A Rouge Relay Node Attack Detection and Prevention in 4G Multihop Wireless Network using QOS-Aware Distributed Architecture

Miss. Shraddha V. Pawar[1] , Prof. Sachin P. Patil[2]

[1]*Department of Computer Science and Engineering Annasaheb Dange college of Engineering & Technology,Ashta.*
[2]*Department of Computer Science and Engineering Annasaheb Dange college of Engineering & Technology,Ashta.*

---***---

Abstract - *The WiMAX and LTE are two wireless radio data transmission technologies based on IEEE 802.16 designed to ensure broadband wireless access. This paper considers the problem of detecting rogue node in WiMAX networks. A rogue node is an attacker node that duplicates a legitimate node. It may lead to disturbance in service. In this paper we have proposed an efficient technique for secure data transmission to ensure the security and integrity of the data packet in the WiMAX network. We have used an ECDH algorithm for ensuring secure data transmission.*

***Key Words*: Rogue Node, Distributed Security, Elliptic Curve Diffie Hellman Algorithm(ECDH), Worldwide Interoperable for Microwave Access(WiMAX).**

1. INTRODUCTION

Vehicular communications have received a great deal of attention in recent years due to the demand for multimedia applications during travel and for improvements in safety. Safety applications often require fast message exchanges but do not use much bandwidth. On the other hand, multimedia services require high bandwidth for vehicular users. Hence, to provide mobile broadband services at a vehicular speed of up to 350 km/h. Worldwide interoperable for Microwave Access (WiMAX) and Long-Term Evolution (LTE) are considered the best technologies for vehicular networks. WiMAX and LTE are Fourth-Generation (4G) wireless technologies that have well-defined quality of service (QoS) and security architectures.

WiMAX and LTE resemble each other in some key aspects, including operating frequency spectrum, high capacity, mobility, strong QoS mechanisms, and strong security with a similar key hierarchy from the core network to the access network. However WiMAX and LTE also differ from each other in certain aspects, as they have evolved from different origins. LTE has evolved from 3rd Generation Partnership Projects (3GPP): thus, the LTE network has to support the existing 3G users' connectivity, but there is no such constraint for WiMAX. Particularly, on the security aspect, the WiMAX authentication process uses Extensive Authentication Protocol Tunneled. Maintaining QoS requirements of a specific application has become a significant topic and priority is to maximize the QoS experienced by the user. QoS is the ability of a network to provide premier service to some fraction of total network traffic over specific underlying technologies. QoS metrics are delay, jitter (delay variation), service availability, bandwidth, throughput, packet loss rate. Metrics are used to indicate performance of particular scheme employed. QoS can be achieved by resource reservation (Integrated services), prioritization (differentiated services).

2. EASE OF USE

As the increase in demand for multimedia applications and for the safety of mobile users, providing Internet that supports QoS-aware and safe multimedia services for vehicular networks is mandatory for service providers. The main cause for the MAC layer security threats in 4G vehicular networks is due to certain unprotected MAC management messages between Mobile station (MS) and Base Station (BS). When the control messages are in plain text, the attackers/intruders can easily spoof, modify, and reply those control messages for the intended receiver node. The severity of the security threats may vary based on the modification of those control messages. Similarly, the attackers may send the continuous false packets unnecessarily to the receiving node for the water torture attacks. Many research efforts have been published on MAC layer security threats in both WiMAX and LTE networks and a few of them discussed the implementation of IPSec security for WiMAX networks.

In multihop WiMAX, once the user is registered with the home network the security layer may use three levels of protections for the MAC management messages, i.e., No protection, CMAC, and Encrypted by AES-CCM. As a consequence of adding the encryption support for MAC messages, some of the security threats discussed no longer exist for multihop WiMAX. However, one of the security threats such as rogue RN attack is exists that adds a rouge node/Fake node in network and creates big threaten to the 4G multihop wireless networks. Such attack causes network QoS gets degraded. So there is a need for strong security mechanisms and strict authentication methods to overcome the existing security threats in 4G multihop. But enhancing security should not degrade network QoS.

Hence we proposed **E**lliptic **C**urve **D**iffie-**H**ellman (ECDH) protocol that has proven security strength and low overhead for 4G wireless networks. ECDH is competitor to RSA public key algorithm and has very good security. ECDH consumes less power and suitable for 4G wireless networks.

3. LITERATURE SERVEY

In [1] authors Proposed QoS aware distributed security architecture based on the Elliptic Curve Diffie-Hellman (ECDH) protocol. Worldwide Interoperability for Mobile Access (WiMAX) and Long Term Evolution (LTE) are 4G wireless technologies which have better Quality of Service (QoS) and security architectures. Security threats like Denial of Service (DoS), Water Torture Attack, rouge RN attack, etc in WiMAX and LTE are present issues. So there is a need for strong security mechanisms and strict authentication methods to overcome the existing security threats in 4G multihop wireless networks. But enhancing security should not degrade network QoS.

In [2] authors have researched that there in the VANET communication, especially in Multihop networks the forwarder node authentication is more important. So, we need to provide authentication for each and every hops. Hop by Hop message authentication is required to provide high level security in VANET. Simultaneously, the address of the data origin known by the attacker leads to node capture attack.

In [3] authors have researched on measuring the QoS performance for node protection in 4G wireless networks using network coding. Exclusive OR (XOR) network coding is used to explain the node protection for multihop 4G wireless networks. It is followed by measurement of the QoS performance, such as packet delivery ratio (PDR), latency and jitter, for different scenarios. Failure of a single and two relay node with and without proposed protection scheme is tested along with user's mobility.

In [4] authors proposed Network Protection Codes (NPC) using network coding to protect the operation of the network against link and node failures. Their interest was to find the limits of their NPC and where to deploy their NPC using several network graphs with a minimum number of edges. The authors also considered the problem of providing protection against a single node failure using network coding and reduced capacity technique for wired networks.

In [6] authors proposed, cross layer QoS architecture for 4G heterogeneous network services. QoS engine and cross layer algorithms are the main components. QoS engine is composed of QoS daemon, QoS agent and control module. Cross Layer Architecture monitors and adjusts resources periodically. In the absence of CLA, average latency and average packet loss are reduced by 2% and 8.5% respectively. But throughput achieved is slightly lower in CLA than traditional layered approach.

In these existing research efforts, the authors implemented the relay node protection using network coding for different networks such as wired networks, Wireless Sensor Networks (WSNs) and optical networks. However, the QoS performance of network coding for relay node protection in a multihop wireless network is not tested until now. Also, the relay node protection is very useful for multihop 4G wireless networks.

4. SYSTEM ARCHITECTURE

Figure 1 shows System architecture for proposed system. After generating WiMAX Multihop network and implementing ECDH on it, we generate attack by adding node in existing network. Then ECDH detects the rouge node by using hop-by-hop authentication after completing intial ranging process. By using distributed security architecture we prevent the node which is detected as rouge node and forward massage to next node. This process repeats until destination node found.

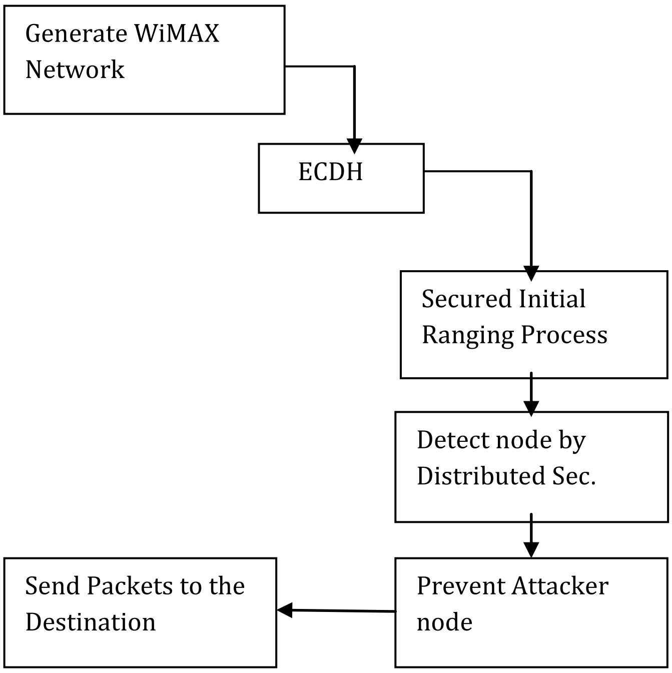

Generate WiMAX Network
ECDH
Secured Initial Ranging Process
Detect node by Distributed Sec.
Prevent Attacker node
Send Packets to the Destination

Fig – 1: System Architecture

5. METHODOLOGY

There are four Modules in system:

5.1. Generation of 4G Multihop Network and ECDH implementation on it.
5.2. Attack Detection
5.3. Attack Prevention
5.4. Performance Evolution

5.1 Generation of 4G Multi Hop WiMAX Network and ECDH implementation-

In this module, we are implementing initial configuration and setup of 4G Multihop WiMAX network in NS 2or NS 3 Network simulator tool. We are adding base station node, mobile station node and relay node. It creates multihop network. Having one base station and multiple mobile stations, relay nodes.Here we are implementing initial ranging process of ECDH. Which is shown in figure 2.After downlink channel synchronization (DL Sync),the MS will send ranging request (RNG_REQ)message. In turn,BS will responds with RNG_RES message. Then the Subsequent steps are following.

- **EAP Based Authentication-**

The authenticator in the 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. A PKM-REQ message contains the details of SIM or X.509 certificate. Then the ASN-GW forwards the PKM-REQ to the 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 Authorization Keys (AK) from the MSK and forwards to the BS. At the same time, the MS also generates the same AK from the MSK. Now, the BS and MS can mutually authenticate each other using AK.

- **Authorization and Security Association-**

Once the device or the user is authenticated by the network, the BS has to authorize the user by its unique Security Association Identity (SAID) using SA-Transport Encryption Key (SA-TEK) challenge messages, as depicted in the second block in Figure 2.

- **Traffic Encryption and MAC Message Encryption-**

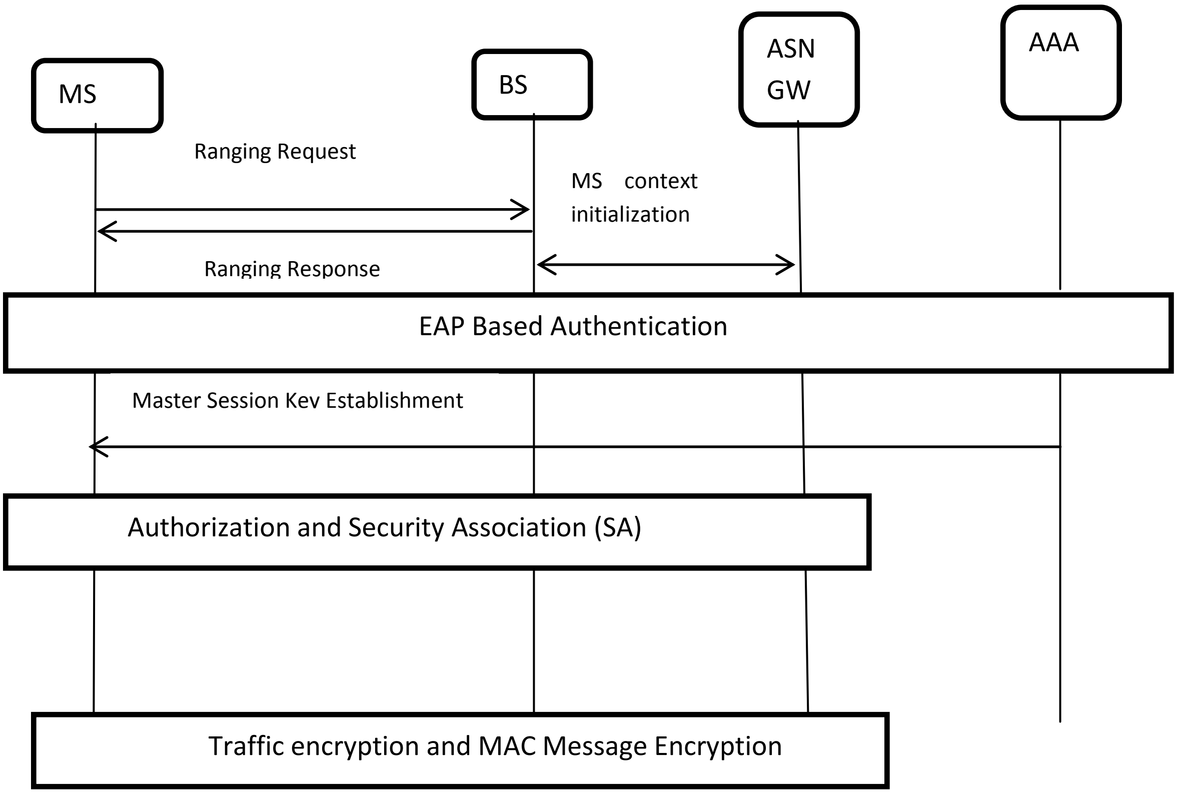

MS
BS
ASN
GW
AAA
Ranging Request
MS context initialization
Ranging Response
EAP Based Authentication
Master Session Kev Establishment
Authorization and Security Association (SA)
Traffic encryption and MAC Message Encryption

Fig – 2 : Initial Ranging Process for WiMAX

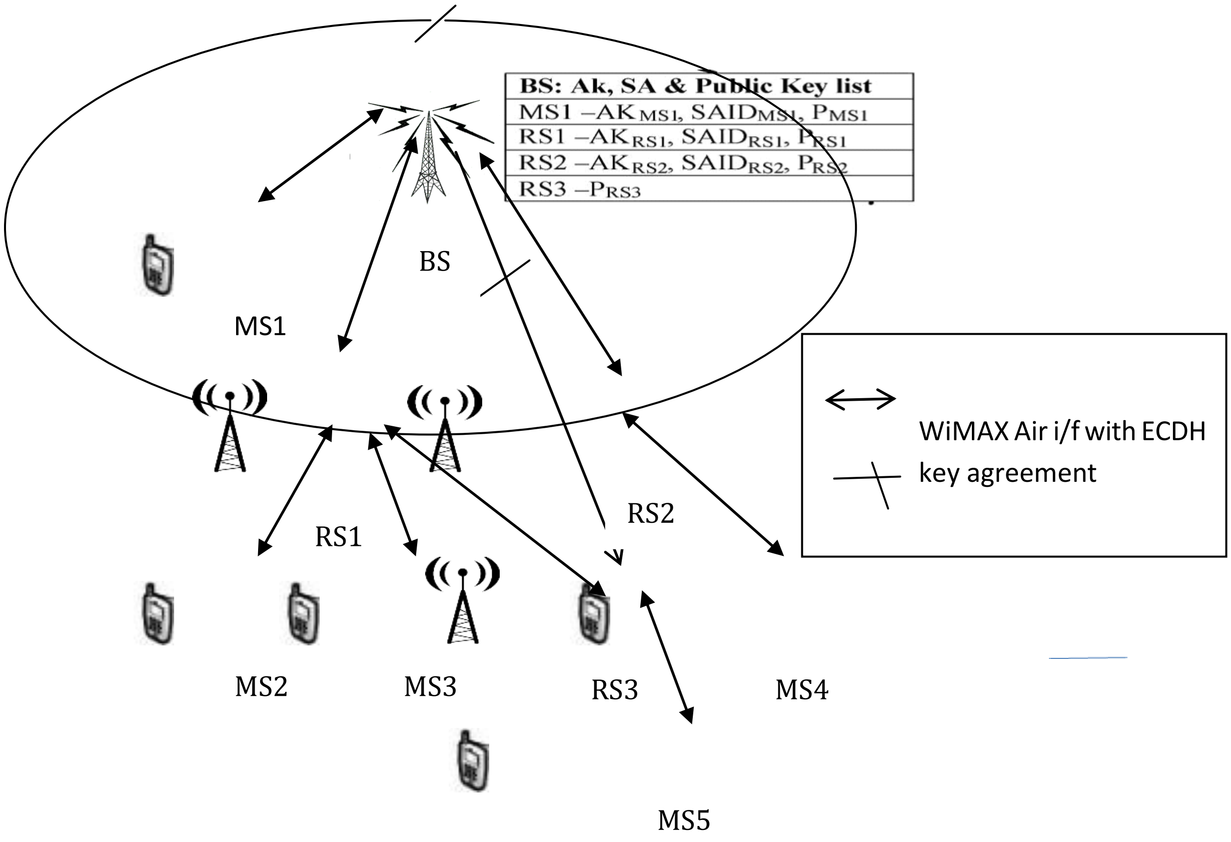
The MS establishes an SA for each service flow where the BS provides both uplink and downlink TEK to encrypt the data. Initially TEK is generated from the EAP-based authentication and then refreshed by BS periodically.

5.2 Attack Detection-

As author Ebrahim Halil Saruthan has proposed system to detect and prevent rouge node in real time wireless network [9] it shows real example of rouge node in network. Different architectures like Access Point (AP) architecture, client architecture etc. are used to Detect and Prevent rouge node. So, we are generating attack in network using simulator.

Network having attack, adds new rouge/fake node to existing one to receive data and hand over to some other nodes, creates traffic jam or to spoof or modify data etc.

Now we have to detect the rouge node with the help of ECDH. First step is secured initial ranging process for 1st hop to nth hop node is shown in figure 3.In initial ranging process as shown in figure. 2 any WiMAX node (MS/RS) wants to establish connection with BS generates the public and private key pairs and sends public key to BS initial ranging code along with RNG_REQ message. Which is encrypted using BS public key.BS responds with RNG_RSP message which is encrypted using BS public key.



BS: Ak, SA & Public Key list
MS1 –AK$_{MS1}$, SAID$_{MS1}$, P$_{MS1}$
RS1 –AK$_{RS1}$, SAID$_{RS1}$, P$_{RS1}$
RS2 –AK$_{RS2}$, SAID$_{RS2}$, P$_{RS2}$
RS3 –P$_{RS3}$

Fig - 3 : Distributed Security using ECDH

BS responds with RNG_RSP message which is encrypted with the MS/RS Public key. Hence MS/RS establish secure tunnel with BS and subsequent MAC messages encrypted using ECDH public key. In secure initial ranging process the only additional bandwidth overhead is the exchange of global parameters and public keys. Now next step is distributed security using ECDH in multihop WiMAX network. To establish hop to hop authentication and to reduce computational overhead of centralized node distributed architecture is necessary. In which new node is actually identified in WiMAX network. Figure 3 shows SA and key management in proposed security architecture.

5.3 Attack Prevention-

This module shows how ECDH helps to prevent RN Attack using key exchange. Neighbor authentication and SA is next step. If the new RS is connected with network, the BS will inform to the updated member list to the existing RSs group in Downlink Channel Descriptor (DCD) message. Now if new RS will find another RS during channel scanning it verifies new RS is genuine or not verifying RS_ID. Then it sends public key and RS_ID to the neighbor RS to establish SA. The neighbor RS will also send the public key in response. At the end of association, RS's generate uplink

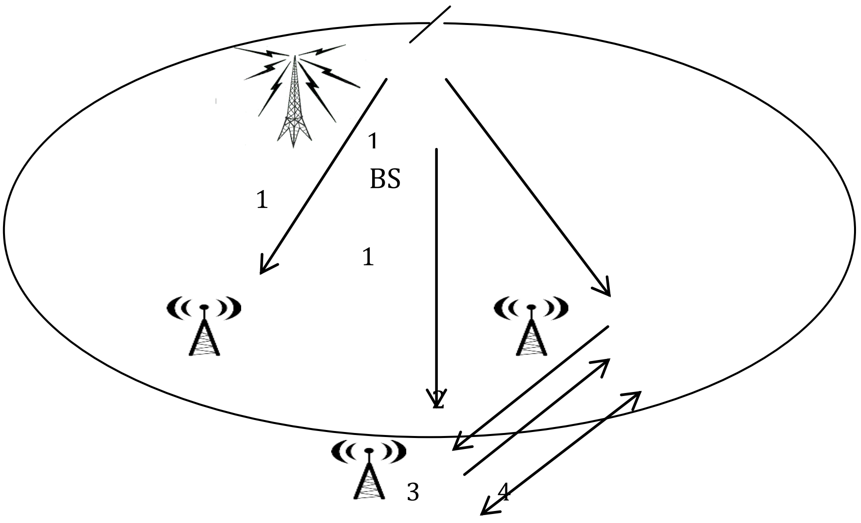


Fig - 4 : Neighbor Authentication Process using ECDH

and downlink CMAC digital signatures among them. Figure 4 shows neighbor authentication process.in step 1, the RS3 receives updated list after ECDH agreement with BS. During scanning process, RS3 may find the DCD and other downlink parameters of RS2 as shown in step 2.Since RS3 knows that RS2 is a legitimate node based on list received from BS, it establishes the ECDH agreement. After that Both share their digital signatures as shown in step 3 and step 4.

5.3 Performance Evaluation-

This module calculates QoS performance and shows that how it maintains its stability after applying ECDH using NS 2 or 3 supporting tools such as X-Graph. We can consider parameters for calculating performance like latency, service availability, jitter, Packet loss rate, throughput performance.

6. CONCLUSION

As the increase in demand for multimedia applications and for the safety of mobile users, providing Internet that supports QoS-aware and safe multimedia services for vehicular networks is mandatory for service providers. To provide high bandwidth support at the vehicular speed of up to 350 km/h, the WiMAX and LTE networks are the preferred candidates. 4G networks have well-defined QoS and security architectures. However, some major security threats such as DoS attack still exist in 4G multihop networks, because certain MAC messages are transmitted only in plain text. For this reason, we have proposed a distributed security architecture using the ECDH algorithm in Layer 2 for 4G multihop wireless networks. In the proposed scheme, the wireless nodes are initially authenticated by the home network and then authorized by the access node. In addition, the proposed scheme requires only a slightly higher bandwidth and computational overhead than the default standard scheme.

REFERENCES

[1] Perumalraja Rengaraju, Chung-Horng Lung, Member, IEEE, and Anand Srinivasan "QoS-Aware Distributed Security Architecture for 4G Multihop Wireless Networks" IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 63, NO. 6, JULY 2014.

[2] Vinoth V. and C. Monica Manoreya "A SAMA Scheme For Improving Qos in 4G Multihop Wireless Networks" Department of Information Technology, Sathyabama University, Chennai, India,VOL 10,no-7,2015.

[3] Perumalraja Rengaraju, Chung-Horng Lung, Anand Srinivasan, "QoS and protection of relay nodes in 4G wireless networks using network coding", 9th International Conference on Wireless Communications and Mobile Computing (IWCMC), Sardinia ,pp. 282 - 287 ,July 2013

[4] S. Aly and A.Kamal, " Networking Coding-Based Protection Strategies Against Node Failures" Proc. of IEEE ICC.,2009.pp.1-5.

[5] S. Aly, A.Kamal and A.Walid, "Network Design and Protection using Network coding" Proc. of IEEE Theory Information Workshop.2010, pp.1-5.

[6] Jiann-Liang Chen, Ming-Chiao Chen, Shih-Wei Liu, Jyun-Yu Jhuo, "Cross-layer QoS architecture for 4G heterogeneous network services", 11th Int.Conf.

Advanced Communication Technology (ICACT 2009),Phoenix Park, pp.73-77,Jan 2009.

[7] A. Rammoorthy,and S. Li.”Protection against Link Errors and Failures using Network Coding in Overlay Networks”,Proc. Of IEEE International Symposium on Information Theory, July 2009,pp.986-990.

[8] A. Kamal,”1+N Network Protection for Mesh Networks:Network Coding-Based Protection using p-Cycles” ,IEEE/ACM Transactions on Networking, Feb 2010,pp.67-80.

[9] Ibrahim Halil Saruthan,”Detecting and Preventing rouge devices on network”SANS institutes 2007.