Military Technical College

Kobry El-Kobbah,

Cairo, Egypt

8th International Conference
on Electrical Engineering

ICEENG 2012

Enhancement of WiMAX Mutual Authentication Protocol

Ahmed Mohamed El-Amin — *Military Technical Research center* — *ahmed_elamin_omran@yahoo.ca*

Alaa El -Din Rohiem — *Military Technical College*

Essam Abd-Elwanees — *Military Technical College* — *mohwanees@yahoo.com*

Abstract

The mutual authentication mechanism in the IEEE802.16e can avoid the man-in-middle attack, and can protect the multi-hop WiMax security in efficiency.An enhanced mutual authentication flow was proposed in this paper, which enhances the security and working efficiency of the mutual authentication in mobileWiMax system. The proposed scheme heightens the security and practicability of WiMax system, which has better referenced value to the improvement of IEEE 802.16e standards.

1. Introduction

In IEEE 802.16 standard, an SS tries all the way to get authentication from BS. But, there exists no regulation for BS to authenticate itself. Because of this lack, a rogue 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. Authentication must be performed from both sides.

In the security mechanism of IEEE 802.16d, the network's base station (BS) authenticated the subscriber station (SS) through the X.509 certificate configured in the system of Worldwide Interoperability for Microwave Access (WiMax). The X.509 certification carried its owner's related information, marked the BS status and contained the digital signature to BS; however this standard lacked mechanism of SS authenticating BS, which caused the camouflage aggressor to legitimate BS easily and carried on the spurious attack to SS. The IEEE802.16e had repaired this crack, increased digital authentication from SS to BS, and realized mutual authentication between the SS and BS. This kind of mutual authentication was based on X.509 certificate and Extensible Authentication Protocol(EAP), it could ensure the multi-hop WiMax security effectively and could reduce the camouflage or invasion from illegal BS; whereas it could be seen that using the RSA signature algorithm in the X.509 certificate had many hidden security trouble, it was known, the RSA security was based on the mathematics problem that the large prime number wasdifficult to decompose, RSA algorithm was not to be discovered the obvious and serious existent security problem in practice; however, with the technology

limitation of generating prime number, the RSA key's production was very troublesome, which also made the encryption/decryption more difficult in some extent [1].
The X.509 certificate was the important guarantee to WiMax's network security, which could be used in the existent cipher system to guarantee its security and efficiency. In this paper, improved WiMax mutual authentication mechanism was proposed, by which WiMax system's security performance was enhanced accordingly.

2. Related work

The RSA algorithm could be used in encryption and the digital signature algorithm; it had been accepted and was thought to be one of most outstanding public key mechanism. The Elliptic Curve Cryptosystems (ECC) was also researched and used extensively because of its fine characteristics. Reference [2] and [3] described the RSA's encryption/decryption algorithm and its anti-attack capability in detail, some shortcomings existed in the practical application was analyzed, which took important guidance roles in bringing forward the new ideas in our paper. Regarding the improvement and expansion of X.509 certificate, some work had already been done. Reference [4] introduced the ECC algorithm's superiority briefly compared with the RSA algorithm, described how to use the ECC algorithm to make the algorithm expansion in the SSL protocol in detail. Reference [5] analyzed the basic principle of ECC, compared with other cipher system, the author also introduced the basic principles and characteristics of WAPI protocol embedded ECC algorithm. Paper [6] discussed the realization method and the security in the ECC system. Reference [7] pointed out the 802.16d existent security problems on the base of analyzing its security mechanisms; Reference [8] summarized the 802.16e related security mechanism, such as authentication, handshake protocol, and key agreement and so on. Reference [9] and [10] argued WiMax security mechanism, analyzed the Privacy Key Management protocol (PKM) and security threat to multi-hop WiMax network, which also has useful effect for our study.

3. Improved mutual authentication scheme

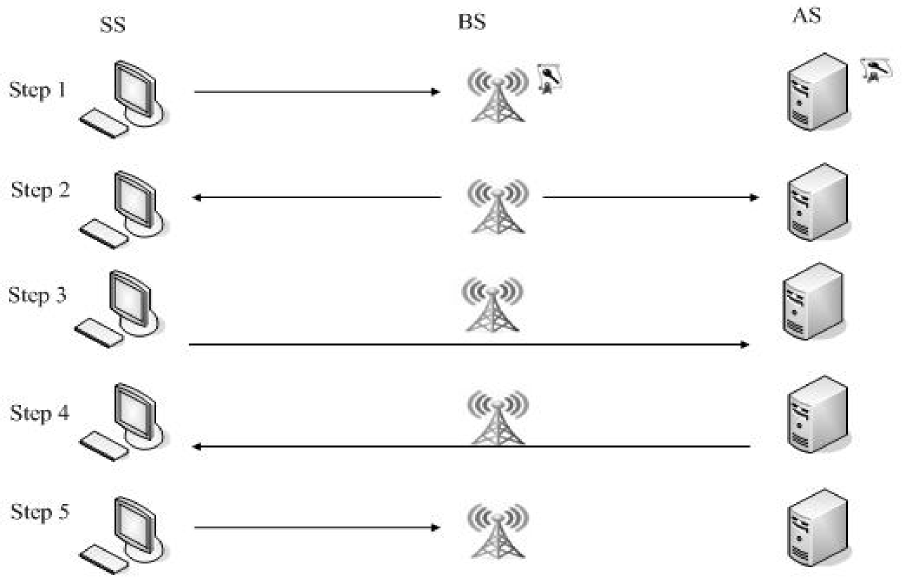
IEEE 802.16 authentication process:

At present, X.509 [IETF 2459] version3 certificate is widely used in IEEE802.16 standard, main parameters are shown in [11]. In multi-hop WiMax network, the main entities include subscriber station (SS) and base station (BS), in IEEE802.16e, the authentication and key exchange process between SS and BS are as following [12] :
1. SS sends an authentication information message to BS. The message includes X.509 digital certificate which contains the information of SS manufacturer, the legitimacy of the SS equipment can be verified by BS.
2. SS sends an authorization request message to BS for the sake of requesting BS to authenticate the legitimacy of the SS. The message includes manufacturers' X.509 certificates, the cipher algorithms supported by SS, SS basic ID number, 64- bit random number produced by SS and the RSA digital signature about the above information.
3.After BS verifies the identity of SS, BS will activate one of encryption algorithms and protocols which are shared with SS, then sends authorization key (AK) to SS and encrypts it using SS's public key by RSA algorithm, the reply message includes the BS's digital signature containing the entire authorized information encrypted by the RSA algorithm. If BS rejects the authorization request from SS, BS will not send messages to SS.

4. SS sends the confirmation message encrypted by RSA to BS. The information covers a random number produced by BS and authentication result code (AuthResult Code) which represents the success or failure of the certification. Only if the authorization request is rejected, the Error-code and display-string will appear with denoting request being refused and its reasons respectively. In order to acquire re-authorization continuously, it is necessary for SS to send authorization request periodically to BS for updating the AK.

Improved authentication mechanism:

IEEE802.16e standard has provided a kind of useful security strategy, reducing security threats effectively such as replay attacks, DoS attacks and intermediary attacks [12]. Based on IEEE802.16e standard, our proposed improved ideas in multi-hop WiMax mutual authentication is, to amend the mutual authentication process by increased the authentication steps from SS to BS, and depend on the first time mutual authentication between the SS and BS.The BS sends the crdentials of the SS to the Mobile Switching Office (MSO) which directly send this certificate to all base-stations in each cell located in the same cluster and waiting for confirmation messages from each BS in the cluster included that the SS credentials saved in the BS memory .that is; only legitimate BS can continue the mutual authentication process, which can avoid a false, illegal deception or attack from BS to SS and enhance the timing used to authenticate this SS when move between cells.
During the time of transmission, an SS initiates the session. It sends its identifications, capabilities and other requirements to the BS. After checking the documents the BS sends back Authorization Reply to the SS. This reply must be checked whether it is from the legitimate BS or rogue BS. As the SS has no ability to check it, it can get help of a trusted third party. This third trusted party is an Authentication Server (AS) which must be in the knowledge of SS. The AS and the BS know each other as they are manufactured by the manufacturer this way. After getting the Auth Reply from the BS, the SS will send it to the Authentication Server (AS). The BS will also forward information containing its own ID, SSID and SS credentials to the AS. The AS willjudge both side information's received from the BS and the SS and return the confirmation to the SS. In this message, if SS finds that the BS is a legitimate one, it will continue its transmission. Otherwise, it will end further communication with the BS.



Step 1: SS communicates BS
Step 2: BS communicates SS and AS
Step 3: SS communicates AS
Step 4: AS communicates SS
Step 5: SS communicates BS

Figure 1: The Mutual Authentication process to avoid Rogue BS attack

The figure1 shows the new authentication protocol to avoid rogue BS. Here the BS sends back the Auth Reply message to the legitimate SS where it also includes its ID which the SS will present to Authentication Server (AS). If any attacker tries to involve the network, it will be captured by Authentication Server. However, legitimate BS will not allow any other party but the legitimate SS as it checks its ID and other credentials. DES (Data Encryption Standard) encryption can be used in all private-public key cases.

Communication with the Authentication Server:

The BS and the AS know each other from the commencement as they are manufactured this way. An AS permits only a legitimate BS and no other disturbing elements. The SS knows equally the BS and the AS so that it can verify the BS from the trusted AS. The following scenario shows the overall messaging diagram of a successful authentication transmission between a BS and an SS where both of them obtain help from the trusted third party the AS (Authentication Server). All the messages are described below in the following message exchanging diagram:

Message 1: *SS - BS: Cert (SS) (AuthReq message) | TS (Time Stamp)*
Message 2: *SS - BS: Cert (SS) | Capabilities | BCID | TS*
Message 3: *BS - SS: KUSS (AK) | SeqNo | Lifetime | SAIDList | BSID*
Message 4: *BS - AS: BSID | SSID | KUss*
Message 5: *SS - AS: E (KRss, [SSID | BSID])*
Message 6: *AS - SS: E (KUss, [Confirmation Message])*
Message 7: *SS - BS: E (Further Communication)*
Message 8: *BS – MSO E (SS credentials)*
Message 9: *MSO – BS E (Conformation Message)*
Message 10: *MSO – All BSs in the same cluster E (SS credentials)*
Message 11: *BSs – MSO E (Confirmation Message)*

Message 1: SS communicates with BS.
Message 2: SS initiates the communication presenting its own certificate and credentials named as capabilities with time stamp only to defend overflowing from thieves for the BS.
Message 3: the BS presents its own ID and other documents by encrypting with SS public key,
Message 4: the BS also sends the credentials of SS to the AS. However, the BS and the AS are established by the manufacturer and they know each other as trust equipment.
Message 5: the SS gives the credentials that it received from the BS to the AS encrypting by its own private key.
Message 6: the AS knows the SS's public key from the BS and sends back the confirmation message after observing the message.
Message 7: Protected communication starts between the SS and the BS.

Message 8: BS sends the credentials of SS to the mobile switching office as (MSO) encrypted using public key of MSO.

Message 9**:** MSO Sends back confirmation message to the base station and could be encrypted using BS Public key.

Message 10**:** MSO sends the credentials of the SS to all the base-stations in the cells located at the same cluster with the SS encrypted using the Public key of each base-station.

Message11: BSs sends back confirmation message to the MSO could be encrypted using MSO public key.

Man in Middle Attack and Denial of Service Attack Prevention:

These both attacks are omitted from this scenario. We can review that how these attacks can take place for the subscriber. When an attacker gets the initial data that a subscriber sends to the BS for the first time, the attacker may get a copy of it and tries to send the same data to the BS again and again. The BS then considers the original SS as a fake one and denies to service. But, in this proposed scenario, the attacker cannot send data the BS as there used a time stamp. Because of using time stamp, the BS will not allow any more unencrypted data from that SS. As the BS knows the SS's public key, further transmission that the BS will accept from that SS must be encrypted. And it is not an easy task for the attacker to overcome the time stamp. So, there is no man in middle attack which easily removes the possibility of denial of service attack. Since, the denial of service attack is the last part of man in middle attack in this case.

Replay Attack Prevention:

When the SS sends its ID and initial credentials, an attacker can get it and then continuously sends to the BS. The BS considers the legitimate SS as a fraud and denies. When the legitimate SS tries to connect later, the BS may block it permanently from the network. This is replay attack in which an attacker though cannot read the data of the legitimate SS but can bring the SS out of the network a time stamp is needed for it. The data type of time stamp is simply time identifying when the action, messaging or transmission takes place. Time stamps usually have fixed length validity period. A signature on some data (either in a certificate or message) that includes a specified time or period of time (length can be in milliseconds) during which a key or data is valid is called a timestamp. Any transmission or communication after this time period will not work out by the system which makes the system secure from outside attack as attackers are trying to reach when the period is over (as attacker needs time to process and retransmit).

This will inform the BS about the time and an attacker will not acquire success in his bad motivation. This procedure can be shown in the previous messages. In these messages it is shown that an SS contacts with the BS by using a time stamp. The BS also sends back its ID to the SS which is BSID (Base Station ID). The SS sends this ID to the AS to check the BS status.

4. Conclusion

In this paper, we improved process in multi-hop WiMax mutual authentication where it verified to enhance the security of subscriber to avoid fake base stations and solve the problem of handoff authentication time. The proposed algorithm shows how to establish mutual authentication. This algorithm has a better reference value and positive effect to the improvement of IEEE 802.16e standard which enhances the security and practicability in multi-hop WiMax system at the same time, system cost and calculation complexity are increased in some sort accordingly, also the overhead communication in the network will increased many times.

There are a lot of security issues remain to be solved yet. Authentication and authorization are fundamental to every wireless technology, because without strong security the technology is not comfortably utilizable. The future work is to focus on the problems in the proposed enhancement protocol when employed in a network simulator such as (OPNET or NS-2). Also security performance analysis and calculation overhead analysis must be done.

5. References

[1] Luo Wei, Guo Da, SONG Mei. The present status and development of WiMax security strategy [J].MobileCommunications, 2006,11-27.

[2] 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.

[3] Yang Weizhong, Li Tong, Hao Lin. The security risks in RSA encryption system. Journal of YunnanUniversity(Natural Sciences Edition), 2004, 26(3): 212- 215.

[4] LvJunwen, Song Tao, Si Tiange. Realization of SSL protocol by using of ECC [J].Computer engineeringand design. 2006, 27(10) :1715-1717.

[5] ShenWeifeng. ECC security strategy study in wireless LAN [J].Jiangxi Communication Technology. 2007 (1):18-20.

[6] LIU Chun, Zhang Fengyuan, Zhang Qishan. The comparison and realization between RSA and ECC algorithm based on smart cards [J].Computerengineering and application. 2007, 43(4):96-98.

[7] Li Huizhong, Chen Huifang, Zhao Wendao. The security vulnerability and solution in IEEE802.16 [J].Modern telecommunications technology.2005(1):26-27.

[8] TIAN Haibo, PANG Liaojun, WANG Yumin. Key Management Protocol of the IEEE 802.16e[J]. WuhanUniversity Journal of Natural Sciences.2007, 12(1):59- 62.

[9] David Johnston, Jesse Walker. Overview of IEEE 802.16 Security [J]. IEEE Security and Privacy, 2004, 2(3):40-48.

[10] SenXu, Manton Matthews, Chin-Tser Huang. Security issues in privacy and key management protocols of IEEE 802.16[C]. Proc. of the 44th annual Southeastregional conference. New York: ACM Press, 2006. 113-118.

[11] 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

[12] 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