A Security Architecture for Wimax Networks

Shahid Hussain
SZABIST Islamabad Pakistan

Muhammad Naeem Khan
SZABIST Islamabad
Pakistan

Muhammad Ibrahim
E-lecturer virtual University

ABSTRACT
Wimax is one of the fast growing technologies in the world as compare to other wireless networks. IEEE has defined standard IEEE 802.16 for Wimax. Wimax growing rapidly due to the services it's provides and long range accessibility, but still Wimax facing a lot of security issues and threats like jamming , DDOS , Rogue Base station attack ,Reply Attack and so on.Wimax furnish different security mechanism for unauthorized access ,Encryption, Authentication etc. and several security architecture , mechanism areproposed. But still Wimax is under attack like Rogue Base station Attack And Reply Attack.so in this paper we proposed a new and unique security model and Encryption technique on the basis of existing model to secure Wimax from Rogue Base station Attack and reply attack. We perform the simulation through NS-2

Keywords
Authentication, Authorization, EAP, RSA,ECC(Elliptic curve cryptograph), Rogue Base station etc.

1. INTRODUCTION
Wimax is a Wide area wireless network standard. IEEE 802.16 has the capability to provide high speed Internet access to village's areas and other locations not in the range of Wired Networks. Wimax provide high speed up to 70 Mbps over the area of 30 mile. It's also an alternative to satellite Internet services. IEEE 802.16 standard called Wimax is a broadband wireless access metropolitan area network which also sometimes called wireless MAN[8]. Wimax is different in performance speed and area covariance. IEEE 802.16 is a new technology and not deployed yet widely because of the security threats the Wimax networks facing, but now a day the Wimax networks are the more focusing area for the research because of the services it's provides. So security is the main issue for Wimax technology. There are two main entries in Wimax which are attacked by the intruder Subscriber station (SS) and Base station (BS).In wireless network and Wimax there are different types of attacks. Discuss a little bit these terms Repudiation, Fabrication, Modificationand interceptionbut our focus is Reply attacks and Rogue Base station attacks. [1]A rouge Base station attack is a type of attack in which the attacker station that imitates a legitimate Base station and this occur due to the inadequate of Two way Authenticationmechanism between the Base Station and Subscriber Station and due to no verification of Base Station [2]. So to overcome the problems Wimax networks facing especially inthe area of security to tackle these attacks efficiently, we have worked on the existing security architectures for the Wimax and find out the drawbacks of these architectures, also discuss these drawbacks briefly and finally proposed a new model for the Wimax networks to tackle the problem of Rough Base station and Reply attacks.

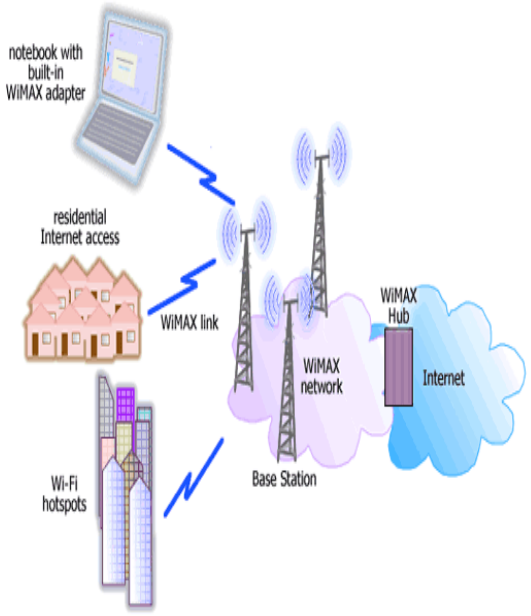

Figure 1. A Sample Wimax Network

2. AN OVERVIEW OF THE PAST WORK RELATED TO WIMAX SECURITY
Up to now different architectures have been proposed, which used different technique forWimax networks security. Raheel *et al* proposed [3] a concise model for fixed and mobile Wimax to enhance the security of network and authentication protocols. In this proposed architecture the author's shows a focus onto improve the Wimax security and to overcome the vulnerabilities in the authentication protocols. Theyhave analyzed several currently deployed techniques for the security of Wimax and cover both the secure communication as well as the risk analysis mechanism. The exiting models have also several drawbacks and the author's [4] work on the existing security architecture for Wimax. Threats to wimax network have been analyzed and discuss various classes of wireless attacks on Wimax. They also discuss several wireless security protocols for the Wimax security i.e. WEP,EAP etc and its working mechanism. They also provide a solution for these threats to some extent. Another proposedmodel for Wimax security is a trusted scheme for the identity of Wimax. [5] This architecture have three layers,Evaluation layer , Authentication layerand Identity layer. In Identity layer only identity is assign to each entity secondly trusted attributes of each entity is spread in Evaluation layer and lastly the Authentication layer can judge the results which comes from Evaluation layer. For security point of view the scheme can preclude the unlicensed terminal access, unlicensed user access, unlicensed BS attacks and message modification.

They have tackled each of these functions at a different layer of the model, which also increase the security of the system, but by this way the performance of the system decreases. Author's Masood Habib el al have proposed security architecture on the basis of existing security model. The enhancement is done on the basis of performance and security. The purpose of new model [6]is based on communication security between the BS and MS. The original model divides into three phases. In the first phase they discuss (DSA) Data security Association,(ASA) Authorization security association are in the second phase while the key exchange between BS and MS are in the third phase. The detail comparison is shown between the original model and proposed model. The existing model uses primary security Association (PSA) Static SA and Dynamic SA while the propose model the Security Association are the same but have done some amendments in the original model to get fast communication, securely and Save memory. For Authentication purpose the Existing model uses X.509 certificate for MS. Access control, Authentication and confidentiality X.509 certificate are sustain by the Mobile station while Digital certificate the public key of MS are present. The propose model uses Warless Transport Layer Security certificate in place of X.509 certificate. WTLS are different fromX.509 certificate because WTLS have the property to decrease the size and processing. Another advantage of WTLS is that it save memory and avoid extra memory. Another main change in the original Hashing Technique. The original model uses HMAC hashing technique which is not Reply protected while the propose model uses One key Message Authentication Code (OMAC), from the comparison it is concluded that OMAC is more efficient hashing technique than HMAC. Another architecture for the Wimax networks [7],authorization key management exchange scheme from Base Station to subscriber station. The main issue discussed here is authorization key (AK) generation by authorization protocol because the subscriber station (SS) must always trust that the Base station each time generate a new key which is different from the previous generated key there must be need perfect random number generator to enable both the SS and BS to solve the AK problem. They point out that, there are various issues in key management exchange scheme, The size of TEK Identifier Which Leads to Reply Attack to solve this problem the size of TEK must be increased for Secure communication. They also propose solution for it to use AES for encryption instead of DES. They discuss different security services and its procedure to achieve it but the main focus of the paper is to achieve authorization in key management.

As we see that all the previous work and models presented in different papers by different authors, which deals with Wimax security system with different Architecture and I accredit that the model proposed in this paper is more efficient for the Wimax system not only in the case of security but also increase the performance of the system.

3. RELATED WORK

In this Paper the authorsanjay et al have discussed the security mechanism of Wimax,[1] like Authentication, Encryption, Authentication and availability And disputation of Wimax security architecture where Network Reference Model is follows the standard for end to end communication. The Network Reference Model (NRM) network divide into two parts connectivity service Network (CSN) and Access service Network (ASN).The Base station Traffic the Base Station Traffic and monitoring are perform by ASN while CSN control the ASN and end users. The CSN also provide Authentication, Authorization and Availability. He also briefly discuss various threats like Rogue Base Station attack, DOS, Network Manipulation with spoofing and management frame etc. from the paper it is concluded that Wimax is still not flawless but up to some extent it is secure because most of the threats are identified and a little are hidden**.** Physical and MAC layer also play an important role in security architecture [2]. deepti et al havegiven the protocol layer architecture and security architecture for Wimax, The protocol layer architecture is made up of two main layers the physical layer and Medium Access layer (MAC).The working of physical layer is to provide two way mapping between the Medium Access layer (MAC) protocol data unit while physical layer work is modulation of radio frequency signals receiving and transmission of frames. While in the security architecture phase the security sub layer perform three main operations secrecy, Authentication and Authorization the sub layer contain two main protocols the securing data packet across fixed network, Data Encryption. The secure distribution and data key service are providing by key management protocol (PKM).He discusses various threats to MAC layer and physical layer. The author's also discuss some attacks and what are the security requirements to secure Wimax. The focusing point of the paper is rogue base station attack, which is discussed briefly in the paper

4. EXISTING SECURITY MODEL

The Wimax existing security model consist of three phases, called Authorization key exchange material and Encryption which is shown in the figure2.

Starting from the first phase the MS first send the Authentication information message to the Base station. The information message contains. X.509 certificate of the MS. The purpose of this message is to establish connection with the BS. After the authentication info message immediately the MS send the Authorization request to the Base Station to get authorization key [9].

The authorization request message consist of

- X.509 certificate
- Security capability
- SAID

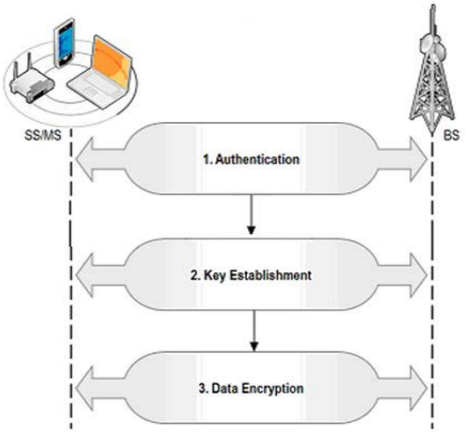

Figure 2. Existing Security Model

SAID is unique for each primary security Association (SA) while security capability is the description of encryption of encryption algorithm here in the existing model RSA is used which is supported by MS. When BS receive the message first it verified the certificate of MS if it is valid the BS generate the AK otherwise reject it. After generating the authorization key the MS receive the authorization reply message from the BS. The message include

- AK sequence number
- AK encrypted by RSA
- Life time of AK
- X.509 certificate

With the use of AK the BS and MS calculate the HMAC and KEK. The HMAC and KEKare used in key exchange phase for traffic encryption key. Now in the next phase mean the key establishment phase the MS send the Traffic encryption Key (TEK) message to the BS. The message send by MS include.

- AK sequence number
- SAID
- HMAC key

The HMAC key is used for the generation of HMAC digest which give the security that both have the same AK and then BS check the validity of HMAC digest. . if it is valid the BS send the TEK Reply message. The reply message receive by the MS which include

- AK sequence number
- SAID
- Traffic encrypted key
- HMAC Digest
- TEK Life Time.

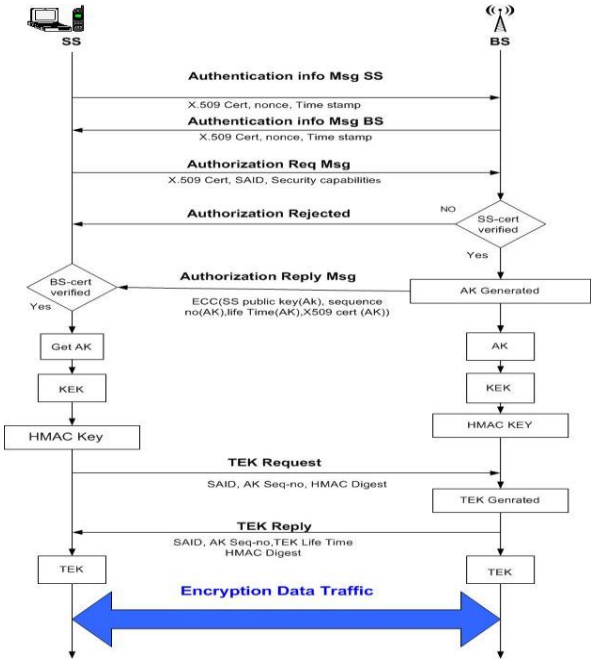

Figure 3. Proposed security Model

Now come to the last phase because both MS and BS have TEK.so only the MAC PDU is encrypted by TEKMAC header and CRC checksum is not involved when encrypted the MAC PDU.

5. PROPOSED WIMAX SECURITY MODEL

The proposed security model for Wimax is shown in the figure 3. As compare to the existing model only the mobile Station (MS) can send authorization request to the Base Station (BS). But the proposed security model both the BS and MS will authenticate himself with each other.So in the proposed model the MS first send authentication message to the BS which contain vendor certificate, time stamp, and nonce of the MS. The benefit of Timestamp and nonce is that it can verify the message is fresh or old. Through the use of nonce and Time stamp in authentication process we can secure the network from Reply Attack.As the BS receive the authentication message from the MS and verify it the BS send his Authentication request to the MS Which include vendor certificate (X.509) of BS, nonce and Time Stamp. The benefit of sending authentication request message to MS is that to secure network from Rogue Base Station Attacks. The MS verify the BS and Authorization Request Message send to the BS the message contain MS certificate , SAID, Security capability.

As soon as the BS receive the Authorization Request message it verify the certificate of MS for the purpose that the MS is valid or not ,if it is not valid the BS reject it otherwise validate the MS and BS send Authorization reply message and generate AK. The AK is encrypted with Elleptic Curve Cryptography (ECC) public key of MS, At this step the MS verify the BS certificate if it is valid the MS verify the extract the ACK key from the message and calculate HMAC and KEK.

Now in the key exchange phase the MS send TEK request to the BS the message include , AK Sequence no, HMAC Digest and SAID. The BS receive the TEK request message and validate HMAC digest if it is valid BS generate the TEK and send TEK reply to MS , the TEK reply message include SAID, AK sequence number, TEK life time and HMAC digest.

The last phase called data Encryption Phase in this phase the MAC PDU that is to be transferred between BS and MS is encrypted with TEK while CRC and MAC header are excluded mean not encrypted.

6. SIMULATION STUDY AND RESULTS

We used ns-2 simulator for validating the results of our work. We have analyzed the encryption and decryption time of RSA and elliptic curve (ECC) key and tested with various file sizes keeping key size unchanged.

In the figure 4 we show the performance of Cryptographic Algorithm in term of Encryption time. Graph shows encryption time for both RSA and ECC where size of ECC key is **163** bits long and RSA is **1024** bits key size, providing the same security strength. RSA takes **280 ms** for encrypting **100 Kbits** file and RSA takes **340 ms** for encrypting the same

file. We can clearly see that ECC is taking less time for encryption and decryption as the key size is small and providing the same key strength as compared to RSA. We can clearly see that ECC is taking less time for encryption and decryption as the key size is small and providing the same key strength as compared to RSA. Thus we can conclude that ECC is efficient in terms encryption time.

Table 1 : Comparative analysis of existing and proposed model

ATTACKS	EXISTING MODEL 1 [3]	EXISTING MODEL 2 [6]	PROPOSED MODEL
DOS ATTACK	NO	YES	YES
REPLAY ATTACK	YES	YES	YES
ROGUE BASE STATION ATTACK	NO	NO	YES
MAN IN THE MIDDLE ATTACK	YES	NO	YES

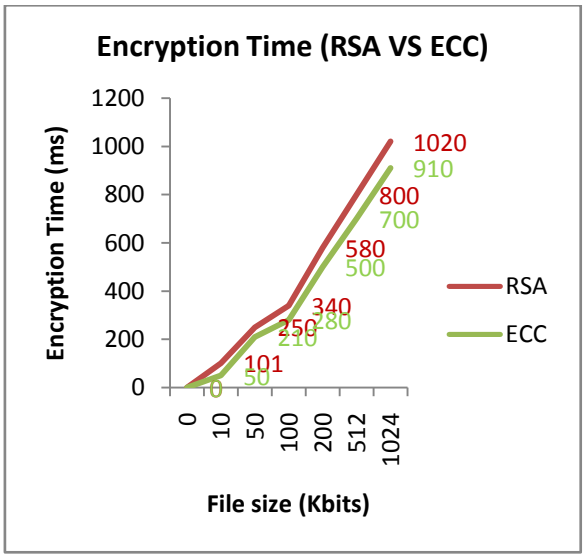

Figure 4. RSA VS ECC Encryption Time

In the figure 5 we can see the results relating to the performance of ECC and RSA in term s of Decryption time. Graph shows Decryption time for both RSA and ECC where size of ECC key is 163 bits long and RSA is 1024 key size, having the same key strength. We can clearly see that ECC is taking less time for encryption and decryption as the key size is small and providing the same key strength as compared to RSA. We can clearly see that ECC is taking less time for Decryption and decryption as the key size is small and providing the same key strength as compared to RSA. Thus we can conclude that ECC is also efficient in terms Decryption time.

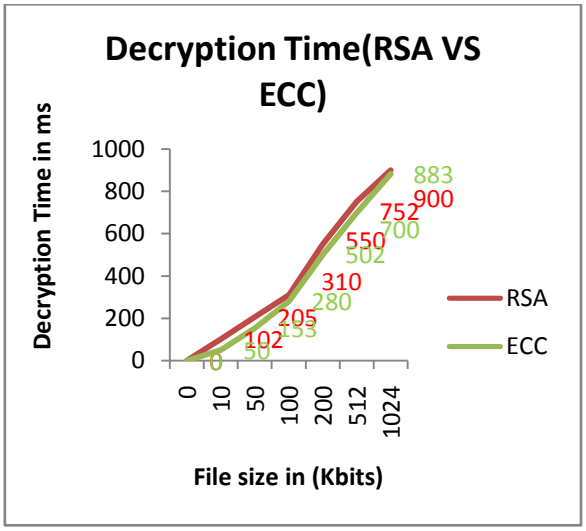

Figure 5. RSA VS ECC Decryption time

7. COMPARISON OF PROPOSED MODEL WITH EXISTING MODELS ON BASIS OF ATTACK HANDLING

Different Wimax Security Models are proposed in different papers. The strength of their Models against different attacks have been discussed, on the basis of literature review and brief study of existing model we select two models and compare with our propose model as shown in the Table 1

The existing two models for Wimax can either handle one are two possible attacks in the given, Dos attack, Replay attack, Rogue base station attack and Man in the middle attack, and does not able handle all these attacks, which is the main deficiency in these models. While our proposed model in this paper for the Wimax, is able to handle all these attacks successfully. For DOS Attack Exclusion Our Proposed model uses a strong Encryption Technique by replacing RSA with ECC, Replay Attack are excluded by Using Nonce and Time Stamp, Rogue Base station Attack and Man in the middle Attack are eliminated by using Two way authentication mechanism. We have checked the results of the simulation for the model in NS-2.which show positive results.

8. CONCLUSION AND FUTURE WORK

To review the current and past trend for talking the security in Wimax network. And provide some solution for the making of security and privacy. More tightens comparative threat analysis have done regarding in Wimax security.

In this paper we propose some enhancement in the existing model. To make Wimax more efficient .we uses two way authentications between base station and the subscriber station. To eliminate the Rogue base station Attack. Another improvement done on our paper is the use of nonce and time stamp which eliminate reply and DOS attack. For security we propose some enhancement in our model to improve the capabilities andencryption Time. The comparison of ECC and RSA has done which shows that ECC is better than RSA due to smaller key size. In the last we compare propose model

performing different attacks with reference to existing model the result shows that our model is more efficient and tackle all attacks while existing model tackle one or two attacks.

9. REFERENCES

[1] Sanjay P. Ahuja, Nicole Collier, "An Assessment of Wimax Security", Communications and Network , May 2010.

[2] Deepti,Deepika Khokhar, Satinder Pal Ahuja," A Survey of Rogue Base station Attack In Wimax /IEEE802.16", International Journal of Advanced Research in Computer Science and Software Engineering,2012.

[3] Raheel M. Hashmi, Arooj M. Siddiqui, M. Jabeen, Secure Network Authentication Protocol (ISNAP) for IEEE802.16" International Conference on Information and Communication Technologies, 2009. ICICT '09.IEEE 2009

[4] Mahmoud Nasrel din,HebaAslanMagdy E Hennawy Adel El-Hennawy,"WiMax Security", 22nd International Conference on Advanced Information Networking and Applications Workshops IEEE 2008.

[5] Ergang Liu, Kaizhi Huang and Liang Jin,"The Design of Trusted Access Scheme Based On Identity For WiMAX Network", First International Workshop on Education Technology and Computer Science IEEE 2009.

[6] Masood Habib, Tahir Mehmood, Fasee Ullah Muhammad Ibrahim,"Performance of Wimax Security Algorithm", International Conference on Computer Technology and Development IEEE 2009.

[7] Lang Wei-min, Wu Run-sheng, Wang jian-qiu,"A Simple Key Management Scheme based on Wimax", International Symposium on Computer Science and Computational Technology IEEE 2008.

[8] Perumalraja Rengaraju ,Chung-Horng Lung, Anand Srinivasan"Design of Distributed Security Architecture for Multi hop Wimax Networks", Eighth Annual International Conference on Privacy, Security and Trust IEEE 2010.

[9] Pranita K. Gandhewar, Kapil N. Hande," Performance Improvement of IEEE 802.16 Wimax", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (3) , 2011.