ISSN:0975-9646
Pranita K. Gandhewar et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (3) , 2011, 1309-1311

Performance Improvement of IEEE 802.16 / Wimax Using Elliptic Curve Cryptography

Pranita K. Gandhewar, Kapil N. Hande
Computer Science & Engineering Department
G. H. Raisoni College of Engineering Nagpur, India

Abstrac-: **The IEEE Standard 802.16 (WiMax) promises to provide wireless broadband access to homes, businesses and core telecommunication networks worldwide. However, security is a key concern to the success of IEEE Standard 802.16. Wireless networking is not as secure as other networking technologies. But IEEE 802.16 provides much higher security as compared to other wireless technologies, such as IEEE 802.11 (Wi-fi). IEEE 802.16 provides several security mechanisms, which provides more security by protecting the network against unauthorized access. Many paper provides the security improvement mechanism for WiMax. Many sophisticated authentication and encryption techniques have been embedded into WiMAX but it still exposes to various attacks. This paper provides a mechanism for increasing the efficiency & hence improves the existing model.**

Keywords- **IEEE 802.16, Wi-Max, Security, Authentication, Authorization, Encryption, RSA, ECC.**

I. INTRODUCTION

IEEE 802.16 is also known as WiMAX (Worldwide Interoperability of Microwave Access). WiMAX basically operates on two layers: physical layer (PHY) & MAC layer. MAC layer has three sub-layers, convergence sub-layer, common part sub-layer & security sub-layer. Security is a key concern to the success of IEEE 802.16. IEEE 802.16 security specification can mainly be found within the MAC layer as it consists of security sub-layer [5]. Security sub-layer provides authentication, secure key exchange, encryption and integrity control across the BWA system.

In the 802.16 standard, encrypting connections between the MS and the BS is made with a data encryption protocol applied for both ways. An encapsulation protocol is used for encrypting data packets across the BWA. An authentication protocol, the Privacy Key Management (PKM) protocol is used to provide the secure distribution of keying data from the BS to the MS [4]. Through this secure key exchange, due to the key management protocol the MS and the BS synchronize keying data. The basic privacy mechanisms are strengthened by adding digital-certificate-based MS authentication to the key management protocol. In addition, the BS uses the PKM protocol to guarantee conditional access to network services [1]. The encryption algorithm used at MAC layer in the existing model is the RSA algorithm. In the proposed model, we use ECC (Elliptic Curve Cryptography) algorithm.

The main objective of this paper is to enhance the security & improve the performance of the BWA system by using ECC algorithm instead of RSA. There are many advantages of using ECC over RSA. The main advantage of using ECC is that it provides same level of security as that of the RSA at lower key size. Lower key size requires less memory as well as less bandwidth. As it uses lower key size the time required to compute the ECC key is also minimum. Low computation time consumes low power & hence requires low computational power. Also the time required to break the ECC key is much higher than the time required to break the RSA key.

Section II gives the brief overview Security Associations. Existing security model of IEEE 802.16 is given in section III & the proposed model is explained in the section IV. Finally, conclusion is given in the section V.

II. SECURITY ASSOCIATIONS

A Security Association (SA) is defined as the set of security information shared between a BS and one or more of the MSs connected to that BS in order to support secure communications across the WiMAX to access network. SA provides a set of security information by which secured communication can be established. By means of the SA a MS is authorized for a WiMAX-service.

Security associations (SAs) maintain the security state relevant to a connection. IEEE 802.16 uses an identifier known as security association identifier (SAID) SAID is a 16-bit identifier which uniquely identifies SA. SAs are managed by the BS. When authentication event takes place the BS gives the MS a list of security association associated with its connection.

IEEE 802.16 uses two types of SA: data SA & authorization SA, but explicitly defines only one i.e. data SA, which protects transport connection between one or more MSs & one BS [2].

The data SA consists of following components:

- A 16-bit SA identifier (SAID)
- Two traffic encryption keys (TEKs) for data encryption
- Two 2-bit key identifier one for each TEK
- TEK lifetime
- A 64-bit initialization vector (IV) for each TEK
- Encryption Algorithm (DES in CBC mode or AES in CCM mode)
- H-MAC digest
- Types of data SA (primary, static or dynamic)

There are three basic types of data SAs: Primary, Static & Dynamic [3]. Generally MS has a primary SA for its secondary management connection & two more for the downlink & uplink links. Management & data transport connections are mapped to these SAs & secured according to the security mechanisms defined in SAs. Static SAs are provisioned within the BS. They are only initiated if the MS intends to use a new service & are dynamically terminated when data transfer in the service ends. Dynamic SAs are created & deleted as required in response to the initiation & termination of specific service flow. These are dynamically

generated by the BS & provided to the MS. Both the static & dynamic SAs can be shared by multiple MS.

Authorization SAs are responsible for authorization of the MS. They are used by the BS in order to establish the Data SA between BS and MS.

The authorization SA consists of the following components:

- X.509 digital certificate identifying the MS
- 160-bit authorization key, which is generated by the BS & used for the generation of key encryption key (KEK) & calculation of H-MAC digest.
- A 4-bit AK identifier
- 32-bit AK lifetime
- 128-bit KEK, used by the BS to encrypt the TEK
- A downlink HMAC key
- An uplink HMAC key
- A list of authorized data SA

III. Fundamentals of Existing Security Model

Existing Security model consists of three phases, namely MS authorization, Exchange of key material & Encryption of data traffic [3]. This is shown in the following fig. 1.

In the first phase, MS first sends the authentication information message to the BS. This message includes the X.509 certificate of the MS. MS sends this message to the BS for requesting the connection with the BS. Immediately after the authentication information message, MS sends the authorization request message to the BS to get the authorization key (AK) from the BS. This message consists of X.509 certificate, SAID which is unique for each primary SA, & security capabilities. Security capabilities are nothing but a description of the encryption algorithm supported by the MS. Here in the existing model, it is RSA encryption algorithm. When BS receives this message, it first verifies the certificate of the MS. If it is valid, BS generates the authorization key, otherwise authorization will be rejected. After generating the authorization key, BS sends the authorization reply message to the MS. This message includes authorization key encrypted with the RSA public key of MS, Authorization key sequence number, lifetime of authorization key & X.509 certificate of the BS. The MS & BS then calculates the key encryption key (KEK) & the HMAC key using the authorization key (AK). These two keys are then used for the TEK key exchange phase.

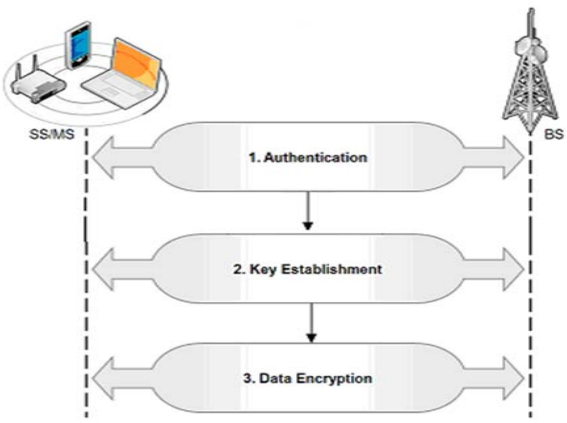

Fig. 1: 802.16 Secure Communications

In exchange of key material phase, the exchange of TEK will be initialized. TEK i.e. traffic encryption key is required for the encryption of the data that is to be transferred between MS & BS. TEK is generated by the BS randomly. In this phase, the MS first sends the TEK request message to the BS requesting the key material. This message includes, SAID which is unique, AK sequence number using which BS can determine which HMAC key should be used for generating the HMAC digest, & HMAC digest, which ensures that MS & BS posses same authorization key. BS receives this message from the MS & checks the validity of the HMAC digest. If it is valid, BS sends the TEK reply message to the MS. TEK reply message includes the authorization key sequence number, SAID, traffic encryption key, TEK lifetime & the HMAC digest.

Now, MS & BS both have the TEK. Finally in third phase, the MAC PDU has been encrypted with the TEK. While encrypting the MAC PDU, MAC header & the optional CRC checksum is not involved [6].

IV. Proposed Security Model

The proposed security model is shown in fig. 2. As in the existing security model, when MS wants to connect to the BS, MS sends an authentication information message (Authentication Info Msg). This message contains vendor certificate of the MS serving BS to examine trustworthiness of the MS.

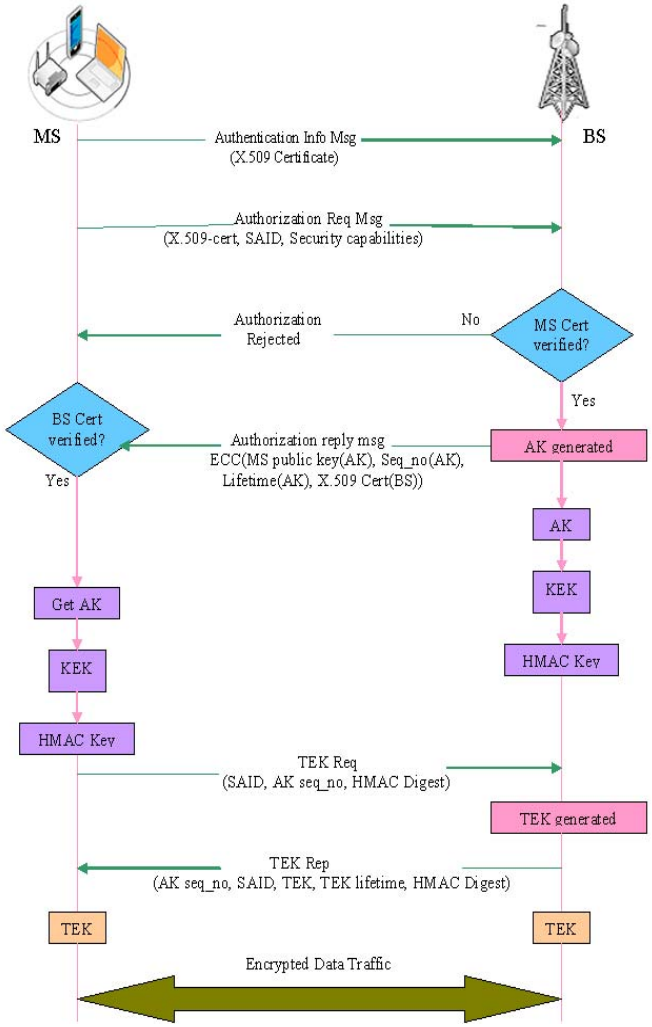

Fig. 2: Proposed Security Model

As soon as authentication information message is sent to the BS, MS sends authorization request message (Authorization Req Msg) to the BS requesting the authorization key (AK). Authorization request message contains:

- MS certificate
- SAID
- Security capabilities.

When BS receives an authorization request message, it verifies the MS certificate. If the certificate is not legal then authorization rejected & if it is legal, BS generates the AK & sends an authorization reply message (Authorization Rep Msg). This message includes:

- AK encrypted with ECC public key of MS
- 4-bit sequence number
- Lifetime of AK
- X.509 certificate of BS

The proposed security model uses Elliptic Curve Cryptography (ECC) algorithm for encryption. At this step BS also calculates the KEK & HMAC key (for downlink & uplink). When MS receives an authorization reply message, it verifies the BS certificate. If it is valid, it extracts the AK from the message & calculates the KEK & HMAC key (for downlink & uplink).

After successful authentication, next step is to initiate the key exchange phase. In this phase, MS first sends the TEK request (TEK Req) to the BS. This message includes:

- SAID
- AK sequence number
- HMAC digest

When BS receives this message, it first validates the HMAC digest. If it is valid, BS generates the TEK & sends the TEK reply (TEK Rep). TEK reply message contains:

- SAID
- AK sequence number
- TEK
- TEK lifetime
- HMAC digest

When key exchange phase is successfully completed, the MAC PDU that is to be transferred between MS & BS is encrypted with the TEK excluding MAC header & CRC checksum.

V. CONCLUSION

The existing security model uses RSA algorithm for encryption, while the proposed security model of IEEE 802.16 uses Elliptic curve cryptography (ECC) encryption algorithm. ECC uses smaller key size as compared to RSA. The encryption strength of both the algorithms is same, but key size matters. We know that the devices in the wireless network are battery driven. Using smaller key, we require low computational time, low computational power & small memory. As it requires low computational power, the battery life will get increases.

REFERENCES

[1] Ayesha Altaf, M.Younus Javed & Attiq Ahmed, "Security Enhancements for Privacy and Key Management Protocol in IEEE 802.16e-2005", Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2008.

[2] David, Johnston and Jesse Walker, "Overview of IEEE 802.16 Security", IEEE Computer Society, 2004 IEEE.

[3] Evren Eren, "WiMAX Security Architecture – Analysis and Assessment", IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 6-8 September 2007.

[4] Mitko Bogdanoski, Pero Latkoski, Aleksandar Risteski, Borislav Popovski, "IEEE 802.16 Security Issues: A Survey", 16th Telecommunications ForumTELFOR 2008, November 25-27 2008.

[5] Ms. Pranita K. Gaandhewar & Prof. Kapil N. Hande, "A Survey on IEEE 802.16: Security Threats & Solutions", 2011 International Conference on Network Communication & Computer, 21-23 March 2011.

[6] Rakesh Kumar Jha, Dr. Upena D. Dalal, "A Journey on WiMAX and its Security Issues", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 1 (4) , 2010, 256-263, 2010.