# Security Issues in Privacy and Key Management Protocols of IEEE 802.16

Sen Xu Manton Matthews Chin-Tser Huang
Department of Computer Science and Engineering
University of South Carolina
Columbia, SC 29208, USA
{xu4, matthews, huangct}@cse.sc.edu

## ABSTRACT

Without physical boundaries, a wireless network faces many more security threats than a wired network does. Therefore, in the IEEE 802.16 standard a security sublayer is specified in the MAC layer to address the privacy issues across the fixed Broadband Wireless Access (BWA). Several articles have been published to address the flaws in IEEE 802.16 security after the IEEE standard 802.16-2001 was released. However, the IEEE standard 802.16-2004 revision does not settle all the discovered problems and additional flaws remain. This paper gives an overview of the IEEE 802.16 standard, focusing on the MAC layer and especially the security sublayer. We analyze the security flaws in the standard as well as in related works, and illustrate possible attacks to the authentication and key management protocols. Possible solutions are also proposed to prevent these attacks. Finally, we propose a security handover protocol that should be supported in the future 802.16e for mobility.

## Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General – *Security and protection*; C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design – *Wireless communication.*

## General Terms

Algorithms, Design, Security, Standardization.

## Keywords

IEEE 802.16, authentication, key management, roaming.

## 1. INTRODUCTION

As a member of IEEE 802 group, IEEE 802.16 is the standard to specify the air interface of fixed Broadband Wireless Access (BWA). IEEE 802.16 was first designed to provide the last mile for Wireless Metropolitan Area Network (WMAN) with line-of-sight (LOS) working at 10-66GHz bands. The latest version, IEEE standard 802.16-2004 [2], which consolidates previous standards, also supports non-line-of-sight (NLOS) within 2-11GHz bands and mesh nodes. The developing IEEE 802.16e aims to provide mobility in BWA.

With the exploding growth on wireless communication in recent years, security issues in wireless networks also become a growing concern. Security requirements for wireless networks are similar to those for wired networks. However, wireless networks are inherently less secure compared to their wired counterparts due to the lack of physical infrastructure. Therefore, special attention should be paid to the security of wireless networks.

Security goals for wireless networks can be summarized as follows. Privacy or confidentiality is fundamental for secure communication, which provides resistance to interception and eavesdropping. Message authentication provides integrity of the message and sender authentication, corresponding to the security attacks of message modification and impersonation. Anti-replay detects and disregards any message that is a replay of a previous message. Non-repudiation is against denial and fabrication. Access control prevents unauthorized access. Availability ensures that the resources or communications are not prevented from access by DoS attack. Detailed discussion of the security requirements, together with corresponding attacks and possible solutions, can be found in [17] and [18].

In a WMAN, both the Base Station (BS) and Subscriber Station (SS) face almost all those attacks mentioned above. The 802.16 standard specifies a security sublayer at the bottom of the MAC layer. This security sublayer provides SS with privacy and protects BS from service hijacking. There are two component protocols in the security sublayer: an encapsulation protocol for encrypting packet data across the fixed BWA, and a Privacy and Key Management Protocol (PKM) providing the secure distribution of keying data from BS to SS as well as enabling BS to enforce conditional access to network services.

The PKM protocol uses X.509 digital certificates, RSA public-key algorithm, and strong encryption algorithm to perform key exchanges between SS and BS, with a client/server model. IEEE 802.16 employs two-tier key systems. The PKM protocol first authenticates SS to BS, establishing a shared secret (Authentication Key, or AK for short) via public-key cryptography, then SS registers to the network, during which AK is used to secure the exchange of Transport Encryption Keys (TEK).

A certificate sent by SS allows BS to authenticate a legitimate SS. On the other hand, SS also needs to authenticate BS to keep away from malicious ones. That is because through the

*ACM SE'06*, March 10-12, 2006, Melbourne, Florida, USA

open air interface, SS has no other way to differentiate legitimate BS from malicious adversaries. Previous works have addressed the necessity of mutual authentication as well as mechanisms to counter attacks on 802.16. However, there are still some flaws in their protocols. This paper analyzes those possible attacks to both BS and SS, and proposes a revised PKM protocol to solve those problems.

WMAN also intends to support mobility in the developing 802.16e standard. Researchers in IEEE 802.16e task group (TGe) have proposed some mechanisms for security roaming of key association for fast handover in the new standard. However, their schemes only support backward secrecy for the target BS (TBS), without forward secrecy for the serving BS (SBS). Moreover, most vulnerabilities in 802.16 protocols are still applicable in 802.16e. In this paper, we propose a security roaming protocol. Our protocol can prevent those attacks. It also supports backward secrecy and forward secrecy to some extent.

This paper is organized as follows. In Section 2, we introduce related works. Section 3 analyzes the Authentication Protocols in 802.16. In Section 4, we focus on the Key Management (Registration) Protocol. Possible attacks are illustrated and solutions are proposed in both Sections 3 and 4. In Section 5, we propose a security roaming protocol for 802.16e. Finally, we conclude our presentation and describe some future work in Section 6.

## 2. RELATED WORKS

Since the first version of IEEE 802.16 [1], a few papers have been published to introduce this new standard and address the security issues. In [15], Roger Marks gives a technical overview of 802.16. There are also some other papers that review this standard, such as [3]. Some books such as [19] and [16] aim to enable operators to deploy and set up a network with standards-based equipment, and run it profitably as well. That is beyond the scope of this paper. Few of these papers and books tackle the security issues. It is clear that so far WMAN has been less investigated than WLAN. With its great potential in the future's wireless service, WMAN deserves more attention than what it gets now.

The authors of [8] review the 802.16 standard, and analyze its security in many aspects, such as vulnerability in authentication and key management protocols, failure in data encryption, and lack of explicit definition. Mutual authentication is the major contribution proposed by [8], which enables SS to authenticate BS as well.

In fact, the need for mutual authentication in wireless network is not a novel topic. It has been widely studied in the scope of WLAN. In [6], the author gives an overview of the 802.11 management operation and brings forward the need for mutual authentication. There are also many other papers dealing with this topic, such as [9] and [4]. In WLAN, WS needs to authenticate AP while AP authenticates WS. However, the authentication and key management protocols in 802.11 and 802.16 are based on different methods. IEEE 802.11 applies the shared-key authentication method, while IEEE 802.16 is based on public-key authentication algorithm, specifically, X.509 certificate. Therefore, the authentication and key management in IEEE 802.16 needs separate study.

In the developing standard IEEE 802.16e, mobility is supported in WMAN. [5] gives an overview of handoff schemes on different kinds of networks, such as GSM, UMTS, 802.11, HIPERLAN 2, and proposes the requirements for handoff procedures in 802.16. [11] proposes a draft for IEEE 802.16e handoff. Some comments have been submitted to the TGe for inter-BS handoff, for example [12]. Due to the limited capability of wireless devices, such as power and computation ability, it is important to reduce the computation for encryption or decryption. Thus a fast handover is proposed, which establishes and exchanges the keying information inside the wireless access network, so as to get fast and efficient intra-domain mobility or micro-mobility control. The fast handover is based on the extension authentication protocol, which is implemented in 802.16 PKMv2 [13]. [10] applies this micro mobility protocol and proposes the LPM (last packet marking) scheme, which aims to minimize handover delay and eliminate packet losses during handover.

Based on previous works, [7] proposes a secure roaming of key association for fast handover in IEEE 802.16, which provides perfect forward secrecy. [20] gives comments on modifying some keying materials which should be exchanged during the roaming. Several types of attacks mentioned before, such as replay attack and interception, are also applicable to this protocol.

## 3. WEAKNESS AND ENHANCEMENT OF AUTHENTICATION PROTOCOL

### 3.1 General Attacks on Authentication Protocols

Before we start to analyze the authentication protocol of 802.16, we would like to introduce some typical attacks on authentication protocols. Message replay attack is one of the most common attacks on authentication and authenticated key establishment protocols. If the messages exchanged in an authentication protocol do not carry appropriate freshness identifiers, then an adversary can easily get himself authenticated by replaying messages copied from a legitimate authentication session. Man-in-the-middle attack is another classic attack and is generally applicable in a communication protocol where mutual authentication is absent. Other familiar attacks include parallel session attack, reflection attack, interleaving attack, attack due to type flaw, attack due to name omission, and attack due to misuse of cryptographic services. Detailed discussion and examples of these attacks can be found in [14].

### 3.2 Authentication Protocol in 802.16

An SS begins authorization by sending an Authentication Information message which contains the SS manufacturer's X.509 certificate. This message is largely informative and the BS may choose to ignore it. Afterwards the SS sends an Authorization Request message (Auth-REQ) to its BS. In response to Auth-REQ, the BS validates the requesting SS's identity, determines the encryption algorithms and protocols to be shared with the SS, generates an AK, and sends the AK to SS. The authentication protocol is illustrated in Figure 1.

Message 1. SS → BS : Cert (SS. Manufacturer)
Message 2. SS → BS : Cert (SS) | Capabilities | BCID
Message 3. BS → SS : $KU_{ss}$ (AK) | SeqNo | Lifetime | SAIDList

**Figure 1. Authentication Protocol in 802.16**

In Figure 1, Cert (SS. Manufacturer) is the X.509 certificate of SS's manufacturer, and Cert(SS) is SS's X.509 certificate. The X.509 basic fields include the certificate version, serial number, signature, issuer, validity, subject, subject public key info, issuer unique ID, subject unique ID, and extensions. Capabilities are the SS-supported authentication and data encryption algorithms. BCID is the Basic Connection ID of SS, which equals to its primary security association ID (SAID). $KU_{SS}$(AK) is the Authentication Key encrypted by SS's public key. SeqNo is a 4-bit sequence number for AK. Lifetime gives the number of seconds before AK expires (32 bits). Finally, SAIDList contains the identities and the properties of the single primary SA and zero or more static SAs for which SS is authorized to obtain keying information.

Since message 1 is optional and only informative, we begin the security analysis from the next message. Message 2 is sent in plaintext but eavesdropping is not a problem since the information is almost public and is preferred to be sent in plaintext to facilitate authentication. However, BS may face a replay attack from an adversary who intercepts and saves the authentication messages sent by a legitimate SS previously. Although an adversary eavesdropping the messages cannot derive the AK from message 3 because it does not have the corresponding private key, the adversary still can replay message 2 multiple times and thus either exhaust BS's capabilities or force BS to deny the SS who owns that Cert(SS). The reason is that, if BS sets a timeout value which makes BS reject Auth-REQ from the same SS in a certain period, the legitimate request from the victim SS will also be ignored. In this case a Denial of Service attack occurs to the victim SS.

To avoid these replay attacks, we suggest adding a timestamp to message 2, together with a signature of SS which provides message authentication and non-repudiation. The signature uses SS's private key to encrypt the critical information in message 2.

Similarly, message 3 also exposes SS to replay attacks. Even worse, SS also faces the fraudulence from an adversary who intercepts its Auth-REQ message. The adversary can make its own Auth-Reply message with the AK generated by itself, thus gaining control of the communication of the victim SS. This is a typical man-in-the-middle attack, which brings forward the need of mutual authentication, i.e. SS needs to authenticate BS as well. This can be done by adding BS's certificate in message 3. The timestamp received from message 2 is also included in message 3 to ensure SS that this message 3 corresponds to its request. Timestamp from BS assures its aliveness and freshness. Signature of BS is added at the end of message 3, which provides the authentication and non-repudiation of this message. The revised protocol with the proposed modifications is shown in Figure 2.

Message 1. SS → BS : Cert (SS. Manufacturer)
Message 2. SS → BS : $T_S$ | Cert (SS) | Capabilities | SAID | $SIG_{SS}$ (2)
Message 3. BS → SS : $T_S$ | $T_B$ | $KU_{SS}$ (AK) | Lifetime | SeqNo | SAIDList | Cert (BS) | $SIG_{BS}$ (3)

**Figure 2. Revised Authentication Protocol**

In Figure 2, $T_S$ and $T_B$ are timestamps generated by SS and BS respectively; $SIG_{SS}$ (2) is the signature of SS over message 2; $SIG_{BS}$ (3) is the signature of BS over message 3.

Nonce is a possible alternative to timestamp in the authentication protocol. In [8], the authors use nonce instead of timestamp. Their protocol is shown in Figure 3.

Message 1. SS → BS : Cert (SS. Manufacturer)
Message 2. SS → BS : $N_S$ | Cert (SS) | Capabilities | SAID
Message 3. BS → SS : $N_S$ | $N_B$ | $KU_{SS}$ (pre-AK) | Lifetime | SeqNo | SAIDList | Cert (BS) | $SIG_{BS}$ (3)

**Figure 3. Authentication Protocol with nonce in [8]**

However, the exchange of nonces only assures SS that message 3 is a reply corresponding to its request. The BS still faces the replay attack because BS cannot tell whether message 2 is sent recently or it is just an old message.

The authors of [8] also suggest passing the pre-AK to SS instead of AK, and let SS and BS derive AK from the pre-AK at both ends. If the generation of AK exhibits significant bias, adding freshness in the AK may prevent the exposure of the AK. However, this cannot provide freshness as they claimed. If the pre-AK is compromised, the attacker can easily derive the AK by the same algorithm applied by the SS and BS, with the same freshness identifiers (such as nonce or timestamp) which are sent in plaintext. Thus the distributedly derived AK is barely more secure than the BS-generated AK.

Nonce and timestamp are two major methods for the verification of message freshness and principal aliveness. The main drawback of timestamp is that it needs the communicating parties to maintain time synchronization, which is considered to be difficult over the network. However, in 802.16, the SS and BS have already synchronized with each other during the initial ranging, right before they begin authentication procedure. Thus the synchronization is not a problem for applying timestamps here due to the nature of 802.16.

## 4. ANALYSIS AND MODIFICATION OF KEY MANAGEMENT PROTOCOL

In this section, we continue to analyze the key management protocol of 802.16. After achieving authentication, SS begins to request keying materials. SS sends a Key-Request message to the BS periodically, corresponding to one of its legitimate SAIDs. The BS responds with a Key-Reply message, containing the BS's active keying material for the specific SAID. This procedure is shown in Figure 4.

Message 1. BS → SS: SeqNo | SAID | HMAC (1)
Message 2. SS → BS: SeqNo | SAID | HMAC (2)
Message 3. BS → SS: SeqNo | SAID | OldTEK | NewTEK | HMAC (3)

**Figure 4. Key Management Protocol in 802.16**

In this protocol, message 1 is optional. BS sends re-key message (message 1) to SS only if BS regards it necessary to re-key before SS requests it. BS will choose a SAID from the SAIDList which the SS is allowed to access. SeqNo is the sequence number of AK provided by BS to this SS in the authentication protocol previously. This number allows the SS (and BS in the next message) to determine which HMAC_KEY_D (HMAC_KEY_U in the next message) was used to authenticate the message. HMAC(1) is the digest of message 1 under HMAC_KEY_D. Both of the downlink HMAC key (HMAC_KEY_D) and the uplink HMAC key (HMAC_KEY_U) are derived from the AK. By computing the value HMAC(1), it allows SS to detect message corruption or forgery.

Upon receiving message 1, SS will reply with the Key-Request message (message 2). If SS does not receive message 1 from BS before the current key expires, SS will send the normal Key-Request message when the current key is about to expire, where the SAID is chosen by SS itself from the SAIDList, to request a refresh of keying material for this specific SAID. HMAC(2) is the digest of message 2 under HMAC_KEY_U, which assures BS the authentication of the message.

BS will reply with the Key-Reply message (message 3) immediately after receiving the request from SS, which includes keying materials. At all times BS maintains two active sets of keying material per SAID. The OldTEK is the keying materials for the old (currently used) TEK, and the NewTEK is the keying materials for the new (to be used after the current one expires) TEK. The keying materials include the TEK encrypted by the KEK (Key Encryption Key), which is also derived from the AK. In addition, the set of keying materials also includes the CBC initialization vector and the remaining lifetime of each set of keying materials. HMAC(3) is the digest of message 3 under HMAC_KEY_D. As in message 1, HMAC(3) assures SS that message 3 is from BS and has not been modified.

Message replay attack is also one of the major threats to the key management protocol. In [8], the authors claim that the SS cannot recognize reused data SAs, just like it cannot recognize reused authorization SA in authentication protocol. However, if the adversary resends message 3 to SS after the SS has already exchanged some keying materials with BS, the SS can easily tell whether message 3 is relative to its request. This is because each SAID maintains two set of keying materials, and the OldTEK in the recently received Key Reply Message should be the NewTEK in the previous Key Reply Message. Therefore, in order to launch the replay attack, the adversary must fool the SS at the very beginning, i.e., the first time SS requests keying materials. But now the adversary will face another obstacle. The correct use of the AK provides a way for both SS and BS to check the validity of the Key Management Protocol instance. If the adversary intends to replay an old Key Reply message, the HAMC_KEY_D used in HMAC(3) must be derived from the AK that the SS currently uses. So the only chance for this replay attack to succeed is that the adversary eavesdropped and saved a former sequence of exchanged key request and reply messages, and the Key Management Protocol is reset which makes SS requesting totally new keying materials. This attack can be simply avoided by forcing SS to request a new AK every time the current Key Management Protocol instance fails and is reset. But this requires re-authentication.

In [8], the authors also suggest it should tie messages to a particular protocol instance in order to prevent replays from succeeding against the key management. Their solution is to add the nonces exchanged in the previous Authentication Protocol as the instance identifier. However, the correct use of the AK already provides a way to identify these instances. The SeqNo of AK provides some relationship between the instance of Authentication Protocol and the instance of related Key Management Protocol. Although this 4-bit number is prone to be reused thus makes the Key Management Protocol vulnerable to replay attack, the digest of these messages exchanged during Key Management provides a way to ensure both parties the validity of the legitimate AK. In order to succeed in this replay attack, the adversary should not only replay the SeqNo, but also replay the correct HMAC message whose encryption key is derived from the currently used AK in the corresponding Authentication Protocol instance. The failure of binding Key Management Protocol instance to its corresponding Authentication Protocol instance will happen only if there is a coincidence that another instance of Authentication Protocol happened to have the same AK and the same SeqNo. Due to the random generation of AK, this can be regarded extremely rare.

Although SS is somewhat free from the replay attacks on message 3, BS is still vulnerable to replay attacks on message 2. The reason is the Key-Request Message does not have the Keying Material like the Key-Reply Message, which allows the receiver to compare with its previously received message. Thus if an adversary replays the Key-Request message to BS, the BS has no way to recognize whether it is a fresh request from SS or an old one. Therefore, BS will reply with message 3 that assigns new Keying Materials to SS, which SS did not request at all. This can cause frequent exchange of keying materials, resulting in exhausting BS's capabilities, or the confusion in the use of TEK. This situation is quite the same as the one BS faces in the Authentication Protocol.

Similar replay attacks happen to SS on message 1 as well. This replayed message will make SS send message 2. Besides the effects on BS, this will eventually make SS and BS exchange the keying materials which they do not want to. That is because SS will think it is the BS who requests the rekeying by sending message 1, which is indeed sent by the adversary; while on the other hand, the BS will think it is the SS who requests the rekeying.

A timestamp is also a suitable identifier to be added in these Key Management messages to provide freshness. But the signature is unnecessary since the digest already provides the message authentication. The revised protocol is illustrated in Figure 5.

Message 1. BS → SS: $T_{B2}$ | SeqNo | SAID | HMAC (1)
Message 2. SS → BS: $T_{B2}$ | $T_{S2}$ | SeqNo | SAID | HMAC (2)
Message 3. BS → SS: $T_{S2}$ | $T_{B2}$ | SeqNo | SAID | OldTEK | NewTEK | HMAC (3)

**Figure 5. Revised Key Management Protocol**

Since message 1 is optional, SS will set $T_{B2}$ to 0 in message 2 if it initiates the rekeying; and $T_{B2}$ in message 3 is generated by BS in responding to SS's request to assure SS the freshness and aliveness. If BS initiates the rekeying, $T_{B2}$ is generated in message 1 by BS and SS should include it in message 2 to assure BS the freshness and aliveness, but BS can omit it in message 3 by setting it to 0.

## 5. SECURE ROAMING OF KEY ASSOCIATION DURING HANDOVER

Due to the resource constraints on most mobile (subscriber) stations (MSS), it may be too expensive for the MSS to re-authenticate every time it hands over to another BS because the authentication protocol is based on public key infrastructure. Thus fast handover is proposed, and the security roaming of key association becomes crucial.

The security roaming of key association scheme proposed in [7] supports perfect backward secrecy, i.e. the target BS (TBS) cannot derive keys used by the serving BS (SBS) from the roaming key association sent by SBS, thus is kept blind from the communication between the roaming MSS and its SBS. However, this scheme does not support forward secrecy. Since the PKMv2 is still under development, we propose a scheme for secure roaming of keying materials for handover based on the basic PKM protocol. Our protocol supports both backward secrecy and forward secrecy, and prevents many attacks mentioned before as well. Though it is not based on PKMv2, the idea is similar and it can be easily modified to be implemented in PKMv2.

We skip the handover procedure for conciseness, and focus on the security roaming of the keying materials. The details of handover procedure can be found in the references such as [11]. Keying materials should be encrypted and sent from serving BS to target BS through the backhaul. Obviously, this can be done by letting serving BS encrypt the message with target BS's public key and add its signature at the end. However, this requires two public key encryptions for both communicating parties, which could be very expensive. Due to the frequent communication between BSs, it is desirable to distribute a shared secret key (SK) to each pair of BSs within the network domain. This secret key can also be used in many other applications, such as multicast. There are many ways to establish and distribute the SK, which is beyond the scope of this paper. Here we assume the TBS and SBS have already established the SK.

If TBS accepts the Handover Request from SBS, the SBS will send message 1 that contains keying materials required by the TBS to communicate with the roaming MSS.

Message 1. SBS → TBS: T1, MSS, SK (MSS, T1, RAK)

where RAK is the Roaming Authentication Key, which is derived from the AK shared by SBS and MSS. T1 is a timestamp. And TBS replies with an Acknowledgement (ACK) as shown in message 2.

Message 2. TBS → SBS: T1, N1, SK (T1, N1)

where N1 is a nonce from TBS. It provides freshness in ACK. The nonce will also be used as the identifier for this roaming protocol instance. After receiving ACK from TBS, SBS will send message 3 to notify MSS that TBS is ready to accept his roaming. This message also includes the RAK.

Message 3. SBS → MSS: T2, N1, Ready-to-Roam TBS, AK (TBS, RAK, T2, N1)

After exchanging handoff messages with its SBS, MSS begins initial ranging with the TBS, and achieves re-authentication without sending the X.509 certificate.

Message 4. MSS → TBS: T3, N1, Re-auth, RAK (T3, N1)

Message 5. TBS → MSS: T3, RAK (new-AK, T3)

where new-AK is the current AK shared by MSS and TBS.

Notice that the SBS is still able to intercept the future communication between MSS and TBS. SBS may intercept message 5 and get the new-AK as long as it has the RAK, therefore decrypt the subsequent messages exchanged between MSS and TBS. But it is better than simply using the RAK. A possible enhancement is letting TBS and MSS derive the new-AK in a distributed manner instead of letting TBS generate and distribute it. Both MSS and TBS contribute to the new-AK (possibly by the exchanged nonce). However, the threat to the forward secrecy still exists. So it only provides the forward secrecy to some extent.

## 6. CONCLUSION AND FUTURE WORKS

In this paper, we analyze the vulnerability in authentication and key management protocols of 802.16. Our revised protocols can prevent many kinds of attacks, such as replay attacks to BS and SS. We also propose a security roaming protocol for 802.16e, which provides fast handover and guarantees backward and forward secrecy to some extent.

As we discussed before, the 802.16e is still under development. The proposed mobility will bring up more problems in authentication and key management protocols and make them more vulnerable. Therefore, we should pay more attention to the security issues in the drafts from TGe before they are approved as standards. Secure roaming in PKMv2 needs more works to finish. Mesh network in 802.16 also needs separate study. Multicast is another issue in the new standard, where authentication and key management protocols should be revised to facilitate the multicast functions.

## 7. REFERENCES

[1] IEEE std 802.16-2001: Air Interface for Fixed Broadband Wireless Access Systems, 2002.

[2] IEEE std 802.16-2004: Air Interface for Fixed Broadband Wireless Access Systems, 2004.

[3] Intel white paper, "IEEE 802.16 and WiMax: Broadband Wireless Access for Everyone," 2004.

[4] William A. Arbaugh, Narendar Shankar, Y.C. Justin Wan, "Your 802.11 Wireless network has No clothes (March 2001)," http://www.cs.umd.edu/~waa/wireless.pdf

[5] Avi Freedman, Zion Hadad, "Handoff Schemes Overview and Guidelines for handoff Procedures in 802.16," IEEE C802.16sgm-02/24, 2002.

[6] Matthew S. Gast, *802.11 Wireless Networks: The Definitive Guide*, O'Reilly, 2002.

[7] Kihun Hong, Souhwan Jung, Ki Jun Lee, Brian Lee, Jungwook Wang, "Secure Roaming of Key Association for Fast handover," IEEE C802.16e-04/407, 2004.

[8] David Johnston, Jesse Walker, "Overview of IEEE 802.16 Security," *IEEE Security & Privacy*, May/June 2004.

[9] Richard R. Joos, Anand R. Tripathi: Mutual Authentication in Wireless network (June 1997); http://cs.engr.uky.edu/~singhal/CS685-papers/joos97mutual.pdf

[10] Kyung-ah Kim, Chong-Kwon Kim, Tongsok Kim, "A seamless handover Mechanism for IEEE 802.16e Broadband Wireless Access," International Scientific-Practical Conference (ISPC) Communication-2004, August 2004.

[11] Itzik Kitroser, "IEEE 802.16e handoff draft," IEEE C802.16e-03/20r1, 2003.

[12] Changhoi Koo, Sohyun Iim, Jungje Son, "Inter-BS communication for IEEE 802.16e handoff," IEEE 802.16e-03/29, 2003.

[13] Jeff Mandin, 802.16e Privacy Key Management (PKM) version 2, IEEE C802.16e-02/131r1, 2002.

[14] Wenbo Mao, *Modern Cryptography: Theory and Practice*, Pearson Education, Prentice Hall PTR, 2004.

[15] Roger Marks, "A technical Overview of the WirelessMAN Air Interface for Broadband Wireless Access," IEEE C802.16-02/05, 2002.

[16] Ron Olexa, *Implementing 802.11, 802.16 and 802.20 Wireless network*, ELSEVIER, July 2004.

[17] Kaveh Pahlavan, Prashant Krishnamurthy, *Principles of Wireless Networks: A unified Approach*, Pearson Education, Prentice Hall PTR, 2002.

[18] William Stalling, *Cryptography and Network Security: Principles and Practices, 3rd edition*, Pearson Education, Prentice Hall PTR, 2003.

[19] Daniel Sweeney, *WiMax Operator Manual: building 802.16 Wilreless Networks*, Apress, 2005.

[20] Feng Tian, DongXin Lu, Rui Li, "Comment on Security Roaming of Key association for Fast Handover," C802.16e-04/571r1, 2005.