-2)
Check if f(GTEKn-2)==GTEKn-1
Send GTEKn-2
Save GTEKn-2
...
...

Figure 2. Avoiding key forgery by a GTEK hash chain