Hindawi Publishing Corporation
EURASIP Journal on Wireless Communications and Networking
Volume 2010, Article ID 926275, 11 pages
doi:10.1155/2010/926275

Research Article

Novel Approaches to Enhance Mobile WiMAX Security

Taeshik Shon,[1] Bonhyun Koo,[1] Jong Hyuk Park,[2] and Hangbae Chang[3]

[1] *Convergence S/W Laboratory, DMC R&D Center, Samsung Electronics, Dong Suwon P.O. Box 105, Maetan-3dong, Suwon-si, Gyeonggi-do, 442-600, Republic of Korea*
[2] *Department of Computer Science and Engineering, Seoul National University of Technology, 172, Gongreung 2-dong, Nowon, Seoul 139-743, Republic of Korea*
[3] *Department of Business Administration, Daejin University, San 11-1, Sundan-Dong, Pocheon-Si, Gyunggi-Do 487-711, Republic of Korea*

Correspondence should be addressed to Hangbae Chang, hbchang@daejin.ac.kr

Received 26 February 2010; Accepted 5 July 2010

Academic Editor: Liang Zhou

The IEEE 802.16 Working Group on Broadband Wireless Access Standards released IEEE 802.16-2004 which is a standardized technology for supporting broadband and wireless communication with fixed and nomadic access. After the IEEE 802.16-2004 standard, a new advanced and revised standard was released as the IEEE 802.16e-2005 amendment which is foundation of Mobile WiMAX network supporting handover and roaming capabilities. In the area of security aspects, compared to IEEE 802.16-2004, IEEE 802.16e, called Mobile WiMAX, adopts improved security architecture—PKMv2 which includes EAP authentication, AES-based authenticated encryption, and CMAC or HMAC message protection. However, there is no guarantee that PKMv2-based Mobile WiMAX network will not have security flaws. In this paper, we investigate the current Mobile WiMAX security architecture focusing mainly on pointing out new security vulnerabilities such as a disclosure of security context in network entry, a lack of secure communication in network domain, and a necessity of efficient handover supporting mutual authentication. Based on the investigation results, we propose a novel Mobile WiMAX security architecture, called RObust and Secure MobilE WiMAX (ROSMEX), to prevent the new security vulnerabilities.

1. Introduction

More and more, our life is closely related to a variety of networking environments for using Internet-based services and applications. The ever-changing trends of our lifestyle require faster speed, lower cost, more broadband capacity, as well as nomadic and mobility support. Due to these reasons and demands, IEEE 802.16 working group has created new standards with mobility access called the IEEE 802.16e-2005 amendment. It has also been developed by many working groups of the Worldwide Interoperability for Microwave Access (WiMAX) Forum, similar to Wi-Fi in IEEE 802.11 standards. The WiMAX Forum tries to coordinate the interoperability and compatibility of various company products as a field standard. Specifically, Mobile WiMAX technology is considered as one of the best next-generation wireless technologies because it can support high-speed, broadband data transmission, fully-supported mobility, and wide coverage and high capacity [1–4].

From a security viewpoint, the Mobile WiMAX system based on the IEEE 802.16e-2005 amendment has more enhanced security features than the existing IEEE 802.16-based WiMAX network system. The improved core part of the security architecture in Mobile WiMAX, called PKM v2, is operated as a security sublayer in a MAC layer like PKMv1 in IEEE 802.16-2004. The PKMv2 provides a message authentication scheme using HMAC or CMAC, device/user authentication using EAP methods, and confidentiality using AES-CCM encryption algorithm [5, 6]. Even though Mobile WiMAX uses more enhanced security schemes supported by PKMv2, it can not guarantee the reliability of the whole Mobile WiMAX systems and network architectures. In addition, open architecture and various applications of Mobile WiMAX could cause much more risks to try to compromise Mobile WiMAX network than existing systems. In Mobile WiMAX, the network domain consists of a link domain between Subscriber Station (SS) and the Base Station (BS), access network domain, and mobility domain. Each network domain has a possibility of potential risks. In case of a link domain, the Mobile WiMAX does not support any security features to authenticate peers and encrypt initial entry control and user data. In access network domain of Mobile WiMAX, it only provides a regular guideline for protecting inter-network data based on IP security, even it is not a scope of IEEE 802.16e. In addition, a handover which is one of the most distinguished features in Mobile WiMAX is left alone without security functionalities. Specifically, the problem is very critical when the handover is supporting fast handover optimization option. Therefore this paper focuses on three kinds of security vulnerabilities and their countermeasure according to each Mobile WiMAX network domain. Finally, we present security architecture of Mobile WiMAX network as called Robust and Secure MobilE WiMAX (ROSMEX).

The rest of this paper is organized as follows. In Section 2, we study an overview of Mobile WiMAX security and analyze known security vulnerabilities and attacks. In Section 3, new security threats and the related works in Mobile WiMAX network are examined. In Section 4, we propose possible solutions in order to cope with the new threats we mention in Section 3. In Section 5, the comparison and analysis of the proposed approaches with the current approaches are presented. In Section 6, we discussed a reliable Mobile WiMAX architecture including our proposed solutions. In the last section, we conclude with a summary and discussion of future work.

2. Background

The first stage of IEEE 802.16 standard was released in 2004; many researchers have tried to analyze the new standard's vulnerabilities and deal with possible attacks. In this section, we describe an overview of security features in Mobile WiMAX. Moreover, this paper analyzes the known existing security vulnerabilities and attacks [7–10].

2.1. Overview of Mobile WiMAX Security. IEEE 802.16e-2005 amendment-based Mobile WiMAX supports many good security features as compared to the fixed IEEE 802.16-based WiMAX security schemes. Basically, the Privacy Key Management sublayer in the MAC layer of IEEE 802.16-2005 is a core part which comprises the WiMAX security. The PKM sublayer provides not only key related management functions but also strong protection for encrypting traffic and EAP-based flexible authentication for accessing valid users and devices. In the Mobile WiMAX system, more enhanced PKMv2 is supported, together with various cryptographic suites. In the research of [3, 4] from WiMAX Forum, the security features of the PKMv2-based Mobile WiMAX consist of Key Management Protocol, Device and User Authentication, Traffic Encryption/Decryption, Control Message Authentication, Hard Handover, and IP Mobility Support. PKMv2-based key management protocol manages and maintains various keys for EAP authentication, message authentication, traffic encryption, handover (Authentication Key transfer), and multicast/broadcast security.

2.2. Known Vulnerabilities and Attacks. The security architecture of Mobile WiMAX is partially originated from wireless networks based on IEEE 802.11. In the case of IEEE 802.11-based wireless networks, a great deal of security-related research has already been studied, and a few vulnerabilities have been known as those in [7, 8]. Among many interesting researches, John Bellardo and Stefan Savage's research [7] showed a possibility of Denial of Service attacks using identity vulnerability and Media Access Control vulnerability in MAC layer of IEEE 802.11 at the USENIX conference. In this section, we investigate well-known vulnerabilities based on the IEEE 802.16 network architecture from the existing researches [9, 10].

In the case of an attack using Auth Invalid vulnerability, Auth Invalid event is internally generated by the SS when there is a failure authenticating a Key Reply or Key Reject message, or externally generated by the receipt of an Auth Invalid message sent from BS to SS. If SS sends Key Request message with unauthenticated MAC code, BS responds to Key Request with Auth Invalid. Thus, when SS receives the Auth Invalid message, SS will transit from Authorized state to Reauth Wait state, and SS will wait there until SS gets something new from BS. If the Reauth Wait time is expired before SS receives something from BS, SS sends a Reauth Request in order to get into the network again. Also while SS is in Reauth state, SS may receive an Auth Reject message. This is a "Permanent Authorization Failure." When SS receives such a message he is pushed into silent state, ceases all subscriber traffic, and will be ready to respond to any management message sent by BS. This way the attacker is able to manipulate the Authorization State Machine. Moreover, the Auth Invalid message is not safe and is easy to modify because HMAC- or CMAC- based message authentication is not provided and PKM identifier is not included. Auth Invalid contains only the error code identifying the reason and the display string describing the failure condition. Even better for attackers, this message's error code provides stateless Auth Invalid with unsolicited property.

Finally, in a security vulnerability known as a Rogue BS attack, SS can be compromised by a forged BS. At this time, SS maybe believe he is connected to the real BS. Thus, the forged BS can intercept SS's whole information. In other words, the rogue BS attack is a kind of Man-In-The-Middle attack which is one of the well-known attacks in wireless networks. In IEEE 802.16 using PKMv1, Auth Request message includes only the contents for SS authentication itself without correspondent BS's authentication. When SS tries to establish a connection to BS, there is no way to confirm whether the BS is authorized or not. The authorization process based on RSA authentication protocol allows only BS to authenticate SS in PKMv1. Thus, it is possible to masquerade as a Rogue BS after sniffing Auth-related message from SS. However, in the case of Mobile WiMAX using PKMv2, it is difficult to use the Rogue BS vulnerability because mutual authentication function between SS and BS is mandatory during authorization process. In authorization state, the mutual authentication has two modes. In one mode, RSA-based mutual authentication is used for only mutual authentication. In the other mode, mutual authentication is followed by EAP authentication during initial entry process.

2.3. Related Works. Recently there are a lot of Mobile WiMAX researches and related to its security. In [11], the authors focused on the EAP-based security approach when a Mobile WiMAX user wants to get a handover service. The possible solutions for secure handover in IEEE 802.16e networks are proposed, and the handover protocol guarantees a backward/forward secrecy while giving little burden over the previous researched handover protocols. However, the proposed approaches are not considered the overhead of EAP authentication procedure according to frequent handover. If the frequent handover is occurred, the preauthentication mechanism-based PKMv2 is closely coupled to system performance. In [12–14], the research reviewed the study of WiMAX and converged network and security considerations for both the technologies. They presented many security issues and vulnerability in Mobile WiMAX and then proposed possible solutions. In addition, the papers discuss all the security issues in both point-to-multipoint and mesh networks and their solutions. Some performance-related researches are studied. In [15], the authors analyzed the performance effect when RSA and ECC algorithms are used in WiMAX. However, the research is only evaluating the result, not proposing new approach using ECC-based cryptographic approach. Moreover, the initial network procedure in Mobile WiMAX is not effectively secured that makes man-in-the-middle attack possible. In [16], Diffie-Hellman (DB) key exchange protocol enhance the security level during network initialization. The modified DH key exchange protocol is fit into mobile WiMAX network to eliminate existing weakness in original DH key exchange protocol. But, it can cause additional overhead to distribute initial DH random number, and it can not present the concrete modified DH scheme.

3. New Security Threat

3.1. Initial Network Entry Vulnerabilities. According to IEEE 802.16e-2005 standard, the Mobile WiMAX network performs initial Ranging process, SS Basic Capability (SBC) negotiation process, PKM authentication process, and registration process during initial network entry as illustrated in Figure 1. Initial network entry is one of the most significant processes in Mobile WiMAX network because the initial network entry process is the first gate to establish a connection to Mobile WiMAX. Thus, many physical parameters, performance factors, and security contexts between SS and BS are determined during the process. However, specifically, the SBC negotiation parameters and PKM security contexts do not have any security measures to keep their confidentiality. So, the possibility of exposure to malicious users or outer network always exists in initial network entry process. Even though Mobile WiMAX has a message authentication scheme using HMAC/CMAC codes and traffic encryption scheme using AES-CCM based on PKMv2, the security schemes are only applied to normal data traffic after initial network entry process not to control messages during initial network entry. Therefore, it is necessary to prepare a solution to protect important messages such as security negotiation parameters in SBC messages and security contexts in PKM messages during initial network entry.

3.2. Access Network Vulnerabilities. The WiMAX Forum defined Network Reference Model (NRM) which can accommodate the requirements of WiMAX End-to-End Network Systems Architecture [4] for Mobile WiMAX network. The NRM is a logical representation of Mobile WiMAX architecture consisting of the following entities: SS, Access Service Network (ASN), and Connectivity Service Network (CSN). SS means one of the mobile devices that would like to join Mobile WiMAX network. ASN is a complete set of network functions needed to provide radio access to Mobile WiMAX subscribers. ASN consists of at least one BS and one ASN Gateway (ASN/GW). Also, CSN is a set of network functions that provide IP connectivity services to the WiMAX subscribers. CSN consists of AAA Proxy/Server, Policy, Billing, and Roaming Entities. Basically, Mobile WiMAX architecture originated from the IEEE 802.16 standards. At the view point of NRM, IEEE 802.16 standards only define a set of functions between SS and BS. It means that the security architecture given by IEEE 802.16 standards does not cover intra-ASN and ASN-to-CSN. In Figure 2, we are able to distinguish a secure domain covered by IEEE 802.16 standard and insecure domains required additional security services. In the case of communication range between SS and BS, the exchange of messages during network entry process (by the end of registration process) is belonging to insecure domain A. The security threat of insecure domain A is already mentioned in Section 3.1, and a possible solution will be described in Section 4. On the other hand, the communication range after network entry (at the beginning of normal data traffic) belongs to the secure domain because it can be protected by TEK encryption scheme and message authentication function using HMAC/CMAC. Thus, there remain two insecure domains: insecure domain B between BS and ASN/GW and insecure domain C between ASN and CSN. The reason we called the areas insecure domains is because Network Working Group in WiMAX Forum just assumes that the insecure domain B as illustrated in Figure 2 is a trusted network without suggesting any security function [4]. Moreover, in the case of insecure domain C, the research of [4] only mention a possibility of applying an IPSec tunnel between ASN and AAA (in CSN) [4]. Therefore, in order to make a more robust Mobile WiMAX network, more concrete and efficient countermeasures are needed.

3.3. Handover Vulnerabilities. Mobile WiMAX supports a variety of handover methods for mobile access. There are three handover methods supported within the IEEE 802.16e-2005 amendment: Hard Handover (HHO), Fast Base Station

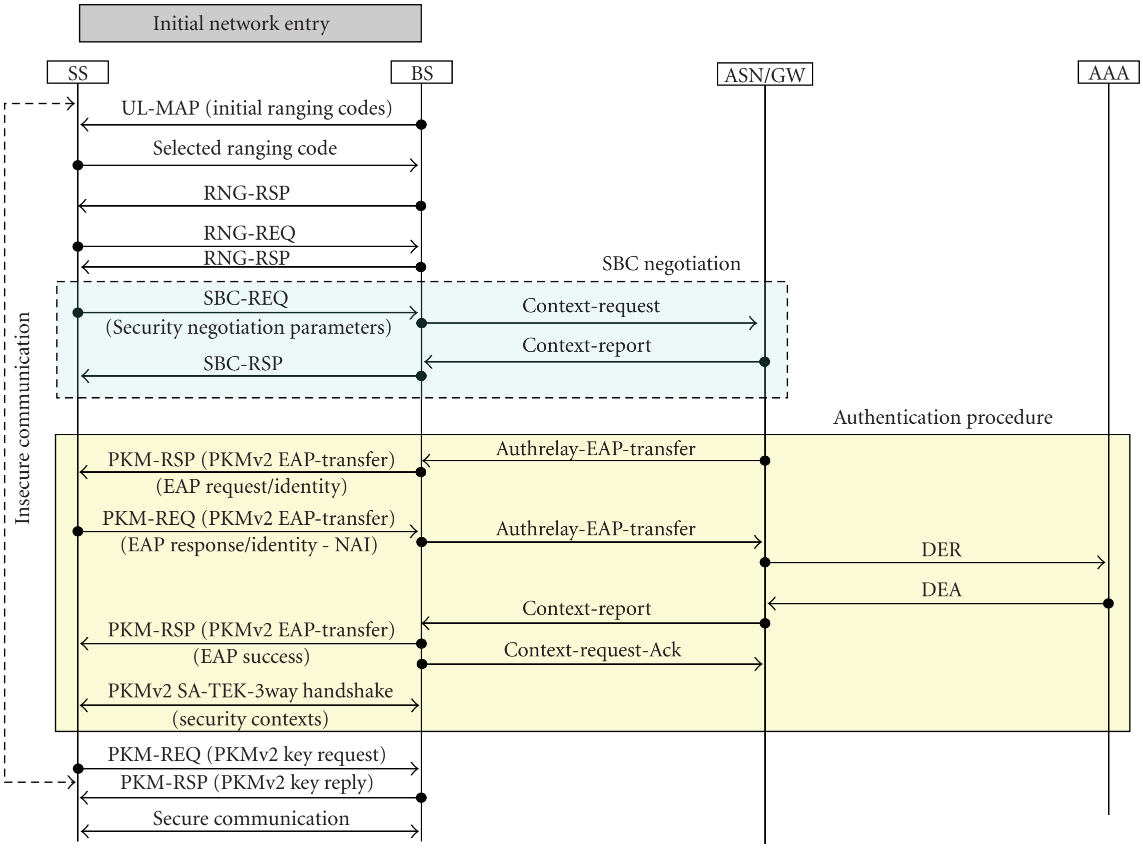

Figure 1: Overview of initial network entry procedure.

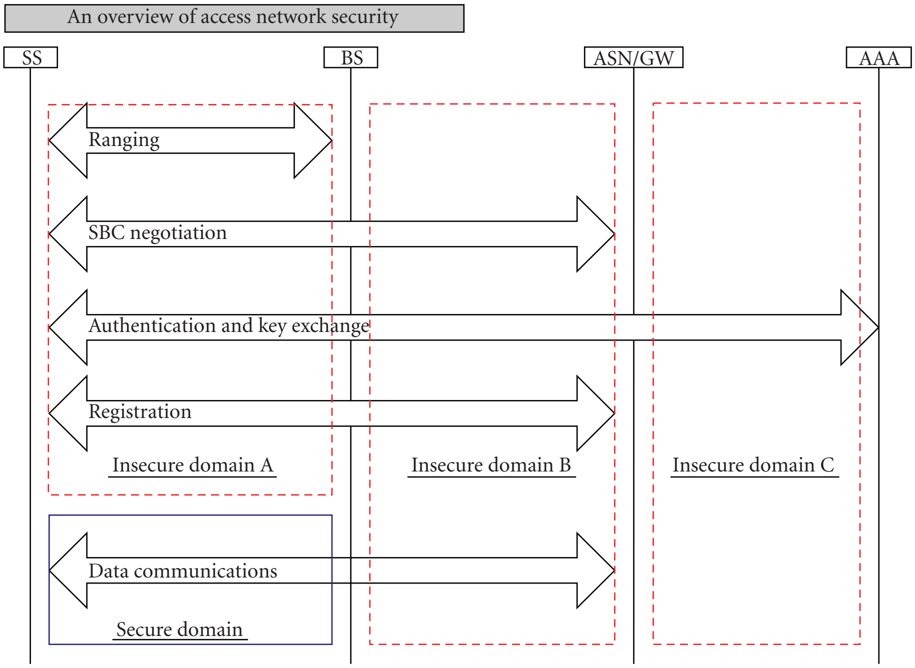

Figure 2: Overview of access network security.

Switching, and Macro Diversity Handover. Of these, the HHO is the only mandatory one in Mobile WiMAX. Especially, HO process optimization flags are supported for providing seamless mobility service. The HO optimization flag consists of eight kinds of optimization options and are used as an aim to shorten a network re-entry process when occurring handover. Among the HO optimization flags, PKM authentication phase (HO optimization flag #1) and PKM TEK creation phase (HO optimization flag #2) are related to Mobile WiMAX security as illustrated in Figure 3. If these two flags are used, PKM authentication phase and TEK creation phase do not occur during the re-entry process in handover. Therefore, even though HO optimization flag #1 and #2 are necessary to fast handover to decrease HO latency for real-time services, these flags can give a chance to cause critical security holes to malicious users like a lack of valid entity authentication and man-in-the-middle attack. Supporting security-related HO optimization, flags are tradeoff between handover performance and secure communication. Thus, a possible alternative is required which can cope with the security vulnerability and does not interrupt seamless mobility service during handover.

4. Proposed Countermeasures

4.1. Approach to Initial Network Entry Vulnerabilities. Although much significant information is exchanged during initial network entry, there are not appropriate methods to protect critical information in the entry process. In order to eliminate the security vulnerability during initial network entry, this paper applies Diffie-Hellman (DH) key agreement scheme [17] to initial ranging procedure. Basically, DH key agreement is to share an encryption key with global variables known as prime numbers "p" and "g" a primitive root of p. However, the original DH scheme has a threat of Man-in-the-Middle attack. Thus, in this paper, we suggest a kind of modified DH scheme using hash authentication. In a ranging process, one of the ranging codes is used as a prime number seed, and then hash authentication is applied to the exchanging process for protecting Man-in-the-Middle attack.

In Figure 4, initial ranging procedure is started when SS receives UL-MAP message including ranging codes. Among the received ranging codes, SS selects one of the ranging codes ($\mathrm{RC_i}$) in SS's step 1. If $\mathrm{RC_i}$ consists of $\mathrm{A_1}$ and $\mathrm{A_2}$, SS sends only a part of $\mathrm{RC_i}$ (A1 or A2) and Hash value of $\mathrm{RC_i}$ to BS in order to protect Man-in-the-Middle attack. In BS's step 1, BS receives a part of $\mathrm{RC_i}$(A1) and the hashed value $\mathrm{H(RC_i)}$. BS finds A2 from ranging code pool using A1, and then BS authenticates SS through verifying the received hash value. Thus, the selected ranging code is not only Mobile WiMAX communication but also used for generating a prime number "p" as one of global variables in DH process. In SS's step 2, 3, and 4, SS generates the other global variable "g" and public/private key pair and then sends them to BS. BS receives a public key of SS and global variables (prime number and its primitive root). If the received key and variables are verified, BS also sends his public key to SS in BS's step 3. Thus, BS and SS can share DH global variables and public key with each other through initial ranging process. Of these, they can generate a shared common key called "pre-TEK" separately and establish secret communication channels in step 4 and 5 separately. Therefore, the proposed approach can protect SBC security parameters and PKM security contexts using the shared traffic encryption key (pre-TEK) during initial network entry procedure.

4.2. Approach to Access Network Vulnerabilities. As we already mentioned, PKM which is the main security architecture in Mobile WiMAX only covers wireless traffic between SS and BS because other communication ranges required security functions that are beyond IEEE 802.16e-2005 standard. Moreover, technical documents of Network Working Group (NWG) in WiMAX Forum assume that ASN network is trusted and AAA connections between ASN and CSN may be protected with IPSec tunnel. However, there are a lot of possibilities new security holes to happen including various zero-day attacks. Moreover, IPSec requires additional s/w and h/w facilities for supporting whole Mobile WiMAX domains. Thus in this paper, we present a simple and efficient key exchange method using a device-certificate. Basically, network devices in Mobile WiMAX have a device certificate, so they can be applied to make more robust access to network domain based on PKI structure. In order to applying device certificate based approach to access network domain, we assume that Mobile WiMAX devices are certified from public authority and they can verify certificates of each other using certificate chain. In Figure 5, all devices in Mobile WiMAX have their own certificate and a certificate chain for verification. If BS would like to exchange important messages with ASN/GW, BS needs to generate a session encryption key for secure communication between BS and ASN/GW. In this case, BS first searches for an appropriate certificate (including correspondent's public key) to verify ASN/GW's identity and obtain public key. After getting public key, BS generates "asn-TEK" as a session encryption key for secure communication with ASN/GW. Using the "asn-TEK," BS encrypts a message and sends the encrypted message together with the encrypted "asn-TEK" key using ASN/GW's public key, Timestamp, and Authority's certificate to ASN/GW. When ASN/GW receives the messages from BS, ASN/GW first tries to verify the authority's certificate and checks the validation time from Timestamp. If the verification process is successful, ASN/GW decrypts the "asn-TEK" key and the original message. Thus, a problem of insecure communication between BS and ASN/GW can be solved by using "asn-TEK" key as a encryption key between BS and ASN/GW. In the case of ASN-to-CSN, the proposed method generates a common encryption key called "asn-csn-TEK" using the same method as a way for BS-to-ASN/GW to establish secure connection. In Figure 5, we can show an example using "asn-csn-TEK".

4.3. Approach to Handover Vulnerabilities. In Mobile WiMAX, a handover process adopts a kind of fast handover method based on Handover (HO) process optimization flags to provide seamless communication by reducing the number of message exchange. However, such a handover process still

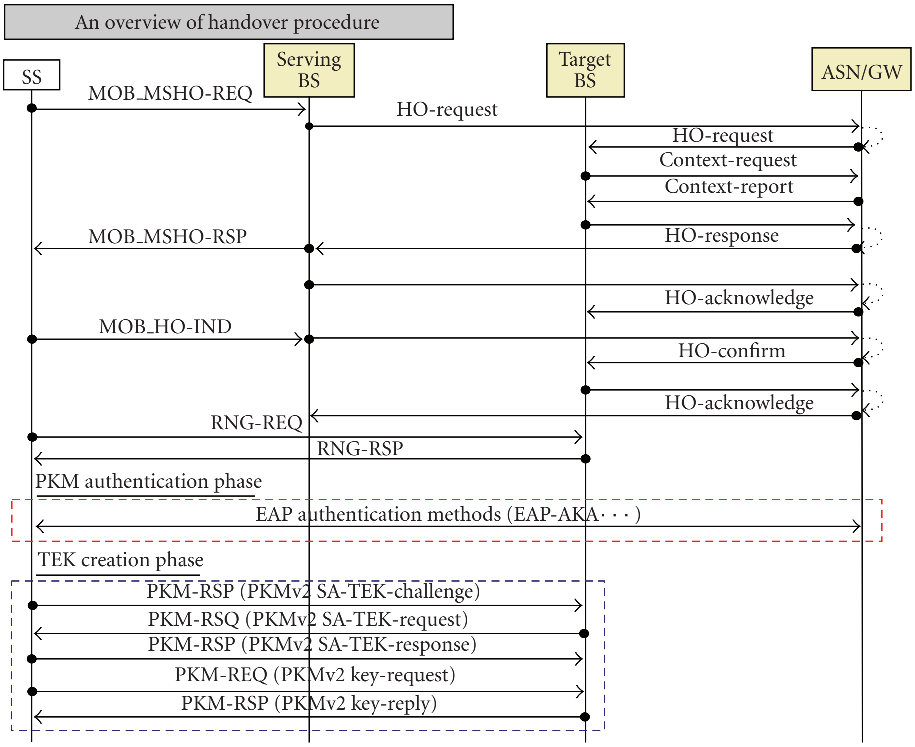
An overview of handover procedure
SS
Serving BS
Target BS
ASN/GW
MOB_MSHO-REQ
HO-request
HO-request
Context-request
Context-report
MOB_MSHO-RSP
HO-response
HO-acknowledge
MOB_HO-IND
HO-confirm
HO-acknowledge
RNG-REQ
RNG-RSP
PKM authentication phase
EAP authentication methods (EAP-AKA· · ·)
TEK creation phase
PKM-RSP (PKMv2 SA-TEK-challenge)
PKM-RSQ (PKMv2 SA-TEK-request)
PKM-RSP (PKMv2 SA-TEK-response)
PKM-REQ (PKMv2 key-request)
PKM-RSP (PKMv2 key-reply)

Figure 3: Overview of handover procedure.

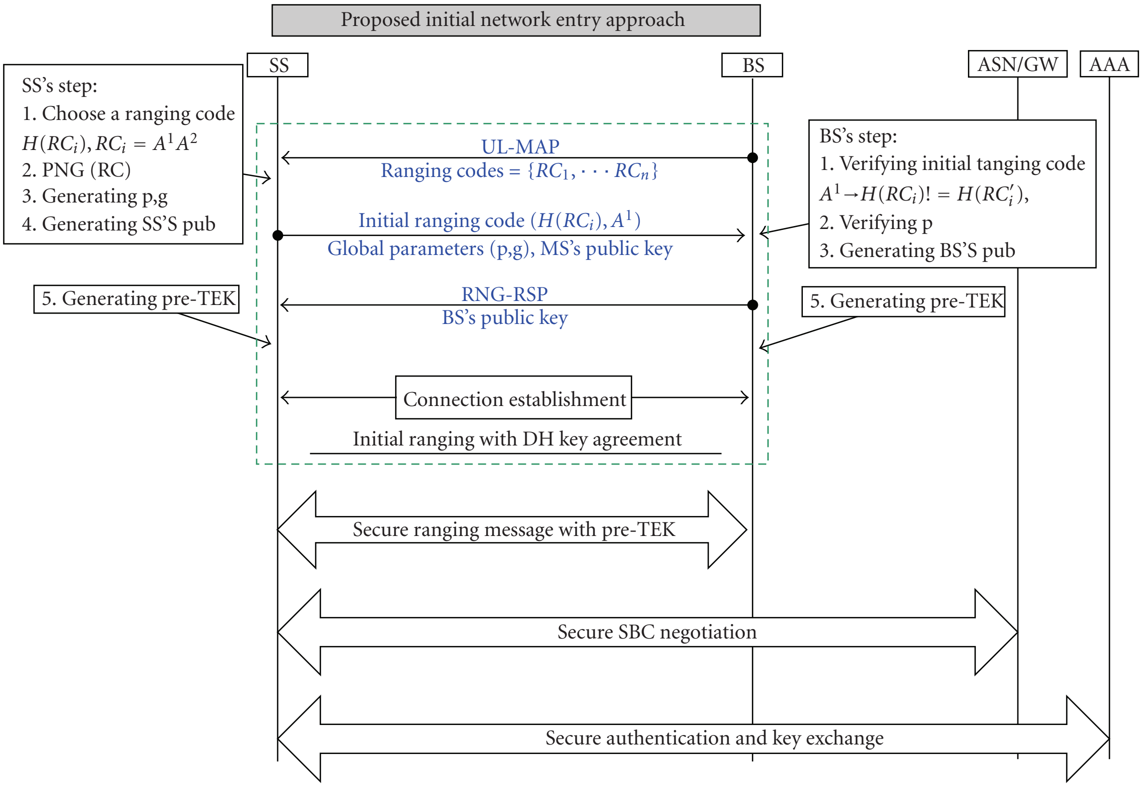
Proposed initial network entry approach
SS
BS
ASN/GW
AAA
SS's step:
1. Choose a ranging code
$H(RC_i), RC_i = A^1A^2$
2. PNG (RC)
3. Generating p,g
4. Generating SS'S pub
UL-MAP
Ranging codes = $\{RC_1, \cdots RC_n\}$
BS's step:
1. Verifying initial tanging code
$A^1 \rightarrow H(RC_i)! = H(RC_i')$,
2. Verifying p
3. Generating BS'S pub
Initial ranging code $(H(RC_i), A^1)$
Global parameters (p,g), MS's public key
5. Generating pre-TEK
RNG-RSP
BS's public key
5. Generating pre-TEK
Connection establishment
Initial ranging with DH key agreement
Secure ranging message with pre-TEK
Secure SBC negotiation
Secure authentication and key exchange

Figure 4: Proposed network initial entry approach.

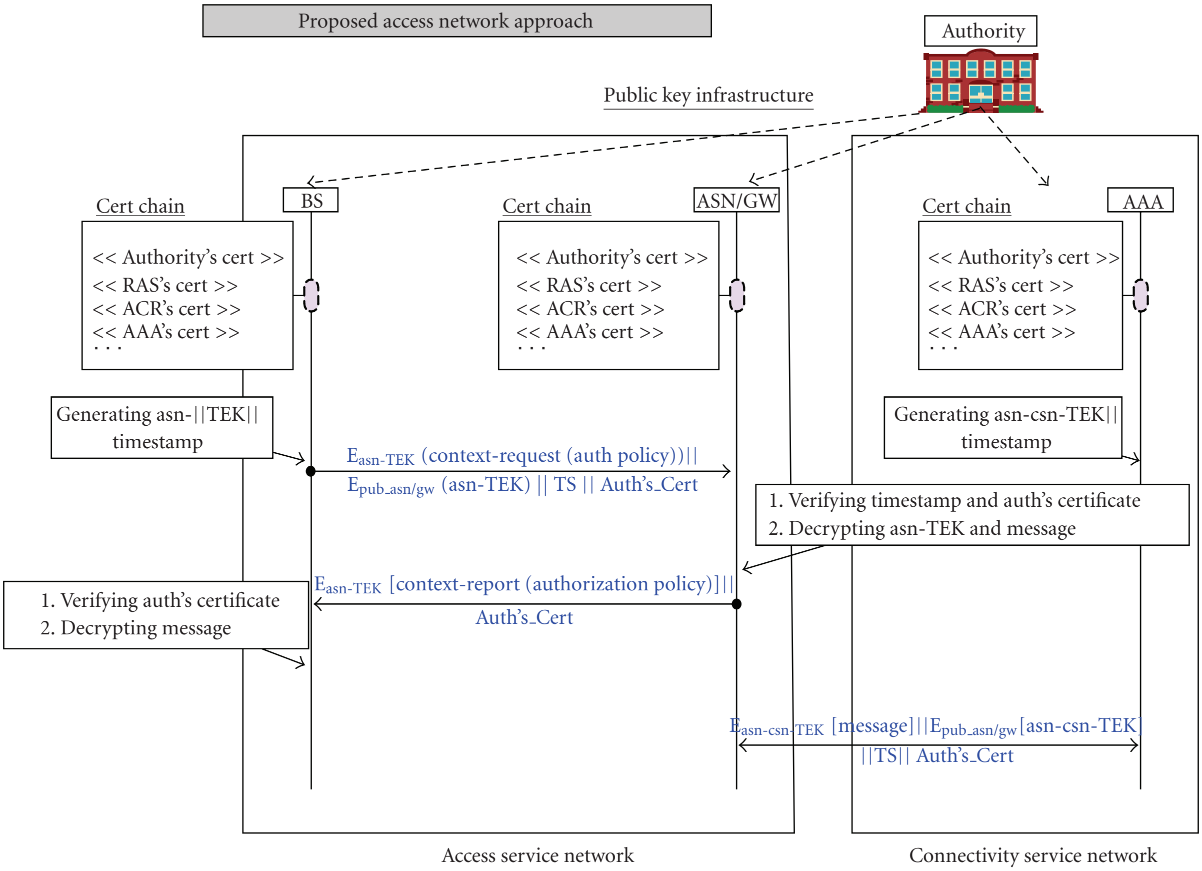
Proposed access network approach
Authority
Public key infrastructure
Cert chain
BS
<< Authority's cert >>
<< RAS's cert >>
<< ACR's cert >>
<< AAA's cert >>
. . .
Cert chain
ASN/GW
<< Authority's cert >>
<< RAS's cert >>
<< ACR's cert >>
<< AAA's cert >>
. . .
Cert chain
AAA
<< Authority's cert >>
<< RAS's cert >>
<< ACR's cert >>
<< AAA's cert >>
. . .
Generating asn-||TEK|| timestamp
Generating asn-csn-TEK|| timestamp
$E_{\text{asn-TEK}}$ (context-request (auth policy))||
$E_{\text{pub\_asn/gw}}$ (asn-TEK) || TS || Auth's_Cert
1. Verifying timestamp and auth's certificate
2. Decrypting asn-TEK and message
$E_{\text{asn-TEK}}$ [context-report (authorization policy)]||
Auth's_Cert
1. Verifying auth's certificate
2. Decrypting message
$E_{\text{asn-csn-TEK}}$ [message]||$E_{\text{pub\_asn/gw}}$[asn-csn-TEK]
||TS|| Auth's_Cert
Access service network
Connectivity service network

Figure 5: Proposed access network approach.

has a problem as we already mentioned in Section 3.3—handover vulnerability. In this section, new handover approach with embedded mutual authentication parameters is proposed. The proposed HO approach includes a few additional fields for the embedded parameters of providing mutual authentication such as Nonce, Certificate (Cert), Authorization Key (AK), and Acknowledge (Ack). First, the challenge-response scheme with Nonce, Cert, and AK is used to provide Target BS (TBS) authentication. Moreover, HMAC/CMAC tuple is used for SS authentication as well as message authentication. Thus, the proposed approach can take an effect on mutual authentication using the embedded parameters even though HO optimization process is used.

From message 1 to message 3 in Figure 6, TBS authentication is first processed during HO-Request process. When HO process is started, Serving BS (SBS) sends HO-Request message with Nonce to TBS. TBS replies HO-Response with an encrypted Nonce and Cert to SBS. If SBS verifies the included Nonce and Cert in HO-Response message, SBS sends HO-confirm message with Ack to TBS, and then TBS authentication is finished. In the case of MS authentication, CMAC/HMAC tuples are applied to authenticate MS as illustrated message 4 and 5 in Figure 6. After HO process, MS tries the Ranging process and TBS can authenticate MS using MAC code verification because RNG-REQ message includes CMAC/HMAC tuple generated by AK.

Therefore, our proposed method takes an effect on getting confidentiality by including a few information fields in the existing HO message in spite of using additional HO optimization flags. This approach enhances security and performance factors during handover without full authentication process based on PKMv2.

5. Comparison of the Proposed Approaches

5.1. Mobile WiMAX-Based DH Approach in Initial Entry Procedure. In order to protect a vulnerability of initial network entry, modified DH approach was proposed in this paper. The proposed approach provides both confidentiality and countermeasure against Man-in-the-Middle attack in comparison with IEEE 802.16e and original DH scheme. Moreover, there are not communications overhead because the parameters of the proposed approach are embedded in the existing initial ranging message exchange. However, the modified DH approach performs a couple of cryptographic operations. Even though the processing delay is very small and the original DH-based scheme is one of the best known schemes for communication system security, more optimized cryptographic operations for Mobile WiMAX entry process are considered in the near future. Table 1 shows that the proposed approach provides confidentiality and countermeasure against man-in-the-middle-attack.

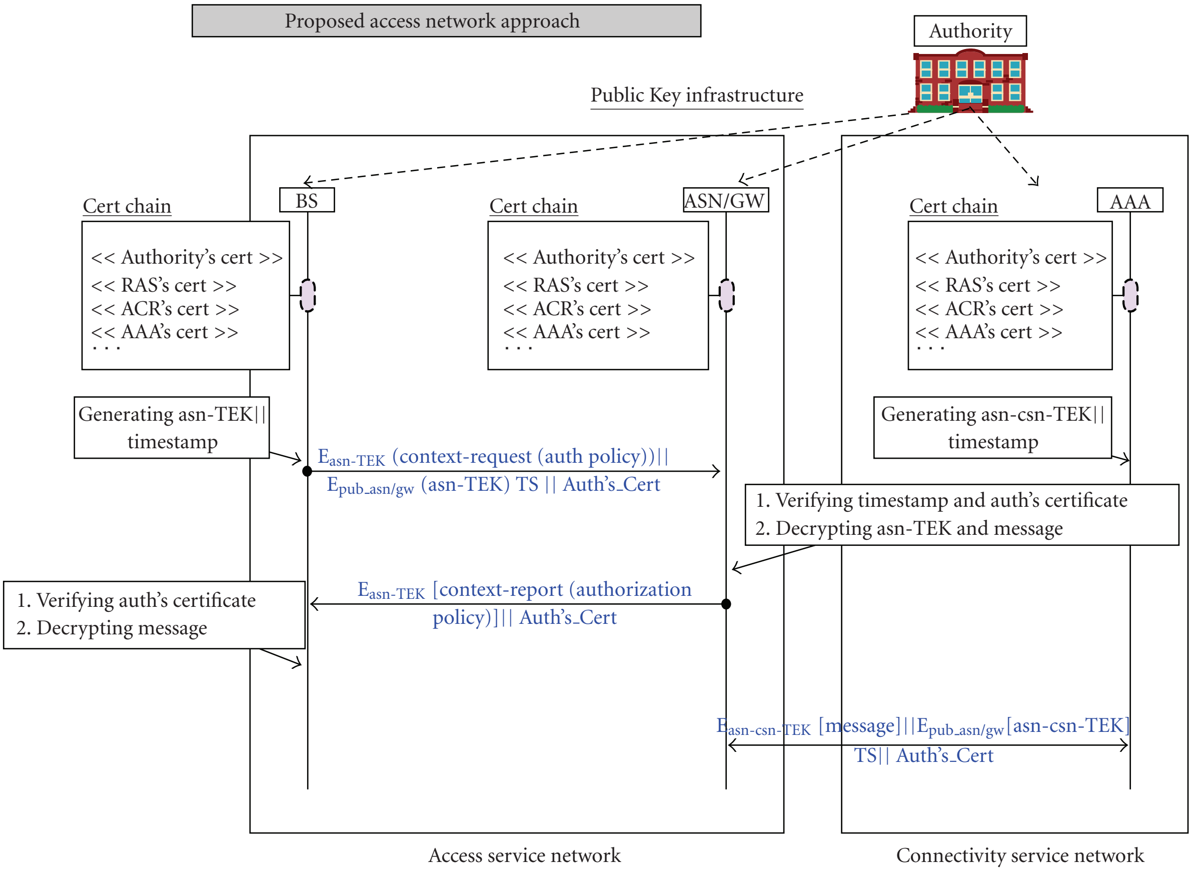
Proposed access network approach
Authority
Public Key infrastructure
Cert chain
BS
<< Authority's cert >>
<< RAS's cert >>
<< ACR's cert >>
<< AAA's cert >>
. . .
Cert chain
ASN/GW
<< Authority's cert >>
<< RAS's cert >>
<< ACR's cert >>
<< AAA's cert >>
. . .
Cert chain
AAA
<< Authority's cert >>
<< RAS's cert >>
<< ACR's cert >>
<< AAA's cert >>
. . .
Generating asn-TEK|| timestamp
Generating asn-csn-TEK|| timestamp
$E_{asn\text{-}TEK}$ (context-request (auth policy))|| $E_{pub\_asn/gw}$ (asn-TEK) TS || Auth's_Cert
1. Verifying timestamp and auth's certificate
2. Decrypting asn-TEK and message
$E_{asn\text{-}TEK}$ [context-report (authorization policy)]|| Auth's_Cert
1. Verifying auth's certificate
2. Decrypting message
$E_{asn\text{-}csn\text{-}TEK}$ [message]||$E_{pub\_asn/gw}$[asn-csn-TEK] TS|| Auth's_Cert
Access service network
Connectivity service network

Figure 6: Proposed handover security approach.

Moreover, in the side of performance consideration, it does not have any communication overhead, but a little bit security overhead. In [16], the authors proposed a similar approach to apply the enhanced DH scheme to Mobile WiMAX network initialization process. Basically the DH approach including ours is better than the existing approach. However, the Rahman's approach is not clear to understand and they can not provide how the random is generated and distributed to others to use DH scheme.

5.2. Mobile WiMAX's Device Certificate-Based Key Exchange in Access Network. In Mobile WiMAX network domain, IPsec has been recommended as one of solutions to provide network security. However, every device in Mobile WiMAX has to be installed and support IPSec functionality in order to use IPSec-based security services. Thus, the proposed approach concentrated on simple and efficient key exchange without any additional features. In Table 2, we can see that IPSec needs two-phase negotiation procedure (6 ~ 9 times message exchange) and a little bit complex security operation such as security association, key exchange, and key generation. On the other hand, the proposed approach provides very intuitive and systematic solution (2 times message exchange) using a device certificate. Although the proposed approach uses certificate-related functions such as signing and verifying, it does not have any side-effect in Mobile WiMAX network because the overhead and delay of certificate-based operations are already verified in the RSA-based authentication scheme in IEEE 802.16e standard. The RSA-based certificate approach is similar to the proposed approach but it requires much processing delay than our ECC-based certificate approach. In case of RSA approach, the processing delay is about 120 ms. On the other hand, in ECC case it is only under 100 ms.

5.3. Mutual Authentication Approach in Handover Procedure. Fast mobility support is one of the most distinguished capabilities in Mobile WiMAX. However, it can not support an authentication function during handover because of using HO optimization. The proposed approach used embedded parameters for mutual authentication during handover process. Thus, at the view of security aspect, the proposed approach can provide mutual authentication in comparison with the default IEEE 802.16e handover scheme. Moreover, in performance analysis, it shows low processing overhead (1 time encryption/decryption for verifying Nonce) and no communication delay because it does not cause any additional authentication-related message exchange. In case of Hur's [11] approach, it is based on EAP-based pre-authentication. However, it can not be a stable solution under frequent handover environment. In Mobile WiMAX, the dynamic mobility is one of the best advantages.

Table 1: Security and performance analysis in network entry security.

		IEEE 802.16e	Applying original DH	Rahman's approach [16]	Proposed approach
Security	Confidentiality	None	O	O	O
	Man-in-the-middle attack	None	None	O	O
Performance	Processing overhead	—	Random number and key generation	Random number and key generation	Random number and key generation and hash processing
	Communication overhead	—	None	Not clear to generate and distribute DH values	None

Table 2: Security and performance analysis in access network.

		IEEE 802.16e	Applying IPSec	Certificate approach with RSA 1024 bit	Proposed approach with ECC 163 bit
Security	Confidentiality	None	O	O	O
Performance	Processing overhead	—	High SA negotiation/IKE/key generation	Medium (Depends on key size) Certification operation/key generation	Low (depends on key size) Certification operation/key generation
	Communication overhead	—	High 2 phase 6 ~ 9 times packet exchange	Low 1 phase 2 times packet exchange	Low 1 phase 2 times packet exchange
	Requiring additional features	—	O	None	None

Table 3: Security and performance analysis in handover security.

		IEEE 802.16e Handover	Hur's [11] Approach	Proposed handover approach
Security	Mutual authentication	None	O	O
Performance	Processing overhead	None	High (depends on EAP protocols)	Low 1 time encryption/decryption
	Communication overhead	None	High (depends on the number of handover)	None

6. Discussion of Secure and Robust Mobile WiMAX with Proposed Approach

This paper proposed novel approaches to minimize security risks in Mobile WiMAX network. We showed a reliable Mobile WiMAX architecture applying the security approaches called RObust Secure MobilE WiMAX (ROSMEX) as illustrated in Figure 7. In ROSMEX, the enhanced network entry process has an initial ranging process with modified DH key agreement. The approach assigns a temporary Security Association (e.g., pre-TEK and predefined cryptographic suites) to prevent a primary management connections between SS and BS. Thus, ROSMEX can give confidential communications to whole wireless communication range because the proposed approach generates temporary traffic encryption key and then uses the key for traffic encryption before SBC negotiation. Moreover, ROSMEX supports secure communications in all access networks. Any two entities in Mobile WiMAX can establish a secure channel using device certificate-based simple and efficient key exchange. The approach eliminates all possibilities of disguising as a valid entity in Mobile WiMAX. In Section 5.2, we already knew that it is a more efficient method than IPSec approach.. Finally, ROSMEX can support secure mobility despite omitting authentication and TEK phases by using HO optimization flags. The improved HO process has embedded mutual authentication parameters in order to provide authentication during handover. The challenge-response scheme embedded in HO messages authenticates TBS, and SS is authenticated by MAC scheme. Specifically, our proposed approaches do not need any additional message passing and do not prevent original control flow

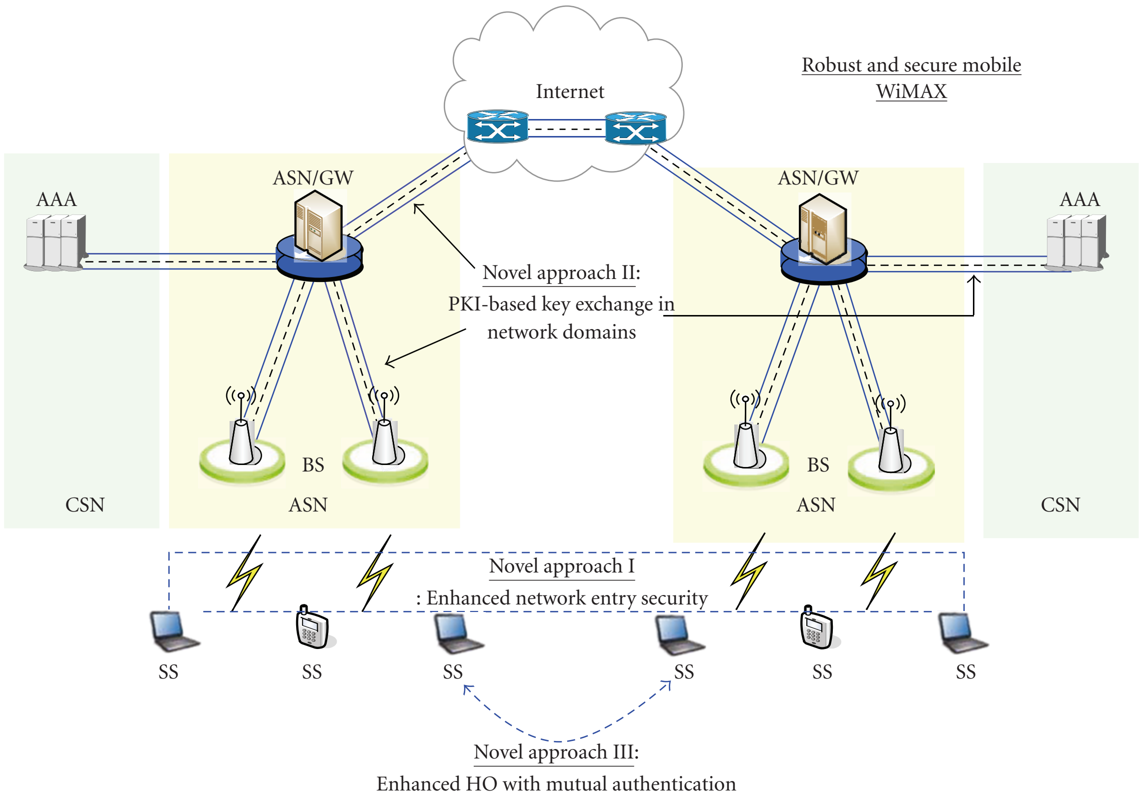
Robust and secure mobile WiMAX
Internet
AAA
ASN/GW
ASN/GW
AAA
Novel approach II:
PKI-based key exchange in network domains
BS
ASN
CSN
BS
ASN
CSN
Novel approach I
: Enhanced network entry security
SS
SS
SS
SS
SS
SS
Novel approach III:
Enhanced HO with mutual authentication

Figure 7: Robust and secure mobile WiMAX network.

of Mobile WiMAX. Therefore, ROSMEX architecture with enhanced security countermeasures can satisfy not only the security requirements but also performance requirements during Initial Network Entry, Access Network Communication, and Handover process.

7. Conclusion

Mobile WiMAX is one of the best candidate systems to accommodate demands for broadband wireless access. It can support worldwide roaming capabilities, superior performance, low latency, supporting all-IP core network, advanced QoS, and security. Moreover, Mobile WiMAX can cooperate with existing and emerging networks. However, Mobile WiMAX technology is not perfect and is not an ultimate solution for beyond 3G networks, but a kind of bridging system toward 4G networks. In the case of security aspects in Mobile WiMAX, it still has a potential possibility of a few security-related vulnerabilities.

In this paper, we investigated new security vulnerabilities such as a disclosure of secret contexts during initial entry procedure, a lack of a protection mechanism in access network communication, and a possibility of rogue SS or BS attacks during HO process (in case of using HO optimization flags). Therefore, in order to eliminate the security vulnerabilities, we proposed three possible countermeasures. In the case of an initial entry process threat, modified DH key agreement is applied to initial ranging process to generate session encryption key. Using the temporal encryption key, the messages including security contexts can be protected during initial entry procedure. Secondly, a simple key exchange scheme based on device certificate was proposed as a solution to settle the vulnerability of the access network. Thus, each network component in ASN and CSN can generate session encryption keys and the correspondents also can verify them. Finally, the handover threat could be reduced using the modified HO procedure approach including a challenge-response scheme and MAC code verification in the existing HO messages.

Based on the proposed approaches, we analyzed and compared our approach called ROSMEX architecture with the existing solutions. We believe that our ROSMEX architecture will contribute to make an enhanced Mobile WiMAX network. In future work, more research for IMT-advanced architecture is needed.

Acknowledgment

This research was supported by the MKE (The Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Center) support program supervised by the NIPA (National IT Industry Promotion Agency) (NIPA-2010-C1090-1031-0004). Moreover, a preliminary version of this paper appeared in NBIS 2007, September 3–7, Regensburg, Germany [18]. The revised paper includes new related work in Section 2.3, the updated security analysis in

Section 5 with the existing approaches and overall parts like abstract, introduction, and conclusion are rewritten, and the main approach was also revised with coherence.

References

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

[2] "IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems, Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum," IEEE Std 802.16e-2005. IEEE, 2005.

[3] WiMAX Forum, "Mobile WiMAX: The Best Personal Broadband Experience," 2006.

[4] WiMAX Forum, "WiMAX End-to-End Network Systems Architecture—Stage 2, 3," 2006.

[5] Airspan, "Mobile WiMAX security," Airspan Networks Inc. 2007, http://www.airspan.com.

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

[7] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: real vulnerabilities and practical solutions," in *Proceedings of the 12th USENIX Security Symposium*, vol. 12, Washington, DC, USA, August 2003.

[8] C. Wullems, K. Tham, J. Smith, and M. Looi, "A trivial denial of service attack on IEEE 802.11 direct sequence spread spectrum wireless LANs," in *Proceedings of the Wireless Telecommunications Symposium (WTS '04)*, pp. 129–136, 2004.

[9] D. Johnston and J. Walker, "Overview of IEEE 802.16 security," *IEEE Security and Privacy*, vol. 2, no. 3, pp. 40–48, 2004.

[10] M. Barbeau, "WiMax/802.16 threat analysis," in *Proceedings of the 1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks (Q2SWinet '05)*, pp. 8–15, 2005.

[11] J. Hur, H. Shim, P. Kim, H. Yoon, and N.-O. Song, "Security considerations for handover schemes in mobile WiMAX networks," in *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC '08)*, pp. 2531–2536, Las Vegas, Nev, USA, March-April 2008.

[12] M. Habib and M. Ahmad, "A review of some security aspects of WiMAX and converged network communication software and networks," in *Proceedings of the 2nd International Conference on Communication Software and Networks (ICCSN '10)*, pp. 372–376, 2010.

[13] P. Rengaraju, C.-H. Lung, Y. Qu, and A. Srinivasan, "Analysis on mobile WiMAX security," in *Proceedings of IEEE Toronto International Conference on Science and Technology for Humanity (TIC-STH '09)*, pp. 439–444, September 2009.

[14] S. S. Hasan and M. A. Qadeer, "Security concerns in WiMAX," in *Proceedings of the 1st South Central Asian Himalayas Regional IEEE/IFIP International Conference on Internet (AH-ICI '09)*, November 2009.

[15] M. Habib, T. Mehmood, F. Ullah, and M. Ibrahim, "Performance of WiMAX security algorithm: the comparative study of RSA encryption algorithm with ECC encryption algorithm," in *Proceedings of the International Conference on Computer Technology and Development (ICCTD '09)*, vol. 2, pp. 108–112, November 2009.

[16] M. S. Rahman and M. Md. S. Kowsar, "WiMAX security analysis and enhancement," in *Proceedings of the 12th International Conference on Computer and Information Technology (ICCIT '09)*, pp. 679–684, December 2009.

[17] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[18] T. Shon and W. Choi, "An analysis of mobile WiMAX security: vulnerabilities and solutions," in *Proceedings of the 1st International Conference on Network-Based Information Systems (NBiS '07)*, vol. 4658 of *Lecture Notes in Computer Science*, pp. 88–97, September 2007.