2009 International Conference on Computer Technology and Development

# Performance of WiMAX Security Algorithm
## *(The Comparative study of RSA Encryption Algorithm with ECC Encryption Algorithm)*

Masood Habib, Tahir Mehmood, Fasee Ullah, Muhammad Ibrahim
Department of Computer Science & IT
Shaheed Zulfikar Ali Bhutto Institute of Science and Technology
Islamabad, Pakistan
masoodshalmani@gmail.com, tahir@szabist-isb.edu.pk, faseekhan@yahoo.com, ibrahimislamian@yahoo.com

***Abstract*—IEEE 802.16, known as WiMax, is at the top of communication technology drive because it is gaining a great position in the next generation of wireless networks. Due to the evolution of new technologies wireless is not secured as like others networking technologies. A lot of security concerns are needed to secure a wireless network. By keeping in mind the importance of security, the WiMax working groups has designed several security mechanisms to provide protection against unauthorized access and malicious threats, but still facing a lot of challenging situations. An authentication and authorization model provides protection for a network or technology and protects its resources from unauthorized use. This paper examines the threats which are associated with MAC layer and physical layer of WiMax and also proposes some enhancements to the existing model for improving the performance of the encryption algorithm. The paper proposes some techniques in the existing model to enhance its functionality and capability. Simulation is done using Qualnet4.5 simulation tool and the results are given at the end.**

***Keywords- Wireless networks; WiMAX 802.16; Authentication; Authorization; Security mechanisms.***

## I. INTRODUCTION

Security of a network plays a key role in the performance of a network. Security is more important than ever before due to many reasons. When a network is implemented poorly, security threats and attacks always exist. But if that network is made fully secure by implementing high level of security, there will be a fewer amounts of security threats. Applying security to a network is too much costly than its advantages. Both Network operator and the network user are playing a key role in the security providence to a network and are concerned over network security.

There has been great evolution in wireless communications over the last few years. The wireless communication is so much open to threats. Radio transmission should be made secure so that the communication becomes secure. WiMax is an emerging wireless technology used for deploying broadband wireless metropolitan area network (WMAN) [1]. WiMax technology offers many features with a lot of flexibility and has replaced many of the existing telecommunication technologies. Not only does 802.16/WiMax provide network access anytime anywhere, but it also offers higher speed at longer distances. A lot of security concerns are needed to secure the end users, the core network, the application servers, and everywhere in between. Strong security mechanisms are needed for WiMax to secure it from vulnerabilities and threats. Because the security mechanisms used by old technologies are not applicable for new technologies.

By keeping in mind the vulnerabilities and threats to 802.16e/WiMax that arises during the authentication and authorization phase, this paper proposes the some improved techniques for the performance & security. These techniques will be more secure, more reliable, and also will save time and space.

Section II gives an overview of IEEE 802.16; we briefly describe existing security model in Section III and proposed enhancements in the exiting model are discussed in Section IV. Section V describes security mechanism of the proposed model while in the section VI the Comparison between both models is discussed. Finally we conclude in Section VII. In last references are given.

## II. FUNDAMENTALS OF WIMAX

WiMax is an emerging broadband wireless last mile technology to provide higher speed at longer distances from 30 to 50 miles and its transfer rate is up to 70 Mbps.

Initial version of the 802.16 standard was operating in 10-to-66-GHz [1], [2], [3] providing line-of-sight connectivity and supports data rate up to 134Mb/s. The other standard 802.16a provide non line-of-sight transmission and provide lower frequency band (2 to 11 GHz). These two classes of WiMAX systems are fixed WiMax and mobile WiMax. Fixed WiMax provide fixed services while the mobile WiMax provides mobility. IEEE designated standards for fixed wireless applications as 802.16-2004 and 802.16e-2005 for mobile WiMax. The latest 802.16 standard adds support for mobility of SS (Subscriber Station). So when there is mobility the threats and attacks also increases. According to [4] Additional 802.16 standards are in the works and will cover:

- *802.16b — Quality of service,*
- *802.16c — Interoperability, with protocols and test-suite structures,*
- *802.16d — fixing things not covered by 802.11c, which is the standard for developing access points,*

*802.16e — Support for mobile as well as fixed broadband.*

802.16/WiMax operates on two layers, the physical (PHY) layer and the Media Access Control (MAC) layer. Threats are always there to both layers. But the physical

978-0-7695-3892-1/09 $26.00 © 2009 IEEE
DOI 10.1109/ICCTD.2009.192

layer is much vulnerable to threats as compared to MAC layer. The physical layer (PHY) handles signal connectivity, error correction, initial ranging, registration, bandwidth requests, and connection channels for management and data. The MAC layer manages connections and security [5].

Physical layer is below the security sub layer, that's why the physical layer is open to the threats. The threats to the physical layers of WiMax are *scrambling* [6] and *jamming* [6]. The security implemented at the MAC layer has several shortcomings especially with respect to Authentication and confidentiality. The serious threats are to the level of authentication. While establishing new connection many problems arise regarding the authentication level and also to authorize the authenticate person. Many of the security problems are solved but still some attacks are not yet been countermeasure, and new attacks are taking birth on daily basis may be on hourly basis.

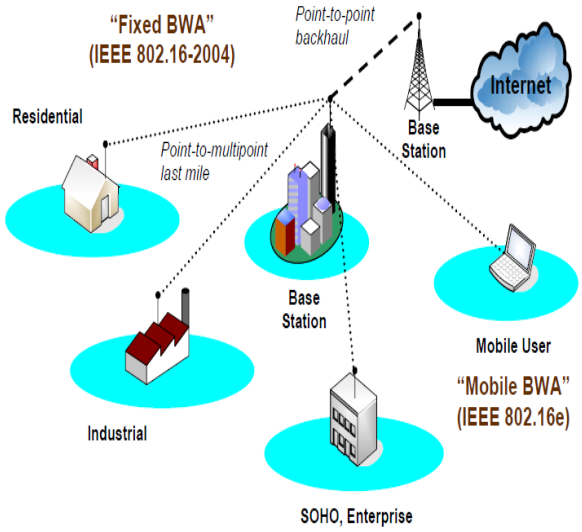


Figure 1. WiMax Applications [8]

In WiMax applications, there is a Base Station (BS) and multiple Subscriber Stations (SSs). The connection between the Base Station (BS) and the Subscriber Stations (SSs) may be Point-to-Point or may be Point-to-Multi Point. IEEE 802.16 Point-to-Multi Point (PMP) mode is a networking infrastructure where every SS (Subscriber Station) communicates directly with the BS.

## III. EXISTING SECURITY MODEL

The purpose of WiMax network is to expand the range and access of wireless systems. The existing security model is about the security association and security keys generation or establishment when the MS is entering the network range of a BS. The Model shows the main key elements as entities and the relation ship between them is also shown. Three types of security associations are sketched in the model namely primary, static and dynamic. These three security associations are types of data SA (Security Association). WiMax architecture uses different mechanisms, to establish a secure communication between BS and MS. Security Associations (SAs) are used by both MS and BS to establish a new connection. A Security Association (SA) is defined as the set of security information shared between a BS and one or more of the MS's connected to that BS in order to support secure communications across the WiMax access network [7]. There are two main types of security association; first one is Data Security Association and second is Authorization Security Association. Data SA is further divided into three types, namely Primary SA, Static SA and Dynamic SA. Each MS has one primary SA, and primary SA is established when the MS is initialized. The Static SA is created when the BS initializes the MS. And the last SA, Dynamic SAs are dynamically generated by the BS and are used for transport connections when needed. Second type of Security Association is Authorization SA which is used for the authorization purposes. The BS uses the Authorization SA to establish the Data SA between MS and BS. Other entities shown in Figure 2 are AK (Authorization Key), X.509 certificates, HMAC etc. X.509 certificate is held by the MS, the public key of the MS is present in its digital certificate, which is used for access control, authentication and confidentiality. MS uses it public key for communication with the BS. When authenticated the MS sends an authorization request message to the BS, the BS generates an AK (Authorization Key) having a sequence number and a life time and passes it to the MS in an encrypted form with public key of MS having sequence number 0-15. The hashing technique used in this model is HMAC which is not providing replay protection. Another key which is KEK (Key Encryption Key) used for encryption purpose. The KEK and HMAC both are calculated from the AK. In last the TEKs are generated and KEK encrypt these TEKs at the time of TEK request reply. When the TEK is obtained the exchange of data or information is started and communication is established [3].

## IV. PROPOSED ENHANCEMENTS IN THE EXITING MODEL

Due to some complexities in various models of WiMax networks, security has been more stringently placed into WiMax. It is the responsibility of the network service provider to develop comprehensive security strategies for designing a secure network. Otherwise, the network and the users will become vulnerable to threats and hackers. To study the security of WiMax we have to understand the primary protection methods of WiMax security.

In the existing model some of the enhancements are done to enhance the performance and security of the model. For this purpose some mechanisms are proposed in the existing model by keeping in mind their level of security and functionality. The model is based on the communication of BS and MS. And the main theme of this model is security. When an MS enters the network range of a BS, the SS and BS communicate with each other to provide authenticity and to authorize one another. The model is subdivided into three phases. 1st Phase discus the Data security association, Authorization security Association (SA) is in 2nd phase while the 3rd phase is about the Exchange of KEYS.

### A. *Data Security Association*

Before starting the connection process the MS uses the Data SA to communicate for connection request. Three types of data Security Associations are shown in the model namely Primary SA, Static SA and Dynamic SA. Data SA has a 16 bit SA identifier SAID, a cryptographic cipher identifier, which uses Data Encryption Standard (DES) in CBC mode for protection of data during transmission. Also have two TEKs (Traffic Encryption Keys), one is used as current operational key and the other as TEK. A 64 bit initialization vector (IV) is used for each SA. The life time of the TEK is from 30 minutes to 70 days. Generally an MS can have two or three SAs (Security Associations).

### B. *Authorization Security Association*

Authorization SA is used for authentication purpose, to provide authentication between MS and BS. In 802.16e/Mobile WiMax there is mutual authentication, so the BS will authenticate the MS and the MS will also authenticate the BS. The Authorization SA consists of an AK (Authorization Key) of size 60 bits, having a life time range from 1 to 70 days. The default life time value of an AK is 7 days. Another key KEK (Key Encryption Key) is also used having a size of 112 bits 3DES key, the KEK is used for the distribution of TEKs. An authorization SA also uses hash functions to provide authenticity between MS and BS. [9] States that BS use Authorization SAs to configure Data SAs on the SS (Subscriber Station).

In the original model the X509 certificates are send to the BS by the MS but here in the proposed model the usage of X509 certificate are changed and WTLS certificate is used instead of X.509 certificate. WTLS reduces the space occupied by the X509 certificates because it has a small serial number and issuer unique ID etc. Another change regarding the original model is the changing of the encryption algorithm, ECC (Elliptic Curve Cryptography) is used instead of RSA (Rivest, Shamir, and Adleman) encryption. RSA using 1024 bit of key but on the other side ECC is using only a key size of 163 bits and having the same encryption strength as compared to the RSA. So here the memory is saved due to small key size. The hashing function used in the existing model is HMAC (Hash function-based Message Authentication Code) but OMAC (One-key CBC MAC) can also be used for the hashing purpose. This OMAC algorithm is extremely simple, and has proven to be quite secure against replay attack.

### C. *Exchange of KEYS*

To encrypt the data a key is needed known as TEK which uses AK (Authorization Key). The Message Authentication Key (HMAC Key) and the KEK are derived from the AK by the BS and MS individually. The TEK is generated by BS after the request of MS from the BS and is sent in an encrypted form to the MS. The TEK is encrypted by 3DES having 112 bits KEK or AES (Advanced Encryption Standard) is used for the encryption purpose using 128 bits KEK. The Authentication of Key Exchange message is done by HMAC hashing technique. At last the communication is established and the exchange of information is started in a secure way.

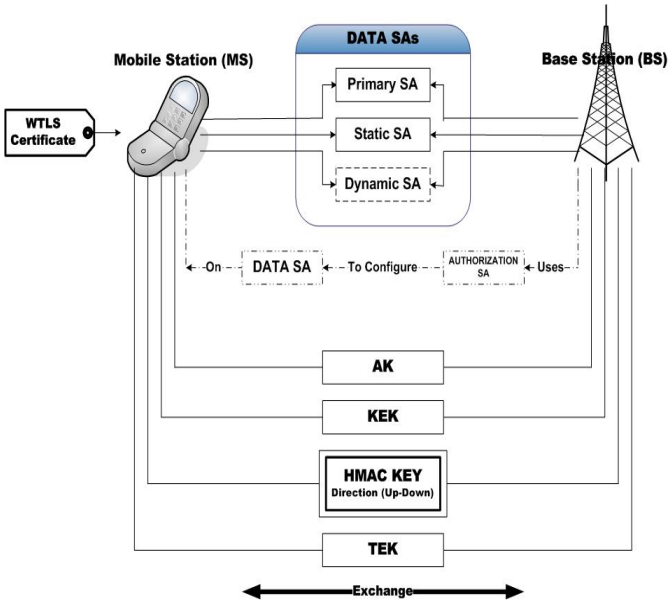


Figure 2. Proposed Model general view

## V. SECURITY MECHANISM OF THE PROPOSED MODEL

The communication between the BS and MS takes place in steps. Security Association, Authorization, Authentication and lastly the data encryption are followed in a sequence. In fixed WiMax, unilateral authentication is followed where BS authenticate the MS only, means one sided authentication but in mobile WiMax the technique for authentication is mutual authentication where BS authenticate MS and MS authenticate BS. The communication steps are given by.

**Step 1:** In order when an MS wants to connect to a BS, initially the MS sends an Authentication Information Message to the BS which includes its certificate as: **MS→BS**: Cert MS. The MS cert is the WTLS certificate; firstly the BS validates the certificate optionally just to examine the trustworthiness of the MS (Mobile Station).

**Step 2:** In the second step the MS will send an authorization request message to the BS for the Authorization Key (AK) and also for identifying the security association between them. The request consists of the WTLS certificate, a SAID (Security Association Identification), security algorithm to define security capabilities. **MS→BS**: Cert MS, SAID, Capabilities. Now the BS will check the Validity of the MS by examining the MS certificate. In response of this message two conditions may occur if the MS is a legitimate one then ok, but if the MS's identity is not legitimate then the BS sends a reject message to the MS and discard the communication.

**Step 3:** When the MS passed the identity phase, then in third step the BS generates an authorization key (AK) and send an authorization reply message to the MS. The authorization reply message contains, Authorization Key

(AK) encrypted with the MS public key, AK life time, sequence number of the AK, also sends the BS's WTLS certificate to verify it and complete the phase of mutual authentication. In the authorization reply message the encryption is done by using Elliptic Curve Cryptography (ECC). In the original model it was RSA. The Authorization reply message will be. **BS→MS**: ECC-encrypt (MS public key (AK)), Seq_No (AK), life time (AK), SAlist (MS), Cert (BS). Now when the MS got the message from the BS it can validate the authenticity of the BS by validating its certificate. If verified so it get AK if not verified then end the communication process. After getting the AK both the BS and MS calculate the KEK and the Hashing technique from the AK. Hashing technique used is Hash function-based message authentication code (HMAC).

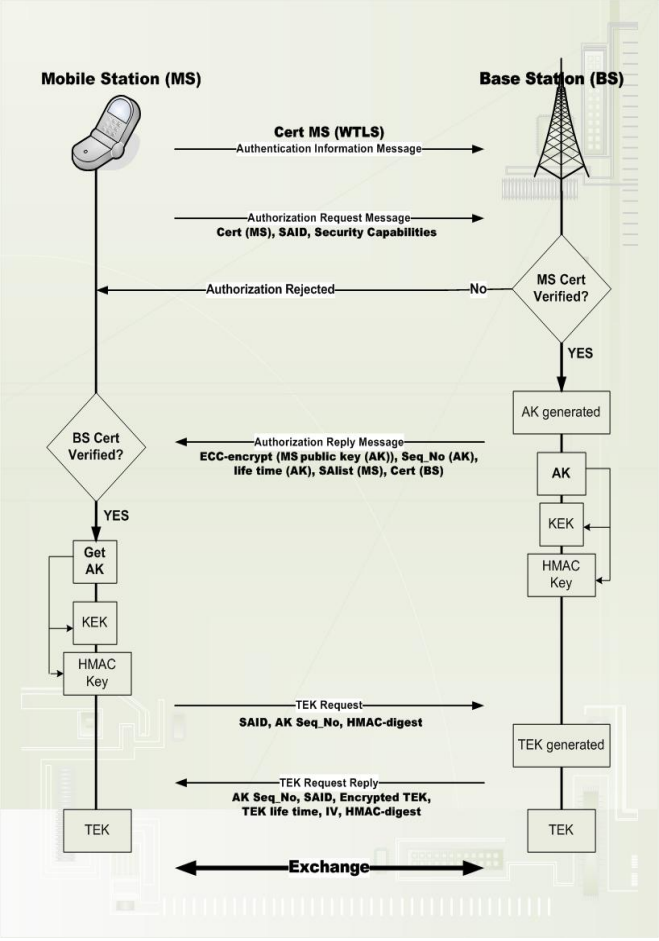


Figure 3. Security Mechanism of the Proposed Model

**Step 4:** The forth step deals with the Traffic Encryption Key (TEK) exchange which is used for the encryption of the data. The MS sends a Key Request message to the BS, which is the first message for requesting key for encryption. This message contains AK sequence number, a security association identifier (SAID), and the HMAC-digest used for the key request to check the integrity. **MS→BS**: SAID, AK Seq_No, HMAC-digest.

**Step 5:** The BS generates the TEK after getting the TEK request message from the BS and sends a TEK request reply message to the MS and sends the TEK to the MS, the MS will use the TEK for the encryption of the data. **BS→MS**: AK Seq_No, SAID, Encrypted TEK, TEK life time, IV (Initialization Vector), HMAC-digest. So when the MS got this reply message it decrypts the TEK and finally has a TEK. Now both the MS and BS got the TEK.

**Step 6:** when the TEK is exchanged between the MS and the BS, a security communication is established between the two parties, the MS (Mobile Station) and the BS (Base Station). For encryption the DES in CBC mode and AES in CCM mode are used to avoid attacks and errors regarding the data. And at last the exchange of information is started.

## VI. COMPARISON OF BOTH SECURITY MODELS

The purpose of WiMax network is to expand the range and access of wireless systems. The existing security model is about the security association and security keys generation or establishment when the MS is entering the network range of a BS. The original model uses primary SA, Static SA and Dynamic SA at the start. In the proposed model shown in Figure 2, the Security associations are the same. Both models are using Authorization Key (AK) for authorization purpose. Other entities like KEK (Key Encryption Key) and the TEK are the same as in the original model. Just few of enhancements are done in the existing model to save memory, to get fast communication and to communicate securely.

In the original model the MS uses X.509 certificates for authentication purpose. X.509 certificate is held by the MS, the public key of the MS is present in its digital certificate, which is used for access control, authentication and confidentiality. We have proposed the WTLS certificate instead of X.509 Certificate. The main difference between a X.509 certificate and a WTLS certificate is that WTLS has reduced size and also the processing speed, required in order to better go with the constraints imposed by narrowband radio link and the processing capacity in mobile equipment. The size of the serial number and issuer ID etc are reduced in the WTLS certificate as compared to X.509 certificate, which helps to avoid the usage of extra memory and save store memory. The original model is using a hashing technique named HMAC to make a secure communication but it doesn't provide replay protection so here OMAC (One-Key message authentication code) which is an efficient hashing technique than HAMC can be also be used.

In the Authorization phase the original model use RSA encryption algorithm for encryption which is having a key size of 1024 bits, but if we use the ECC (Elliptic Curve Cryptography) encryption method instead of RSA because the of having a small key size than RSA. The encryption strength of both the techniques is the same but the key size matters so we propose the ECC encryption technique in our model as shown in Figure 3.

## VII. SIMULATION STUDY

We used QualNet 4.5 simulator tool for our simulation. The simulation scenario consists of a Base Station (BS) and two mobile stations (MS's). One mobile node is in the range of the BS and is attending a call then came to idle mode. Another Mobile Station (MS) is entering the range of the BS, which shows the initial communication (The Authorization Phase) between the BS and the MS. The general parameters of the simulation scenario are given in the Table 1.

TABLE I. GENERAL SIMULATION PARAMETERS

| PARAMETERS | VALUES |
|---|---|
| Encryption Rate | 500 Kb |
| Number of Nodes | 3 |
| Simulation Time | 3 min |

As we have used ECC (Elliptic Curve Cryptography) having a key size of 163 bits as an alternative of RSA which have a key size 1024 bits for encryption in our model.

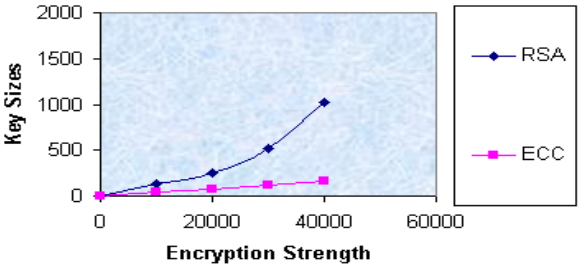


Figure 4. Key Size and Encryption Strength of RSA and ECC

The encryption strength of both the techniques is the same but the key size matters. The description is shown in Figure 4. In the given figure we can see in detail that the key size of ECC is much smaller than that of RSA but having the same encryption strength. So the result may show that the cracking of both the techniques will take the same time.

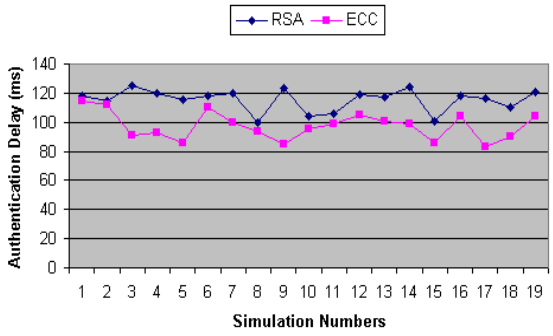


Figure 5. Delay using RSA and ECC

We construct two duplicate scenarios, one uses RSA and other one uses ECC for Authorization in Authentication phase. Figure 5, shows the delay in authentication phase in both the scenarios.

We run the simulation scenario for 19 times and From the results we conclude that ECC has less delay than RSA while having a smaller key as compared to RSA as shown in Figure 5. In the scenario we have compared two different techniques to choose the best of both and we concluded that ECC is better than RSA.

## VIII. CONCLUSION

If we want to achieve End-to-end secure communication then the security has to be kept in mind. WiMax is designed with a lot of security mechanisms to make it secure form the threats, but still not so secure from threats. We can countermeasure these attacks by using wireless protocols and strong encryption techniques.

We have proposed some enhancements to the existing model to improve its capabilities and encryption strength for security. The comparison of the RSA and ECC was done and we conclude that ECC is much better that RSA having a smaller key size (163 bits) than RSA which is 1024 bits. The delay was calculated and the delay in ECC was smaller than RSA. Another change that was done by changing the X.509 certificates is also competent because the WTLS certificates will help us to reduce the memory storage. More research is needed in this area to enhance the performance and security measures.

## REFERENCES


[1] William C. Y. Lee, "Wireless and Cellular Telecommunications" Third Edition, Chapter 7.

[2] M. Nasreldin, Heba Aslan, M. El-Hennawy, A. El-Hennawy, "WiMax Security" International Conference on Advanced Information Networking and Applications 2008, IEEE.

[3] Michel Barbeau, "WiMax/802.16 Threat Analysis" ACM Int. Workshop on Quality of Service & Security in Wireless and Mobile Networks, Q2SWinet '05, October 13, 2005.

[4] Deepak Pareek "WiMax Taking Wireless to the MAX" By Auer Bach Publications, Taylor & Francis Group Boca Raton New York, 2006

[5] Prof. Dr. Ing. Evren Eren, Prof. Dr. Ing. Kai-Oliver Detken "WiMax-Security – Assessment of the Security Mechanisms in IEEE 802.16d/e"

[6] Mahmoud Nasreldin, Heba Aslan, Magdy El-Hennawy, Adel El-Hennawy, "WiMax Security" International Conference on Advanced Information Networking and Applications 2008, IEEE.

[7] White Paper "Mobile WiMax Security" by Airspan Networks Inc. 2007.

[8] Dr. Kitti Wongthavarawat "IEEE 802.16 WiMAX Security" *Presented at 17th Annual FIRST Conference, Singapore July 1, 2005*

[9] Jamshed Hasan "Security Issues of IEEE 802.16 (WiMax)",2006