Analysis on Mobile WiMAX Security

Perumalraja Rengaraju, Chung-Horng Lung, Yi Qu
Department of Systems and Computer Engineering
Carleton University, Ottawa, Ontario, Canada
{rpraja, chlung, quyi }@sce.carleton.ca

Anand Srinivasan
EION Inc.
Ottawa, Ontario, Canada
anand@eion.com

***Abstract*— Security support is mandatory for any communication networks. For wireless systems, security support is even more important to protect the users as well as the network. Since wireless medium is available to all, the attackers can easily access the network and the network becomes more vulnerable for the user and the network service provider. In the existing research, there is lack of integrated presentation of solutions to all the security issues of mobile WiMAX network, which is important for researchers and practitioners. This paper discusses all the security issues in both point-to-multipoint and mesh network and discusses their solutions. In addition, a new recommendation is also proposed for one of the security issues.**

Keywords – WiMAX; Security

I. Introduction

WiMAX is the emerging broadband wireless technologies based on IEEE 802.16 standards [1]. The security sublayer of the IEEE 802.16d [1] standard defines the security mechanisms for fixed and IEEE 802.16e [2] standard defines the security mechanisms for mobile network. The security sublayer supports are to: (i) authenticate the user when the user enters in to the network, (ii) authorize the user, if the user is provisioned by the network service provider, and then (iii) provide the necessary encryption support for the key transfer and data traffic.

The previous IEEE 802.16d standard security architecture is based on PKMv1 (Privacy Key Management) protocol but it has many security issues. Most of these issues are resolved by the later version of PKMv2 protocol in IEEE 802.16e standard which provides a flexible solution that supports device and user authentication between a mobile station (MS) and the home connectivity service network (CSN). Even though both of these standards brief the medium access control (MAC) and physical (PHY) layer functionality, they mainly concentrate on point-to-multipoint (PMP) networks. In the concern of security, mesh networks are more vulnerable than the PMP network, but the standards have failed to concentrate on the mesh mode.

Various methods have been proposed to address the security flaws revealed in the standards. However, there is lack of an integrated view of all solutions and comparison of those solutions. The integrated presentation is important to researchers and practitioner to understand the problem domain effectively and probably propose more secure mechanisms in the future. The objective of this paper is to conduct a comprehensive survey on existing security mechanisms and compare them. In addition, a recommendation for one security issue is also provided.

The rest of the paper is organized as follows: The network architecture and its security supports are discussed in the next section. Section III discusses the PMP and mesh network security issues and its counter measures from the existing research efforts. Section IV is the conclusion.

II. Network Architecture and security supports

A. Point-to-Multipoint Network

The goal of the IEEE 802.16e Security Sublayer is to provide the mutual authentication for access control and confidentiality of the data link layer [2]. It has two component protocols: (i) an encapsulation protocol for data encryption and authentication algorithms, (ii) a key management protocol (PKM) providing the secure distribution of keying data from the BS to the MS [2]. The following describes the main functionalities in more detail.

Authentication in IEEE 802.16e: Authentication addresses establishing the genuine identity of the device or user wishing to join a wireless network [32]. In IEEE 802.16e authentication is achieved by using the public key interchange protocol, which ensures not only authentication but also the establishment of encryption keys. The PKM protocol allows three types of authentication [3]:

i. RSA based authentication - X.509 digital certificates together with RSA encryption
ii. Extensible Authentication Protocol (EAP) based authentication
iii. RSA based authentication followed by EAP authentication

In the RSA based authentication, a BS authenticates the MS by virtue of its unique X.509 digital certificate which has been issued by the MS manufacturer. The X.509 certificate contains the MS's Public Key (PK) and its MAC address. When requesting an AK, the MS sends its digital certificate to the BS. The BS validates the certificate and then uses the verified PK to encrypt an AK which is then sent back to the MS. All the MSs that use RSA authentication have factory installed private/public key pairs together with factory installed X.509 certificates.

In the case of EAP based authentication [3], the MS is authenticated either through a unique operator issued credential, such as a SIM or though an X.509 certificate. WiMAX forum suggests any of the three following methods and the choice is depends on operator's implementation:

i. EAP-AKA (Authentication and Key Agreement) for SIM based authentication,

ii. EAP-TLS (Transport Layer Security) for X.509 based authentication

iii. EAP-TTLS (Tunneled TLS) for MS-CHAPv2 (Microsoft-Challenge Handshake Authentication Protocol)

The security architecture of the EAP-TLS is defined in RFC 5216 [33] and it is robust as long as the user understands potential warnings about false credentials.

Fig.1 shows the layering of PKMv2 user Authentication protocols. PKMv2 transfers EAP over the IEEE 802.16 air interface between MS and BS in Access Service Network (ASN). Depending on the Authenticator location in the ASN, a BS may forward EAP messages over Authentication Relay protocol to Authenticator. The AAA client on the Authenticator encapsulates the EAP in AAA protocol packets and forwards them via one or more AAA proxies to the AAA Server in the CSN of the home Network Service Provider (NSP), which holds the subscription with the Supplicant.

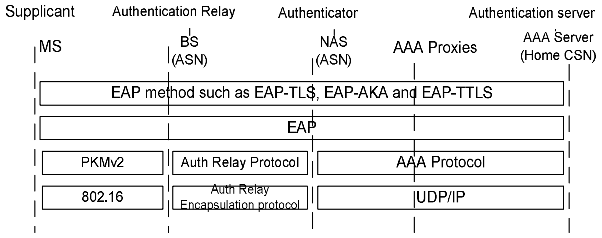

Fig. 1: *PKMv2 User Authentication Protocols [3]*

User Authorization [3, 10]: This is a request for an AK as well as for an SA identity (SAID) to authorize the user credentials. The Authorization Request includes MS's X.509 certificate, encryption algorithms and cryptographic ID. In response, the BS carries out the necessary validation (by interacting with an AAA server in the network) and sends back an Authorization reply which contains the AK encrypted with the MS's public key, a lifetime key and an SAID. After the initial authorization from AAA, the BS reauthorizes the MS periodically.

Traffic Encryption [1]: Application data are encrypted by Traffic Encryption Key (TEK), which is generated as a random number in the BS using the TEK encryption algorithm. The Key Encryption Key (KEK) is used for encrypting the TEK before the key transfer from BS. The KEK is 128 bits long, which is derived directly from the 160 bits long AK.

Privacy and key management [15]: A PKM protocol instance establishes a data Security Association (SA) between BS and MS. A SA is defined as the set of security information shared between a BS and one or more of the MSs connected to that BS in order to support secure communications across the WiMAX access network. Three types of SAs have been defined - primary, static and dynamic [1]. Each MS establishes a primary SA during the MS initialization phase. Static SAs are provided within the BS. Dynamic SAs are created and destroyed in real time in response to the creation and termination of service flows. Each MS can have several service flows on the go and can therefore have several dynamic SAs. The Hashed Message Authentication Code (HMAC) digests are used to encrypt the message transfer. By computing the value HMAC, MS and BS detect forgeries.

Network Entry Procedure [3]: Fig.2 shows the detailed Network entry procedure suggested by the NWG. Upon successful completion of ranging, the MS SHALL send the SBC_Req message and BS in ASN SHALL respond to the MS by sending the SBC_Rsp, see step (1) in Fig. 2. During this SBC negotiation, the PKM version, PKMv2 security capabilities and authorization policy including requirements and support for Device Authentication are negotiated. This causes the Authenticator to begin the EAP sequence.

EAP Exchange: The authenticator in ASN sends an EAP-Identity request to the MS and the MS will respond to the request by sending PKM-REQ (PKMv2 EAP-Transfer) message, as depicted in step (2).

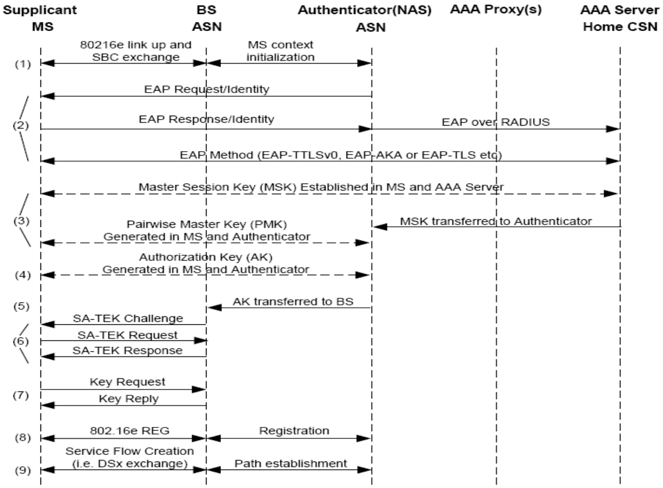

Fig. 2: PKMv2 Procedure during Initial Network Entry [3]

Master Session Keys (MSK and EMSK) establishment: The Home AAA Server generates the MSK and EMSK, and then transfers the generated MSK to the Authenticator in the ASN. The EMSK is retained at the Home AAA Server to generate the mobility keys. From the MSK, both the MS and the Authenticator generate a Pairwise Master Key (PMK) as per IEEE 802.16e specifications, as shown in step (3).

Authentication Key (AK) generation: The Authenticator and the MS generate the AK from the PMK based on the algorithm specified in the IEEE 802.16e, as shown in step (4).

AK Transfer: The Key Distributor entity in the Authenticator delivers the AK and its context to the Key Receiver entity in the Serving BS, as depicted in step (5).

SA-TEK exchange: The MS and the BS perform PKMv2 in three-way handshake procedure as per IEEE 802.16e specification, as shown in step (6).

TEK message transfer, Registration and service flow creations are the subsequent process based on IEEE 802.16e standard, as shown in steps (7), (8) and (9).

B. Mesh Network

WiMAX mesh mode network has mesh base stations. New subscriber stations are called as client nodes (CNs) and the active subscriber stations are called sponsor nodes (SNs), since SNs have the capability to sponsor new CNs. The nodes which are one hop away are called neighbor nodes and more than one hop distance nodes are called extended neighbor nodes [1].

The CNs will continuously scan every possible frequency channel and build the physical neighbor list. From the established neighbor list, the new node selects a sponsor node having the best signal quality. Then, the new node synchronizes its time with the chosen sponsor node and sends out a Network Entry Request message (MSH-NENT message with Type=0x02) [1]. The joining node authenticates itself to the sponsor node using an *Operator Authentication Value [5]*, which is an authenticated hash of the MAC address and the node serial number using the shared secret authorization key (AK) as depicted below.

HAMC (MAC address|Node Serial Number|AK)

Upon receiving this entry request message, the sponsor node will evaluate the request and decide to open or reject a sponsor channel for the new node. If the sponsor node finds an invalid operator authentication value or excess propagation delay or not possible to support additional new nodes, it will reject the entry request and respond in MSH-NCFG message with Type=0x03. If the sponsor node accepts the request, it will send out MSH-NCFG message with Type=0x02. Then, the new node acknowledges the acceptance by replying MSH-NENT message with Type=0x01 [1].

Authorization and TEK exchange [8]: The new node performs the authorization via the sponsor node. First it sends the privacy key management request (PKM-REQ) message with authentication information. Subsequently, the new node sends PKM-REQ message with authorization request PKM-REQ: Auth Request to the sponsor node with the fields indicating X.509 certificate and supporting cryptographic algorithms. The sponsor node will tunnel the received messages over UDP/IP to the authentication node. In response to the authorization request, the Authentication Node validates the requesting new node's identity, determines the encryption algorithms and authentication key, and sends back the PKM Response message with authorization reply (PKM-RSP) to the sponsor node. Then, the sponsor node forwards the message [8] to the new node as shown in Fig.3.

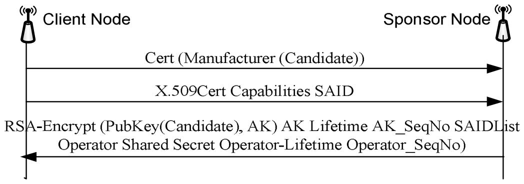
Client Node
Sponsor Node
Cert (Manufacturer (Candidate))
X.509Cert Capabilities SAID
RSA-Encrypt (PubKey(Candidate), AK) AK Lifetime AK_SeqNo SAIDList
Operator Shared Secret Operator-Lifetime Operator_SeqNo)

Fig. 3: *Client Node Authorization*

The first exchange is the Key Request message which contains the candidate node's X.509 certificate and SAID. The Key Request message is protected from modification with a HMAC digest. The Key Reply message includes the current AK sequence number, SAID, and Traffic Encryption key parameters-encrypted with the candidate node's public key. The TEK parameters include the old and new TEKs, their remaining lifetime and a 2-bit sequence number. The key reply message also contains an HMAC digest. Nodes use the Operator Shared Secret to calculate the HMAC digest for key request and key reply.

Neighbor Authentication [8]: Once the node has been successfully authorized, it activates a TEK exchange for each SAID with its neighbors. The messages are shown in Fig.4.

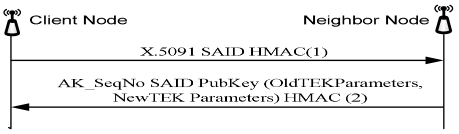
Client Node
Neighbor Node
X.5091 SAID HMAC(1)
AK_SeqNo SAID PubKey (OldTEKParameters,
NewTEK Parameters) HMAC (2)

Fig. 4: *Neighbor Node Authentication*

Registration and connectivity: Now the joining node can register and obtain an IP address and start forming links to other nodes in the mesh with the same AK value.

III. SECURITY ISSUES AND COUNTER MEASURE - ANALYSIS

Security threats may occur in both the PHY and the MAC layers [22]. The attacker attacks with Radio Frequency (RF) channel for PHY layer threats. For MAC layer threats, the attackers spoof, modify and reply the MAC layer messages. In this paper, we concentrate only on MAC layer issues. The following sub-sections discuss the PHY layer security threats and MAC layer security threats along with counter measures.

A. PHY layer security issues[6], [22]and [24]:

Scrambling and jamming are the two possible threats in PHY layer. For scrambling, the attackers will scramble the uplink slots of other MS's by their own data and make it unreadable for BS. Jamming at the physical layer is a kind of denial-of-service (DoS) attack that uses intentionally interfering radio communication by introducing the noise to disrupt the reception of messages in both uplink and downlink.

B. MAC layer security issues in PMP Network

The causes of MAC layer security issues are due to certain un-encrypted MAC management messages. The major security issues in PMP network are,

1. DoS/Reply attacks during MS Initial network entry
2. Latency during handover and unsecured pre-authentication
3. Downgrade attack
4. Cryptographic algorithm computational efficiency
5. Bandwidth spoofing

Each security issue and its counter measures are discussed below:

1. DoS/Reply attacks during MS Initial network entry: When the MS enter into the network, it scans the downlink channel and synchronizes with it. In the downlink, BS announces the range of initial ranging code for MS. The MS selects any one of the ranging code and sends it to BS for initial ranging. The BS responds to the successful reception of ranging code by Ranging Response (RNG-RSP) message. The RNG-RSP message is used to nullify the offsets of frequency, time and power used by the MS. Then the MS goes for SBC-REQ and other procedures as shown in Fig.2. The message flows before SA-TEK are un-encrypted nature. So the attacker can decode the MAC messages, modify and re-send it to BS or MS. The security issues during initial network entry are: (i) RNG-RSP vulnerability (ii) Auth-Request and Invalid vulnerability and (iii) Rogue BS.

In *RNG-RSP vulnerability*, the attacker modifies the RNG-RSP message and sets the status as failed, then re-sends it to MS. So the MS goes for initial ranging again. If the attacker continuously sets the RNG-RSP status as failed, the MS can not access the network. This leads to the DoS attack.

This RNG-RSP vulnerability is solved by Diffie-Hellman (D-H) key agreement [7]. Fig.5 shows the secured initial ranging and network entry procedure using D-H key agreement. In this MS generates the global prime numbers p, q and the secret key. Then it sends the prime numbers p and q to BS along with ranging code. Now the BS can generate the shared secret key from the global prime numbers p and q as per D-H key algorithm. Using the shared secret key the BS encrypts the RNG-RSP message. So the attacker can not modify the status. This secured initial network-entry process (SINP) [10] also solves Auth-Request vulnerability.

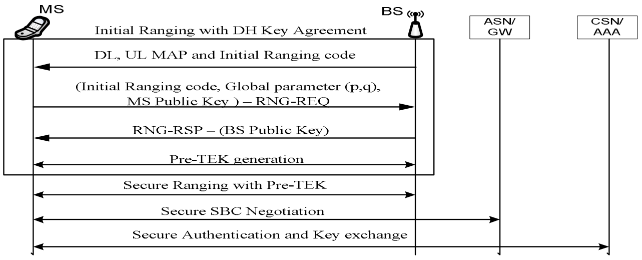
MS
BS
ASN/ GW
CSN/ AAA
Initial Ranging with DH Key Agreement
DL, UL MAP and Initial Ranging code
(Initial Ranging code, Global parameter (p,q), MS Public Key) – RNG-REQ
RNG-RSP – (BS Public Key)
Pre-TEK generation
Secure Ranging with Pre-TEK
Secure SBC Negotiation
Secure Authentication and Key exchange

Fig. 5: Initial Network entry with D-H Key Agreement [7]

For *Auth-Request and Invalid vulnerability*, the attacker captures the Auth-Request message and re-sends it to BS continuously. So the BS would be confused with the continuous request and sets the Auth-Response as failure. Some time the attacker may captures Auth-Response message from BS and re-sends to MS after time out period.

This issue can be solved by either introducing nonce [15] or time stamps [20]. By adding nonce or time stamp, MS and BS identifies if the authorization message is proper. So the attacker can not modify the messages. When comparing nonce and time stamp, time stamp is more secure and avoids the replay attack. If the attacker captures the authorization response message and resends it after the time of expiry, the MS can identify with the time stamp value. Fig.6 shows the authorization request/response messages with time stamps, where, T_S and T_B denote the time stamps of MS and BS in the authorization request/response messages, respectively.

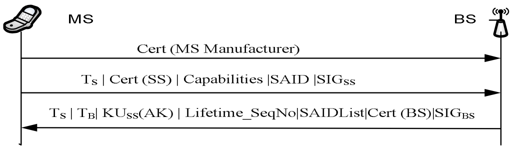
MS
BS
Cert (MS Manufacturer)
T_S | Cert (SS) | Capabilities |SAID |SIG_{SS}
T_S | T_B| KU_{SS}(AK) | Lifetime_SeqNo|SAIDList|Cert (BS)|SIG_{BS}

Fig. 6: *Authorization req/resp with time stamps*

In [25] the authors suggested the Wireless Public Key Infrastructure (WPKI) to solve the authentication vulnerability. The same issue is solved by visual cryptography in [14]. Since it requires the trusted third party (TTP) server for the implementation, it may not be suitable when considering the end to end network architecture.

In *rogue BS attack*, the SS cannot verify that any authorization protocol messages it receives were generated by an authorized BS. So any rogue BS can create a response. To solve this issue, the SS has to authenticate the BS [15]. The PKMv2 in standard 802.16e solves it by mutual authentication.

Solution: From the above discussion, the D-H key agreement [7] is more suitable for initial network entry issues. It solves the both RNG-RSP and Auth-Response vulnerability.

2. Latency during handover and unsecured pre-authentication: When handover occurs, the MS is re-authenticated and authorized by the target BS. The re-authentication and key exchange procedure increase the handover time, which affects the delay sensitive applications. In handover response message, BS informs the MS whether MS needs to do re-authentication with the target BS or not. If the MS is pre-authenticated by target BS before handover, then there is no need of device re-authentication but user authorization is still necessary.

For the above issue, the authors [12] proposed two schemes to avoid the device re-authentication. The first scheme adopts the standard EAP but instead of standard EAP method used in handover authentication, an efficient shared key-based EAP method is used using EMSK. Let MSK_i and $EMSK_i$ be the master and extended master session keys in the ith authentication phase, then MS and AAA will generate the MSK_{i+1} and $EMSK_{i+1}$ from the existing MSK_i and $EMSK_i$ keys before handover takes place. So the device authentication and key (MSK, EMSK) exchange is avoided. The second method skips the standard EAP method and the device authentication is done by SA-TEK three-way handshake in PKMv2 process. Since this method avoids the standard procedures, it is not suitable for implementation.

The handover latency can be reduced by simple pre-authentication schemes [19]. But pre-authentication schemes are inefficient and insecure [12].

Another approach for reducing the handover latency is using PKI infrastructure [17] for mutual authentication between target ASN and the MS before handover. Since the messages are encrypted using the public key, security is assured.

Mobile IP (MIP) scheme [26] is the new approach to solve the above issue. In this scheme, pre-negotiation with the target BS is in layer 3 MIP tunneling protocol.

Solution: For the above issue, MIP scheme [26] is more efficient than the other methods, since the messages are more secured by tunneling protocol and it further reduces the latency during IP connectivity phase. If the MS doesn't have the MIP support, shared key-based EAP is efficient.

3. Downgrade attack [32]: The first message of the authorization process is an unsecured message from MS telling BS what security capabilities it has. An attacker could, therefore, send a spoofed message to BS containing weaker capabilities in order to convince the BS and the attacked MS to agree on an insecure encryption algorithm.

Solution: A possible solution for downgrade attack is that the BS could ignore messages with security capabilities under a certain limit [32].

4. Cryptographic algorithm computational efficiency: The number of bits needed for encryption in RSA is more than Elliptic Curve Cryptography (ECC) for a required encryption, which increases the computation time.

Solution: ECC is the good substitute for RSA-based public key cryptography [21, 25]. ECC can achieve the same level of security as RSA with smaller key sizes. 160-bit ECC provides comparable security to 1024-bit RSA and 224-bit ECC provides comparable security to 2048-bit RSA. Another advantage of ECC is that it offers faster computational efficiency and well as memory, energy and bandwidth savings.

5. Bandwidth spoofing: In bandwidth spoofing, the attacker grabs the available bandwidth, by sending the un-necessary BW request message to BS [18].

Recommendation: To solve the bandwidth spoofing, we recommend that the radio resource management in the BS should check the local policy function (LPF) and then allocates the bandwidth only if the MS has necessarily provisioned. This *new recommendation* is based on QoS model suggested by the WiMAX forum [3].

C. MAC layer security issues in Mesh Network

In WiMAX mesh architecture, the CN should maintain the neighbor list after the initial network entry. While creating the neighbor list, it will verify the neighbor validity by neighbor authentication procedures [8]. So the possible threats in the mesh network are,

1. Man-in-middle attack during Initial network entry
2. Man-in-middle attack during neighbor authentication
3. Encryption load issues
4. Bandwidth spoofing

1. Man-in-middle attack during Initial network entry [5,8,9,18,21]: In mesh mode, there are more chances that malicious node can act as the SN and spoof the new node information during network entry and during time of neighbor establishment. For authentication, the CN has to authenticate with the sponsor node using operator shared secret (OSS) key which is similar to AK in PMP mode. The OSS key is common for all the nodes in the mesh network. This *Sponsor Node Impersonation* leads to *Man-in-the Middle/Reply Attack.*

To prevent the SN impersonations, CN should verify the sponsor node joining message. In [5], the authors proposed a scheme which assigns a different secret authorization key for each node. This key is used in the Mesh PKM Request and Mesh PKM Response to authenticate the joining node to the authorization server and vice versa. The authorization message flow is shown in Fig. 7. The PKM request and response messages are depicted below.

Mesh PKM Request

$\mathrm{MAC}_{joining} \mid \mathrm{SERIAL}_{joining} \mid \mathrm{H}\{\mathrm{MAC}_{joining}|\mathrm{SERIAL}_{joining}|\mathrm{AK}_{joining}\}$

Mesh PKM Response

$\mathrm{MAC}_{base} \mid \mathrm{SERIAL}_{base} \mid \mathrm{H}\ \{\mathrm{MACb}_{ase}|\mathrm{SERIAL}_{base}|\mathrm{AK}_{joining}\}$

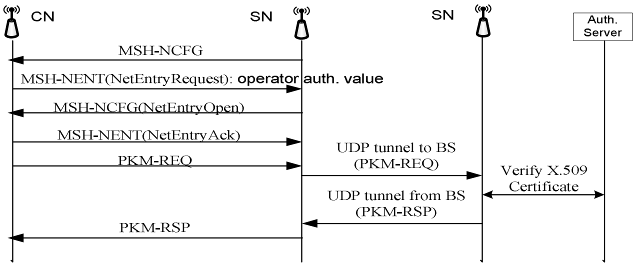

Fig. 7: *Network entry and authentication of a new node [5]*

The *Man-in-the Middle attack* during authorization is solved by adding the time stamp [8] or nonce [21] similar to the PMP issue. The authorization message flows along with time stamp is shown in Fig.8. The last two messages of original message sequences are added with time stamps and the third message is used for mutual authentication.

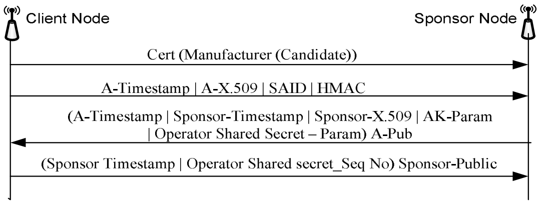
Client Node
Sponsor Node
Cert (Manufacturer (Candidate))
A-Timestamp | A-X.509 | SAID | HMAC
(A-Timestamp | Sponsor-Timestamp | Sponsor-X.509 | AK-Param | Operator Shared Secret – Param) A-Pub
(Sponsor Timestamp | Operator Shared secret_Seq No) Sponsor-Public

Fig. 8: *Authorization request/response with time stamp*

Solution: From the above discussion, the centralized authentication server scheme solves the SN impersonation [5] during authentication and time-stamp solves the man-in-middle attack during authorization.

2. Man-in-middle attack during neighbor authentication: This is similar to initial network entry, man-in-middle attack. During neighbor authentication, the attacker spoofs the security information of CN.

Solution: The same time stamp technique is used for authenticating the neighbor node. The message sequence with time stamp [8] from CN to SN in (1) and SN to CN (2) as depicted below

T_C | Candidate-X.509 | SAID | HMAC (1)

T_C | T_N | AK_SeqNo | Neighbor-X.509 | SAID| PubKey (OldTEK, NewTEK) | Lifetime | HMAC(2)

3. Encryption load issues: In mesh mode, the SN decrypts each payload and then transfers the traffic to the BS after encrypting the data with its own OSS key. This leads to encryption load issue and data insecurity.

Solution: To solve the encryption load issue [5], the encryption should be done between the subscriber and the BS and not just to the next hop. So the SN simply forwards the traffic, in its encrypted form, to and from the mesh BS. For this purpose, the authors [5] introduced a new mesh sub-header which contains the ids of the transmitting node, the sponsor node, and the mesh BS node. This differs from the current standard containing only the transmitting node id. The SN can use these ids to route without having to decrypt the message.

4. Bandwidth spoofing: The issue and the recommendation are similar to PMP network.

IV. Conclusion and Future work

The IEEE 802.16e based WiMAX network provides better security architecture, compared to 802.16d, and basically secures the wireless transmission using different components such as X.509 certificates, PKMv2, the Security Associations, encryption methods and the Encapsulation Protocol. However, it still lacks complete security solutions due to certain unsecured MAC management messages and the mesh network is not analyzed clearly. The existing individual research considered the issues such as secured ranging, authentication, and authorization during key exchange phase, handover and neighbor authentication. In this work, all the existing research efforts were analyzed based on the end to end network architecture and suitable solutions have been suggested.

For PMP network, the integrated solution consists of D-H key agreement for secured initial network entry, MIP scheme to avoid the latency and pre-authentication issue during handover, neglecting the SBC-Req if the security capabilities are under certain limit and ECC algorithm to improve the computational efficiency from the existing research. For mesh network, the integrated solution consists of centralized authentication server along with different OSS for secured initial network entry, data forwarding to avoid the encryption load issue and time stamp in authentication message for SN and neighbor authentications from the existing research. The new recommendation for bandwidth spoofing in both PMP and mesh networks is the BS allocates the uplink bandwidth only if the user is necessarily provisioned.

We are working further to find the solutions for Physical layer security threats and the simulations for the discussed counter measures to create the complete solution.

Acknowledgment

This project is funded by EION Wireless and Ontario Centres of Excellence (OCE), Ottawa, Canada.

References

[1] IEEE 802.16-2004, “IEEE Standard for Local and Metropolitan Area Networks —Part 16: Air Interface for Fixed Broadband Wireless Access Systems,” IEEE Press, 2004.

[2] IEEE 802.16-2005, “IEEE Standard for Local and Metropolitan Area Networks —Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems,” IEEE Press, 2005.

[3] WiMAX Forum: WiMAX End-to-End Network Systems Architecture (Stage 3: Detailed Protocols and Procedures) Release 1, V.1.3.0 , 2008.

[4] K.Lu, Y.Qian and H.-H.Chen, “Wireless Broadband Access: WiMax and Beyond-A Secure and Service-Oriented Network Control Framework for WiMAX Networks,” *IEEE Comm. Mag.*, May 2007, pp. 124–130.

[5] B.Kwon, et al., “A Security Scheme for Centralized Scheduling in IEEE 802.16 Mesh Networks,” *Proc. of Military Comm. Conf.*, 2007, pp. 1–5.

[6] W-M-Lang,, R-S Wu and J-Q Wang, “A Simple Key Management Scheme Based on WiMAX,” *Proc. of Int’l Symp. On Comp. Science and Computational Tech.*, 2008, pp. 3–6.

[7] T.Shon and W.Choi, “An Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions”, *T. Enokido, L. Barolli, and M. Takizawa (Eds.):* LNCS 4658, 2007, pp. 88–97.

[8] H.Zara and K.Shoab, “An Augmented Security Protocol for WirelessMAN Mesh Networks,” *Proc. of Int’l Symp. on Comm. and Info. Tech.*, 2006, pp. 861–865.

[9] H.Jin, L.Tu, G.Yang and Y.Yang, “An Improved Mutual Authentication Scheme in Multi-Hop WiMax Network,” *Proc. of Int’l Conf. on Comp. and Electrical Engg.*, 2008, pp. 296–299.

[10] T.Han, N.Zhang, K.Liu, B.Tang and Y.Liu, “Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions,” *Proc. of 5th Int’l Conf. on Mobile Ad Hoc and Sensor Syst.*, 2008, pp. 828–833.

[11] P.Narayana, et al., “Automatic Vulnerability Checking of IEEE 802.16 WiMAX Protocols through TLA+,” *Proc. of 2nd IEEE Workshop on Secure Network Protocols*, 2006, pp. 44–49.

[12] H-M.Sun, S-Y.Chang, Y-H.Lin and S-Y.Chiou, “Efficient Authentication Schemes for Handover in Mobile WiMAX,” *Proc. of 8th Int’l Conf. on Syst. Design and Applications*, 2008, pp. 44–49.

[13] O.Kyas, “Mobile WiMAX for networks with enhanced security and reliability requirements,” *Proc. of Military Comm. Conf.*, 2007, pp. 1–4.

[14] A.Altaf, R.Sirhindi and A.Ahmed, “A Novel Approach against DoS Attacks in WiMAX Authentication using Visual Cryptography”, *Proc. of 2nd Int’l Conf. on Security Info. Syst. and Tech.*, 2008, pp. 238–242.

[15] D.Johnston and J.Walker, "Overview of IEEE 802.16 Security," *IEEE Security and Privacy Mag.*, 2004, vol.2, issue 3, pp. 40–48.

[16] C-T.Huang and J.M.Chang, “Responding to security issues in WiMAX networks,” *IEEE Comp. Society IT Professional Mag.*, 2008, pp. 15–21.

[17] H-M.Sun, Y-H.Lin, S-M.Chen and Y-C.Shen; “Secure and fast handover scheme based on pre- authentication method for 802.16-WiMAX,” *Proc. of IEEE Region of 10 Conf.*, 2007, pp. 1–4.

[18] L.Maccari, M.Paoli and R.Fantacci, “Security Analysis of IEEE 802.16, Communications,” *Proc. of Int’l Conf. on Comm.*, 2007, pp. 1160–1165.

[19] J.Hur, H.Shim, P.Kim, H.Yoon and N-O.Song, “Security Considerations for Handover Schemes in Mobile WiMAX Networks,” *Proc. of Int’l Conf. on Wireless Comm. and Networking*, 2008, pp. 2531–2536.

[20] S.Xu, M.Matthews and C-T.Huang, “Security Issues in Privacy and Key Management Protocols of IEEE 802.16,” *Proc. of ACM 44th Annual Southeast Regional Conf.*, 2006, pp. 113–118.

[21] Y.Zhou and Y.Fang, “Security of IEEE 802.16 in mesh mode,” *Proc. of IEEE Military Comm. Conf.*, 2006, pp. 1–6.

[22] D.Hu and Y.Wang; “Security Research on WiMAX with Neural Cryptography,” *Proc. of Int’l Conf. on Info. Security and Assurance*, 2008, pp. 370–373.

[23] Y.Kim, H-K.Lim and S.Bahk; “Shared Authentication Information for Preventing DDoS attacks in Mobile WiMAX Networks,” *Proc. of 5th IEEE Conf. on Consumer Comm. and Networking*, 2008, pp. 765–769.

[24] M.Nasreldin, H.Asian, M.El-Hennawy, and A.El-Hennawy, “WiMAX Security,” *Proc. of 22nd Int’l Conf. on AINAW*, 2008, pp. 1335–1340.

[25] F.Liu and L.Lu, “A WPKI-based Security Mechanism for IEEE 802.16e, IEEE Communications Society,” *Proc. of Int’l Conference on Wireless Comm., Networking and Mobile Computing*, 2006, pp. 1–4.

[26] C-K.Chang and C-T.Huang, “Fast and Secure Mobility for IEEE 802.16e Broadband Wireless Networks,” *Proc. of Int’l Conf. on Parallel Processing*, 2007, pp. 46–46.

[27] S.Xu and C-T.Huang, “Attacks on PKM Protocols of IEEE 802.16 and its later versions,” *Proc. of 3rd Int’l Symp. on Wireless Comm. Systems*, 2006, pp. 185–189.

[28] L.Maccari, M.Paoli and R.Fantacci, “Security analysis of IEEE 802.16,” *Proc. of IEEE Int’l Conf. on Comm.*, 2007, pp. 1160–1165.

[29] A.Altaf, M.Y.Javed and A.Ahmed, “Security Enhancements for Privacy and Key Management Protocol in IEEE 802.16e-2005,” *Proc. of 9th ACIS Int’l Conf.*, 2008, pp. 335–339.

[30] T.Haibo, P.Liaojun and W.Yumin, “Key Management Protocol of the IEEE 802.16e”, *Wu han Univ. J. of Natural Sciences* Vol.12 No.1, 2007.

[31] F.Yang, H.Zhou, L.Zhang and J.Feng, “An improved security scheme in WMAN based on IEEE standard 802.16,” *Proc. of Int’l Conf. on Wireless Comm. Networking & Mobile Computing*, 2005, pp.1191–1194.

[32] Bart Sikkens, “Security issues and proposed solutions concerning”, *8th Twente Student Conf. on IT*, 2008.

[33] D. Simon, B. Aboba and R. Hurst,"The EAP-TLS Authentication Protocol", RFC 5216, 2008.