



Design, Verification and Implementation of Enhanced PKM WiMAX Authentication Protocol

Ahmed Mohamed El-Amin, Salah El-agooz, Alaa El-Din Rohiem Shehata and Essam Abd-Elwanees Amer

Abstract– Worldwide Interoperability for Microwave Access (WiMax/ IEEE 802.16), is new technology based on wireless metropolitan area network. Privacy Key Management (PKM) protocol is responsible for providing the secure distributions of keying data from Base station (BS) to Subscriber station (SS). PKMv1, PKMv2, and enhanced PKMv1 described with formal analysis and verified using Scyther tool [1]. PKMv1 is vulnerable to replay, DOS, Man-in-the middle attacks since there is no mutual authentication. The proposed design is more secure to prevent the network from the previous attacks. A simple implementation is done using Wireless Open Access Research Platform (WARP) and programming language C#.NET.

Index Terms– Authentication, Authorization, Base Station, Connections, Encryption, IEEE 802.16, Methods and Mobile Station

I. INTRODUCTION

WiMAX defines Privacy Key Management (PKM) protocol in security sub-layer, which assures the security of connections access in WiMAX channel. PKM protocols has two goals, one is to provide the authorization process and the other is to secure distribution of keying data from Base station (BS) to SS/MS (Mobile Station). PKM uses X.509 certificates and symmetric cryptography to secure key exchange between an SS and BS. There are two versions of PKM. The first version (PKMv1), used in IEEE 802.16-2004 standard. The second version (PKMv2), extended to work with the mobile WiMAX IEEE 802.16e [2.6.7].

The IEEE std 802.16-2004 supports operations both in PMP and mesh modes [5]. Later, the IEEE std 802.16e modifies the existing PKM protocol and renames it to PKMv1. The amendment also defines that PKMv2 supports the mobile subscribers in PMP mode where the operations in the mesh mode are not supported. Unlike PMP, in the mesh mode the BS and SSs coordinate among themselves to transmit packets in a multi-hop manner, even though Wireless Mesh Networks are a hot topic in both the industry and research Contexts. So, the PKMv1 is enhanced and modified in this paper to improve the security and meet these requirements [10, 11, 16, 17].

So, only PKMv1 is enhanced since we are interested to work with mesh mode and the improvement of this protocol can solve the main attacks we mentioned before.

In this paper, we present an overview of security flaws in PKMv1, PKMv2, and modified PKMv1. We perform formal analysis and verification on IEEE 802.16e standard using Scyther tool [3], in order to extract the main security flaws and threats that might exist in such procedures; we perform some modifications on the mechanism of PKMv1 to enhance the security and the efficiency of the protocol. We also implement the protocol using Wireless Open Access Platform (WARP) and programming language C#.NET.

II. WIMAX SECURITY

The IEEE 802.16e standard has two versions of PKM, the PKMv1 and PKMv2. The authorization protocol used in PKM is basically 3 way handshake protocol between the SS and BS. The authentication in PKMv1 is just from the SS but not from BS [5, 12, 17]. Because of this lack, a fake BS may pretend as a legitimate BS which is not possible for an SS to recognize. Therefore BS must authenticate itself as SS does. Mutual authentication is the solution [5].

Message 1 is sent from the SS to BS consisting of the X.509 certificate together with the capabilities and Basic Connection Identity (BCID), message 2 is sent again from the SS which contains the certificate of itself. Finally BS reply to SS containing the AK encrypted with SS public key along with sequence number, lifetime and AK and Security Associations Identity List (SAIDL) [5, 14].

PKMv1 Authentication Protocol:

The formal definition of the authentication scenario of PKMv1 described above is shown as follows:

MS to BS: Mancert (MS);
 MS to BS: MsCert, Capabilities, SAID;
 BS to MS :{ AK}pk(Ms), SAIDlist, AKSeqno;

In PKMv2, the major security problems were solved. X.509 certificates are used for RSA based authentication. In case of PKMv1 only one way X.509 certificate used but in case of PKMv2 three-way authentication is used.

At the first SS sends its MCerss (Manufacturer's Certificate) and then sends its own CerSS which is X.509 certificate along with a nonce; a 64 bit random number generated by the SS, BC-Identity and cryptographic Capb (capabilities). BC-Identity is assigned to SS when it enters in a network and requests for ranging. BS responds by sending some information and a nonce when the authorization request message from SS is rived. Additionally, for mutual authentication BS attaches its certificate (CerBS) in response to SS. BS also includes its signatures for validity in response message to SS. A 256 bit key (Pre-Au-K) with the SS's identifier (SSID) is encrypted by the BS with the public key of SS. A 4 bit sequence number (Seq_No) for the authorization key (and its life time with the SAID's List (SAIDL) are sent by the BS. After validating the message from BS, the SS sends the acknowledgement message with nonce created by BS and MAC address (MACSS) of the subscriber station. Authorization Key (AK) transmitted by BS to SS in previous message is used to encrypt the Nonce BS (BS generated random number) and MACSS [5, 14].

PKMv2 Authentication Protocol:

The formal definition of the PKMv2 authentication protocol is shown as follows:

MS to BS: Mancert (MS);
 MS to BS {MsCert,Capabilities,SAID,Ns}sk(MS)
 BS to MS :{{prePAK}pk(MS),SAIDlist,Ns,Nb,
 prePAKSe
 prePAKlifetime,BsCert}sk(BS);
 MS to BS :{Nb}sk(MS);

III. THE PROPOSED AUTHENTICATION PROTOCOL

We analyze our enhancements of security and privacy in WiMax networks into 5 steps as shown in Fig. 1:

1. Problem Formalization and Analysis
2. Protocol Design
3. Protocol Verification
4. Implementation
5. Evaluation

A. Problem Formalization and Analysis

As discussed in the previous section, the existing protocol still vulnerable to replay ,DOS, and Man -in -the Middle attacks when analyzed using Scyther tool [1, 2, 3, 4] . Some solutions are introduced to solve those attacks in our design. To prevent both Man-in-the-Middle attack and replay attack we add timestamp. There is only main problem with timestamp is that it requires time synchronization between MS and BS.

In wireless communication time synchronization is considered to be difficult (particularly under mobility). But in

IEEE 802.16e it is assumed that the synchronization is done between MS and BS.

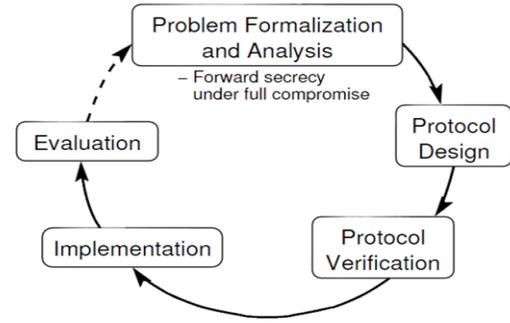


Fig. 1: Steps for protocol analysis, Verification, Implementation and Evaluation

B. Protocol Design

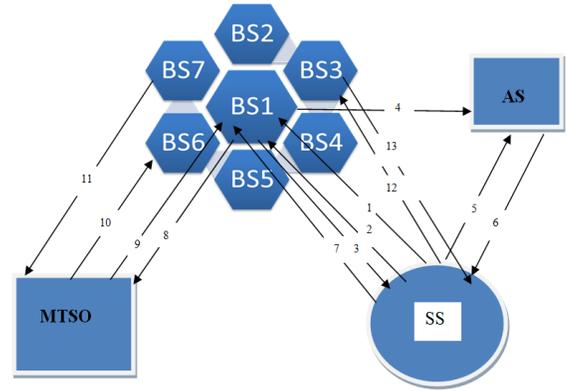


Fig. 2: State Diagram of the proposed protocol

- 1: SS - BS: Cert (SS) (AuthReq message) | TS (Time Stamp)
- 2: SS - BS: Cert (SS) | Capabilities | BCID | TS
- 3: BS - SS: KUSS (AK) | SeqNo | Lifetime | SAIDL | BSID
- 4: BS - AS: BSID | SSID | KUss
- 5: SS - AS: E (KRss, [SSID | BSID])
- 6: AS - SS: E (KUss, [Confirmation Message])
- 7: SS - BS: E (Further Communication)
- 8: BS - MTSO E (SS credentials)
- 9: MTSO - BS E (Confirmation Message)
- 10: MTSO - All BSs in the same cluster E (SS credentials)
- 11: BSs - MTSO E (Confirmation Message)
- 12: SS - TBS Cert (SS) (Auth Req message) | TS
- 13: TBS - SS E (KUss, [confirmation Message, BSID,

Our proposed authentication protocol improved the WiMAX mutual authentication by increased the authentication strength between SS and BS using timestamp and authentication server appears as trusted third party to

authenticate the BS to SS and solve the main problem of rouge BS.

Also to enhance the timing and communication overhead during the handoff we use a new idea through the scenario to enhance the security and efficiency of the network.

C. Protocol Verification

In this section, we formally verify the IEEE 802.16e PKMv1 enhanced protocol using the scythe tool [3.4]. Scyther tool were developed by Cas Cremers in 2007 [1]. Scyther, is a formal protocol analysis tool, for the symbolic automatic analysis of the security properties of cryptographic protocols (typically confidentiality or variants of authenticity). It assumes perfect cryptography, meaning that an attacker gains no information from an encrypted message unless he knows the decryption key. Scyther takes as input a role-based description of a protocol in which the intended security properties are specified using claims. Claims are of the form claim (Principal, Claim, Parameter), where Principal is the user's name, Claim is a security property (such as 'secret'), and Parameter is the term for which the security property is checked. The description of a protocol is written in SPDL language. For the protocol verification, Scyther can be used in three ways [1, 2, 3, 4]:

- *Verification claim:* Scyther verifies or falsifiers security properties.
- *Automatic claims:* if user does not specify security properties as claim event the scythe automatically generates claims and verifies them.
- *Characterization:* each protocol role can be characterized. Scyther analyses the protocol and provides a finite representation of all traces that contain an execution of the protocol role. Scyther generates attack graph for counter example, and represents individual attack graph for each claim.

Ensuring WIMAX protection means that we should satisfy these requirements to protect this network against different attacks:

Property 1- Confidentiality

This claim is fulfilled if the MS/SS has the guarantee that all exchanged user data is secret. The exchanged user data messages between the MS and the BS is called Msg. Every information (α) in Msg should remain secret [1, 2, 3, 4]. The formalization of information confidentiality is given below:

$$\forall \alpha \in \text{Msg} (\text{claim}(\text{SS}, \text{Secret}, \alpha)) \quad (1)$$

Property 2- Authenticity

This claim is fulfilled if an outsider, who keeps track of the communication, cannot relate the traffic to a specific MS [2]. In order to fulfill authenticity the MAC address of the MS which identifies it must remain secret. The MAC address is included in the MS's certificate (MsCert) [1, 2, 3, 4]. The formal definition of pseudonymity is given below:

$$\text{Claim}(\text{SS}, \text{Secret}, \text{SSCert}) \quad (2)$$

Property 3- Integrity

This claim is fulfilled if the BS and the SS have the guarantee that all exchanged keys (described as key) are secret and unique. We have included an additional restriction that only claims concerning sessions between trusted agents are evaluated. Its formal definition is shown as follows [1, 2, 3, 4]:

$$\forall \text{key}(\text{claim}(\text{BS/SS}, \text{Secret}, \text{key})) \quad (3)$$

Property 4- Access control

A WIMAX network should have a correct mechanism to verify that a given user is authorized to use a particular service [14]. A service should always be bound to an authenticated user. Its formal definition is given as follows [1, 2, 3, 4]:

$$\forall \alpha \in \text{Msg} (\text{claim}(\text{BS}, \text{Secret}, \alpha)) \quad (4)$$

Property 5- Freshly of messages

An important part of security protocols is the generation of fresh values which are used for challenge-response mechanisms (often called nonces), or as session keys. This claim is fulfilled if the BS and MS/SS have the guarantee that the session key is fresh [1, 2, 3, 4]:

$$(\text{claim}(\text{BS/SS}, \text{Fresh}, \text{key})) \quad (5)$$

IV. MODELING ENHANCED PKMV1 WITH MUTUAL AUTHENTICATION IN SPDL LANGUAGE

```

/*
 * PKMv1 with Mutual Authentication and timestamp
 * (Handover Version)
 * Designed by: Ahmed M. ElAmin
 */
// The protocol description
protocol PKMv1 ( SS , BS1 , AS , MTSO , BS2)
{
role SS
{
send_1 (SS,BS1,Mancert(SS));
send_2 (SS,BS1,Certss,cap,SAID,Ts);
read_3
(BS1,SS,{AK}pk(SS),SAIDlist,AKseq,BS1ID,lifetime);
send_5 (SS,AS,{SSID,BS1ID}sk(SS));
read_6 (AS,SS,{confmsg}pk(SS));
send_11 (SS,BS2,Certss,cap,SAID,Ts);
read_12 (BS2,SS,{confmsg,AK}pk(SS),BS1ID,ASID,Ts);
send_13 (SS,BS2,{confmsg}pk(BS2));
// The properties ( claim events)
claim_ss1(SS,Secret,Certss);
claim_ss4(SS,Secret,Data);

```

```

claim_ss5(SS,Secret,Key);
}
role BS1
{
read_1 (SS,BS1,Mancert(SS));
read_2 (SS,BS1,Certss,cap,SAID,Ts);
send_3
(BS1,SS,{AK}pk(SS),SAIDlist,AKseq,BS1ID,lifetime);
send_4 (BS1,AS,BS1ID,SSID,pk(SS));
send_7
(BS1,MTSO,{SSID,BS1ID,ASID}pk(MTSO),lifetime);
read_8 (MTSO,BS1,{confmsg}pk(BS1));
// The properties ( claim events)
claim_bs13(BS1,Secret,Data);
claim_bs14(BS1,Secret,Key);
}
role AS
{
read_4 (BS1,AS,SSID,BSID,pk(SS));
read_5 (SS,AS,{SSID,BSID}sk(SS));
send_6 (AS,SS,{confmsg}pk(SS));
}
role MTSO
{
read_7
(BS1,MTSO,{SSID,BS1ID,ASID}pk(MTSO),lifetime);
send_8 (MTSO,BS1,{confmsg}pk(BS1));
send_9 (MTSO,BS2,{SSID,BS1ID,ASID}pk(BS2),lifetime);
read_10 (BS2,MTSO,{confmsg}pk(BS2));
}
role BS2
{
read_9 (MTSO,BS2,{SSID,BS1ID,ASID}pk(BS2),lifetime);
send_10 (BS2,MTSO,{confmsg}pk(BS2));
read_11 (SS,BS2,Certss,cap,SAID,Ts);
send_12 (BS2,SS,{confmsg,AK}pk(SS),BS1ID,ASID,Ts);
read_13 (SS,BS2,{confmsg}pk(BS2));
/// The properties ( claim events)
claim_bs23(BS2,Secret,Data);
claim_bs24(BS2,Secret,Key);
}
}

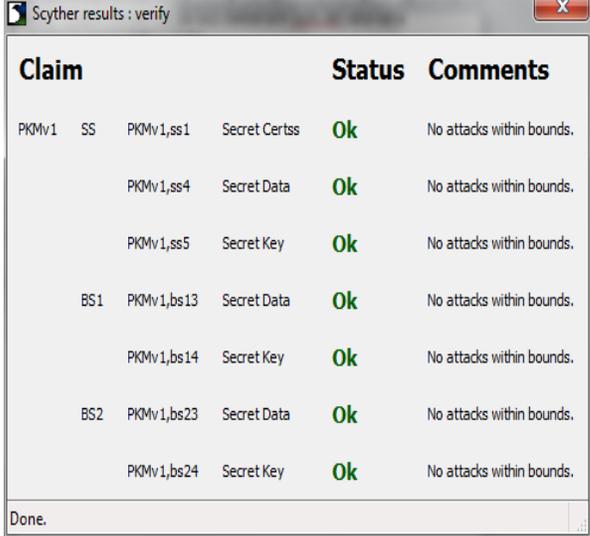
```

V. ANALYSIS OF THE PROPOSED DESIGN

This model is going to be challenged with the following requirements using the Scyther tool.

1. Property 1 and 2: In the formal analysis it is proved that an intruder cannot obtain the SS/MS certificate (MsCert) and data exchange between MS and BS.
2. Property 3: In the formal analysis it is proved that the authorization key exchanged in the authentication protocol is
3. Property 4: It is proved that unauthenticated user cannot access the services provided, and cannot impersonate another user. Also, it is not possible to modify the data by an unauthorized individual.

4. Property 5: It is proved that an adversary cannot obtain the unique pre-PAK. Timestamp used in the protocol to prevent replay and man-in-the-middle attack.



Claim	Status	Comments
PKMv1 SS PKMv1,ss1 Secret Certss	Ok	No attacks within bounds.
PKMv1,ss4 Secret Data	Ok	No attacks within bounds.
PKMv1,ss5 Secret Key	Ok	No attacks within bounds.
BS1 PKMv1,bs13 Secret Data	Ok	No attacks within bounds.
PKMv1,bs14 Secret Key	Ok	No attacks within bounds.
BS2 PKMv1,bs23 Secret Data	Ok	No attacks within bounds.
PKMv1,bs24 Secret Key	Ok	No attacks within bounds.

Fig. 3: Scyther verifies or falsifiers security properties for the proposed authentication protocol

Fig. 3 shows that all the claims used to verify the security properties for the proposed authentication protocol with a status (OK) for all the claims and there is no attacks within bounds are found.

A. Protocol Implementation

The simulation process used the following in its testing environment.

1. Windows7 platform
2. The socket class in the .NET framework
3. TCP/IP Protocol
4. Wireless Open Access Research Platform (WARP)
Two boards works as transceivers.
5. Some encryption and decryption capabilities.
6. Programming language C#.NET



Fig. 4: WARP board

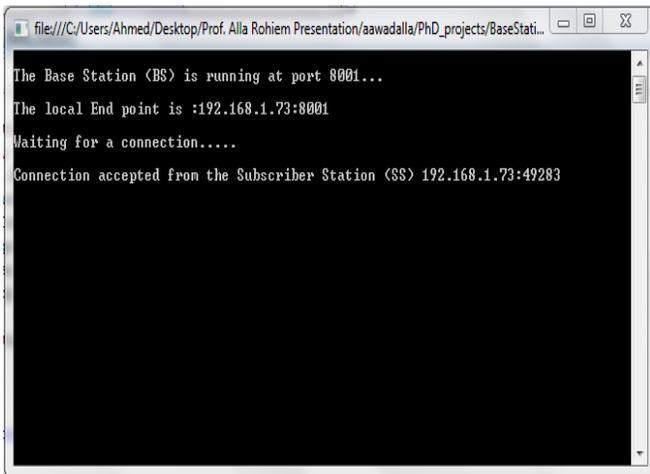


Fig. 5: BS accepted the connection from SS

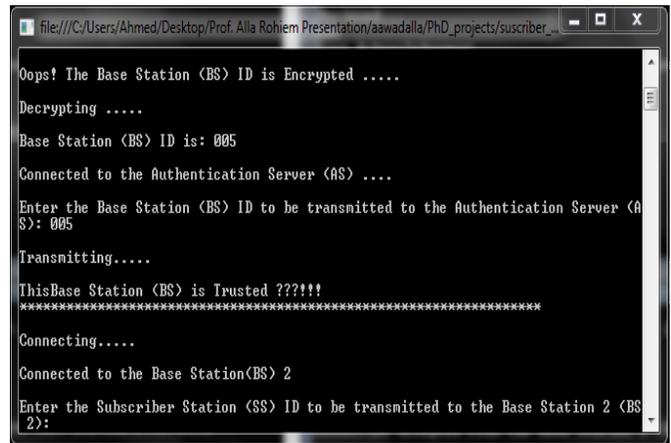


Fig. 8 : Windows for the C# programs for the proposed authentication protocol including that the BS is Trusted

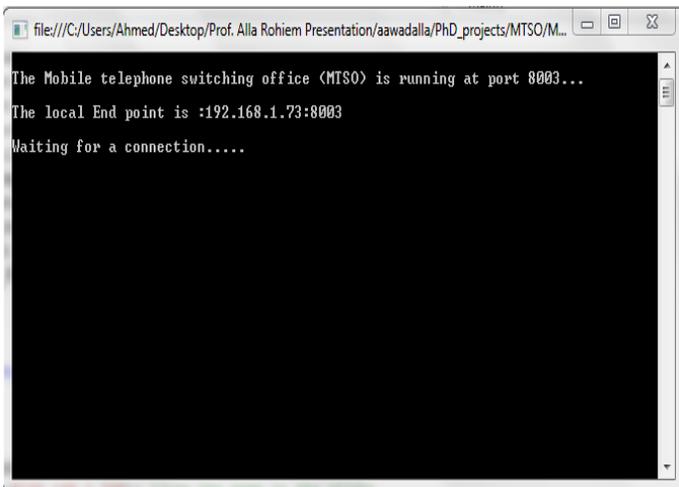


Fig. 6: MTSO waiting the connection from the BS

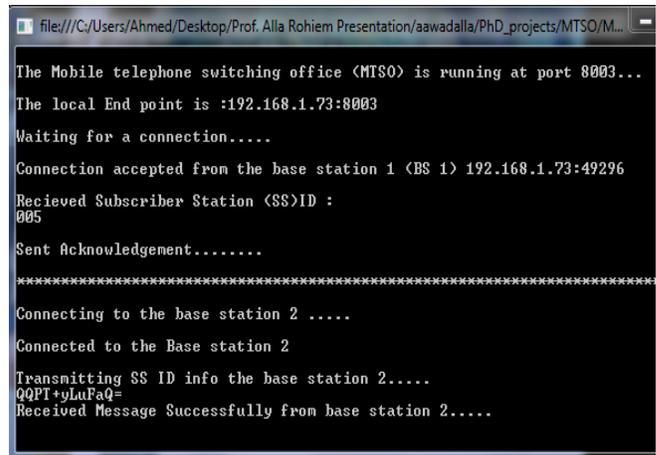


Fig. 9: windows for the C# programs for the proposed authentication protocol including the connection of the MTSO with BS1 and BS2

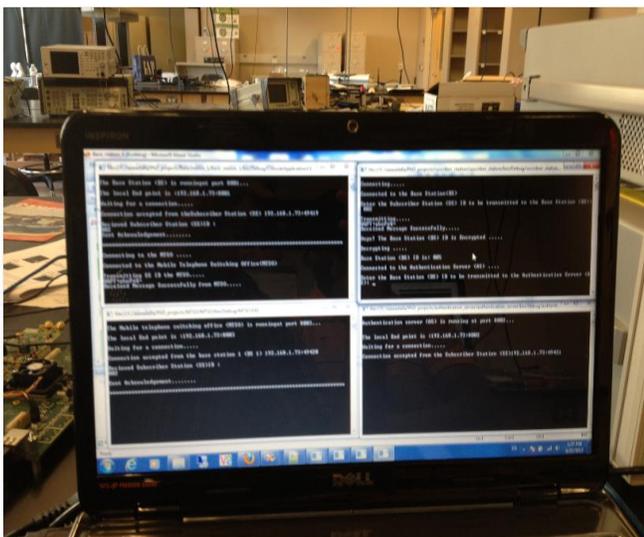


Fig. 7: windows for the C# programs for the proposed authentication protocol

Fig. 4 – Fig. 9 show the components and some software programming windows for the lab. Experiments we used to apply the real time implementation of the enhanced PKMv1 Authentication protocol.

VI. CONCLUSION AND FUTURE WORK

The paper analyzes the vulnerabilities in the both versions of authentication protocol PKMv1 and PKMv2. As seen in the formal analysis, the secrecy and uniqueness of the keying material distributed and the no theft of service possible claims are valid in both PKMv1 and PKMv2. However, pseudonymity and information confidentiality are broken in both versions of PKM. A revised authentication protocol is proposed by using timestamp and new security scenario. The new solution is efficient to tackling the various security threats such as replay, man in the middle and DOS attacks. The revised authentication protocol is expected to provide better secure platform for IEEE 802.16(e).

REFERENCES

- [1] Noudjoud Kahya, Nacira Ghoulmi, Pascal Lafourcade, Formal Analysis of PKM using Scyther Tool 2012 International Conference on Information Technology and e- Services
- [2] Kahya Noudjoud, Debbah Adel and Nacira Ghoulmi WiMAX Security – A Formal Analysis using Scyther tool International Conference on Computational Techniques and Artificial Intelligence (ICCTAI'2012) Penang, Malaysia
- [3] Ahmed M. Taha1, Amr T. Abdel-Hamid, and Sofiène Tahar Formal Verification of IEEE 802.16 Security Sublayer Using Scyther Tool 2009 ESR Groups France
- [4] Ahmed M. Taha1, Amr T. Abdel-Hamid, and Sofiène Tahar Formal Formal Analysis of the Handover Schemes in Mobile WiMAX Networks. IEEE 2009.
- [5] Mohammad Hossain, Analysis and Assessment the Security Issues of IEEE 802.16/WiMax Network Masters Thesis: MEE10:24 Telecommunication System Department of Telecommunication System School of Electrical Engineering Blekinge Institute of Technology SE – 371 79 Karlskrona, Sweden
- [6] Luo Wei, Guo Da, SONG Mei. The present status and development of WiMax security strategy [J]. Mobile Communications, 2006, 1127.
- [7] Cao Jianguo, Wang Dan, Wang Wei. The research based on the RSA public key cryptography security [J]. Computer technology and development, 2007, 17(1): 172-176.
- [8] Yang Weizhong, Li Tong, Hao Lin. The security risks in RSA encryption system [J]. Journal of Yunnan University(Natural Sciences Edition), 2004, 26(3): 212- 215.
- [9] Lv Junwen, Song Tao, Si Tiange. Realization of SSL protocol by using of ECC [J]. Computer engineering and design. 2006, 27(10) :1715-1717.
- [10] Shen Weifeng. ECC security strategy study in wireless LAN [J]. Jiangxi Communication Technology. 2007 (1):18-20.
- [11] LIU Chun, Zhang Fengyuan, Zhang Qishan. The comparison and realization between RSA and ECC algorithm based on smart cards [J]. Computer engineering and application. 2007, 43(4):96-98.
- [12] Li Huizhong, Chen Huifang, Zhao Wendao. The security vulnerability and solution in IEEE802.16 [J]. Modern telecommunications technology. 2005(1):26-27.
- [13] TIAN Haibo, PANG Liaojun, WANG Yumin. Key Management Protocol of the IEEE 802.16e [J]. Wuhan University Journal of Natural Sciences. 2007, 12(1):59- 62.
- [14] David Johnston, Jesse Walker. Overview of IEEE 802.16 Security [J]. IEEE Security and Privacy, 2004, 2(3):40-48.
- [15] Sen Xu, Manton Matthews, Chin-Tser Huang. Security issues in privacy and key management protocols of IEEE 802.16[C]. Proc. of the 44th annual Southeast regional conference. New York: ACM Press, 2006. 113-118.
- [16] IEEE Standard for Local and Metropolitan Area Networks. Air Interface for Fixed and mobile Broadband Wireless Access Systems, IEEE Std 802.16e [S]. New York: IEEE Press, 2006
- [17] Huixia Jin, Li Tu, Gelan Yang, Yatao Yang. An Improved Mutual Authentication Scheme in Multi-Hop WiMAX Networks. IEEE 2008 International Conference on computer and Electrical Engineering, China