Enhanced Security Scheme to Support Secure and Fast ASN-anchored Mobility in Mobile WiMAX

Chang-Seop Park[1] and Hyun-Sun Kang[2]
[1]Department of Computer, Dankook University
Chonan, Choongnam 330-714 – Republic of Korea
[e-mail: csp0@dankook.ac.kr]
[2]Department of General Education, Namseoul University
Cheonan, Choongnam 331-707– Republic of Korea
[e-mail: sshskang@nsu.ac.kr]
Corresponding author: Chang-Seop Park

Received July 25, 2011; revised September 18, 2011; accepted October 7, 2011; published November 29, 2011

Abstract

Without providing a proper security measure to the handover procedure in Mobile WiMAX, several security attacks can be mounted. Even though security schemes have been previously proposed for this purpose, they are still vulnerable to several security attacks due to fatal design flaws. A newly proposed security scheme in this paper is based on the framework of authentication domain and concept of handover ticket. A method of establishing security associations within the authentication domain is proposed, and a lightweight security measure to protect the management messages associated with the handover is also proposed. Especially, using the handover ticket, the new security scheme can defend against a *Redirection Attack* arising from a compromised base station. The new security scheme is comparatively analyzed with the previous security schemes in terms of *Replay*, *Session Hijacking*, *Man-In-The-Middle*, and *Redirection* attacks.

Keywords: WiMAX, handover, security, privacy key management, pre-authentication

The present research was conducted by the research fund of Dankook University in 2011.

DOI: 10.3837/tiis.2011.11.019

1. Introduction

Mobile WiMAX is a mobile broadband wireless-access solution based on IEEE 802.16e-2005 [1] which enables convergence of mobile and fixed broadband networks. IEEE 802.16 specifications only deal with the MAC and PHY layers, while the WiMAX Forum's Network Working Group (NWG) has developed a network reference model (NRM) [2] to serve as an architecture framework for WiMAX deployments, which includes the end-to-end network requirements, architecture, and protocols of WiMAX, using IEEE 802.16e-2005 as the air interface. Unlike IEEE 802.11-based WLAN, WiMAX has been designed with security in mind from the beginning. WiMAX security relies on an authenticated key management protocol called PKM (Privacy Key Management). IEEE 802.16-2004 [3] introduces the PKMv1 protocol as the key management method. Later on, PKMv1 protocol was improved by the IEEE 802.16e-2005, which introduced PKMv2 protocol.

Handover management is the process of initiating and ensuring a seamless handover of a mobile station (MS) from one base station (BS) to another. The BS associated with the MS before the handover is called a serving BS while the new BS is referred to as a target BS. The MS should establish a new security association with the target BS after the handover, which is required for mutual authentication and session key derivation. If the MS performs an EAP authentication with the AAA (Authentication, Authorization, and Auditing) server every time it registers to another BS, then it induces a long latency that is hindrance to the seamless handover, because the EAP authentication accompanies several message exchanges between the MS and AAA server. Nevertheless, it is not desirable to re-use the security association used before the handover, which creates a domino effect [4]. Namely, if the security of one BS is compromised, then this can lead to compromising the security of all previous BSs (backward secrecy) and the following BSs (forward secrecy). To strike a balance between security and performance, several security schemes [5][6][7][8][9] have been proposed to reduce the latency due to the authentication after the handover, which are based on the ASN-anchored mobility framework introduced in the WiMAX Forum's NRM [2]. On the other hand, there are various management messages exchanged among the network entities to complete the handover successfully. If they are not properly protected, then several security attacks such as *Session Hijacking*, *Man-In-The-Middle*, *Redirection*, and *DoS* attacks can be mounted to disturb the normal handover procedure.

Our contribution in this paper is threefold. First, a security framework to protect the management messages exchanged during the handover is proposed. The WiMAX standard assumes that those messages are exchanged securely, without specifying a concrete security mechanism. A couple of research papers have proposed schemes to protect these messages. However, they are not robust against various security attacks, which will be reviewed comparatively with our proposed security scheme. Second, a method to optimize the handover procedure is proposed to speed up the handover. That is, using a timestamp as a nonce in our proposed security scheme, it is shown that the number of the management messages associated with security can be reduced. Third, a case of a compromised BS is considered in this paper. If a BS is compromised, then the radio link with the BS can be eavesdropped, which is unavoidable. Furthermore, the compromised BS can be used to hijack or redirect a victim MS's session with a normal BS to the compromised BS. A concept of handover ticket is proposed to defend against those security attacks arising from a compromised BS. This paper is organized as follows. Section 2 introduces the security issues in the Mobile WiMAX

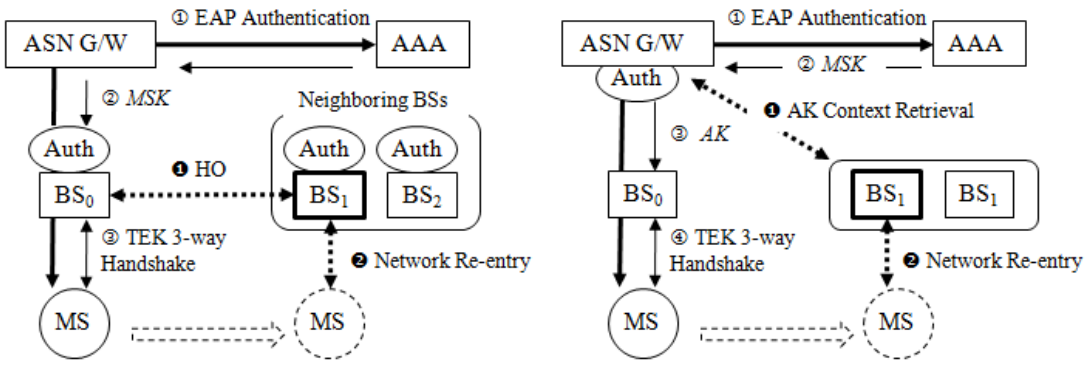
handover as well as a background on the Mobile WiMAX and Mobile WiMAX handover. In Section 3, a new security scheme for achieving a secure Mobile WiMAX handover is proposed as well as a method to optimize the handover protocol in terms of performance. Security analysis on the proposed security scheme is given and a comparative analysis with previous security schemes is also provided in Section 4. Finally, the concluding remarks are given in Section 5.

2. Security in Mobile WiMAX and Previous Works

Fig. 1 shows the Access Service Network (ASN) architecture developed by WiMAX Forum [2], where one or more base stations (BSs) are controlled by an ASN Gateway (G/W). There are two important functional entities in the ASN architecture, one of which is an *Authenticator* that provides key management and AAA client functionality. The other *is Anchor DP* (Data Path) acting as a layer 2 traffic aggregation point within an ASN. The BS is responsible for providing the air interface to the mobile station (MS), and cooperates with the ASN G/W to provide an ASN-anchored mobility to the MS. There are two deployment models: the Integrated deployment model and Standalone deployment model. In the Integrated deployment model, the *Authenticator* is co-located with the BS, while the *Authenticator* is within the ASN G/W in the Standard deployment model, as is shown in **Fig. 1**.

2.1 Authorization Protocol in Mobile WiMAX

The security of the network access in Mobile WiMAX is done with respect to PKM (Privacy Key Management) protocol whose main purpose is mutual authentication and key derivation. The current version of the PKM protocol is PKMv2, where most security weaknesses [10][11][12][13][14][15] found in the previous version, PKMv1, have been eliminated. The PKMv2 supports two modes of authentication: RSA-based authentication and EAP-based authentication. Since it is more likely that EAP will become the de facto authentication method for Mobile WiMAX access control, it is assumed that the security of the initial network access and the handover are based on the PKMv2's EAP-based authentication and associated key derivation.



(a) Integrated Model **(b)** Standalone Model

Fig. 1. ASN Architecture of Mobile WiMAX

When an MS first enters the Mobile WiMAX network through BS_0 as shown in **Fig. 1-(a)**, the MS performs an EAP authentication (①) with the AAA server via BS_0. After a successful authentication, an MSK (Master Session Key) is shared between the MS and AAA, and is

securely delivered to BS_0 (②, more precisely the *Authenticator* in BS_0). After deriving a PMK (Pairwise Master Key) by truncating the MSK to 160 bits, both the MS and BS_0 compute an authorization key AK_0 from the PMK. The generation process is as follows:

- $PMK = Truncate\ (MSK, 160)$
- $AK_j = DOT16KDF\ (PMK, MS, BS_j, \text{“AK”}, 160)$, where $j = 0, 1, 2, \ldots$ (1)

On the other hand, in the Standalone model of **Fig. 1-(b)**, after a successful authentication, the MSK is securely delivered to the ASN G/W (②, the *Authenticator* in the ASN G/W). Subsequently, the ASN G/W transports the authorization key AK_0 to BS_0 (③).

The *Dot16KDF* algorithm is a counter mode construction that may be used to derive an arbitrary amount of keying material from the source keying material. *MS* and BS_j denote the Layer 2 addresses of MS and BS_j, respectively. Based on AK_0, a mutual authentication and key exchange (*TEK* 3-*way Handshake*) are performed between the MS and BS_0 to share a common TEK (Traffic Encryption Key) to secure the data transfer between them. TEK_0 generated by BS_0 is transported to the MN after being encrypted with AK_0.

2.2 Secure Handover in Mobile WiMAX

When an MS handover occurs from a serving BS (BS_0) to a target BS (BS_1) as shown in **Fig. 1-(a)**, a *Network Re-entry* consisting of several steps (*Ranging*, *Authorization*, …) should be performed between the MS and BS_1, where the *Authorization* procedure includes the EAP authentication and *TEK* 3-*way Handshake*. Since there is no pre-established security association between the MS and BS_1, the MS should perform another full EAP authentication with the AAA server to be connected with the target BS (BS_1), which induces a long delay. Therefore, to skip the time-consuming EAP authentication, IEEE 802.16e [1] introduces a *Handoff Optimization* (HO), which allows an old AK (AK_0) to be reused with the target BS. Namely, BS_0 delivers it to BS_1. However, HO does not guarantee a perfect forward secrecy, which means that if AK_0 is compromised before handover, then the wireless link between the MS and target BS is also compromised.

To speed up the *Authorization* procedure during the Mobile WiMAX handover and to guarantee the perfect forward secrecy, a proactive key distribution scheme has been proposed [3][8][9]. As a result of a successful EAP authentication between the MS and AAA server as in **Fig. 1**-(a), the MSK is generated. Then, the AAA server distributes a distinct PMK derived from the MSK proactively to each of neighboring BSs, which will be the candidate target BSs for the MS's handover from the current serving BS. The generation process that is different from (1) is as follows:

- $PMK_j = DOT16KDF\ (MSK, MS, BS_j, \text{“AK”}, 160)$, where $j = 0, 1, 2, \ldots$
- $AK_j = Truncate\ (PMK_j, 160)$ (2)

Namely, while BS_0 is the serving BS for the MS in **Fig. 1-(a)**, PMK_1 and PMK_2 are distributed to BS_1 and BS_2, respectively, by the AAA server. When the MS starts a handover from BS_0 to BS_1, the MS and BS_1 can perform the *TEK* 3-*way Handshake* based on PMK_1 without performing another full EAP authentication.

On the other hand, when an MS handover occurs from a serving BS (BS_0) to a target BS (BS_1) as shown in **Fig. 1-(b)**, the BS_1 performs an AK *Context Retrieval* procedure with the ASN G/W to request a new AK (AK_1) to be shared with the MS, which is generated using (1). Based on AK_1, the MS can perform the *TEK* 3-*way Handshake* with BS_1 as a part of the

Network Re-entry procedure. A full handover protocol under the Standalone model is more complex than it is shown in **Fig. 1-(b)**, which will be presented in more detail in Section 3 when our security scheme is proposed. The Mobile WiMAX standard [1][2] assumes that all the management messages associated with handover are protected in terms of secrecy and integrity. However, no security schemes associated with it are defined within the standard. A couple of security schemes [7][9] have been proposed for the purpose of protecting the handover-related messages. Both schemes are based on the public-key encryption and digital signature to protect the messages. However, a mutual authentication between two network entities is not provided in both schemes due to the improper design of security schemes. Therefore, they are susceptible to various security attacks. The security weaknesses of those schemes are more elaborated in Section 4.

3. A New Security Scheme for Handover based on Handover Ticket

A security scheme under the Standalone model is proposed to protect the management messages associated with handover, which is also secure against various security attacks against the previous security schemes. In the following, $+K_X$ and $-K_X$ denote a pair of public and private keys of X, where X can be MS (M), ASN G/W (A), or BS (X = 0, 1 for BS_0 and BS_1). N_X and T_X are a random number and a timestamp generated by X, respectively. $[\ m\ ]_K$ is a symmetric encryption of m using a secret key K. While $[\ m\ ]_{+K_X}$ denotes the encryption of m with the public key $+K_X$, $Sig(-K_X)$ is a digital signature based on the signing private key $-K_X$ covering all preceding fields. $MAC(K)$ is the message authentication code computed over all preceding fields of a message using a symmetric key K.

3.1 Assumptions and Design Principles

First, it is assumed there is a pre-established security association between the MS and the AAA server, based on which the MS is initially allowed to enter the Mobile WiMAX network and a key hierarchy is also established as in (1). On subscription to the Mobile WiMAX service, the MS is provided with its own credential to authenticate itself to the network. The credential is shared secret between the MS and the Mobile WiMAX service provider. Since the service provider stores the subscriber's credential in the AAA server, it is reasonable to assume that there is a pre-established security association between the MS and the AAA server. Second, for the purpose of securing the management messages during the handover, it is also assumed that the network entities such as BSs and the ASN G/W are configured to possess their own public-key certificates when initially being deployed in the Mobile WiMAX network. However, the certificates are not directly used to protect the handover messages. Instead, they are used to generate a pairwise long-term symmetric key between any two network entities when an authentication domain is established for the first time within the Mobile WiMAX network. An access service network (ASN) in **Fig. 1** becomes an *Authentication Domain* when security associations between any two BSs or between a BS and ASN G/W are established. Third, instead of random numbers, timestamps are employed by our proposed scheme to guarantee the freshness of each handover message. In Mobile WiMAX, the timestamp representing a transmission time of a handover message has been already employed to allow the receiving network entity to estimate the message propagation delay. Therefore, it can also be used for our security purpose. Nonetheless, strict time synchronization between two network entities is not required for security since the timestamp is more like a sequence number in our proposed scheme. Forth, it is also assumed that an attacker cannot access or modify the secret information and timestamp values in the neighbor caches of the MS and BSs.

3.2 Handover Procedure under Standalone Model

Under the Standalone model, a handover from a serving BS to a target BS consists of two phases as shown in **Fig. 2** [2]: *Handover Preparation* phase and *Handover Action* phase. A MS can initiate the handover by transmitting a **MOB-MSHO-REQ** message. If the serving BS (BS_0) receives the **MOB-MSHO-REQ**, then it sends a **HO-REQ** message containing the MS information to one or more candidate target BSs (BS_1, BS_2, BS_3) neighboring BS_0 over the backbone network, to notify that the MS intends to handover. If the serving BS (BS_0) receives the **HO-RSP** messages from the candidate target BSs, then it informs the MS of the selected target BSs by sending the **MOB-BSHO-RSP**. The *Handover Action* phase begins when the MS receives the **MOB-BSHO-RSP**. The MS chooses a final target BS (BS_1) and sends a **MOB-HO-IND** message to notify the serving BS of the final decision. Then, the **HO-CNF** and **HO-ACK** messages are exchanged between the serving BS (BS_0) and target BS (BS_1) to confirm the MS's decision. The connection of the serving BS with the MS is now terminated. In order to re-connect with the target BS (BS_1), another full EAP authentication should be performed between the MS and AAA server via the BS_1.

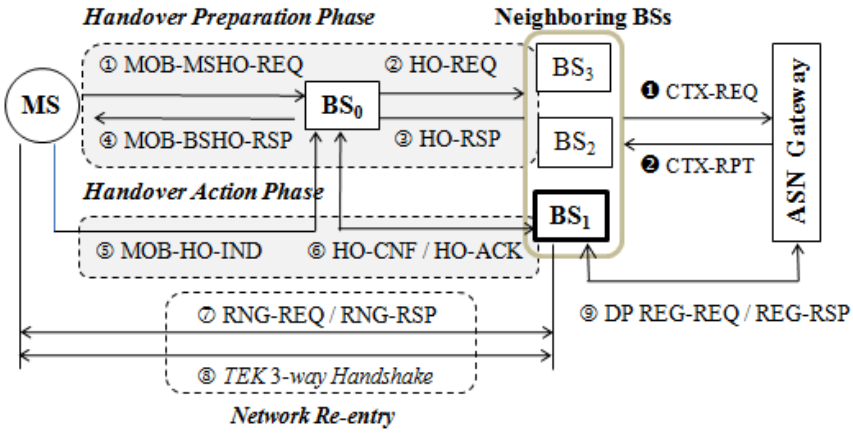


Fig. 2. Handover Procedure under the Standalone Model

However, since it induces a long latency to hinder a smooth handover, the WiMAX Forum introduces a *Context Retrieval* procedure between the target BS and ASN G/W. Since the MSK/PMK shared with the MS is stored in the *Authenticator* within the ASN G/W, the target BS (BS_1) can obtain an authorization key AK_1 computed from PMK as in (1), directly from the ASN G/W using the *Context Retrieval* procedure (**CTX-REQ** / **CTX-RPT** messages); it can be carried out during *Handover Preparation* phase. When *Handover Preparation* and *Handover Action* phases are finished, the *Network Re-entry* starts with a *Ranging* procedure (**RNG-REQ** and **RNG-RSP** messages are exchanged between them). The *Ranging* process is required to adjust all PHY parameters for the wireless link. Subsequently, a *TEK* 3-*way Handshake* can be performed based on the authorization key AK_1 shared between them. If the MS is successfully connected with BS_1, then BS_1 exchanges a **Data Path** (DP) **REG-REQ** and **REG-RSP** messages with ASN G/W to switch the data traffic for the MS from BS_0 to BS_1.

3.3 Bootstrapping Security in Authentication Domain

An *Authentication Domain* is logically defined in the Access Service Network (ASN) consisting of ASN G/W and one or more BSs (BS_j, j = 0, 1, 2, …, n-1), as is shown in **Fig. 1**, when security associations among the network entities are established. ASN G/W plays a role

of security controller in the *Authentication Domain*. When BSs are deployed in ASN for the first time, they perform the "one-time" *Authentication Domain Registration* procedure with ASN G/W to establish security associations (long-term symmetric keys) with other network entities. Eventually, the long-term symmetric keys can be used to protect the management messages associated with the handover in **Fig. 2**, which will be explained in Section 3.4.

ASN G/W is initially configured with a pair of its own public and private keys, $(+K_A, -K_A)$, and the public keys of BSs, $+K_j$. Each BS_j is also configured with a pair of its own public and private keys, $(+K_j, -K_j)$, and the public key of ASN G/W, $+K_A$. *Neighbor_BS* (BS_j) denotes a set of candidate target BSs that the MS can handover from the current serving BS_j. *Neighbor_Key* (BS_j) is defined as a set of long-term symmetric keys that the BS_j shares with each neighboring BS. When an *Authentication Domain Registration* procedure starts, each BS_j and ASN G/W generate personal keys K_j and K_A, respectively, and *Neighbor_Key* (BS_j) is computed as follows:

■ *Neighbor_Key* (BS_j)
■ $= \{ K_{jx} \mid K_{jx} = prf(K_j, K_x, BS_j, BS_x)$ and $BS_x \in$ *Neighbor_BS* $(BS_j) \}$. (3)

Each BS_j also shares a distinct long-term symmetric key K_{jA} with the ASN G/W. Namely, $K_{jA} = prf(K_j, K_A, BS_j, ASN\ G/W)$, where *prf* (.) is a pseudo-random function. For example, suppose K_j is the personal key of BS_j for $j = 0, 1, ..., 5$. If *Neighbor_BS* $(BS_0) = \{BS_1, BS_2, BS_3\}$ and *Neighbor_BS* $(BS_1) = \{BS_0, BS_4, BS_5\}$, then *Neighbor_Key* $(BS_0) = \{K_{01}, K_{02}, K_{03}\}$ and *Neighbor_Key* $(BS_1) = \{K_{10}, K_{14}, K_{15}\}$, where $K_{01} = K_{10}$.

When establishing an *Authentication Domain*, each BS_j registers itself with ASN G/W by sending the following *Registration_Request* message.

■ For each BS_j where $j = 0, 1, 2, \ldots$
■ BS_j generates a random personal key K_j and a timestamp T_j.
■ $BS_j \Rightarrow$ G/W : *Registration_Request* $\{ T_j, [K_j]_{+K_A}, Sig\ (-K_j) \}$

When receiving the *Registration_Request* message, ASN G/W responds with the following *Registration_Response* message.

■ ASN G/W generates a random personal key K_A.
■ For each BS_j where $j = 0, 1, 2, \ldots$
■ ASN G/W computes *Neighbor_Keys* (BS_j) and K_{jA}, and generates a timestamp T_A.
■ $BS_j \Leftarrow$ G/W : *Registration_Response* $\{T_A, [K_{jA}, Neighbor\_Keys\ (BS_j)]_{+K_j}, Sig\ (-K_A) \}$

Each BS_j maintains a neighbor cache consisting of $|$ *Neighbor_BS* $(BS_j) | + 1$ entries. Each entry is 3-tuple (ASN G/W, K_{jA}, T_A) or (BS_x, K_{jx}, T_x), where $BS_x \in$ *Neighbor_BS* (BS_j) and $K_{jx} \in$ *Neighbor_Key* (BS_j). T_x is a timestamp generated by each neighboring BS_x and sent to BS_j. After the *Authentication Domain Registration* procedure is finished, the neighbor cache of BS_j is initialized as (BS_x, K_{jx}, $T_x = 0$) and (ASN G/W, K_{jA}, T_A). The reason why $T_x = 0$ is that there was no message exchange between two BSs during the *Authentication Domain Registration* procedure. ASN G/W also maintains a neighbor cache consisting of n entries, each of which is for BS_j, $j = 0, 1, 2, \ldots, n\text{-}1$. Each entry is also 3-tuple (BS_j, K_{jA}, T_j). **Fig. 3** shows the neighbor caches of BS_1 and ASN G/W after finishing the *Authentication Domain Registration* procedure.

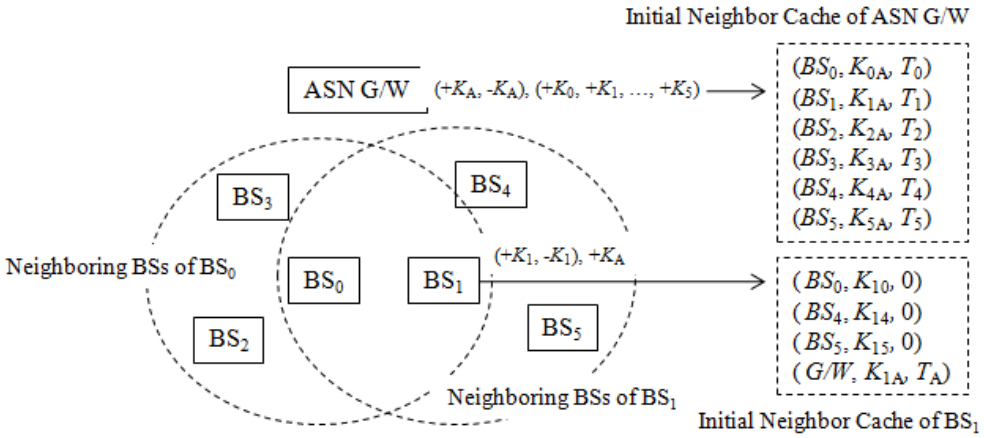


Fig. 3. Neighbor Caches of BS and ASN G/W

Once the *Authentication Domain* is established, the neighbor caches of the BS_j and ASN G/W are padded with the entries of MSs whenever they join the Mobile WiMAX network. As a result of the successful EAP authentication of an MS with the AAA server via BS_j, entries for the MS, (MS, AK_j, $T_M = 0$), and (MS, BS_j, MSK, PMK_j, $T_M = 0$) are inserted into the neighbor caches of BS_j and ASN G/W, respectively.

3.4 Secure Handover Scheme

Based on the long-term symmetric keys shared between network entities, the management messages during the handover can be protected. Unlike previous security schemes [7][9] using random numbers, our proposed security scheme employs timestamps to guarantee the freshness of handover messages. As mentioned in 3.3.2, each BS_j and ASN G/W maintains their own neighbor caches to store the previous timestamps received from other network entities. The MS also maintains its own neighbor cache for such purpose. To simplify the notations, we assumed that each timestamp included in the handover message is distinct even though its notation is identical, which means T_M in ① and T_M in ⑤ are distinct (T_M in ① < T_M in ⑤). As in **Table 1**, each message is integrity-protected by the MAC (Message Authentication Code) is computed using the shared symmetric key. Each protocol message has several inherent Information Element (IE) fields described in [1][2]. However, since most of them are not related to security, they are excluded for explanation simplicity. Instead, only the security-related fields are shown in each message.

In **Table 1**, the handover messages of ①, ④, and ⑤ are protected with AK_0, which is an authorization key derived from a previous handover or an initial EAP authentication with the AAA server. On the other hand, BS_0 and BS_1 share a long-term symmetric key K_{01}, based on which a session key $SK_{01} = prf\ (T_0, K_{01})$ is computed and used to protect the handover messages of ②, ③, and ⑥. During the *Handover Preparation* phase, when BS_0 receives the **MOB-MSHO-REQ**, it sends a **HO-REQ** message containing the MS information to one or more candidate target BSs neighboring BS_0 over the backbone network to notify that the MS intends to handover as explained in Section 3.2. Namely, {②, ❶, ❷, ③ } are repeated for each $BS_i \in Neighbor\_BS(BS_0)$. The list of candidate target BSs are prepared by the MS through a scanning process and included in the **MOB-MSHO-REQ** message. During the *Handover Action* phase, the MS chooses one of them as a final target BS (BS_1 in **Fig. 2** and **Table 1**).

Table 1. Security Scheme for Handover Messages

		Handover Message	Security Fields	
①	MS ⇒ BS_0	MOB-MSHO-REQ	T_M, HT, $MAC(AK_0)$	Handover Preparation
	$HT = [\ T_M, MS, Neighbor\_BS(BS_0), MAC(SK_{MA})\ ]$			
②	BS_0 ⇒ BS_i	HO-REQ	T_0, HT, $MAC(SK_{0i})$	
❶	BS_i ⇒ G/W	CTX-REQ	T_i, HT, $MAC(SK_{iA})$	
❷	G/W ⇒ BS_i	CTX-RPT	T_A, $[\ masked\_AK_i\ ]_{SK_{iA}}$, $MAC(SK_{iA})$	
	$PMK_i = DOT16KDF\ (MSK, T_M, MS, BS_i, \text{“AK”}, 160)$ $AK_i = Truncate\ (PMK_i, 160)$ $SK_{MA} = prf\ (T_M, MSK)$ $Mask_i = prf\ (BS_i, SK_{MA})$ $masked\_AK_i = AK_i \oplus Mask_i$			
③	BS_i ⇒ BS_0	HO-RSP	T_i, $MAC(SK_{0i})$	
④	BS_0 ⇒ MS	MOB-MSHO-RSP	T_0, $MAC(AK_0)$	
⑤	MS ⇒ BS_0	MOB-HO-IND	T_M, $Mask_1$, $MAC(AK_0)$	Handover Action
⑥	BS_0 ⇒ BS_1	HO-CNF	T_0, $Mask_1$, $MAC(SK_{01})$	
⑥	BS_1 ⇒ BS_0	HO-ACK	T_1, $MAC(SK_{01})$	
	$AK_1 = masked\_AK_1 \oplus Mask_1$			
⑦	MS ⇒ BS_1	RNG-REQ	T_M, $MAC(AK_1)$	Network Re-entry
⑦	BS_1 ⇒ MS	RNG-RSP	T_1, $MAC(AK_1)$	
⑧	MS ⇔ BS_1	*TEK 3-way Handshake* (can be omitted: see Section 3.5)		
⑨	BS_1 ⇒ G/W	DP REG-REQ	T_1, $MAC(SK_{01})$	
⑨	G/W ⇒ BS_1	DP REG-RSP	T_A, $MAC(SK_{01})$	

$BS_i \in Neighbor\_BS(BS_0)$

When each handover message in **Table 1** is received, it is processed according to *Algorithm* 1. Suppose *handover-message* { *T*, …, *MAC*(*SK*) } is sent from *X* to *Y* and *neighbor_cache* of *Y* contains an entry for *X*, (*X*, *K*, *stored_T*), where if *X* or *Y* is *MS*, then *K* = *AK*. When *Y* receives the handover message, it is processed as follows:

[*Algorithm.* 1: *Procedure for processing a received handover message*]

- If $T \le stored\_T$, then drop the message silently;
- If *X* = *MS* or *Y* = *MS*, /* *compute a session key SK* */
  then $SK \leftarrow AK$ /* *AK* is already a session key between *MS* and *BS* */
  else $SK \leftarrow prf\ (T, K)$; /* *compute a session key SK* using a long-term symmetric key *K* */
- Using *SK*, compute a MAC value, *computed_MAC*(*SK*);
- If $MAC(SK) \neq computed\_MAC(SK)$,
  then drop the message silently;
- $stored\_T \leftarrow T$; /* *replace the timestamp in the neighbor cache by the one in the message.* */

For example, when receiving a **HO-REQ** message, BS_i first checks if T_0 in the message is

greater than the one in its neighbor cache. If successful, then BS_i computes the same $SK_{0i} = prf(T_0, K_{0i})$ and verifies the correctness of the MAC value. Next, the timestamp in the neighbor cache is replaced by T_0 in the message. As a response to the message, BS_i sends a **HO-RSP** message that contains T_i and the corresponding MAC value.

Now, we concentrate on two items, "*HT*" and "*masked_AK*$_i$", passed during the handover. The HT (Handover Token) generated by the MS is used to notify the ASN G/W that the handover is actually triggered by the MS itself, not any other network entity. is the ability to combat a compromised BS attack is a useful functionality, which will be more elaborated in Section 4.5.

■ $HT = [T_M, MS, Neighbor\_BS(BS_0), MAC(SK_{MA})]$ (4)

The meaning of HT is that the MS intents to handover from BS_0 to one of $Neighbor\_BS(BS_0)$. It is authenticated with a session key $SK_{MA} = prf(T_M, MSK)$ derived from *MSK* shared with the ASN G/W. When HT is finally delivered to the ASN G/W through the **CXT-REQ** message, HT is verified after checking the timpetamp and MAC value of the **CXT-REQ** message. Upon successful verification of both of them, ASN G/W computes AK_i for BS_i. The generation process, which is different from (1) and (2), is as follows:

■ $PMK_i = DOT16KDF(MSK, T_M, MS, BS_i, \text{"AK"}, 160)$
■ $AK_i = Truncate(PMK_i, 160)$ (5)

However, unlike Mobile WiMAX standard [2] and previous schemes [7, 9], $masked\_AK_i$ ($= AK_i \oplus Mask_i$) is sent to BS_i instead of AK_i, where $Mask_i = prf(BS_i, SK_{MA})$. The reason for masking AK_i with $Mask_i$ is that if BS_i is not chosen as a final target BS, then AK_i needs not to be known to BS_i. On the other hand, if it is chosen, then the mask will be removed during the *Handover Action* phase. Namely, when the MS decides to handover to BS_1, the **MOB-HO-IND** message contains $Mask_1$ to obtain AK_1 ($= masked\_AK_i \oplus Mask_i$) as in **Table 1**. Subsequently, based on AK_1, the MS and BS_1 can perform a *TEK* 3-*way Handshake*. When the *Network Re-entry* procedure is successfully finished, BS_1 exchanges **Data Path** (DP) **REG-REQ** and **REG-RSP** messages with the ASN G/W to switch the data traffic for the MS from BS_0 to BS_1. Unless these messages are properly protected, an attacker can redirect data traffic for a victim MS to another BS.

3.5 Combining Ranging Process with TEK 3-way Handshake

As a part of *Network Re-entry* procedure, *Ranging* and *TEK* 3-*way Handshake* are subsequently performed between the MS and new BS_1. The following is a simplified version of the *TEK* 3-*way Handshake* (*T3H*) [1]:

■ $BS_1 \Rightarrow MS : T3H1\ \{ N_1, \ldots, MAC(AK_1) \}$
■ $MS \Rightarrow BS_1 : T3H2\{ N_M, N_1, \ldots, MAC(AK_1)\}$
■ $BS_1 \Rightarrow MS : T3H3\{ N_M, N_1, \ldots, [TEK_1, \ldots]_{AK_1}, MAC(AK_1) \}$ (6)

TEK 3-*way Handshake* is for achieving mutual authentication between the MS and BS_1 based on an authorization key AK_1. It also establishes a new TEK (TEK_1) to protect the data traffic between them, namely BS_1 generates and transports an encrypted TEK_1 to the MS. Owing to two security fields in the **RNG-REQ** and **RNG-RSP** messages in **Table 1**, a function of *TEK* 3-*way Handshake* can be integrated into the *Ranging* process so that *TEK* 3-*way Handshake*

can be omitted. When receiving the **RNG-REQ** message, the BS_1 checks whether T_M is valid and whether the MAC value is correct using AK_1. If the verification is successful, then the BS_1 can authenticate the MS. On the other hand, when receiving the **RNG-RSP** message, the MS does the same verification as BS_1 did, and can authenticate BS_1. Finally, a new TEK can be derived as follows:

■ $TEK_1 = prf\,(AK_1, MS, BS_1, T_M, T_1)$ (7)

During the *TEK* 3-*way Handshake* in (6), a TEK is encrypted and transported by BS_1 to the MS. However, generating a session key unilaterally by one party is usually recognized as insecure [10]. Therefore, the TEK is derived from values contributed by both parties as in (7).

4. Security Analysis and Comparisons

In this Section, our proposed scheme is comparatively analyzed with two previous schemes [7][9] in terms of security. After the security weaknesses of [7][9] are pointed out, it is shown that such weaknesses are not found in our proposed scheme.

4.1 Nonce and Replay Attack

If a random number is used to guarantee the freshness of a certain message, then it should work in a challenge-response way. In [7], random numbers, N_1 and N_A, are employed for the freshness of the **CXT-REQ** and **CXT-RPT** messages as follows:

■ $BS_1 \Rightarrow$ G/W : CXT-REQ { [N_1]$_{+K_A}$, $Sig(-K_1)$ }
■ G/W $\Rightarrow BS_1$: CXT-RPT { […, N_1, N_A]$_{+K_1}$, $Sig(-K_A)$ } (8)

It is assumed that BS_1 and ASN G/W know each other's public key, $+K_A$ and $+K_1$, respectively. The random number N_1 in the **CXT-REQ** message is a kind of challenge value to ASN G/W. Since it is included as a response value in the **CXT-RPT** message, BS_1 can verify the freshness of the **CXT-RPT** message. However, ASN G/W cannot verify whether or not the **CXT-REQ** message is replayed. In order for ASN G/W to verify it, N_A generated by the ASN G/W should be included in the **CXT-REQ** message. So, it is not feasible to guarantee the freshness of both messages without introducing an additional message when random numbers are used. There are two methods to remedy this problem. First, the ASN G/W keeps a list of all N_1's generated and sent by BS_1. When receiving N_1, ASN G/W first checks if it can be found in the list. If it is not found, then it can be considered as a fresh N_1 and can continue the protocol. However, keeping a list of all N_1's sent by BS_1 is a big burden on ASN G/W and is not possible in some cases. Second, the timestamp can be used as in our proposed scheme.

■ $BS_1 \Rightarrow$ G/W : CXT-REQ { T_1, …, $MAC(SK_{1A})$ }
■ G/W $\Rightarrow BS_1$: CXT-RPT { T_A, …, $MAC(SK_{1A})$ } (9)

When receiving each message, the timestamp is first verified as to whether or not it is greater than the one in the neighbor cache. Namely, the freshness of the message is guaranteed by the freshness of the timestamp. Furthermore, the correct MAC value verifies whether or not the message is sent from the legitimate entity. Our scheme does not store all received timestamps, but a single timestamp is received previously.

4.2 Mutual Authentication and Man-In-The-Middle Attack

When a handover message is exchanged, mutual authentication based on an established security association should be performed between a sender and a receiver to defend against Man-In-The Middle or rogue BS attacks. In [9], a security association between them is established on the fly as follows:

- $BS_0 \Rightarrow BS_1$: HO-REQ { N_0 }
- $BS_1 \Rightarrow$ G/W : CXT-REQ { [SK]$_{+K_A}$, T_1 }
- G/W $\Rightarrow BS_1$: CXT-RPT { […, AK_0]$_{SK}$ }
- $BS_1 \Rightarrow BS_0$: HO-RSP { [N_0, …]$_{AK_0}$ } (10)

It is assumed that BS_1 knows a public key $+K_A$ of ASN G/W in advance and there is no security association between BS_0 and BS_1. AK_0 is an authorization key shared between the MS and BS_0, which is also known to ASN G/W. By exchanging **CXT-REQ** and **CXT-RPT** messages, BS_1 and ASN G/W share a session key KS generated by BS_1, while BS_1 and BS_0 share AK_0. As a response to the challenge N_0, BS_1 sends encrypted N_0 to BS_0. However, there is a fatal design flaw in [9]. ASN G/W cannot verify whether or not the **CXT-REQ** message is sent from the legitimate BS_1 since anyone can prepare and send the message using ASN G/W's public key $+K_A$. Namely, there is no mutual authentication between them. Suppose a rogue BS (BS_R) receives the **HO-REQ** message. Then, BS_R impersonating legitimate BS_1 exchanges **CXT-REQ** and **CXT-RPT** messages with ASN G/W, and finally obtains AK_0. So, BS_R can respond to the challenge from BS_0. On the other hand, in our proposed scheme, each pair of messages is mutually authenticated as verified in (9) so that a MITM attack is infeasible.

4.3 Uncontrolled Handover and Session Hijacking Attack

Through a *Context Retrieval* procedure, an authorization key AK to be shared with an MS is distributed to a target BS. Therefore, if an attacker (A) can forge a **CXT_REQ** message, then the authorization key can be retrieved and exploited to mount a *Session Hijacking* attack. Suppose a victim MS is being serviced through BS_i and an attacker within a service area of BS_j tries to hijack a connection with the MS, where $i \neq j$.

- A (BS_j) $\Rightarrow$ G/W : CXT-REQ
- G/W $\Rightarrow$ A (BS_j) : CXT-RPT { …. AK_j … } (11)

First, the attacker disguising a legitimate BS_j sends a forged **CXT_REQ** message to ASN G/W and obtains AK_j as in (11). The attacker now tries to re-connect with BS_j. Under a normal handover procedure, the attacker's network re-entry attempt is blocked by BS_j since BS_j did not participate in any handover procedure so that it does not have the victim handover context of a MS. However, the Mobile WiMAX standard [2] allows a MS to perform an uncontrolled (unprepared) handover, which occurs when the MS tries to re-enter a target BS that did not participate in the normal *Handover Preparation* and *Action* phase. That is, the MS can start a *Ranging* process with the target BS without sending ① and ⑤ as in **Fig. 2**. This may occur due to suboptimal radio planning conditions. Therefore, the attacker can successfully re-connect with BS_j since it has already obtained AK_j. To defend against this attack, the message should be properly authenticated and the AK delivered to BS_j should also be encrypted. The security scheme proposed in [9] is not secure against this kind of *Session Hijacking* attack. As can be seen in (10), since the **CXT-REQ** message is not authenticated by ASN G/W, the attacker can

forge the **CXT-REQ** message and can obtain AK. On the other hand, in our proposed scheme, a **CXT-REQ** message is authenticated based on a long-term symmetric key and timestamp, so that the *Session Hijacking* attack cannot affect our security scheme.

4.4 Perfect Forward and Backward Secrecy

An authorization key AK_j shared by an MS and BS_j must not be reused with other BSs or MSs. Failure to do so may result in domino effect problems, where a compromise of the key enables an attacker to decrypt information exchanged anywhere and anytime on the network. From a security viewpoint, the *Handover Optimization* (HO) introduced in the Integrated deployment model of WiMAX Network is not secure in terms of both perfect forward secrecy (PFS) and backward secrecy (PBS). In [9] as seen in (10), AK_0 shared between the MS and BS_0 is reused with BS_1, and it is also a security association between BS_0 and BS_1. So, it is susceptible to the domino effect.

Suppose BS_{j_i} is the target BS of an MS handover at the *i*-th handover, where BS_{j_0} is an initial serving BS. Let AK_{j_x} and AK_{j_y} be the authorization keys of the MS shared with the BS_{j_x} and BS_{j_y}, respectively, where $x \neq y$. Since the authorization keys are used to encrypt the TEKs, AK_{j_x} and AK_{j_y} should be cryptographically independent. That is, even though one of them is accidentally exposed to an attacker, it should be infeasible to derive the other from the exposed one. If BS_{j_x} is the target BS, then BS_{j_x} can obtain the authorization key AK_{j_x} from ASN G/W through the *Context Retrieval* procedure. In this case, to guarantee the cryptographic key independence, AK_{j_x} should be derived from PMK_{j_x} which is higher than AK_{j_x} in the key hierarchy, as in (1) and (2). A previous scheme proposed in [7] generates the authorization key in this way. However, suppose $BS_{j_x} = BS_{j_y}$, where $x < y$, which means the MS revisits the same BS as it did previously. Therefore, $AK_{j_x} = AK_{j_y}$ if the key generation process in (1) or (2) is used. In this case, the perfect forward and backward secrecy is not guaranteed. In order to solve this problem in our proposed scheme, the authorization key is derived as in (5). That is, the timestamp is included to derive PMK, based on which AK is generated. Therefore, even though the MS revisits the same BS multiple times, the authorization key with the BS is distinct at every visit.

4.5 Compromised BS and Redirection Attack

If a BS is compromised, namely its neighbor cache is exposed to an attacker, then the communication link between the MS and the compromised BS can be eavesdropped. During a *Context Retrieval* procedure, ASN G/W sends an authorization key to the target BS, which will be shared with the MS and target BS. Since the authorization key is encrypted with the session key derived from the long-term symmetric key known to both ASN G/W and target BS, the authorization key is revealed to the attacker if the target BS is compromised. This is an unavoidable threat when the neighbor cache is exposed.

On the other hand, another threat resulting from the compromised BS is to redirect all the MS traffic to the compromised BS. Suppose BS_C is a compromised BS whose neighbor cache is exposed to an attacker (A) and MS_i for $i = 1, 2, \ldots$, are the victim MSs currently being serviced through BS_i different from BS_C. Both BS_C and BS_i are under identical *Authentication Domain* controlled by an ASN G/W. The attacker disguising BS_C sends the following messages to ASN G/W, which are intended for requesting ASN G/W to switch the data traffic for the victim MS_i from BS_i toward BS_C.

- For each MS_i where $i = 0, 1, 2, \ldots$
- A (BS_C) ⇒ G/W : DP REG-REQ { MS_i, BS_i, BS_C, *Nonce*, *MAC*(SK_{CA}) } (12)

KS_{CA} is a session key derived from both *Nonce* and a compromised long-term symmetric key. Since the message is successfully authenticated by ASN G/W, the message is processed by the ASN G/W so that all data traffic of MS_i is redirected from BS_i toward BS_C, as shown in **Fig. 4**.

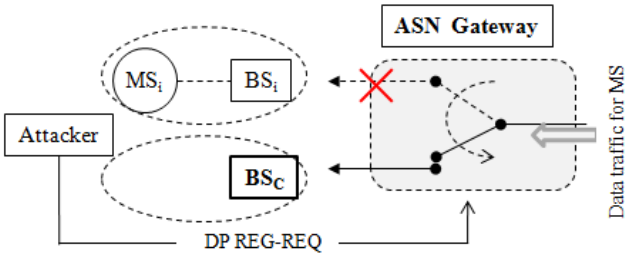


Fig.4. Redirection Attack

However, in our proposed scheme, the Handover Ticket is used and verified by ASN G/W. The attacker cannot forge a valid HT in (4) since it does not know the common secret between the MS and ASN G/W. Therefore, the redirection attack is not feasible in our proposed scheme.

4.6 Security and Performance Comparisons

The result of comparing our proposed scheme with the previous schemes [7][9] is shown in **Table 2** in terms of several security attacks. The reason for selecting [7] and [9] for comparison is that they have been designed under the same model of ASN architecture (Standalone Model) similarly to our proposed scheme. On the other hand, other security schemes such as [5][6][8] have been designed under the Integrated Model and have not specified a detailed security protocol to be analyzed with the security attacks listed in **Table 2**.

Table 2. Security Comparisons

Types of Security Attacks	[7]	[9]	Proposed scheme
Replay Attack	***Insecure*** (random number used)	***Insecure*** (random number used)	*Secure* (Timestamp used)
PFS/PBS (Type 1) PFS/PBS (Type 2)	*Secure* ***Insecure***	***Insecure*** ***Insecure***	*Secure* *Secure*
Session Hijacking Attack	*Secure*	***Insecure*** (with uncontrolled handover)	*Secure*
Redirection Attack (compromised BS)	***Insecure***	***Insecure***	*Secure* (with Handover Ticket)
Man-In-The-Middle Attack	*Secure* (mutual authentication)	***Insecure*** (no mutual authentication)	*Secure* (mutual authentication)

The PBS/PFS is classified into 2 types. Type 1 is the one in case the MS does not visit the same BS as it had previously, while Type 2 is the one in case the MS might visit the BS previously visited. If AK and PMK are derived based on a key hierarchy as in (1), (2), and (5),

then Type 1 is satisfied. However, in case of Type 2, PMK should be derived based on a key hierarchy as well as a timestamp as in (5). Only our proposed scheme satisfies both types of PBS/PFS. When the controlled handover is supported by the Mobile WiMAX network, the security scheme in [9] is not secure against a *Session Hijacking* attack. Finally, even though a BS is compromised, our proposed scheme is robust against a redirection attack owing to the Handover Ticket.

Table 3 shows each of the security schemes proposed for the standard Mobile WiMAX handover protocol. Each of them including ours has only security functionalities embedded into each of the handover messages. No messages have been supplemented for the purpose of security other than the standard handover messages in **Fig. 2**. Our proposed scheme protects each of the handover messages in **Table 3**, while [7][9] protect a part of them, which is also a source of security attack. The handover messages ②, ❶, ❷, and ③ should be sent to each of the neighboring BSs of BS_0 even though they are shown to be sent only to BS_1 in [7][9]. For the comparison of cryptographic operations, the handover messages ②, ❶, ❷, and ③ are considered, since they are commonly protected by each of three security schemes. In [7], four public-key encryptions and four digital signature operations are needed to protect the handover messages. In [9], one public-key operation, three digital signature verification operations, and two symmetric-key operations are required. Five hash operations and one symmetric-key operation are required in our proposed scheme. Therefore, our scheme is computationally more efficient than [7][9]. On the other hand, our scheme requires a bootstrapping procedure to configure an authentication domain. It is to establish security associations between AUTH in ASN G/W and BSs. However, the bootstrapping procedure is performed only once when the Mobile WiMAX network is deployed for the first time. It is a kind of initialization procedure. So, it does not affect the handover performance after the Mobile WiMAX service starts. If an authentication domain consists several BSs, only 2 messages are exchanged between AUTH and each of BSs, where one public-key and one digital signature operation is required for each message.

Table 3. Comparison of Three Secure Handover Schemes

	[7]	[9]	Proposed Scheme
①	Not defined	Not defined	T_M, HT, $MAC(AK_0)$
②	$[\ N_0\ ]_{+K_1}$, $Sig(-K_0)$	N_0	T_0, HT, $MAC(SK_{0i})$
❶	$[\ N_1\ ]_{+K_A}$, $Sig(-K_1)$	$[\ K\ ]_{+K_A}$, T_0, $Cert$	T_i, HT, $MAC(SK_{iA})$
❷	$[+K_M, PMK_1, N_A\ ]_{+K_1}$, $Sig(-K_A)$	$[AK_0]_K$, $Cert$	T_A, $[\ masked\_AK_i\ ]_{SK_{iA}}$, $MAC(SK_{iA})$
③	$[\ N_1\ ]_{+K_M}$, N_0, $Sig(-K_A)$	$[\ N_0, Cert\ ]_{AK_0}$	T_i, $MAC(SK_{0i})$
④	$[\ N_1\ ]_{+K_M}$, N_0	Not defined	T_0, $MAC(AK_0)$
⑤	Not defined	Not defined	T_M, $Mask_1$, $MAC(AK_0)$
⑥	Not defined	$MAC\ (AK_0)$	T_0, $Mask_1$, $MAC(SK_{01})$
⑥	Not defined	$MAC\ (AK_0)$	T_1, $MAC(SK_{01})$

5. Conclusion

A new security scheme for the Mobile WiMAX handover has been proposed in this paper. A

fundamental framework of the proposed security scheme is provided through bootstrapping security in an authentication domain under the ASN architecture. Based on the established security associations among network entities, the management messages exchanged during the handover can be protected from various security attacks. Especially, timestamps have been employed for the freshness of the messages in the proposed security scheme, unlike previous security schemes using random numbers. As a result, it has been shown that our proposed security design can be greatly simplified as well as enhance security. Furthermore, a concept of handover ticket has been introduced to defend against security attacks arising from the compromised BS. To the best of our knowledge, this is the first attempt to design a security scheme against a BS compromised attack.

References

[1] IEEE Std. 802.16e-2005, "IEEE Standard for Local and Metropolitan Area Networks Part l6: Air Interface for Fixed and Mobile Broadband Wireless Access Systems," *IEEE Press*, 2006.

[2] WiMAX Forum, "WiMAX Forum Network Architecture Stage 3: Detailed Protocols and Procedures," Release 1.0 Version 4, WMF - T33-001-R010v04, 2009.

[3] IEEE Std. 802.16-2004, "IEEE Standard for Local and Metropolitan Area Networks Part l6: Air Interface for Fixed Broadband Wireless Access Systems," *IEEE Press*, 2004.

[4] T. Clancy, M. Nakhjiri, V. Narayanan, and L. Dondeti, "Handover Key Management and Re-Authentication Problem Statement," *RFC 5169*, Mar. 2008.

[5] H.M. Sun, Y.H. Lin, S.M. Chen, Y.C. Shen, "Secure and Fast Handover Scheme based on Pre-Authentication Method for 802.16/WiMAX Infrastructure Networks," in *Proc. of TENCON – 2007 IEEE Region 10 Conference*, pp. 1-4, Oct. 30-Nov. 2, 2007. Article (CrossRef Link)

[6] J. Hur, H. Shim, P. Kim, H. Yoon, N.O. Song, "Security Considerations for Handover Schemes in Mobile WiMAX Networks," in *Proc. of IEEE Wireless Communications and NetworkingConference*, pp. 2531-2536, Mar. 2008. Article (CrossRef Link)

[7] S.H. Lee, N.S. Park, J.Y. Choi, "Secure Handover Protocol for Mobile WiMAX Networks," *IEICE Transations on Information and Systems*, vol. E91-D, no.12, , pp. 2875-2879, Dec. 2008. Article (CrossRef Link)

[8] A.M. Taha, A.T. Abdel-Hamid, S. Tahar, "Formal Analysis of the Handover Schemes in Mobile WiMAX Networks," in *Proc. of IFIP International Conference on Wireless and Optical Communications Networks*, pp. 28-30, Apr. 2009. Article (CrossRef Link)

[9] T. Shon, B. Koo, J.H. Park, H. Chang, "Novel Approaches to Enhance Mobile WiMAX Security," *EURASIP Journal on Wireless Communications and Networking*, vol. 2010, Article ID 926275, 2010. Article (CrossRef Link)

[10] D. Johnston, J. Walker, "Overview of IEEE 802.16 Security," *IEEE Security and Privacy*, vo l.3, no.2, pp. 40–8, 2004. Article (CrossRef Link)

[11] E. Eren, K.-O. Detken, "WiMAX Security – Assessment of the Security Mechanisms in IEE E802.16d/e," in *Proc. of the 12th World Multi-Conference on Systemics, Cybernetics and Inf ormatics*, Orlando, Florida, USA, 2008.

[12] S. Xu, C.-T. Huang, "Attacks on PKM Protocols of IEEE 802.16 and Its Later Versions," in *P roc. of the 3rd International Symposium on Wireless Communication Systems*, Valencia, Spai n, 2008. Article (CrossRef Link)

[13] S. Xu, M. Matthews, C.-T. Huang, "Security Issues in Privacy and Key Management Protoc ols of IEEE 802.16," in *Proc. of the 44th annual Southeast regional conference*, Melbourne, F lorida, 2006. Article (CrossRef Link)

[14] E. Eren, "WiMAX Security Architecture – Analysis and Assessment," in *Proc. of the 4th IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*, Dortmund, Germany, 2007. Article (CrossRef Link)

[15] A. Deininger, S. Kiyomoto, J. Kurihara, T. Tanaka, "Security Vulnerabilities and Solutions in

Mobile WiMAX," *International Journal of Computer Science and Network Security*, vol. 7, no. 11, pp. 88-97, 2007.

Chang-Seop Park has been with the School of Electrical Engineering and Computer Science at Dankook University, Republic of Korea, since 1990. He has a Ph.D. and a M.Sc. from Lehigh University (1990 and 1987), as well as a B.A. from Yonsei University (1983). He has been working on the wireless mobile network security during the last 5 years. His research interests include network security, cryptographic protocols, and coding theory.

Hyun-Sun Kang has a Ph.D. and a M.Sc. from Dankook University, Republic of Korea (2007 and 2004). From 2007 to 2009, she worked as a lecturer of Dept. of General Education at Dankook University. She has been with the School of General Education at Namseoul University, Republic of Korea, since 2010. Her research interests include network security and cryptographic protocols.