International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 11 (2017) pp. 3002-3008

A Secure Authentication Scheme for WiMax Network and Verification using Scyther Tool

Anil Sangwan.
Assistant Professor, Electronics and Communication,
University Institute of Engineering and Technology,
Maharshi Dayanand University, Rohtak-124001, Haryana, India.

ORCID: 0000-0002-4935-9992

V R Singh
Professor and Director, Prabhu Dayal Memorial College of Engineering,
College of Engineering, Bahadurgarh-124507, Haryana, India.

Abstract
Recently, the wireless Communication technologies are replacing the wired one. WiMax is one of the wireless communication technologies which provides high speed internet. Like other network technologies the wireless network technologies are also not secured. A lot of security issues were reported in WiMax in various articles. To protect from unauthorized use of resources of a network, authorization and authentication models are developed. Various authentication and encryption mechanisms were proposed for WiMax security but still the WiMax networks are not fully secure and are under the attacks like replay attack, Rouge Base station Attack, Man in the Middle Attack, DoS Attack etc. To increase the capability and functionality of existing models we will propose a security scheme in this article. We will also verify our proposed security scheme using the scyther tool.

Keywords: WiMax, IEEE 802.16, WTLS, Scyther

INTRODUCTION

WiMax which is also known as IEEE802.16 is an emerging wireless broadband technology that can provide a high speed around 70 Mbps over an area of 30 to 40 Miles. First published in 2002, primary version of IEEE802.16 operates in 10-66 GHz [1][2][3] which provides line of sight connectivity. To provide non line of sight connectivity another standard IEEE802.16d was introduced in 2004 which operates in 2-11 GHz frequency band. Another version, IEEE802.16e was available in 2005 which was basically an amendment in IEEE802.16d and it supports mobility and operates in 2-11 GHz band under non line of sight conditions [4]. In last few years there has been a great advancement in wireless communications. Most of the wireless Communication networks are based on radio waves due to which the medium of the network is inherently open to interception. Thus network's security always plays an important role in the presentation of a network. WiMax being a wireless technology it is also inherently open to interceptions and thus the security is a big concern. To secure the end users security concerns are required among core networks, application servers, and in between everywhere. To secure WiMax from threats and vulnerabilities there is a necessity of strong security managements, because for new technologies we need different security managements, other than those used by the old technologies. This article will propose an improved scheme for the security of WiMax by considering the threats and vulnerabilities that arises during authorization and authentication phases. The proposed scheme will be more secure and reliable.

WIMAX ARCHITECTURE AND SECURITY SCHEME

A. WiMax Architecture

The IEEE 802.16 standard constitutes of a protocol stack with precise interfaces [5]. The protocol stack is structured in to two layers, MAC layer and PHY layer. MAC layer has three sub-layers Convergence Sub-layer (CSL), Common Part Sub-layer (CPSL) and the Security Sub-layer which are shown in Fig.1.

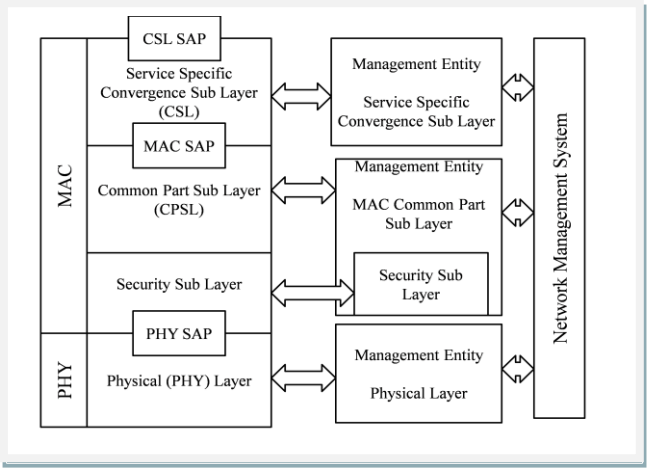

Figure 1. Protocol Layering in WiMax

The mapping of upper level data services with MAC layer service flows and connections are done by the CSL. CSL is of two types: first, Packet CSL that supports Ethernet, IPv4 and IPv6 protocols, Point to point protocol and virtual LAN and second ATM CSL designed for ATM network and service. The Core of the standard is common Part Sub layer (CPSL). Rules and mechanisms for bandwidth allocation, system access, and connection management are defined by the CPSL. Bandwidth request and grant, connection control, uplink scheduling, and automatic repeat request (ARQ) are some of the functions defined here. Communication between the CSL and the CPSL is done by Service Access Point (SAP). Security Sub-layer is in between CPSL and PHY layer. Encryption and decryption of data coming to and from the PHY layer is the main responsibility of this sub layer. This Sub layer is also used for secure key exchange and authentication. With respect to cost, radio capabilities, cell planning and services the PHY layer is designed with high flexibility to permit service providers to optimize system deployments. PHY layer is supposed to operate in 10-66 GHz frequency band [5].

B. Security Scheme

The security method of WiMax technology is distinct by X.509 digital certificates, SA (Security Association), PKM Authorization, Privacy and Key Management and Data Encryption [6][7]. Security policies are imposed by the BS to the SS/MS, so it has the right to use an authorized SA that compliments the attribute of that type of service. Single SS can have one to three different SAs; one/two for uplink/downlink channels and one for the secondary management channel. Primary SA protects the downstream but it cannot protect it in multicast communication and that is the reason static and/or dynamic SAs are used. Data and authorization SA are the two types of SAs which are supported by WiMax standard. Data connections between BS and SS are protected by data SAs and authorization of SS to access the BS is done by authorization SAs by establishing data SA. Identification of SS is done by the X.509 digital certificate. Certificates for BS are not defined in the WiMax standard. Based on Public Key techniques, an authentication algorithm is defined by X.509 digital certificate. X.509 digital certificate contains the public key and MAC address of SS and all SS has their own unique X.509 digital certificate.
The Mobile WiMax based on IEEE 802.16e has more security capabilities than its predecessor WiMax based on IEEE 802.16d standard [5][7]. Most of the issues related to security are contemplated in security Sub layer in Mobile WiMax and is shown in Fig.2.

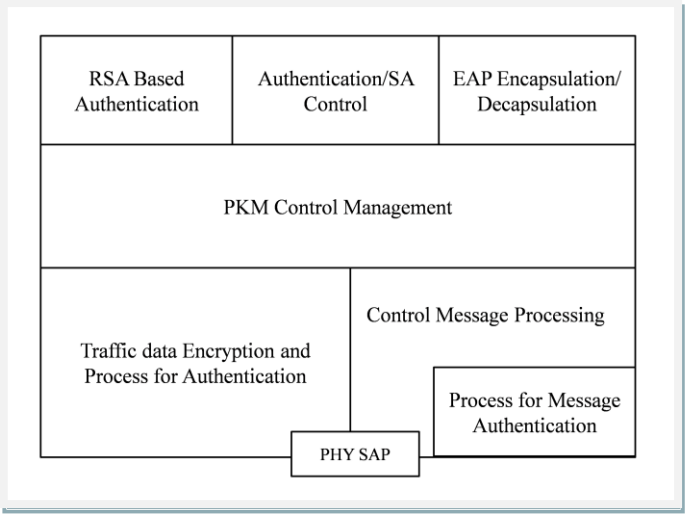

Figure 2. Security Sub-Layer

Authorization, Authentication and Encryption are three fundamental functions incorporated in Security Sub layer and how they are performed is as follows.

1) Authorization

Establishment of encryption keys and authentication is achieved by using public key interchange protocol. Privacy Key Management Protocol is defined in the security sub layer of mobile WiMax based on IEEE802.16, which allows three types of authentication. First type of authentication is based on RSA (Rivest Shamir Adleman). RSA encryption with X.509 digital certificate is used in RSA based authentication. In this mode, authentication between SS and BS is achieved through unique X.509 certificate which has been issued to SS by its manufacturer. MAC address and Public Key (PK) of SS are present in the X.509 digital certificate. To request an authorization Key (AK), SS transmits its X.509 certificate to BS, then BS verifies that certificate if its valid then BS encrypts an AK by using the verified Public Key (PK) and transmits that AK back to SS. X.509 certificates together with public/private key pairs are installed in every SS by manufacturer which uses RSA authentication.

Second type of authentication is based on Extensible Authentication Protocol (EAP) in which the authentication of SS is done either by a unique credential issued by operator such as SIM or by an X.509 digital certificate as discussed above. EAP is of three types. First is Authentication and Key agreement EAP used for authentication based on SIM. Second is Transport Layer Security EAP used for authentication based on X.509 digital certificate, and third is Tunnelled Transport Layer Security EAP used for SS CHAPv2 (Challenge Handshake Authentication Protocol). Choice of type of EAP is made by the operator to determine authentication method.

Third type of authentication is RSA authentication followed by EAP authentication [5][7].

2) Authentication

After authentication Authorization process is carried out between SS and BS. In authentication process SS make a request to BS to seek AK and the Security Association Identity (SAID). The request message for authorization contains X.509 certificate of SS, cryptographic ID and encryption algorithms. In response to the request the BS send an authorization reply to SS which contains the AK encrypted with public key of SS and a life time. The essential validation is done by BS after interacting with Authentication Authorization and accounting (AAA) server present in the network. [5][7].

3) Traffic Encryption

160 bits long Authorization Key (AK) is the result of Authentication and Authorization process. Key Encryption Key is generated unswervingly from the AK. KEK is 128 bits long and it is not used to encrypt traffic data. Thus MS needs another key named Traffic Encryption Key (TEK) from BS. Using TEK encryption algorithm TEK is created in BS as a random number where KEK is used as an encryption key. Then KEK is used for data traffic Encryption [5][7].

RELATED WORK AND EXISTING SECURITY MODEL

The researchers of paper [8] have explained most important classes of intrusion attacks i.e, Fabrication, interruption, modification and interception [8]. They also explained the various schemes for security implemented in the WiMax Network and elaborated that which security scheme is suitable for different kind of attacks. Main attacks include the Replay attacks, [9], identity theft and impersonation [10], and Denial of service (DoS) attacks [3][4]. In DoS, capabilities of system are pooped by repetitive establishment of authentication events on BS or SS. Reuse of captured genuine messages [3][4] is the base of Replay attacks. Synchronization failures and Presence of cloned/illegitimate nodes cause severe threats to security in network. Existing security model is based on the Security associations and generation of security keys or establishment when MS enters the range of BS.[11]. Main key elements in the model are shown as entities and relationship between those entities is also shown. Set of Security information which is shared between MS and BS to provide secure communication in a WiMax Network is known as Security Association (SA) [12]. Data SA and authorization SA are the main types of SAs and both are drawn in the existing Model [11][12]. Primary SA, static SA and dynamic SA are the three types of Data SA. To establish a secure communication between MS and BS different mechanisms are adopted by the WiMax architecture. In order to establish a new connection both MS and BS uses Security Associations. When a MS is initialized, a primary SA is established and every MS has one Primary SA. When BS Initializes the MS, the static SA is generated. Last type of data SA is the Dynamic SAs and they are dynamically created by the BS and are used for transport connections when required. Authorization SA is the second type of SA and is used in the authorization purpose and it is used by BS in order to establish data SA between BS and MS. WTLS certificate, Authorization Key (AK), HMAC etc are the other entities sketched in the model. Every MS has a unique WTLS certificate and it carries the public key of the MS which is further used in authentication, access control and confidentiality. To communicate with BS, MS uses its Public key. After authentication process, authorization request message is sent by the MS to BS and BS creates the Authorization Key (AK) with its Sequence Number and Life time and transmits it back to the MS in encrypted type with MS's public key having sequence Number 0-15 [11][12]. In this model HMAC is used as the hashing technique which does not provide the protection against replay attacks. Key Encryption Key (KEK) is another key which is used for the encryption purpose. AK is used to calculate KEK and HMAC. At last TEKs are created and KEK is used to encrypt the TEK during TEK request reply. Communication gets established and exchange of information or data starts when TEK is obtained. [3][11]

PROPOSED SECURITY MODEL AND SCHEME

A. Proposed Security Model

Owing to several complexities in different models of WiMax networks, security is the biggest concern and has been inflexibly positioned into WiMax network. For designing secure network, the main task of service providers is to develop the security strategies else, networks and users will be at risk to hackers and threats. To comprehend security issues in WiMax, we should have exhaustive acquaintance of the basic protection methods used in WiMax security. Some enhancements are made by us in the existing scheme to enhance its security, for which we propose some techniques in the existing scheme considering their level of functionality and security. Communication between MS and BS is the base of the proposed scheme and main objective of proposed scheme is security. Both MS and BS will authenticate and authorize each other whenever a MS enters into BS's network range and will set up a communication connection. The proposed model is categorized on the basis of Data SA, Authorization SA and KEYs exchange with the use of time stamps (TS) and Nonce as shown in the Fig.3.

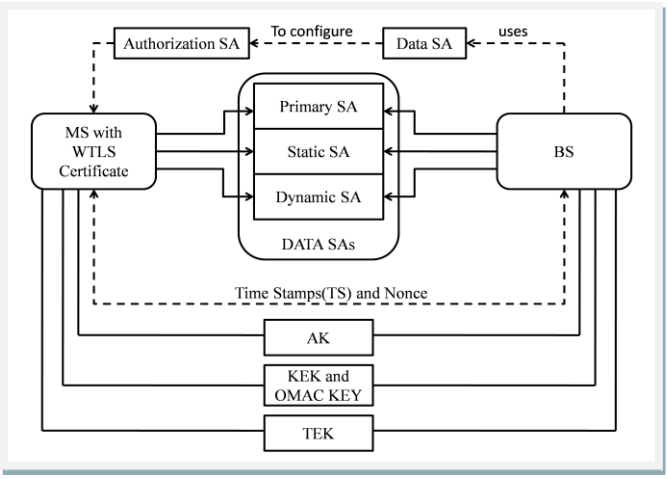

Figure 3. Proposed Security Model

For connection request Data SA is used by MS before initializing the connection process. Data Encryption Standard (DES) in CBC mode is used by Data SA which contains SAID (SA Identifier) and cryptographic cipher identifier for secure data transmission [11][15]. Moreover Data SA use two Traffic Encryption Keys (TEK), one is for current operations and another one as TEK. TEK's life time can vary from 30 minutes to 70 days. Normally two or three SAs are associated with a single MS.

Authentication is provided in between MS and BS by the use of authorization SA. Mutual Authentication is there in IEEE802.16e standard in which MS authenticates BS and BS also authenticates MS. Authorization SA contains an Authorization Key (AK) and Key Encryption key (KEK). Allocation of TEKs is carried out by KEK. Hash functions are also used by the authorization SA in order to provide the authenticity between BS and MS. [11][16]. In the existing scheme WTLS certificate and ECC (Elliptic Curve Cryptography) encryption was used as an alternative of X.509 certificate and RSA (Rivest Shamir and Adleman) encryption. WTLS certificates have a manufacturer unique ID and a serial number smaller than that of X.509 certificate thus reduces the space occupied. ECC was used in the existing model and the benefit of using ECC is that it uses the key size of 163 bits and provides the same encryption strength as that of RSA whereas, the key size in RSA is of 1024 bits. Due to the smaller Key Size the memory will be saved. In our proposed scheme we will use the timestamps and nonce which were not used in the existing scheme. Nonce is very useful in wireless communication as it helps BS identifying the consecutive requests coming from some intruder station and increases the capacity of BS to reject such requests. Thus a BS can recognize the newest requests and is capable to sort out samples of attack i.e, replay attacks. In an authorization reply message, BS sends nonce and timestamp of MS by which an intruder is prevented from forging a BS. Mutual authentication is provided in our proposed Scheme which helps in preventing the rouge base station attack. Man in the middle attack can be prevented by the exchange of nonce between MS and BS. By the use of timestamps a BS can identify the newest requests and thus reply attacks can be prevented. Furthermore, timestamps helps MS as well in identifying the latest messages and thus a MS can identify an AK used by him is new or not. Addition of nonce in the message by BS helps MS to recognize whether the received message with AK is new or not. Thus it's better to include more number of buffers to bear nonce values which were used in previous sessions. This will provide more security between the BS and MS. Timestamps helps in providing the protection from DoS Attacks. The existing scheme uses the Hash Function Based Message Authentication Code (HMAC) as hashing function but in our proposed scheme we will use the OMAC (One Key CBC MAC) as hashing function. OMAC algorithm is very simple and it provides pretty good prevention against the replay attacks.

Traffic Encryption Key (TEK) is required to encrypt the data and TEK uses AK for this purpose. MS and BS independently derive the Message authentication key (OMAC) and KEK from AK. BS generates the TEK on the request of MS and then BS transmits it in encrypted form to BS. OMAC hashing technique is used for the key exchange authentication. In end the connection is established and information is exchanged in a secure manner.

B. Proposed Security Scheme

In this proposed security scheme there is mutual authentication between MS and BS in which BS and MS authenticates each other before exchanging the information. The proposed security scheme is shown in Fig.4. Exchange of information between MS and BS takes place in steps as follows:

STEP 1: Initially when MS wants to set up a communication link with BS, it will send an initial authentication message (INIT) to the BS as follows:-

MS→BS: MSCert.(WTLS), Nonce-1(MS) and TS-1(MS).

In response to the INIT message BS will check the TS-1(MS) and if TS-1(MS) is valid then proceed, else BS will discard the INIT message. BS will also validate the MSCert.(MS) and if MCert.(MS) is valid then proceed else BS will discard the INIT message. So in this step BS will validate the Time Stamp (TS) and digital certificate of MS and if both are valid then BS will accept the further messages from BS.

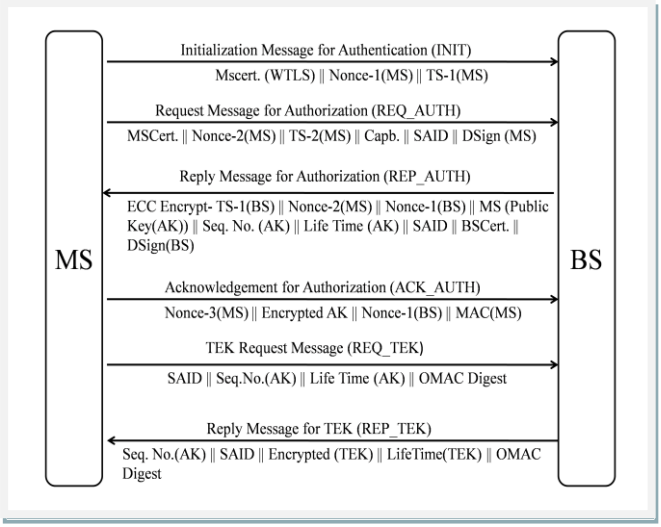

Figure 4. Proposed Security Scheme

STEP 2: In this step MS will send an authentication request message (REQ_AUTH) to BS as follows:

MS→BS: MSCert., Nonce-2(MS), TS-2(MS), Capb., SAID, DSign(MS).

MS generates Nonce-2(MS) and store it then encapsulate Nonce-2(MS) with MSCert., will concatenate SAID and Capb., then generate DSign(MS) for the message and attach it with message, then place TS-2(MS) on the message and send it to the BS.

STEP 3: In this step BS will receive the REQ_AUTH message from MS and will check for two conditions for further communication. First, if TS-2(MS) is valid then BS will proceed else it will discard the communication. Secondly BS validates for MSCert, and DSign(MS), if both the identifications are valid then BS will proceed and store the public key of MS and Nonce-2(MS), else it will discard the communication. Now if all the credentials are valid then BS will send an Authorization Reply message (REP_AUTH) to MS as follows:

BS→MS: ECC Encrypt – TS-1(BS), Nonce-2(MS), Nonce-1(BS), MS Public Key (AK), Seq. No.(AK), Life Time (AK), SAID, BSCert., DSign(BS).

In this message BS generates Nonce-1(BS) and save it, then encapsulates BSCert. with Nonce-1(BS), then generates AK and encrypt that with public key of MS, then concatenate Seq. No. of AK (4 bit), SAID List (2 bit), AK Life Time (32 bit) and Nonce-2(MS). Now BS will combine them in one message and generates Digital Signatures (DSign(BS)) and attach it with message and then will place TS-1(BS) on the message and send it as REP_AUTH message to MS.

STEP 4: In this step MS will receive the REP_AUTH message from BS and validates TS-1(MS) and Nonce-2(BS). If TS-1(BS) and Nonce-2(BS) are valid then MS will proceed else it will discard the communication process. Again MS will validate BSCert and DSign(BS) and if both are valid then MS will proceed else discard the process. After validation MS will decrypt AK and SAID List using private key and will save them along Nonce-1(BS). Then MS will start the key life timer (32 bit) and save the Seq. No. (4 bit) of AK and will establish the association according to SAID List. Now MS will send an acknowledgement message (ACK_AUTH) to BS as follows:

MS→BS: Nonce-3(MS), Encrypted AK, Nonce-1(BS), MAC (MS).

In this message BS retrieves MAC (MS) and stored Nonce-1(BS) and using AK (160 bit) will encrypt and concatenate the MAC (MS) and Nonce-1(BS). Then MS will place TS-3(MS) on message and send it as ACK_AUTH to BS.

After receiving the AK, both MS and BS will calculate KEK and Hashing Key using AK. OMAC is used as the hashing technique in this security scheme.

STEP 5: In this step MS will send a Request message for TEK (Traffic Encryption Key) to BS. TEK is used for data encryption and message is as follows:

MS→BS: SAID, Seq. No. (AK), Life Time (AK), OMAC - digest.

MS will send SAID, Sequence Number of AK, Life Time of AK with OMAC digest as the request message for TEK (REQ_TEK) to BS.

STEP 6: When BS receives REQ_TEK message from MS, BS generates the TEK and sends it back to the MS as TEK reply message (REP_TEK) as follows:

BS→MS: Seq. No (AK), SAID, Encrypted TEK, Life Time TEK, OMAC Digest.

When MS receives this REP_TEK message, it will decrypt the TEK. Now TEK has been exchanged between BS and MS and a secure connection for communication has been established between two. Now BS and MS can interact with each other and share the data securely.

RESULTS AND DISCUSSIONS

In 2007 Cas Cremers developed a protocol verification tool named Scyther [13][14]. The main aim of developing this tool is for the formal analysis of protocols in which the cryptographic protocols are analyzed on the security properties (usually variants of authenticity and confidentiality). Unless and until an attacker does not know the decryption, key he cannot steal the information from encrypted message. Thus perfect cryptography is assumed by this tool. In Scyther security properties of a protocol are specified by the claims and role based depiction of protocol is the input of Scyther. Claims in scyther can be classified as form claim (Parameter, Principal, Claim) where security property is tartan for the term Parameter, Principal is User's name and Claim is another security Property (for instance 'secret'). Security Protocol description language (SPDL) is the language in which the protocol's description is written. There are three ways in which we can use scyther to verify a

protocol [13][14].

1) Verification Claim: Security properties can be verified or falsified using Scyther.

2) Automatic Claims: If Security properties are not specified by a user as Claim Event then Scyther generates and verifies claims automatically.

3) Characterization: Characterization of each protocol can be done using Scyther.

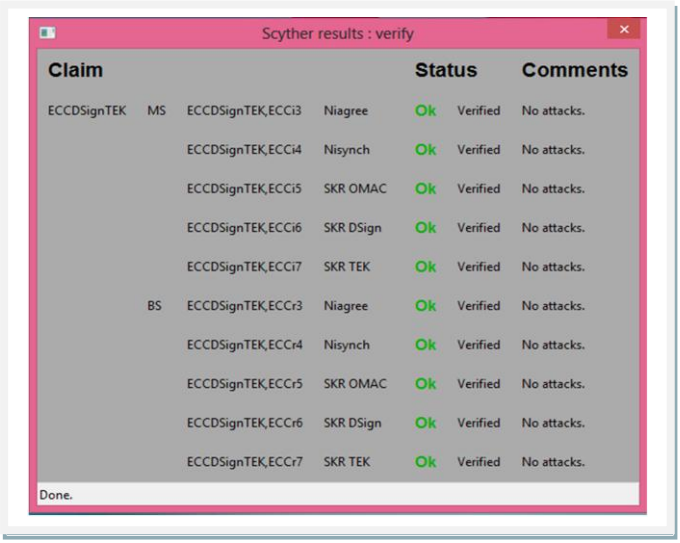

Figure 5. Formal Analysis of Proposed Security Scheme

We wrote our proposed security scheme in SPDL language and then did the formal analysis of the scheme using scyther tool. Fig.5 shows the result of formal analysis of proposed security scheme and the proposed scheme was run for 30 rounds and result clearly shows that the scheme is verified and no attacks can be done to steal the information.

CONCLUSION

Being a wireless technology, WiMax is also susceptible to attacks. We proposed a security scheme to enhance the capabilities and functionality of the WiMax Network so that there will be secure interchange of data. In the proposed scheme ECC encryption was used instead of RSA. ECC has a key size (163 bits) lesser than that of RSA (1024) and it provides same strength as of RSA. Due to mutual authentication in the proposed scheme Man in the Middle Attack and Rouge Base Station attacks can be prevented. Time Stamps and nonce were also used in the proposed scheme to prevent the DoS and Replay attacks. Thus the proposed security scheme is safe and data can be exchanged securely.

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] Raheel M Hashmi, Arooj M Siddiqui, M. Jabeen, K. Shehzad, A Zubair, K S Aleemgeer, "Improved Secure Network Authentication Protocol (ISNAP) for IEEE 802.16" International conference on communications and technology,2009, IEEE.

[5] Tao Han, Ning Zhang, Kaiming Liu, Bihua Tang Yuna an Liu, "Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions" 5th IEEE conference on Mobile Ad Hoc and Sensor Systems, 2008, IEEE.

[6] Raj Jain and Trung Nguyen, "A survey of WiMAX security threats", Project report, 2009.

[7] Daniel SIMION, Mihai-Florentin URSULEANU, Adrian GRAUR, "An Overview on WiMAX Security Weaknesses/Potential Solutions" 11th International Conference on DEVELOPMENT AND APPLICATION SYSTEMS, Suceava, Romania, May 17-19, 2012.

[8] Mahmoud Nasreldin, Heba Aslan, Magdy El-Hennawy, Adel El- Hennaey, "WiMAX Security", Proceedings of the 22nd International Conference on Advanced Information Networking and Applications, pp. 1335-1340, 2008.

[9] Sen Xu, Chin-Tser Huang, "Attacks on PKM Protocols of IEEE 802.16 and Its Later Versions", Computer Science and Engineering Department, University of South Carolina, Columbia, September, 2006.

[10] Michel Barbeau, "Rogue-Base Station Detection in WiMAX/802.16 Wireless Access Networks", School of Computer Science, Carleton University, Ottawa, Canada.

[11] Masood Habib, Tahir Mehmood, Fasee Ullah, Muhammad Ibrahim, "Performance of WiMAX Security Algorithm (The Comparative study of RSA Encryption Algorithm with ECC Encryption Algorithm)" International Conference on Computer Technology and Development, 2009, IEEE.

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

[13] Cremers. C, "Scyther-Semantics and verification of security protocols, "PhD dissertation, 2006 Eindhoven University of technology.

[14] Cremers. C, "The Scyther Tool: Verification, Falsification, and Analysis of Security Protocols?", Department of Computer Science, ETH Zurich, Switzerland Proceedings of the 20th International Conference on Computer Aided Verification 2008, Princeton, USA.

[15] D. Stella Gnana Ruby, and. R. Arasa Kumar,

"Protecting Wimax Entities Against Rogue Base Station And DDoS Attack" pp.1860-1865, IJAER, Volume 10 Number 55 (2015)

[16] M.Uma Devi, and M.Raja Lakshmi, "Development of Efficient Resource Allocation Algorithm for WiMAX Relay Networks"pp.2234-2238, IJAER, Volume 10 Number 55 (2015)