IMPLEMENTATION OF SECURE & COST EFFECTIVE AUTHENTICATION PROCESS IN IEEE 802.16e WiMAX

[1]B.Sridevi, [2]M.Brindha,[3]R.Umamaheswari,[4]Dr.S.Rajaram

[1]Assistant Professor,[2][3]Under Graduate,[4]Associate Professor
Department of Electronics & Communication Engineering
[1][2][3]Velammal College of Engineering & Technology, Madurai.
[4]Thiyagarajar College of Engineering,Madurai
aisveriya@yahoo.com,brindhamayakrishnan@gmail.com,umaramaraj.n@gmail.com

ABSTRACT

The Mobile WiMAX IEEE 802.16e is a neoteric technology providing broadband data access to mobile and stationary users while supporting handover and roaming capabilities. In the area of security aspects, Mobile WiMAX exhibits vulnerabilities while adopting improved security architecture. Bandwidth is an additional overhead in reducing these vulnerabilities. To compensate bandwidth and security, this project focuses on reducing the security vulnerabilities in the initial network entry process and access network of the WiMAX domain with a view to reduce the memory required for key management. This paper proposes the usage of 1.Modified Diffie-Hellman algorithm and 2.Device certificate for key exchange process to provide secure authentication and 3.Compression technique to reduce the memory space and the transmission bandwidth. The 802.16e mobile WiMAX model is implemented using Qualnet and security enhancement is implemented using MATLAB.MYSQL is used as the database for Key storage. This proposed work enhances the security of the WiMAX network and reduces at least 50% of the bandwidth.

KEYWORDS

IEEE 802.16e,WiMAX,Vulnerabilities and security,Diffie-Hellman Key Exchange,Certificate,Bandwidth, Compression.

1. INTRODUCTION

WiMAX, the Worldwide Interoperability for Microwave Access, defined by the IEEE standard as 802.16, is a telecommunications technology that provides wireless and broadband data transmission with high bandwidth and transmission rates between point-to-point links and full mobile cellular access. IEEE 802.16-2004 supports fixed and nomadic nodes whereas IEEE802.16e-2005 the Mobile WiMAX standard derived from Fixed WiMAX supports mobile nodes. IEEE 802.16e works in 2.3 GHz and 2.5 GHz frequency bands utilising PKM V2 key management protocol to protect the network from illicit access. The security architecture of WiMAX 802.16e is in Figure.1.

The overall network may be logically divided into three parts: i. Mobile Stations (MS) or subscriber station (SS) used by the end user .i.e. the mobile devices that would like to join the Mobile WiMAX network. ii. The access service network (ASN) comprising one or more base stations and ASN gateways that form the radio access network at the edge. The ASN interfaces the BS and all-IP core network. The ASN manages radio resources, MS access, mobility, security and QoS. It acts as a relay to CSN for IP address allocation and AAA functions. iii. Connectivity service network (CSN) provides IP connectivity and all the IP core network

DOI : 10.5121/ijdps.2012.3219

functions. The CSN performs policy and admission control, IP address allocation, settlement and billing. CSN hosts the Mobile IP Home Agent, Authorization, Authentication and Accounting (AAA) servers, and Public Switched Telephone Network (PSTN) and VoIP gateways. The CSN is also accountable for internetworking with non-WiMAX networks.

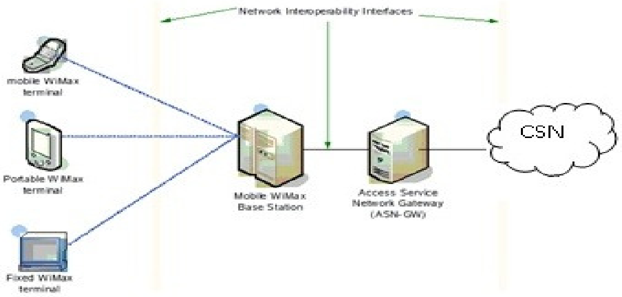

Network Interoperability Intefaces
mobile WiMax terminal
Portable WiMax terminal
Fixed WiMax terminal
Mobile WiMax Base Station
Access Service Network Gateway (ASN-GW)
CSN

Figure.1. WiMAX Security Architecture

From security point of view, IEEE 802.16e-2005 has advanced security features compared to IEEE 802.16e-2004. It uses privacy key management protocol version 2 (PKM V2) whereas the latter uses PKM version 1. In IEEE 802.16 using PKMv1, Authorization Request message includes only the contents for SS authentication. When SS tries to establish a connection to BS, the authorization process based on RSA authentication protocol allows only BS to authenticate SS in PKMv1. There is no way to confirm whether the BS is authorized or not.. Thus, it is possible to masquerade as a Rogue BS after eavesdropping authentication related message from SS. However, in the case of Mobile WiMAX using PKMv2, possibility of Rogue BS attack is reduced. Because mutual authentication function between SS and BS is obligatory during authorization process. Also PKM V2 allows both mutual and unilateral authentication. Also it enables periodic re-authentication/reauthorization and key update. The PKMv2 provides a Message authentication scheme using HMAC or CMAC, device/user authentication using EAP methods, and confidentiality using (Advanced Encryption Scheme in counter with cipher block chaining mode) AES-CCM encryption algorithm. However, there is no guarantee that PKMv2-based Mobile WiMAX network will not have security flaws. PKMV2 based on RSA makes up for the shortcomings of PKMV1, but it does not imply that PKMV2 is absolutely safe, i.e. new attacks may occur. When an MS is switching from one sector to another, the key space is vulnerable i.e., AKs (Authentication key) and TEKs (Traffic Encryption Key) are vulnerable to brute-force attack, Men in the middle attack, replay and Denial of service etc. Therefore this paper focuses on these security vulnerabilities and analyses the memory requirement for key storage and propose their counter measures according to each network domain together with the compression of keys for improved security of the Mobile WiMAX network.

This paper is organized as follows: In Section 2, Mobile WiMAX security is analysed considering various security attacks and vulnerabilities in the network. In section 3, solutions are proposed and algorithms are analysed. Finally section4 results are analysed and section 5 is concluded with a summary and discussion of future works.

2. VULNERABILITIES IN IEEE 802.16

With the publication of the Mobile WiMAX amendment, most of the vulnerabilities were solved in WiMAX. This section explains an assortment of vulnerabilities found in Mobile WiMAX. The security of IEEE 802.16e was only analyzed by a few papers and [1] examined the 3-way TEK exchange and the authorization process and could not find any security leak. Also [2] analyzed the key management protocol using protocol analyzing software and did not detect any problem. But [3] shows, in mobile WiMAX there are some unauthenticated and unencrypted management messages which threat the reliability of the system. These vulnerabilities are due to

a. Unencrypted management Messages
The complete management communication between MS and BS is unencrypted. If an adversary listens to the traffic, he can collect lots of information about both instances.

b. Unauthenticated messages
Mobile WiMAX includes some unauthenticated messages. Their forgery can constrict or even interrupt the communication between mobile station and base station.

2.1. Unencrypted Management Messages

Most of the management messages defined in IEEE 802.16e are integrity protected. This is done by a hash or cipher based message authentication code (HMAC/CMAC) [4]. A couple of management messages are sent over the broadcast management connection. However, some messages are not covered by any authentication mechanism. In WiMAX security architecture, there is no common key for the authentication of Broad casted management messages. An adversary collecting management information can create detailed profiles about MS including the capabilities of devices and security settings associated with the base stations. Using the data offered in power reports, registration, ranging and handover messages, a listening adversary is able to determine the movement and approximate position of the MS. IEEE 802.16 standard defines only a set of functions between SS and BS. It means that the security architecture given by IEEE 802.16 standards does not cover intra-ASN and ASN-to-CSN communication [5] [7]. So these domains become insecure and are illustrated in Figure 2.

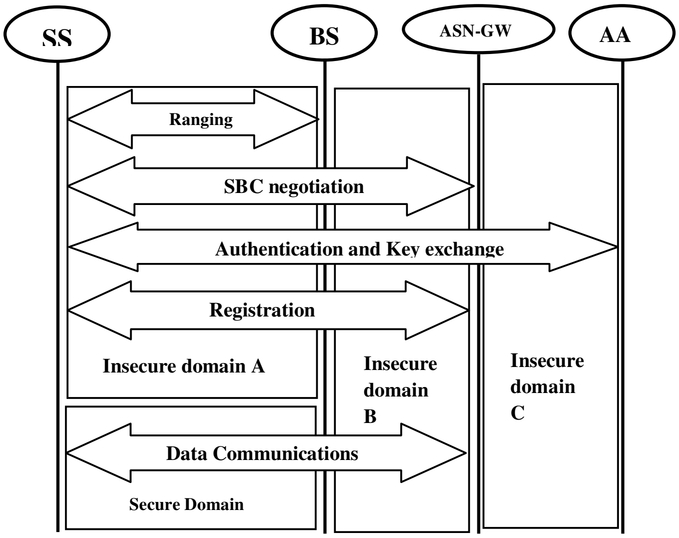


Figure.2.Access Network insecure domains

2.2. Unauthenticated Messages

In Mobile WiMAX, management messages are sent in the clear. When an MS performs initial network entry, it negotiates communication parameters and settings with the BS. A lot of information like security negotiation parameters, configuration settings, mobility parameters, power settings, vendor information, MS's capabilities etc are exchanged. However, specifically, the SBC negotiation parameters and PKM security contexts do not have any security measures to keep their confidentiality. The possibility of exposure to malicious users or outer network always exists in initial network entry process. [6] Even though Mobile WiMAX has a message authentication scheme using HMAC/CMAC codes and traffic encryption scheme using AES-CCM based on PKMv2, the security schemes are only applied to normal data traffic after initial network entry process, not to control messages during initial network entry. An attacker can easily access the security information by listening on the channel.

Initial network entry consists of four processes: Initial Ranging process, SS Basic Capability (SBC) negotiation process, PKM authentication process, and registration process. Initial network entry is the most security sensitive processes in Mobile WiMAX network as it is the first gate to establish a connection to the network. Also many physical parameters, performance factors, and security contexts between SS and serving BS are determined during this process. The initial network process and MS Basic Capability negotiation is illustrated in Figure 3. After initial network entry, the management communication over the basic and primary management connections remains unencrypted (described earlier in section 2.1). As most of the management messages are sent on these connections, nearly all management information exchanged between MS and BS can be accessed by a listening adversary.

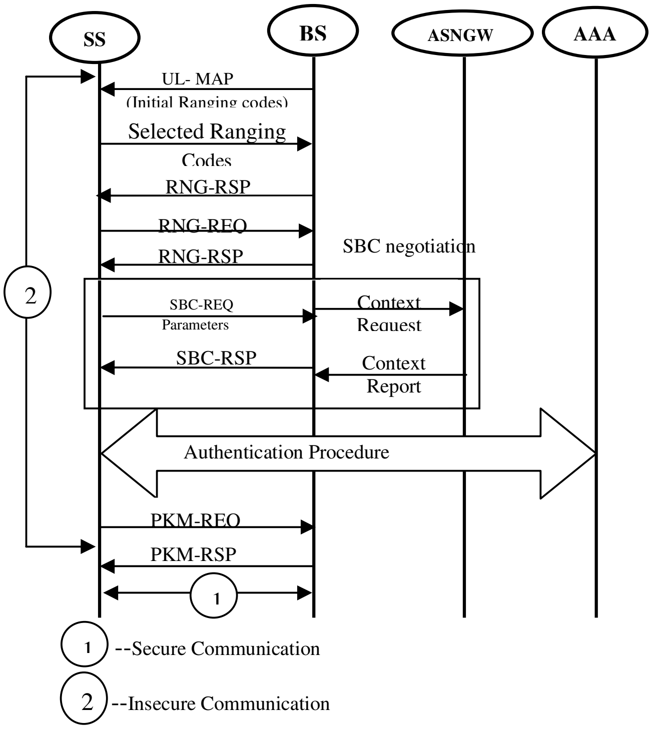


Figure.3. Initial network entry process

3. PROPOSED WORK

3.1. Security Enhancement

3.1.1. Modified Initial Network Entry Process

The Initial Network Entry procedure is the first stage in establishing connection in any WiMAX network. It should not chip in any security flaw. Since key exchange is done through Diffie-

Hellman, possibility for Man in the middle attack makes the network scrawny by eavesdropping, interception and interruption of the management messages, resulting in a breach in the reliability of the entire network as it involves the transmission of unencrypted management messages. Also there is no appropriate method to secure the critical information. Hence it results in lack of confidentiality. To overcome this, it is proposed to modify the Diffie Hellman key exchange process by including Hash based authentication as illustrated in Figure.4.

When MS is powered on, it firsts scans the downlink channel to determine whether it is currently in the coverage of base station. Each MS stores the list of optional parameters, such as DL frequency. MS synchronizes with the stored DL frequency of the suitable BS. Once the DL synchronization is completed, MS can listen to various control messages, from which it obtains the UL parameters. Based on these UL parameters, MS decides whether the channel is suitable or not. If the channel is suitable MS performs ranging, otherwise it again starts scanning the channel. Ranging process acquires timing and power level adjustment to maintain the UL connection with the BS. BS sends a set of ranging codes to the subscriber station for synchronization. Initial ranging procedure is started when SS receives UL-MAP message including ranging codes.

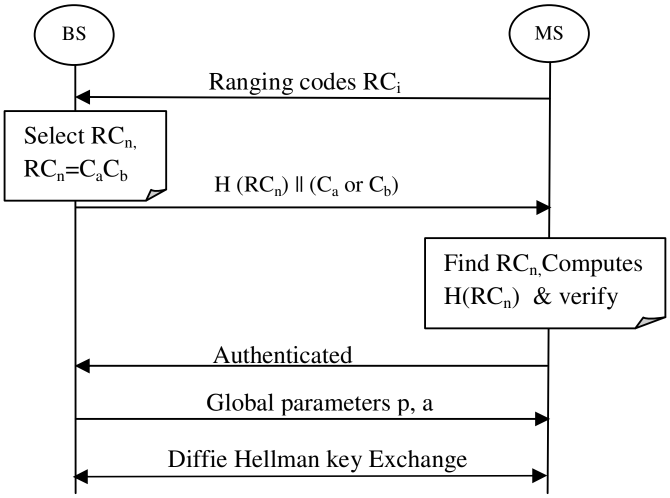


Figure.4. Modified initial network process

```
ALGORITHM-1: Ranging Process
1. BS sends ranging codes $RC_i$ where i=1,2,.....n to MS i.e., $RC_i \rightarrow MS$
2. MS selects a code{ $RC_n=C_a,C_b$ }
3. Computes $H(RC_n) \| (C_a \text{ or } C_b)$
4. Sends $H(RC_n) \| (C_a \text{ or } C_b)$ to BS
5. BS receives $H(RC_n) \| (C_a \text{ or } C_b)$
6. if $(C_a \text{ or } C_b)$ □ $RC_i$ then
      Selects corresponding code $RC_x$
      Computes $H(RC_x)$
7. if $H(RC_x) == H(RC_n)$ then
      MS is authorised
      Starts Diffie-Hellmann Key Exchange
                  (Proceeds as per algorithm 2)
   end if
   else Access denied
   end if
```

Figure.5a Algorithm- Modified Initial Network Entry Process

In the proposed model SS selects any one of the ranging codes say RC_n where $RC_n=C_aC_b$. If the ranging code contains two parts, SS selects any one part and sends the hashed value of the ranging code together with this. On reception BS compares the received ranging code part with the pool of ranging codes and identifies the corresponding complete ranging code. Then it hashes the ranging code and compares it with the received hashed ranging code. If it matches, common key will be shared through Diffie-Hellman key exchange. Else it will be declared as unauthorised user and access will be denied. Once the SS is authorized in further steps, it generates other global variable "*g*" and public/private key pair and then sends them to BS.BS receives a public key of SS and global variables (prime number and its primitive root). If the received key and variables are verified, BS also sends his public key to SS. Thus BS and SS can share Diffie-Hellman global variables and public key with each other through initial ranging process securely. With this key exchange, shared common key called "pre-TEK" is generated which could be used for further encryption of ranging messages for secure communication. Therefore, the proposed method protects the SBC security parameters and PKM security contexts using the shared traffic encryption key (pre-TEK) during initial network entry procedure. The algorithm for this process is illustrated in Figure.5a, 5b.

```
ALGORITHM-2: Diffie-Hellman Key Exchange
1. BS selects
         Prime number p
         Primitive root of P i.e. a such that $a<p$
         Private Key Xa such that $Xa<p$
2. Computes public Key $Ya=a^{Xa} \bmod p$
3. BS sends a,p ,Ya
4. MS selects Private Key Xb such that $Xb<p$
5. Computes public Key $Yb=a^{Xb} \bmod p$
6. MS sends Yb to BS
7. BS and MS computes session key as
$Key\_MS=a^{yb} \bmod p$ ;    $Key\_BS=a^{ya} \bmod p$
such that      Key_MS=KEY_BS
```

Figure.5a Algorithm- Modified Initial Network Entry Process

3.1.2 Modified Access Network Security

PKM security architecture covers only the traffic between mobile station and base station. WiMAX Forum assumes that ASN network is trusted and AAA connections between ASN and CSN may be protected with IPSec tunnel. However, there are a lot of possibilities for new security holes to happen including various zero-day attacks. Moreover, IPSec requires additional software and hardware facilities for supporting whole Mobile WiMAX domains. So this paper proposes a device certificate based key exchange method. All devices in mobile WiMAX network have device certificate. Also, it is assumed that all devices are certified by public authority and certificates can be verified through certificate chain. All devices have a certificate chain together with their own certificate. It is illustrated in Figure.6 and the algorithm is illustrated in Figure.7 and 8.

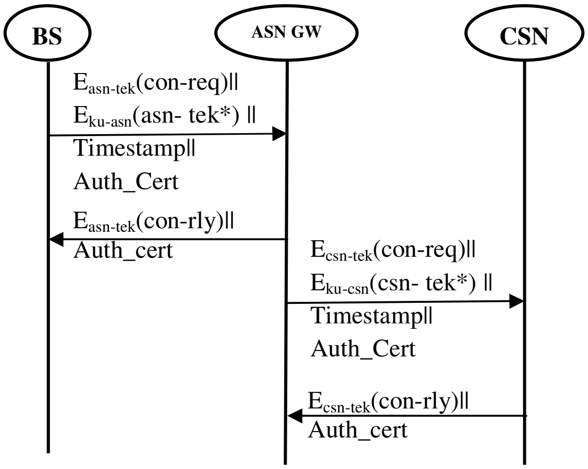


Figure.6. Modified Access Network Entry

BS and ASN-GW should generate a secret session key in order to exchange message with ASN-GW and CSN. BS, ASN-GW, and CSN have the certificate chain. To exchange message, BS encrypts the message with session key generated (ASN-TEK) padded with the time stamp and the authority certificate. A common key would not completely protect the integrity of the message as the key shared by the mobile station can be generated by unauthenticated BS. Consequently in addition with the encrypted message, the session key is also encrypted with the public key of ASN-GW and padded with the message. When ASN-GW receives the message it verifies the authority certificate and then checks the timestamp for validity.

```
ALGORITHM-3: Access Service Network
// Between ASN_GW and BS //
1. BS,ASNGW gets the certificate chain from Authority
        cert_chain =
   {Auth_cert,BS_cert,ASNGW_cert,CSN_cert}
2. BS sends ASN_GW
        $E_{asn-tek}$(con-req) || $E_{ku-asn}$(asn-tek*) ||Timestamp
                    || Auth_cert
3. ASN_GW verifies timestamp & authority certificate
4. if verified then
        Computes $D_{kr-asn}$(asn-tek*)
        Decompress asn-tek*
        Computes $D_{asn-tek}$(req)
   else  Access denied
   end if
5. ASN_GW sends BS , $E_{asn-tek}$(con-rly) || Auth_cert
6. BS verifies authority certificate
7. if Verified then
        Decrypt reply as $D_{asn-tek}$(rly)
   else Deny access
   endif
8. Connection Established
```

Figure.7. Algorithm-Access Service Network Security

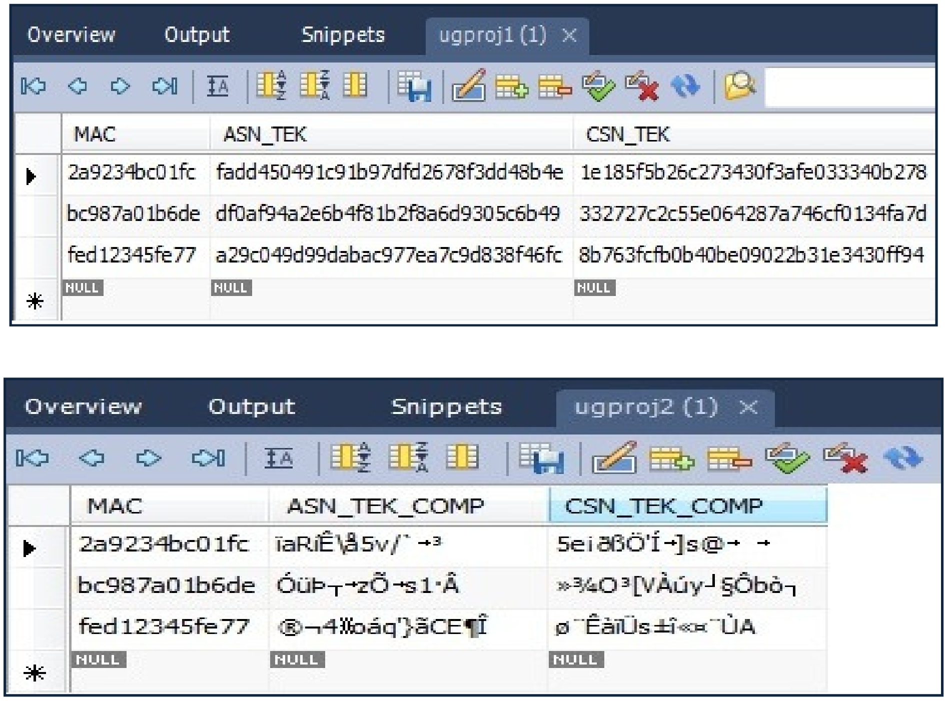
```
ALGORITHM-4: Connectivity Service Network
                    // Between ASN_GW and CSN //
1. ASNGW, CSN gets the certificate chain from
Authoritycert_chain
={Auth_cert,BS_cert,ASNGW_cert,CSN_cert}
2. ASN_GW  sends CSN
      $E_{csn-tek}$(con-req) || $E_{ku-csn}$(csn-tek*) ||Timestamp ||
                    Auth_cert
3.CSN verifies timestamp & authority certificate
4. if verified then
        Computes $D_{kr-csn}$(csn-tek*)
        Decompress csn-tek*
        Computes $D_{csn-tek}$(req)
   else Access denied
   end if
5. CSN sends ASN_GW , $E_{csn-tek}$(con-rly) || Auth_cert
6. ASN_GW verifies authority certificate
7. if  Verified then
         Decrypt reply as $D_{csn-tek}$(rly)
   else Deny access
   endif
8. Connection Established
*→compressed key
```

Figure.8 . Algorithm - Connectivity Service Network.

On successful verification ASN-GW decrypts the message and ASN-TEK key. ASN-GW replies by encrypting the connection reply message with the ASN-TEK padded with the authority certificate. Similarly for Connectivity service network, CSN-TEK is generated as common encryption key. Thus the secret session key eliminates the insecurity existing between BS-ASN-GW and ASN-GW-CSN. Hence a secure communication is established. To enhances the security and to reduce the authentication cost the session key is compressed (compression explained in section 3.2) and then transferred.

3.2 Authentication Cost Reduction

Any secured system can be modelled as a capability-based access control system in which each user is given a set of secret keys to access the granted resources. In resource-constrained devices, the design is sensitive to memory or key storage cost. Data compression saves the transmission time and disk space and more importantly it strengthens the cryptographic security. To crack the cipher, cryptanalysis utilises the pattern found in the plain text. Compression reduces these patterns in the plaintext, thereby increasing the resistance towards cryptanalysis. With a goal to minimize the maximum users' key storage and to enhance security, this paper proposes compression of the cryptographic key. In case of access network security the transferred key is encrypted whereas the buffer space required still remains the same. To reduce this, the transferred key is compressed through Huffman key compression technique and then encrypted for transmission. Huffman coding is an entropy encoding algorithm used for lossless data compression. It uses variable-length code table for encoding. Huffman coding results in prefix code for representing each symbol i.e. the bit string representing some particular symbol is never a prefix of the bit string representing any other symbol. Huffman compression expresses the most common source symbols using shorter strings of bits than are used for less common source symbols.



MAC	ASN_TEK	CSN_TEK
2a9234bc01fc	fadd450491c91b97dfd2678f3dd48b4e	1e185f5b26c273430f3afe033340b278
bc987a01b6de	df0af94a2e6b4f81b2f8a6d9305c6b49	332727c2c55e064287a746cf0134fa7d
fed12345fe77	a29c049d99dabac977ea7c9d838f46fc	8b763fcfb0b40be09022b31e3430ff94
NULL	NULL	NULL

MAC	ASN_TEK_COMP	CSN_TEK_COMP
2a9234bc01fc	ïaRÍÊ\å5v/ˆ →³	5eiãßÖ'Í→]s@→ →
bc987a01b6de	ÓüÞ┬→zÕ→s1·Â	»¾O³[VÀúy┘§Ôbò┐
fed12345fe77	®¬4‰áq'}ãCE¶Î	ø¨ÊàïÜs±í«¤¨ÙA
NULL	NULL	NULL

Figure.9. Database – Key storage

BS compresses ASN-TEK then encrypt and pad it with the encrypted request timestamp and the authority certificate, and send it to ASN-GW.ASN-GW verifies the timestamp and certificate and then decrypt and later on decompress the message. The same procedure is repeated for message transaction in connectivity service network. All the keys are stored in the centralised authority's database as shown in Figure.9

4. RESULTS AND ANALYSIS

The developed IEEE 802.16e mobile WiMAX model using Qualnet , shown in Figure.10, represents 12 mobile nodes. Nodes 1,2,3 represents the access points. Connection between nodes 5 & 10 is through CBR and between nodes 4 & 8 is through FTP. The flags represent the mobility of the nodes.

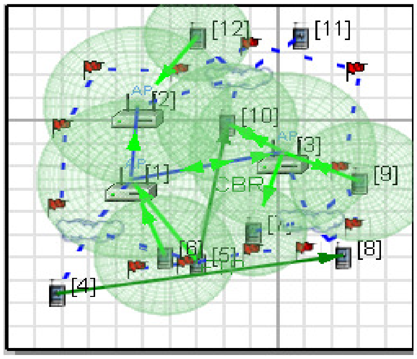
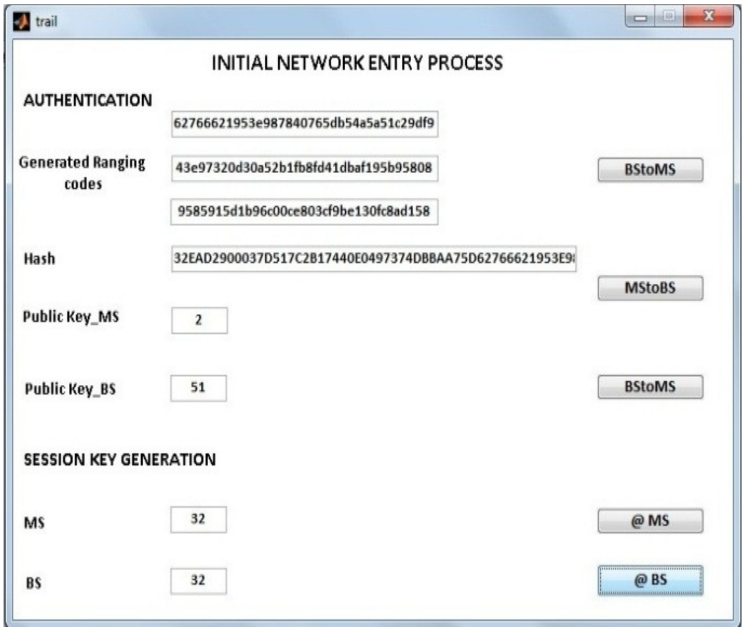


Figure.10 .IEEE 802.16e mobile wimax model

Figure.11 represents the Matlab-GUI implementation of the proposed network entry procedure. It indicates the authentication procedure using Hash based entity verification and Diffie Hellman Key exchange. The Base Station selects and sends three ranging codes to MS.MS selects the first code and compute the hash value and send it back to BS together with its public key. BS after verifying the identity authenticates the MS and sends it public key. With these keys both generate a common session key individually. It has been shown in the result that both the keys generated at BS and MS are identical. With this proposed approach the computation time increases from 0.4840s to 0.8110s and thereby increases the computational effort and security.



INITIAL NETWORK ENTRY PROCESS

AUTHENTICATION

62766621953e987840765db54a5a51c29df9

Generated Ranging codes

43e97320d30a52b1fb8fd41dbaf195b95808

9585915d1b96c00ce803cf9be130fc8ad158

Hash 32EAD2900037D517C2B17440E0497374DBBAA75D62766621953E9

Public Key_MS 2

Public Key_BS 51

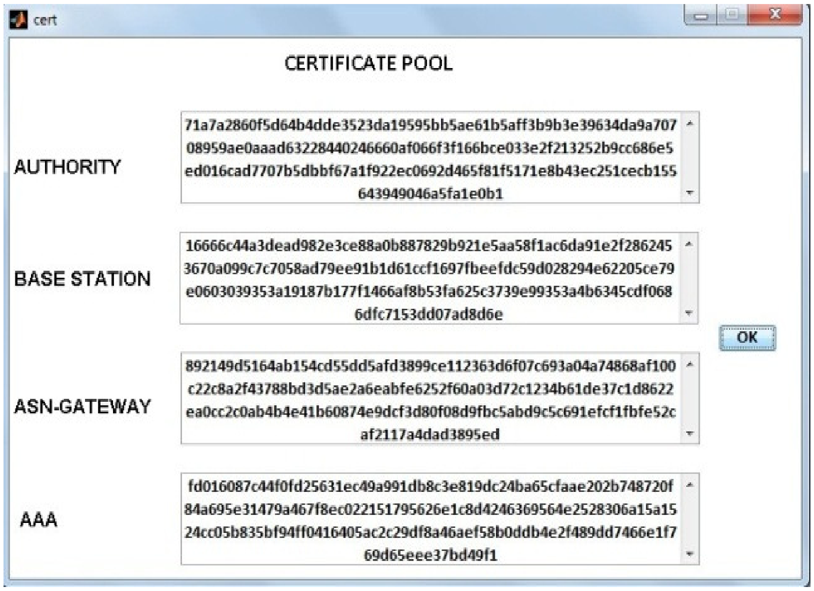
SESSION KEY GENERATION

MS 32

BS 32

Figure.11.Generated Matlab GUI-Initial Network Entry Procedure

In case of access network security since the authentication in based on device certificate, each user holds the certificate chain as shown in Figure.11, issued by the authority from which each user and BS can verify the authenticity of other users.



CERTIFICATE POOL

AUTHORITY

71a7a2860f5d64b4dde3523da19595bb5ae61b5aff3b9b3e39634da9a707
08959ae0aaad63228440246660af066f3f166bce033e2f213252b9cc686e5
ed016cad7707b5dbbf67a1f922ec0692d465f81f5171e8b43ec251cecb155
643949046a5fa1e0b1

BASE STATION

16666c44a3dead982e3ce88a0b887829b921e5aa58f1ac6da91e2f286245
3670a099c7c7058ad79ee91b1d61ccf1697fbeefdc59d028294e62205ce79
e0603039353a19187b177f1466af8b53fa625c3739e99353a4b6345cdf068
6dfc7153dd07ad8d6e

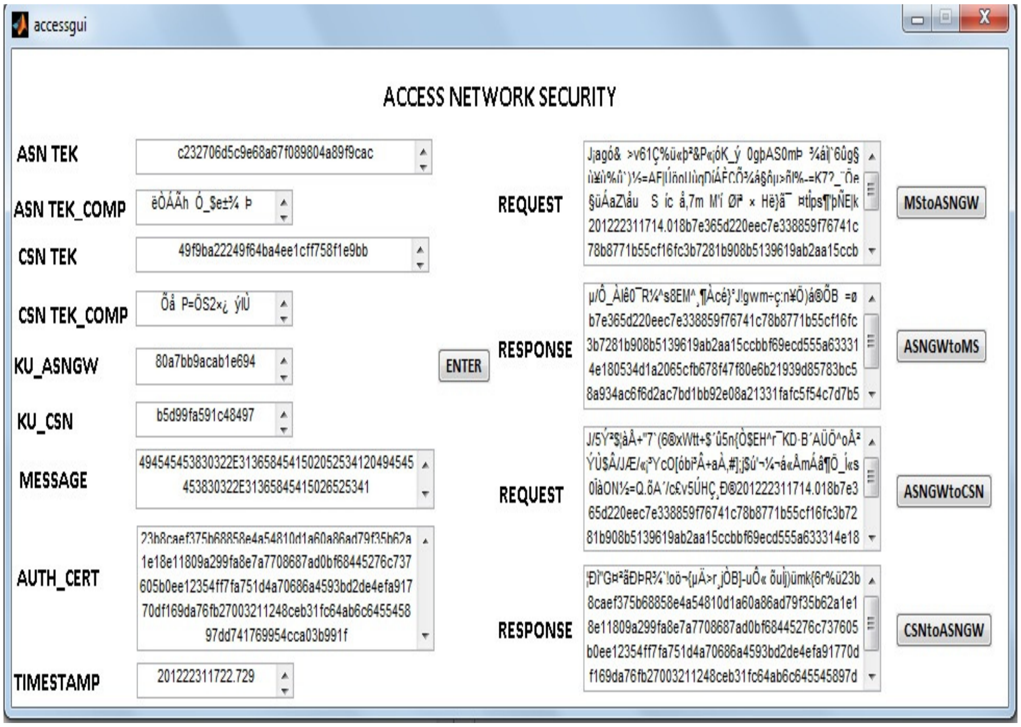
ASN-GATEWAY

892149d5164ab154cd55dd5afd3899ce112363d6f07c693a04a74868af100
c22c8a2f43788bd3d5ae2a6eabfe6252f60a03d72c1234b61de37c1d8622
ea0cc2c0ab4b4e41b60874e9dcf3d80f08d9fbc5abd9c5c691efcf1fbfe52c
af2117a4dad3895ed

AAA

fd016087c44f0fd25631ec49a991db8c3e819dc24ba65cfaae202b748720f
84a695e31479a467f8ec022151795626e1c8d4246369564e2528306a15a15
24cc05b835bf94ff0416405ac2c29df8a46aef58b0ddb4e2f489dd7466e1f7
69d65eee37bd49f1

Figure.12.Generated Matlab GUI-Certificate Pool



ASN TEK c232706d5c9e68a67f089804a89f9cac

ASN TEK_COMP ëÒÁÃh Ó_$e±¾ Þ

CSN TEK 49f9ba22249f64ba4ee1cff758f1e9bb

CSN TEK_COMP Õå P=ÖS2×¿ ýlÙ

KU_ASNGW 80a7bb9acab1e694

KU_CSN b5d99fa591c48497

MESSAGE 494545453830322E313658454150205253412049454545
3830322E313658454150265253 41

AUTH_CERT 23b8caef375b68858e4a54810d1a60a86ad79f35b62a
1e18e11809a299fa8e7a7708687ad0bf68445276c737
605b0ee12354ff7fa751d4a70686a4593bd2de4efa917
70df169da76fb27003211248ceb31fc64ab6c6455458
97dd741769954cca03b991f

TIMESTAMP 201222311722.729

REQUEST
J¡agó& >v61Ç%ü«þ²&P«¡óK_ý 0gþAS0mÞ ¾áì`6ûg§
ì¥ì%î`)½=AF|ÚòoÙùqDíÁÈÇÕ³¼á§ôµ>ñl%-=K7?_¨Õe
§üÁaZ\åu S íc å,7m M'í Øí² × Hë}ã¯ ¤tÎps¶þÑE|k
201222311714.018b7e365d220eec7e338859f76741c
78b8771b55cf16fc3b7281b908b5139619ab2aa15ccb

RESPONSE
µ/Ô_ÀIê0¯R¼^s8EM^¸¶Àcé}°J!gwm÷ç:n¥Ö)á®ÕB =ø
b7e365d220eec7e338859f76741c78b8771b55cf16fc
3b7281b908b5139619ab2aa15ccbbf69ecd555a63331
4e180534d1a2065cfb678f47f80e6b21939d85783bc5
8a934ac6f6d2ac7bd1bb92e08a21331fafc5f54c7d7b5

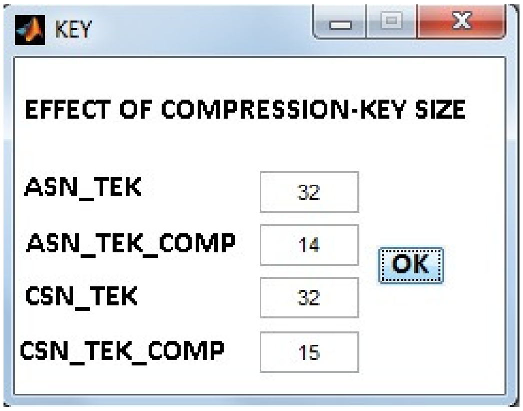
REQUEST
J/5Ý²$¦àÅ+"7`(6®xWtt+$´û5n{Ò$EH^r¯KD-B´AÜÖ^oÅ²
ÝÙ$Â/JÆ/«¡³YcO[óbì²Â+aÀ,#];j$ú'¬¼¬á«ÅmÁâ¶Ö_Í«s
0ÏàON½=Q.õA´/c£v5ÚHÇ¸Ð®201222311714.018b7e3
65d220eec7e338859f76741c78b8771b55cf16fc3b72
81b908b5139619ab2aa15ccbbf69ecd555a633314e18

RESPONSE
¦ÐÌ"G¤²ãÐÞR¾`!oö¬{µÄ>r¸jÒB]-uÔ« õuÌj)ümk{6r%ü23b
8caef375b68858e4a54810d1a60a86ad79f35b62a1e1
8e11809a299fa8e7a7708687ad0bf68445276c737605
b0ee12354ff7fa751d4a70686a4593bd2de4efa91770d
f169da76fb27003211248ceb31fc64ab6c645545897d

Figure.13.Generated MATLAB GUI-Modified Access Network Security

Figure.13 represents the MATLAB generated GUI for the proposed access network security. It shows the various session keys and their compressed counterpart. AUTH_CERT represents the device certificate used for the authentication of the entities. REQUEST and RESPONSE indicates the connection request and response to and fro the entities which includes the encrypted message, key, certificate and the timestamp.

The compression results are discussed below in Figure.14.Results shows that the actual key size 32 hexa digits in reduced to 14(ASN_TEK) , 15(CSN_TEK).This reduces the memory and bandwidth required for key storage and transmission and hence the authentication cost. The compression concept has been implemented for multiple users and the resultant graph is shown in Figure.15. For 32 hex bit data compression reduces the key size varying from 5 to 16 bits. Assuming an average of 10 to 15 bits reduction for single user the graph has been plotted. From the graph it has been identified that without compression total buffer space required for 10 users is 160 bytes. But compression reduces this to more than 50% i.e.63 bytes. Compression increases the computation time to 0.2650s. When the proposed work is done without compression the computation time is 0.2340s whereas under existing approach it is 0.1870s. Even though the computational time increases, computational effort is also increased on the other hand. From the results it has been identified that compression reduces the memory and hence the bandwidth to a minimum of 50%.



EFFECT OF COMPRESSION-KEY SIZE

ASN_TEK 32

ASN_TEK_COMP 14

CSN_TEK 32

CSN_TEK_COMP 15

Figure.14.Generated Matlab GUI-Compression Result

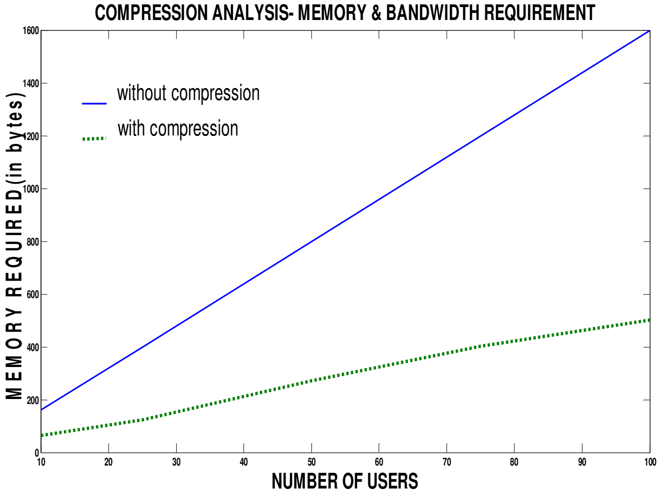


Figure.15. Compression analysis.

5. CONCLUSION & FUTURE WORK

WiMAX has taken WMAN networks to next level. It is therefore vital to explore and perk up the security aspects of such a future generation network. So this paper proposes authentication of management communication and compression as a key to improve the security of the WiMAX network. This approach reduces the possibility for Man in the middle attack, scrambling, jamming and thereby increases the security of the network. Further compression reduces the key size, saves the transmission time and disk space and more importantly it strengthens the cryptographic security. Result shows that compression reduces key buffer space to a minimum of 50% and provides ample reduction in the bandwidth. For further enhancement, our work will also be implemented in hardware using FPGA (Field Programmable Gate Array).

REFERENCES

[1] Yuksel E , (2007) "Analysis of the PKMv2 Protocol in IEEE 802.16e-2005 Using Static Analysis Informatics and Mathematical Modelling", Technical University Denmark, DTU.

[2] Andreas Deininger, Shinsaku Kiyomoto, Jun Kurihara, Toshiaki Tanaka,(*2007*) "Security Vulnerabilities 683 and Solutions in Mobile WiMAX", *IJCSNS International Journal of Computer Science and Network Security,* VOL.7 No.ll.

[3] Taeshik Shon,1 Bonhyun Koo,1 Jong Hyuk Park,2 and Hangbae Chang3:"Novel Approaches to Enhance Mobile WiMAX Security" , *Hindawii.*

[4] Prof. Pranita K. Gandhewar , "Improving security in initial Network entry process of IEEE 802.16" , *International Journal on Computer Science and Engineering.*

[5] Gaurav Soni and Sandeep Kaushal, "Analysis of security issues of mobile wimax 802.16e and their solutions".

[6]Beth N. Komu, Mjumo Mzyece and Karim Djouani, "Formal Verification of Initial Network Entry in WiMAX Networks".

[7] 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.*

[8] Muhammad Sakibur Rahman, Mir Md. Saki Kowsar: (2009) "WiMAX Security Analysis and Enhancement" , *12th International Conference on Computer and Information Technology (Dhaka, Bangladesh.*

[9] Jam shed Hassan , "Security Issues of IEEE 802.16 (WiMAX)"

[10]Wiley, "*WiMAX Security and Quality of Service*" , A John Wiley and Sons, Ltd., Publication.

Authors

B.Sridevi, Assistant Professor of ECE Department of Velammal College of Engineering & Technology, Madurai, obtained her B.E., degree from A.C.C.E.T Karaikudi , Madurai Kamaraj University, Madurai and M.E. degree from Anna University, Chennai. She has 2 years of Industrial experience, 10 years of Teaching,and Research experience. Pursuing Ph.D. in Anna University, Tirunelveli in Networking. She published many research papers in International journals, national and international conferences. Her area of research includes Network Security, Wireless Networks. Email id: [1]aisveriya@yahoo.com

Dr.S.Rajaram working as Associate Professor of ECE Department of Thiagarajar College of Engineering, Madurai, obtained his B.E., degree Thiagarajar College of Engineering from Madurai Kamaraj Univeristy, Madurai and M.E. degree from A.C.C.E.T Karaikudi. He was awarded PhD by Madurai Kamaraj University in the field of VLSI Design. He was awarded PDF from Georgia Institute of Technology, USA in 3D VLSI. He has 16 years of experience of teaching and research. His area of research includes VLSI Design, Network Security, Wireless Networks. He has published many research papers in International journals, national and international conferences.

M.Brindha, Under Graduate scholar, pursuing B.E degree in the Department of Electronics and Communication Engineering at Velammal College of Engineering and Technology, Madurai. Her area of interest includes Computer Networks, Network Security, and Wireless Networks. Email id: brindhamayakrishnan@gmail.com

R.Umamaheswari , Under Graduate scholar, pursuing B.E degree in the Department of Electronics and Communication Engineering at Velammal College of Engineering and Technology, Madurai. Her area of interest includes Computer Networks, Network Security, and Wireless Networks. Email id:umaramaraj.n@gmail.com