Security Issues in Distributed Multihop WiMAX Networks.

Amit Agrawal
Research Scholar
RDVV, Jabalpur (M.P.) INDIA

Dr. J M Keller
Professor
RDVV, Jabalpur (M.P.) INDIA

Dr. R K Dave
Director (PG Courses)
SRIT, Jabalpur (M.P.) INDIA

amit agrawal74@rediffmail.com

***Abstract*—In this paper, we study the existing standards in multihop WiMAX networks and their security issues. For secured communications, it is necessary to have hop-by-hop authentication for any multihop wireless networks. 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]. 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 is not able to consider the security threats for multihop support , network coding, and 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: - WiMAX ; IEEE 802.16 d/e /j/m ; Multi-hop; Security.

I. INTRODUCTION

The recent emergence of the IEEE 802.16 j standard and IEEE 802.16 m 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 [1][2]. 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. According to International Telecommunication Union (ITU), an IMT Advanced cellular system must have target peak data rates of proximately 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 802.16 m standard has stronger security architecture than 802.16d, 802.16e and 802.16 j 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 (EMBS). One of the functionalities used for E-MBS is network coding based retransmission scheme instead of hybrid automatic repeat request (HARQ). 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 (MBRA) [8]. 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 tunnelmode, 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. 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.. 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. 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

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. 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 informs 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 .

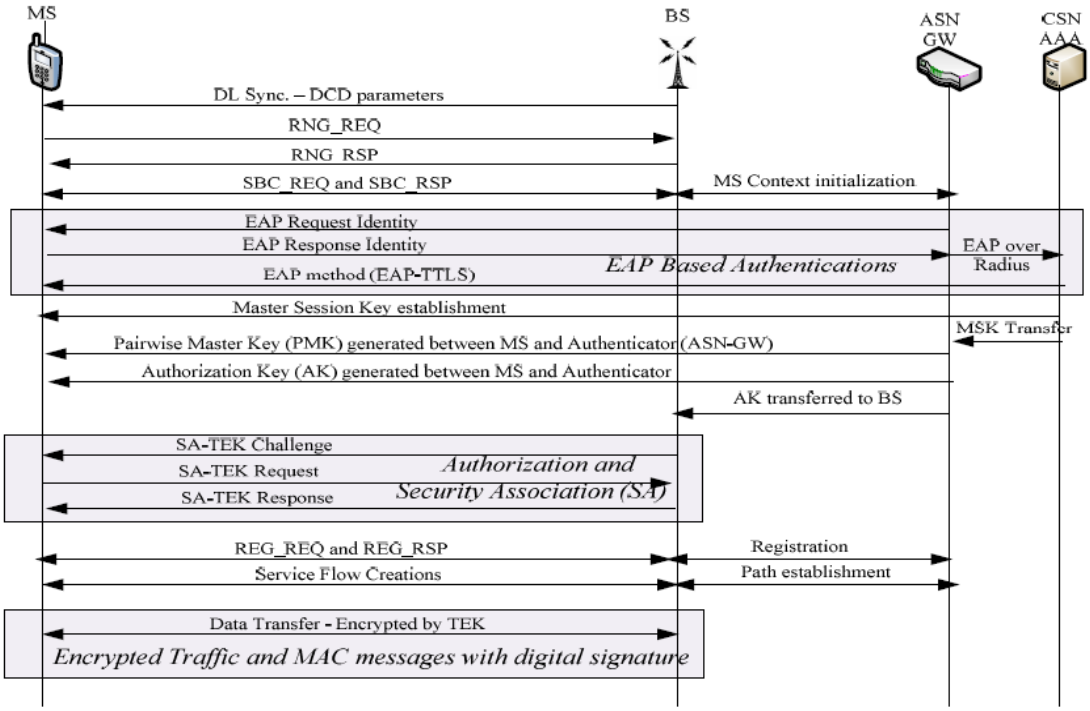

Figure 1. Intial Ranging and network entry in Mobile WiMax

EPA 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 or 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.

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.

B. Security in Multihop WiMAX Networks

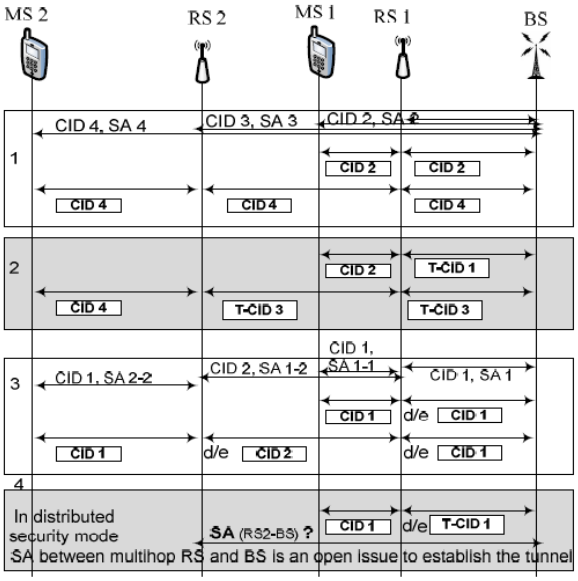

Fig 2 CID and Tunnel Mode Forwarding

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).. 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 AESCCM

∗Instead of re-authentication, key renewal is used (using Key agreement protocol) during fast handover. AMS-ID isused for key derivation purpose and for initial and
handover ranging.*C.*

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 NG_RSP message with failure notification. This may lead to denial of service (DoS) attack [4].

∗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.

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]. 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.

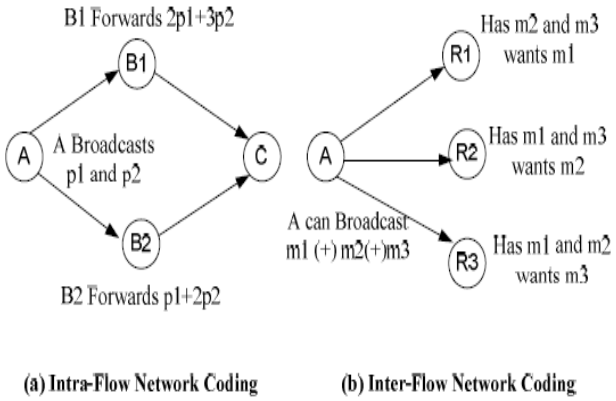

Fig 3 Intra and Inter Flow Coding

IV. PROPOSED DISTRIBUTED SECURITY ARCHTECTURE

***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.

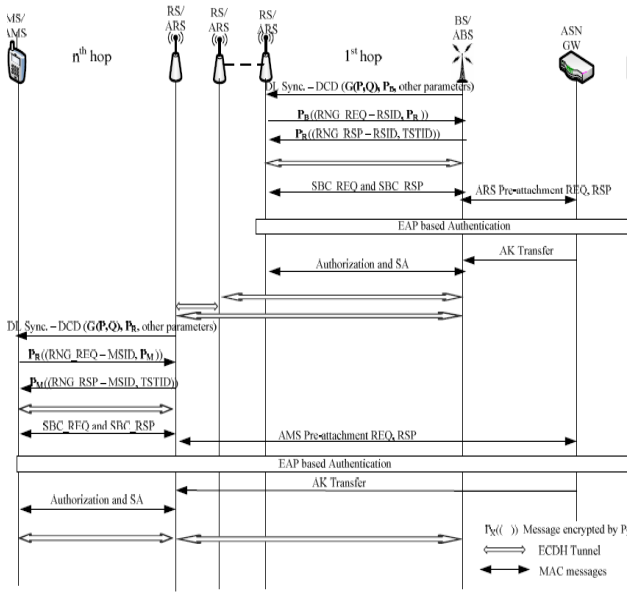

Fig 4 Initial Ranging and Connectivity with EDCH protocol

Here, we recommend to use 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. Using EDCH 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.

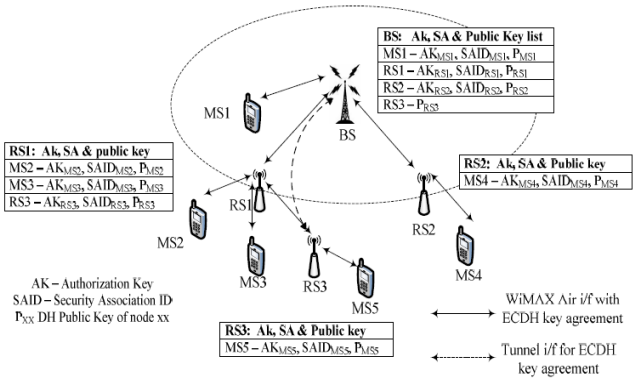

Figure 5. Distributed security architecture using ECDH protocol

Distributed security and multihop connectivity: For the nth hop connectivity (as shown on the left of Figure 5) the cell edge RS broadcasts it's 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. 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 super ordinated RS after the verification of RS/ARS-ID. Then it will associate the neighbor RS by sending it's public key and the RS-ID . 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.

E.. 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

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.

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.. The multi hop 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.

ACKNOWLEDGMENT

I am thankful to organization RDVV Jabalpur, IE (I) Jabalpur Chapter , ShriRam Group of Institutions Jabalpur and TIET Jabalpur for their valuable support during my work. I would also like to thank Prof .(Dr.) S .P. Kostha , Prof (Dr.) Shakti Kostha for their valuable suggestions .

REFERENCES

[1] IEEE 802.16-2009, "IEEE Standard for Local and Metropolitan Area Networks—Part 16: Air Interface for Fixed Broadband Wireless Access Systems," IEEE Press, 2009.

[2] A. DeCarlo, et al., "Distributed Trust Relationship and Polynomial Key generation for IEEE 802.16m Network", Proc. of Mob. WiMAX Symp., 2009, pp 111-116.

[3] J Donga,R Curtmolab and C Nita-Rotarua, "Secure network coding for wireless mesh networks Threats challenges and directions", Int'l Journal for Comp. and Telecom. Ind., 2009, pp 1790-1801.

[4] A Deininger, et al., "Security Vulnerabilities and solutions in Mobile WiMAX", Int'l Journal of Comp Science and Network Security, 2007, pp 7-14

[5] Y. Lee, et al., "Design of Hybrid Authentication scheme and key distribution for mobile multi-hop Relay in IEEE 802.16j", Proc. of Euro American Conf. on Telematics and Info. Sys.,2009.

[6] S Kumar, et al., "Embedded End-to-End Wireless Security with ECDH key Exchange", Proc. of IEEE Midwest Symp. On Cts. and Sys., 2003.

[7] R.Bose, R.Jacoby, "LOS Interference Calculations for LMDS Architecture", Technical Report , Jul 2000.

[8] P. Papazian, G. A. Hufford, R. J. Achatz, R. Hoffman, "Study of the local multipoint distribution service radio channel," IEEETrans. on Broadcasting, Vol. 43, No. 2, pp. 175–184, June 1997.