Design of Distributed Security Architecture for Multihop WiMAX Networks

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

Abstract—In this paper, we study the current security standards in multihop WiMAX networks and their security issues. For secured communications, hop-by-hop authentication is necessary for any multihop wireless networks [5][6]. WiMAX multihop networks provide default hop-by-hop authentication in a distributed security mode only. Apart from this, the multihop standards should consider the existing security issues in mobile WiMAX standard [4]. The new multihop standard IEEE 802.16m has improved functionalities and security support. It provides the solution for medium access control (MAC) – control message issues. At the same time, network coding is used for enhanced-multicast broadcast service (E-MBS) retransmission to improve the performance of MBS. However, the standard IEEE 802.16m/D4 fails to consider the security threats for network coding, multihop support and initial ranging. For the above issues, we propose a distributed security architecture using the Elliptic Curve Diffie-Hellman (ECDH) key exchange protocol. Our proposed architecture solves the network coding and other multihop security issues with the help of neighbor authentication/security association (SA), distributed security architecture and ECDH protocol.

Keywords—IEEE 802.16j; IEEE 802.16m; WiMAX; Multi-hop Relay; Security;

I. INTRODUCTION

The recent emergence of the IEEE 802.16j standard and IEEE 802.16m working group, also well known as Worldwide Interoperable Microwave Access (WiMAX) technology for multihop relay network and advanced air interface network is aimed at extending network coverage as well as ubiquitous computing [2][3]. Both network standards include the new node, relay station (RS) for extending the coverage region and has full compactable to legacy 802.16e mobile stations (MS). So the cell edge MS is able to communicate with the WiMAX base station (BS) through intermediate RSs, which introduces the multihop communications. The goal set out in 802.16m is to develop an advanced air interface to meet the requirements for International Mobile Telecommunications (IMT)-Advanced next generation networks. According to International Telecommunication Union (ITU), an IMT-Advanced cellular system must have target peak data rates of approximately 100 Mbit/s for very high mobility (up to 350 km/hr) and approximately 1 Gbit/s for low mobility scenarios. The IEEE 802.16 standards define only the physical (PHY) and medium access control (MAC) layer functionalities;

higher layer functionalities are out of scope of the standards. Any node, BS, RS and MS that implements 802.16m protocol is called Advanced BS (ABS), Advanced RS (ARS) and Advanced MS (AMS). The MAC Security sub-layer specifies the security functionalities and its implementations. The security sub-layer supports are to: (i) authenticate the user when the user enters into the network, (ii) authorize the user, if the user has provisioned by the network service provider, and then (iii) provide the necessary encryption support for the key transfer and data traffic. The upcoming 802.16m standard has stronger security architecture than 802.16d, 802.16e and 802.16j standards. An overview of security functions defined in the standards is discussed in section III.

One of the popular applications that are widely used in recent wireless networks is group-oriented communications, such as video conferencing and webinar, and etc. IEEE 802.16e introduces a service for multicast broadcast service (MBS), which enables the BS to distribute data simultaneously to multiple MSs. In MBS, the centralized server distributes the data content across multiple BSs, which are called zones. To provide seamless and high quality MBS, IEEE 802.16m standard includes many functionalities for Enhanced-MBS (E-MBS). One of the functionalities used for E-MBS is network-coding based retransmission scheme instead of hybrid automatic repeat request (HARQ).

Network coding [7] is a promising approach for traditional multicast or broadcast services. It is an alternative to the traditional routing networks, and it has been shown that random linear coding can achieve the optimal throughput for multicast and even unicast transmissions [3]. The principle of network coding is that the intermediate nodes actively encode (mix) the incoming packets and forward resulting coded packets, thus each outgoing packet can be a linear combination of incoming packets received from the uplink nodes. However, due to the packet encoding at intermediate nodes and multihop transmissions, network coding based applications are susceptible to potential malicious attacks or resource abuse [7]. This should be considered by the security architecture to avoid the network coding specific threats.

Some of the security threats that exist in fixed and mobile WiMAX standards are due to unencrypted MAC management messages [4] and multicast broadcast rekeying algorithm.
The introduction of multihop relay functionality will introduce further security threats. IEEE 802.16j standard introduced the optional distributed security mode and tunnel mode operations. The distributed security mode provides the necessary hop-by-hop authentication. But the multihop users may not use the tunnel mode operation since the multihop RSs do not have security association (SA) with the BS. Establishing SA between multihop RSs and BS is one of the open issues in multihop WiMAX networks. Even though the standard introduced the optional tunnel mode, distributed security mode and improved architecture, still it has open to a few problems like SA of multihop RSs with BS to use tunnel mode, neighbor authentication for network coding functionality, and so on. For the above issues, we proposed the distributed security architecture with the Elliptic Curve Diffie-Hellman (ECDH) key exchange protocol. The proposed architecture addresses the network coding and other multihop security issues with the help of neighbor authentication/security association (SA), distributed security architecture and ECDH.

The rest of the paper is organized as follows. Section II surveys the existing related work. Section III describes the security architecture from IEEE 802.16 standards and their issues. Section IV is the proposed distributed security architecture with ECDH key exchange protocol. The security analysis of the proposed scheme is presented in section V. The last section VI concludes the paper.

II. RELATED WORK

One of the major issues with multihop wireless networks is hop-by-hop authentication of relay nodes. Another issue is the selection of centralized or distributed security architecture. This problem was addressed in [5] and [6]. The authors in [5] proposed a hybrid authentication scheme, in which initially the MS will be authenticated by the service provider’s authentication server, later the authentication was managed by the access RS. Even for the distributed security mode, the default initial authentication is managed by administration, authenticating and accounting server (AAA) only [1][2]. To establish the distributed hop-by-hop authentication, the RSs exchange their authorization keys (AK) through the BS [5].

Since the AK is root of all other keys generation, exchanging AK is not advisable. Based on this distributed architecture [5], each RS knows the list of all other RS’s AK. In this case, if any one of the node is hacked by the hacker, the whole system is easily hacked. In [6], the distributed trust relationship is established between RSs using k-degree bivariate polynomial keys generated by the AAA server. This leads to the high overhead in AAA server, because a single AAA server has to manage the whole service provider’s network. Another overhead in [6] for mobility-related scenarios is a new shared secret (polynomials) must be distributed.

Our mechanism also follows the architecture presented in [6], but ECDH is adopted for key generation and key exchange between RSs. Apart from that, we also suggest neighbor authentication to solve the network coding related security threats.

The authors in [7] addressed the security threats in multihop wireless mesh networks for network coding. They analyzed both intra-flow and inter-flow network coding security threats. In this paper, those security threats are analyzed for multihop WiMAX networks in section III and the solution is discussed in section IV.

III. OVERVIEW OF WIMAX SECURITY AND NETWORK CODING

A. Security in Fixed and Mobile WiMAX Networks [4]

The security architecture of previous IEEE 802.16d standard is based on PKMv1 (Privacy Key Management) protocol, but it has many security issues like rouge BS introduction. Most of these issues have been resolved by the later version of PKMv2 protocol in IEEE 802.16e standard. IEEE 802.16e provides a flexible solution that supports device and user authentication between a MS and the home connectivity service network (CSN) to solve the rouge BS issue. Both fixed and mobile WiMAX have two-component protocols: (i) an encapsulation protocol for data encryption and authentication algorithms, (ii) a key management protocol (PKMv2) providing the secure distribution of keying data from the BS to the MS. PKMv2 based initial ranging and connectivity is shown in Figure 1.

As presented in Figure 1, after downlink channel synchronization, MS will send the ranging request (RNG-REQ) message in a specified contention slots. Once the BS receives the RNG_REQ, it infomrs the frequency, time and power offset values in the RNG_RSP message. If any collisions occur in a contention slot, BS sends the failure notification in the RNG_RSP message and the MS will repeat the ranging process. Once the MS succeeded in ranging process, it negotiates for basic capabilities in the SBC_REQ and the SBC_RSP messages. The subsequent process, Extensible Authentication Protocol (EAP) based authentication, authorization, SA and secured data transfer are shown in the top shaded block in Figure 1.

EAP based Authentication: Authentication addresses establishing the genuine identity of the device or user wishing to join a wireless network. The Device and User Authentication using EAP provides support for credentials that are subscriber ID module (SIM)-based, universal SIM (USIM)-based or X509 Digital Certificate. The message flows in EAP-TTLS (Tunneled Transport Layer Security) based authentication is shown in Figure 1. The authenticator in access network gateway (ASN GW) sends an EAP Identity request to the MS and the MS will respond to the request by sending PKM-REQ (PKMv2 EAP-Transfer) message. PKM-REQ message contains the subscriber ID module or X509 certificate. Then ASN GW forwards PKM-REQ to AAA server over radius protocol. The AAA server authenticates the device and provides the master session key (MSK) in an EAP-TTLS protocol. Then it forwards MSK to the authenticator. The authenticator generates AK from MSK and forwards to the BS. At the same time MS also generates the same AK from MSK. Now the BS and MS can mutually authenticate each other using AK.
Authorization and SA: Once the device or the user is authenticated by the network, BS has to authorize the user by an unique security association identity (SAID) using SA-TEK challenge messages, as depicted in the second shaded block in Figure 1. The Authorization Request includes MS’s X.509 certificate, encryption algorithms and cryptographic ID. In response, the BS 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 authentication/authorization from AAA, the BS reauthorizes the MS periodically.

Traffic Encryption and Message Protection: The MS establishes a SA for each service flow. For each SA, the BS provides both uplink and downlink transport encryption keys (TEK) to encrypt the data. AES-CCM (Advanced Encryption Standard - Counter with Cipher-block chaining Mode) is the ciphering method used for protecting all the user data over the Mobile WiMAX networks. TEK used for driving the cipher of unicast traffic is generated from the EAP authentication. TEK is refreshed by the BS periodically to add further protections.

MAC Control messages are protected using AES-based CMAC (Cipher based Message Authentication Code), or MD5-based HMAC (Message Digest based Hashed MAC) schemes. For securing the MBS communications, initially the BS transmits the Group Key Encryption Key (GKEK) and Group Traffic Encryption Key (GTEK) to each MS via unicast messages. GKEK is encrypted by the Key Encryption Key (KEK) which is derived from the AK of the MS. MBRA is used to refresh those keys periodically and inform the MS either in unicast or multicast to protect the MBS traffic further.

B. Security in Multihop WiMAX Networks

The basic security architecture in IEEE 802.1dj is pretty much similar to the mobile WiMAX standard. Due to the multihop architecture, some additional features are added on top of the basic architecture. The additional features are:

- The network may use either centralized or distributed security mode. Distributed mode will reduce the burden of BS as well as it reduces the time delay to reauthorize and reestablish the security association of RSs/MSs which are more than one hop distance away from BS.

- An establishment of a Security Zone (SZ): SZs are the set of trusted relationships between a BS and SSs/MSs, or RSs and SSs/MSs. RSs and SSs/MSs become members of a BS’s SZ by authenticating using PKMv2. Upon authenticating, the BS delivers SZ key material (SZ key (SZK) encrypted by SZ key encryption key (SZKEK)) used to provide integrity protection to management messages in the SZ.

- Transport tunnel connections may be established between the BS and an access RS to encapsulate the payload. In IEEE 802.16e, the BS or MS will send the data in the form of bursts (collection of MAC PDUs). Each burst can be identified by their uplink or downlink connection identifier (CID). In multihop network, the intermediate RS can collect the number of bursts from the connected MSs, then encapsulate and send it in a separate CID which is called as tunnel CID (T-CID). Both tunnel mode and non-tunnel mode (normal CID based forwarding scheme) operations are explained in the following paragraph.
For the tunnel mode operation, one or more tunnels may be established between the BS and the access RS after the network entry is performed. In the tunnel mode, MAC PDUs that traverse a tunnel will be encrypted and encapsulated in a relay MAC PDU with the relay MAC header carrying the T-CID (traffic tunnel-CID) or MT-CID (management tunnel-CID) of the tunnel. The station at the ingress of the tunnel is responsible for encapsulating the MAC PDUs into relay MAC PDU, and the station at the egress of the tunnel is responsible for removing the relay MAC header. Stations through which a tunnel traverses may forward the relay MAC PDUs based on the T-CID or MT-CID in the relay MAC header [2]. In Figure 2, blocks 2 and 4 show the tunnel mode data transfer in centralized and distributed security mode, respectively. In the centralized security mode, SA between RS1, RS2 and BS is established after the initial network entry. When MS2 sends any MAC PDU in CID-4, the ingress RS2 encrypts/decrypts the traffic before forwarding it to AMS. The intermediate RS1 forwards the MAC PDU to the BS. For distributed security mode tunnel establishment for multihop RSs is still an open issue, since there are no SA between multihop RSs and the BS.

In CID or burst based forwarding scheme, the forwarding of MAC PDUs by each RS is performed based on the CID contained in the MAC PDU header or management CID of the node. Here, the encryption of the MAC PDU or burst is based on SA-TEK between the communicating nodes. If BS and the end user have SA, then BS/end user may encrypt the data and the intermediate RSs forwards the traffic in the same CID without encrypting/decrypting the traffic. In Figure 2, blocks 1 and 3 show the CID based data forwarding. In the centralized security architecture, the intermediate RSs just forward the MAC PDU in the same CID without decryption and encapsulation, since they do not have the SA-TEK. SA in the distributed security mode is established only with the access node and the BS does not have the SA-TEK of the multihop users. So the intermediate RSs decrypt/encrypt the traffic before forwarding which is shown in Figure 2 as d/e. This introduces the additional overhead for the distributed security mode.

On the other hand, the security architecture of IEEE 802.16m has a few modifications to add more security features and to adapt the network conditions [2]. The modifications are:

- EAP based authentications only supported, not the RSA (Rivest Shamir and Adleman) algorithm.
- Security associations are static (no dynamic associations are supported).
- TEKs are derived at AMS not in ABS and the encryption algorithms are AES-CCM and AES-CTR
- Three levels of MAC management message protections are supported: No protection, CMAC and Encrypted by AES-CCM
- Instead of re-authentication, key renewal is used (using Key agreement protocol) during fast handover. AMS-ID is used for key derivation purpose and for initial and handover ranging.

C. Security Issues in Multihop WiMAX Networks

The security issues in mobile WiMAX networks outlined in IEEE 802.16e are due to unencrypted MAC management messages. That was solved in the IEEE 802.16m standard. But other security issues introduced in multihop WiMAX networks are:

- Initial ranging request (RNG_REQ) message, see Figure 1, is unencrypted. So the intermediate rouge node may receive the RNG_REQ and respond the RNG_RSP message with failure notification. This may lead to denial of service (DoS) attack [4].
- Even though the standard defines both the centralized and distributed security modes, centralized security mode is not advisable. It leads to high overhead in BS. Hop-by-hop authentication is also mandatory to avoid the rouge RSs.
- The data forwarding should use the tunnel mode to reduce overhead. Normal CID mode leads to additional overhead in relays for decrypting/encrypting the data.
- Network coding is used for E-MBS retransmissions. In that, the access RS/ARS may receive the coded packet from more than one super ordinate relays. Since the tunnel mode cannot be used for network coding, it may lead to some network coding security threats.
- In IEEE 802.16m, E-MBS data can be transmitted in broadcast-only carrier from ABS. ARS may not be involved in MBS transmissions. The broadcast-only carriers are transmitted at higher power that is optimized to improve the performance for cell edge user. This may lead to adjacent carrier interference. Apart from this sharing of GTEK between BS and multihop users and MBRA are still the hidden problem in multihop network.

D. Security Threats in Network Coding

There are two general approaches for applying network coding in wireless multihop networks, intra-flow network coding and inter-flow network coding [7]. The intra-flow...
network coding scheme mixes packets within individual flows (p1 and p2 as shown in Figure 3a), while the inter-flow network coding scheme mixes packets across multiple flows (m1, m2 and m3, as depicted in Figure 3b). Figure 3 shows the network model for both network coding types. In WiMAX networks, it may be difficult or not possible to mix two different flows or use the inter-flow network coding scheme, because each packet/burst (one or combination of more than one packets) contains additional information for CID-based flows adopted in WiMAX. The possible threats in intra-flow network coding are forwarding node selection with rate assignment, pollution attacks and entropy attacks in data forwarding and acknowledgement delivery [7]. The pollution attacks can be launched by injecting polluted information or modifying messages and entropy attacks can be regarded as special reply attack. These two attacks are more vulnerable in network coding techniques.

![Figure 3. Intra-flow and inter-flow network coding](image)

IV. PROPOSED DISTRIBUTED SECURITY ARCHITECTURE

In our previous analysis [4], we recommended that Diffie-Hellman (DH) key exchange for solving the DoS attacks during RNG_REQ and RNG_RSP communications, and elliptic curve cryptography (ECC) for reducing the computational overhead. In many practical implementations, it has been proved that ECDH can establish a shared secret over an insecure channel at highest security strength [10][11]. Based on this, our architecture considers ECDH as a part of layer-2 technique in every node. Using ECDH protocol MS/ARS establishes the secured tunnel with BS in the ranging process itself. Three main tasks: initial ranging using ECDH, distributed security architecture and neighbor authentications using ECDH are explained in the remaining paragraphs.

Initial ranging and connectivity: Consider a multihop network scenario with one BS/ABS, a few RSs/ARSs and many MSs/AMSs. The initial ranging and connectivity of the first hop and the nth hop node is shown in Figure 4. First, the BS broadcasts the general parameters and public key of the ECDH along with BS-ID and other downlink channel parameters in the downlink channel descriptor (DCD) message. The ECDH global parameters and BS public key are highlighted in DCD message flow. Second, any node (MS/RS) wants to connect with the BS will generate the public and private key pairs and send the public key to the BS, along with initial ranging code in the RNG_REQ message which is encrypted using the BS public key. If the RNG_REQ message reaches successfully to the BS, BS will then respond with a RNG_RSP message. The BS response message (RSG_RSP) is encrypted with the MS/RS public key. So the BS and MS/ARS establishes a secure tunnel during the initial ranging process itself and further MAC communications also uses the secured tunnel. The remaining steps follow the standard, like the initial device/user authentication was done by the AAA server.

![Figure 4. Initial ranging and connectivity using ECDH protocol](image)
Distributed security and multihop connectivity: For the n\textsuperscript{th} hop connectivity (as shown on the left of Figure 4), the cell edge RS broadcasts its public key and global parameters along with RS/ARS-ID and downlink channel parameters in the DCD broadcast message like that of BS. The MS/RS that wishes to join the RS does the ranging and connectivity similar to connectivity with the BS. Here, the access RS acts as BS for the new user. After the initial device/user authentication (done by the AAA server), the MS/RS establishes a security association with the connected RS (superordinate) / Access RS. If the new connected node is a RS, then the superordinate RS will share the public key of BS and the same global parameters. The new RS will associate with the BS as well by sending its public key to the BS. Any RS which are more than one hop distance away from BS are connected to the superordinate RS and associated with BS. So, the RS that is more than one hop away can send its traffic over the tunnel mode by encrypting the traffic (payload) with BS public key. The intermediate RSs will not decrypt/encrypt the traffic.

In the centralized security architecture, BS alone maintains the SA and encryption keys of both single-hop and multihop MSs and RSs in the network. For the distributed security architecture, the access RS (e.g., the leftmost RS shown in Figure 4) maintains the SA and encryption keys of multihop users. Figure 5 shows the distributed security architecture. From the n\textsuperscript{th} hop connectivity process, it is clear that the access RS acts as BS for their connected nodes and it maintains the encryption and SA keys. At the same time, BS maintains the SA keys of single-hop MSs and RSs as well as ECDH public key of multihop RSs. In Figure 5, the BS maintains the SA and encryption keys of MS1, RS1, and RS2 as well as ECDH public key of RS3. The RS1 maintains the SA and encryption keys of MS2, MS3, and RS3. RS2 and RS3 maintain the encryption keys of MS4 and MS5, respectively. Suppose MS5 wants to send an encrypted data in a tunnel mode, first it encrypts the traffic using SA-TEK associated with the RS3. RS3 then decrypts the traffic using SA-TEK associated with MS5 and encrypts the data using BS’s public key. So the intermediate RS1 is not necessary to decrypt/encrypt the traffic. This architecture is useful for supporting tunnel mode operation.

Neighbor authentication and SA: The BS keeps the RS members list in the network. If any new RS is connected with the network, the BS will inform the updated members list to the existing RSs group and send the list of RSs to the newly connected RS. When the new RS scans the adjacent channel, it may find another superordinated RS after the verification of RS/ARS-ID. Then it will associate the neighbor RS by sending its public key and the RS-ID. The neighbor RS also sends its public key in the response. At the end of association they generate the uplink and downlink CMAC digital signatures from AK and exchange between them. Figure 6 shows the neighbor authentication process. In step 1, the RS3 receives the updated RSs list after the ECDH agreement with the BS. During the scanning process, it may find the DCD and other downlink parameters of RS2 as shown in step 2. Since the RS3 knows that RS2 is a legitimate node based on the list it received from the BS, it establishes the ECDH agreement with the RS2. After the ECDH key agreement, both RS2 and RS3 share their message digests (digital signatures) as shown in step 3 and step 4. This neighbor authentication is useful for receiving network encoded packets since they are unencrypted nature.
In a network coding based communication, the data are unencrypted nature to reduce the overhead of intermediate nodes for decrypting/encrypting the traffic. So the rouge node may introduce the pollution and entropy attacks. To avoid the pollution attack, neighbor authentication is established with the super ordinate nodes. Assuming the intra-flow network coding communication exists for the network as shown in Figure 6. The BS broadcasts the packets to RS1 and RS2. Here the RS1 and RS2 encode the packets in different linear combinations. Now node RS3 receives the packets from both RS1 and RS2 and decodes the packets for MS5. When RS3 receives the network coded packets, it will verify the digital signature of the packet. If the digital signatures are not specific to RS1 or RS2, it will discard the packet. The solution for the entropy attack is explained in the analysis section.

V. SECURITY ANALYSIS

In this section, we analyze how the proposed ECDH implementation with distributed architecture resolves the security issues mentioned section III.

A. DoS attack during Initial Ranging

In our proposed solution, RNG_REQ and RNG_RSP messages are encrypted by the public key of the receiver. So the intermediate rouge node cannot process the message and the system is free from DoS attack during initial ranging.

B. Hop-by-hop Authentication for rouge RS

One of the major issues in multihop wireless network is the introduction of rouge node in a multihop path. Since the proposed architecture follows the distributed security mode, once the joining node is authenticated by the AAA server, the node authenticates the access RS. In this multihop scenario, every RS authenticates its access RS/BS. So the proposed solution avoids the introduction of rouge RS problem.

C. Tunnel Mode Support

In a multihop scenario, if the intermediate nodes decrypt and then encrypt the payload before forwarding, it leads to the additional overhead for that node. On the other hand, if the tunnel mode is used, then BS should know the key for decrypting the traffic. In our approach, since the public key of BS is known to all RSs and BS knows the public key of all RSs, the network supports the tunnel mode operation.

D. Pollution and Entropy Attacks (Network Coding Threats)

Pollution and entropy attacks are the major security threats in network coding based networks. Since the packets are unencrypted nature, attackers may introduce the polluted or stale packets (pollution and entropy attacks). In our approach, every RS authenticates the neighbor RSs and shares the digital signatures information. So the attackers cannot introduce the pollution attacks. For the entropy attack, the RS may introduce the time stamp field in SDU-SN (service data unit - sequence number) extended subheader. So when the RS receives the stale packet, it can check the time stamp and SDU-SN of the received packet with the older packets. If the same SDU-SN exists with older time stamp, it may drop the packet to avoid the entropy attacks.

E. MBS support

In MBS communications, the BS should share the MBS-GTEK to the authorized legitimate user only. In distributed security, BS does not have the AK of multihop users to check whether the user is legitimate or not. In our architecture, BS may send the GTEK to RSs. The RS will share the security key only if the user is authorized to get the MBS traffic. For the MBRA forward/backward secrecy the BS/RS may share GTEK to the new MS only when the MBRA update happens and it updates the key if the user left from the group. For simplicity the network may use a hash function implementation for frequent GTEK updates [9]. Since the AK for GTEK is out of scope in the standard [1], the issue is still open.

F. Mobility (Handoff) support

For the mobility scenarios, two cases are considered: (i) RS mobility (e.g., RS is installed on the top of a train and WiMAX users are inside the train) (ii) MS mobility. Analyses for both scenarios are described below:

RS mobility: In our security architecture, when RS handoff occurs, the authentication and key update can be handled fast, because the target RS knows the list of RSs in the network. With the help of key agreement protocol, it is possible to implement the key renewal, instead of re-authentication as stated in IEEE 802.16m draft. Using the key renewal rather than re-authentication can reduce the handoff overhead.

MS mobility: The scenario for the MS mobility is pretty much similar to the RS mobility. When the MS moves from one RS to the another RS or BS, the current serving RS can inform the necessary information to the target RS or BS using ECDH protocol (PKM encryption). So the target RS or BS renew the encryption keys instead of re-authentication. This reduces the handoff delay as well. Here, even though our model follows the architecture defined in [6], the network is free from key updates during mobility. In their [6] approach, the WiMAX network was divided into hierarchical groups and key generating polynomials are only exchanged among the group. During mobility when a new node tries to join the group, a new shared secret must be distributed to the group. This kind of grouping is not followed in our distributed architecture. So the key updates are not necessary for our architecture on the account mobility.

VI. CONCLUSION

The introduction of multihop network in the IEEE 802.16 standards extends the coverage region and the introduction of advanced air interface supports high data rate at high mobility. This leads to the ubiquitous computing in the network. At the same time, security and fast re-authentication is needed for the multihop, high mobility environment. The IEEE 802.16j and IEEE 802.16m standards consider the existing security threats in mobile WiMAX and some of the multihop issues. However the standards fail to consider the RNG_REQ issue, hop-by-hop authentication, network coding issue, handoff issues and MBS support.
In this paper, we proposed a distributed security architecture using ECDH implementation in layer 2. In the proposed scheme, the nodes (RSs/MSs) are initially authenticated by the AAA server and then authorized with the connected RS/BS. The multihop network issues and its solution using the proposed scheme were analyzed thoroughly with several criteria. It shows that the proposed ECDH implementation with distributed security architecture solves the multihop security issues efficiently. MBRA issue for multihop network is still open and we are working on that.

ACKNOWLEDGMENT

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

REFERENCES


