European Journal of Applied Sciences 7 (2): 86-91, 2015
ISSN 2079-2077

DOI: 10.5829/idosi.ejas.2015.7.2.22154

Security Management in Mobile Node Wimax Without Degrading the Quality of Service (QOS)

Arunima kumari, Abhilasha and Mr. N. Prabakaran

Faculty of Electricals and Electronics, Department of ETCE, Sathyabama University, Chennai, India

Abstract: Our ultimate aim is to provide the high level of security without degraded quality of service that is Security Management in Mobile node Wimax. We can distinguish three main groups of applications: 1) safety applications, 2) traffic efficiency applications and 3) infotainment services (non-safety). The non-safety applications require high bandwidth and strong security to support multimedia services for vehicular users in this fast internet arena. To support multimedia services for vehicular users, the networks that have high bandwidth, such as cellular and satellite networks, are preferred for consideration. Aimed at providing high-speed Internet of 100 Mb/s at a vehicular speed of up to 350 km/h. Strong security architecture and strong authentication methods are needed to manage the existing security threats in 4G multi-hop wireless network. The security of the network is upgraded by using large bandwidth without affecting the quality of service. Thus, considering quality of service of the wireless network, security architecture is proposed. Mobile Multi-hop Relay (MMR) network is one of the emerging technologies, especially LTE-Advanced and the WiMAX. Ensuring security is one of the most imperative and challenging issues in MMR networks. WiMAX is emerging broadband wireless technology y some of Researchers have proposed the Privacy Key Management protocol to ensure the security measures in MMR networks. WiMAX uses either Advanced Encryption Standard (AES) or Digital Encryption Standard DES. However, these protocols still face several security threats, especially Denial of Service (DoS), replay attacks, Man in the Middle (MitM) attacks. Worldwide interoperable for Microwave Access (WiMAX) and Long-Term Evolution (LTE) are two emerging broadband wireless technologies aimed at providing high-speed Internet of 100 Mb/s at a vehicular speed. In this paper, we proposed security management in mobile WiMAX without degrading the quality of service in 4G multihop wireless network using the elliptic curve Diffie-Hellman (ECDH) protocol. Finally,we will do the comparison between the existing trend and our proposed system from the simulation and with the help of graphs.

Key words: RS-relay station · BS-base station · ECDH-Elliptic Curve Deffie-Hellman · WiMAX-World-wide interoperable for Microwave Access

INTRODUCTION

Providing security [1] is one of the major challenging issues in the WiMAX communication arena for the safety as well as the non safety applications. Safety applications deals with the fast message transmission but require less bandwidth, whereas non safety applications require large bandwidth as to support multimedia services for vehicular users. For vehicular communication, we need strong security mechanisms and Authentication process. WiMAX uses Extensive Authentication Protocol which enables users to use enterprise controlled passwords. In wireless communications, both the physical layer (PHY) and the medium access control (MAC) layer can be attacked by the security threats like denial of service, replay attack, man at the middle attack (MITM), data loss etc. For the physical layer threats, attacker hacks the radio frequency channel and for the MAC layer threats attacker can modify or replay the messages. Already some of Researchers have proposed the Privacy Key Management protocol to ensure the security measures in MMR networks.

Corresponding Author: Abhilasha, Faculty of Electricals and Electronics, Department of ETCE, Sathyabama University, Chennai, India.

WiMAX uses either Advanced Encryption Standard (AES) or Data Encryption Standard (DES). However, the protocol still faces several security threats, especially Denial of Service (DoS), replay attacks, Man in the Middle (MitM) attacks.. In Symmetric Key Cryptosystems, same key is used for both Encryption as well as the decryption process. i.e. if K was the key and M was the message, then, we have DK(EK(M)) = M. Asymmetric or Public key or shared key cryptosystems use two different keys for the encryption as well as the decryption process. Both keys can be used interchangeably. One of the keys is made public (shared) while the other key is kept as secret. i.e. let k1 and k2 be public and private keys respectively. Let M be the message, then In Dk2(Ek1(M)) = Dk1(Ek2(M)) = M. In general, symmetric key cryptosystems are preferred over public key systems due to the ease of computation and smaller key length provides the same amount of security as compared to a larger key in Public key systems. But earlier used protocols were not able to identify different kinds of security threats as well as during handover process also, hacker can easily enter into the network., the researchers have considered only the multihop fixed relay technique in which, they have considered the stationary node. But in our proposed system, we are considering WiMAX with multihop mobile relaying technique, in which our main consideration will be the node under mobility. Here, we will use the ECDH protocol ie. Elliptic Curve Diffie-Hellman protocol and will consider only the WiMAX network. In many practical implementations, ECDH has established a secured channel providing the shared secret key over an insecure channel at its highest security strength. This Paper is an extension of the earlier used methods with the objective of providing security without degrading the quality of service. We have made the following contribution in this paper [2].

- We have organized a WiMAX Network Design with the generation of beacon, request and response generation and the data forwarding.
- We have organized WiMAX Attack Design by introducing a fake attack for fake response generation.
- ECDH algorithm implementation for providing security because of the attack in WiMAX.

These models will be validated by using NS-2 Simulation using NAM window and we will do the final comparison between the existing trend and the proposed trend with the use of XGRAPH. The comparison will be based on above mentioned models as well as the security and the QOS (Quality of Service) analysis of proposed system with practical approaches [3].

WiMAX Network Design: THE IEEE 802.16-series standards are expected to provide broadband wireless access for a variety of multimedia services. Like other IEEE 802-series standards, IEE 802.16 gives the specification of wireless communication. IEEE 802.16 e standard is basically used for WiMAX. This is used for Physical layer and MAC layer. To build a complete system, higher layers are still necessary. One of the major function of WiMAX is to develop and standardize the WiMAX Forum Network Architecture [4], which is evolving into Internet Protocol (IP)-based wireless network. The architecture is depicted; the Access Service Network provides wireless radio access for WiMAX subscribers. It consists of one ASN Gateway (ASN GW) and many base stations (BSs). Each ASN is connected to Connectivity Service Network, which provides IP connectivity services.

A WiMAX receiver, which is also referred as Customer Premise Equipment (CPE), may have a separate antenna or could be a stand-alone box or a PCMCIA card that inserted in a laptop or a desktop computer. Working of WiMAX is similar to that of the Wi-Fi, but the coverage area is more as compared to Wi-Fi i.e WiMAX works on larger bandwidth. So far cost of CPE has been the biggest factor for the acceptance of WiMAX at large Scale.

In the past, Broadband Wireless Access (BWA) have been predominantly Line Of Sight (LOS), requiring highly skilled labor and a truck role to install and provide a service to customer [5].

WiMAX has resolved the concept of a self-installed CPE upto an extent, which has always been an issue for BWA from the beginning. A WiMAX base station comprises of internal devices and a WiMAX tower. The coverage area of a WiMAX base station is 50 km or 30 miles. Due to bad weather condition or other issues, it covers upto 10km or 6 miles. WiMAX Forum can be used by any wireless user in its coverage area once they register to it. The WiMAX base stations uses MAC layer which helps in allocation of uplink and downlink to the user as per their requirement.

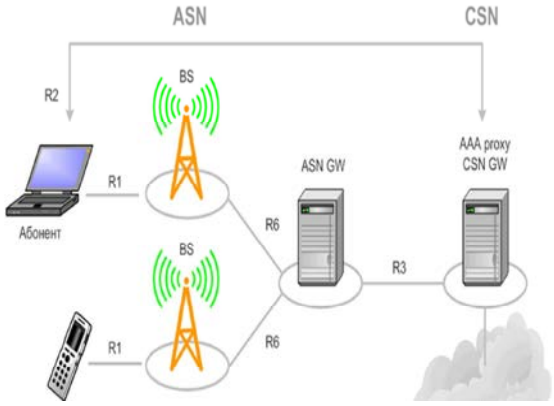

Fig. 1: Distribution of nodes in WiMAX

Once the WiMAX network design is completed which consist of a WiMAX base station, relay nodes and mobile nodes. The working of it is described as:

- Beacon Generation:-Initially source sends a hello message to check the status of all neighbouring nodes. The nodes which receives these beacons updates the routing table.
- Request and Response Generation:-Now nodes will send a RREQ to all the nodes, if a destination node receive the RREQ, it will generate RREP otherwise it will forward to next neighbors.

When source receives the RREP for all destinations which are the nodes participating in the routing all are updated in the routing table.

- Data Forwarding:-After collecting the routing information, nodes will start to forward the data in the given route. The route will change if any link is failed between any nodes in network [6].

WiMAX Attack Design: Attack occurs when handover or call connection [7] is set between the nodes. This is done so that data forwarding from source to destination takes place. This is the phase when attack occurs and the data is hacked.

Call Connection: In order to provide QoS guaranteed services, the subscriber station (SS) is required to reserve the necessary bandwidth from the base station (BS) before any data transmissions. SS reserves bandwidth in order to serve variable bit rate (VBR) for different applications without hindering the QoS provided.

Thus, it is likely that the amount of data to be transmitted is less than the amount of reserved bandwidth. The reserved bandwidth may not be fully utilized all the time. The Bandwidth Requests (BRs) are used to adjust the amount of reserved bandwidth, the adjusted amount of bandwidth can be applied as early as to the next coming frame. The unused bandwidth cannot be utilized in current frame. The SS may be exposed to the risk of degrading the QoS requirement of applications due to the insufficient amount of reserved bandwidth. The IEEE 802.16 network is wireless connection-oriented and defines both the physical and MAC layer. It gives the advantage of having better control over network resource to provide QoS guaranteed services.

If there are 3 or 4 base stations and there are nodes available in each base stations. Any node which is moving and come in intersection area of two base station and if it want to communicate with other base station, at the same time if that base station node want to communicate with his base station, the priority with be given to intersection node and the base station node is allow to wait in queue.

In MIP, load balancing and load control mechanisms have been proposed. The idea is that according to different criteria, Mss are equally served by Has or Mobility Anchor Points (MAPs). However, if the approaches discussed in are used in WiMAX, the loads of the anchored and serving ASN GWs are all affected.

The MSs may also need to perform both ASN Anchored Mobility and CSN Anchored Mobility during an inter-ASN handover. The long handover latency and high packet loss will degrade the service quality. On the other hand, in WiMAX, when performing ASN GW relocation, the load of the anchored ASN GW is reduced but the load of the serving ASN GW is not affected. Although the aforementioned techniques can reduce the load of the old serving ASN GW, the load of the new serving ASN GW is increased. Therefore, only the Anchored MS needs to perform ASN GW relocation to reduce the load of the Anchored ASN GW. The load of the Serving ASN GW is irrelevant. Admission Control (AC) is one of the resource management techniques to limit maximum amount of traffic in the network to guarantee service quality for subscribers.

In wireless and mobile networks, the AC algorithms are much more complicated due to the movement of MSs.

An MS served in current network may move to another network. The connection of the MS may be dropped if the required resources in the target network cannot be supported. Ongoing connection un-broken is considered more important than to introduce a new MS. Hence, a handoff MS is given more priority to access the network resources.

For this purpose, the overall resources are partitioned and some resources are preserved for the handover MSs only. This is called priority-based AC. various priority-based AC algorithms have been proposed. Here, we discuss two commonly used priority-based AC algorithms: cutoff priority Algorithm and Call Assigning Controller algorithm. If the resource in one ASN GW is over-provisioned, the ASN GW may become a performance bottleneck. Another approach is that the number of Bss controlled by each ASN GW can be scaled down to prevent the resource overprovision. However, because the number of BSs controlled by each ASN GW is reduced, this will cause many inter-ASN handovers [8].

Fake Attacks: A fake attack is designed on one of the WiMAX node. Due to the attack the data gets dropped off and doesn't get transmitted.

These attacks [6] may be DoS, route reply, man in the middle attacks, handover etc. These attacks results in traffic, manipulation of information, eve dropping and others.

Hence we are using ECDH algorithm for security purpose. Due to which a secured channel is established between the user and the WiMAX node in the ranging process.

ECDH Algorithm for WiMAX Security: Under this, we are proposing the ECDH Protocol to provide security [1-3] against the hacking as explained in the above module. ECDH [9] is Elliptic Curve Diffie-Hellman Protocol in which we are using the Diffie-Hellman Protocol in combination with the Elliptic Curve Parameters. Elliptic curves are not ellipses, instead, they are cubic curves of the form y3 = x3 + ax + b. Elliptic curves over R2 (R2 is the set R x R, where R = set of real numbers) is defined by the set of points (x, y) which satisfy the equation y3 = x3 + ax + b, along with a point O, which is the point at infinity and which is the additive identity element. The curve is represented as E(R).The following figure is an elliptic curve satisfying the equation y3 = x3-3x + 3.

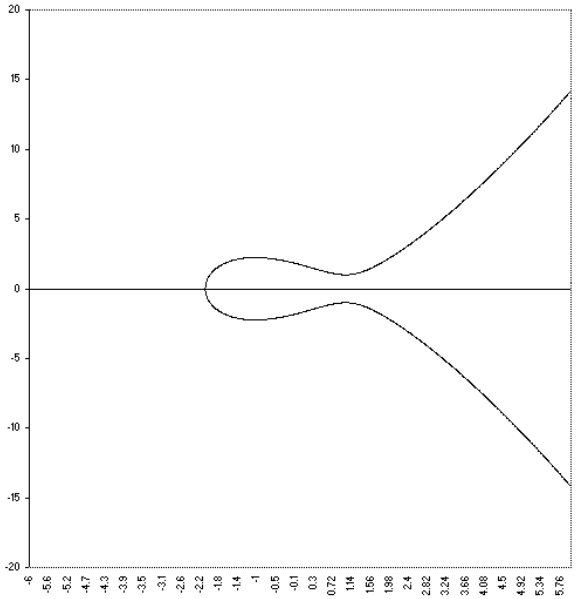

Fig. 2: Elliptic curve over R2: y2 = x3-3x

The public key cryptographic systems involves arithmetic operations on Elliptic curve over finite fields which is determined by elliptic curve domain parameters. The ECC domain parameters of Fq is defined by the septuple as given as D = (q, FR, a, b, G, n, h), where

q: prime power, that is q = p or q = 2m, where p is a prime
FR: representation of field of the method used for representing field elements ? Fq
a, b: field elements, they specify the equation of the elliptic curve E over Fq,

$$y2 = x3 + ax + b$$

G: A base point represented by G= (xg, yg) on E (Fq)
n: Order of point G, that is n is the smallest positive integer such that nG =O
h: cofactor and is equal to the ratio #E(Fq)/n, where #E(Fq) is the curve order.

Diffie-Hellman was the first public-key algorithm invented, back in 1976. It gets its security by calculating discrete logarithms in a finite field. The idea behind Diffie-Hellman algorithm is to generate a private key that can further be used for communication and sharing it in a secure manner. Two people, say user1 and user2, can use this algorithm to generate a secret key and for key distribution. First user1 and user2 agree on large prime numbers n and g such that g is primitive mod n.

User1 and User2 could do this over an insecure channel. User1 and User2 perform the following steps.

- User1 chooses a random large integer x and sends User2 a = gx mod n
- Similarly User2 chooses a random large integer y and sends User1: b = gy mod n
- User1 computes k from b that User2 sent, k = bx mod n
- Similarly User2 computes k' = ay mod n

Both k and k' are equal to gxy mod n. Any person listening to the conversation would only know n, g, a and b. They cannot recover x and y because of the Discrete Logarithm problem. The security lies on choosing large values of n and g.The Diffie-Hellman key exchange protocol can be easily extended to three or more people. The combination of ECC and Diffie Hellman key exchange is the ECDH Protocol which can be as illustrated: ECDH is elliptic curve version of Diffie-Hellman key agreement protocol. The protocol for generation of the shared secret using ECC is as described below [9].

User1 takes a point Q and generates a random number ka

User1 computes the point P = ka Q and sends it to User2 (It should be noted that Q, P are public)

User2 generates a random number kb and computes point M = kb.Q and sends it to User1

User1 now computes P1 = kaM and User2 computes P2 = kbP

P1 = P2 = kb kbQ, this is used as the shared secret key.

An illustration of the above steps is represented below.

After implementing ECDH Protocol, by simulation we can see that the relay node which has been attacked, has been discarded as the key generated by the attacked relay node and the key generated by elliptic curve nodes are not common. Thus, providing the security mechanism and thus preventing the data loss.

RESULTS AND DISCUSSION

For existing and our proposed security scheme, measuring and analyzing both the transmission and delay without effecting the QoS and provides high security. Here, we first compare the delay in the transmission and transmission of packets at the time of attack. Then we use ECDH security scheme using NS2 simulation.

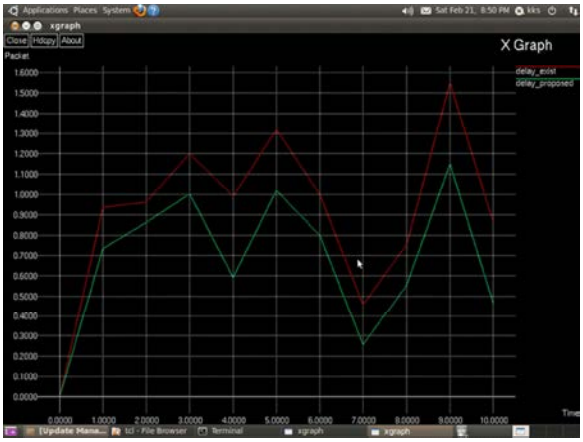

Fig. 3: Graph showing the comparison of the delay in transmission of data packets between the existing system and the proposed system.

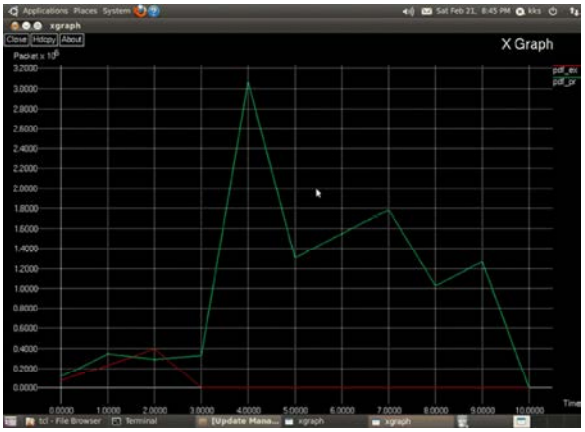

Fig. 4: Graph showing the comparison of transmission of data packets between the existing system and proposed system.

First the WiMAX topology is created in which the node connection is specified. It consists of WiMAX node, Base station and mobile nodes. The transmission and connection of nodes are predetermined. Now fake attack is introduced in one of the relay node due to which data packets are further not transmitted. The ECDH security algorithm develops a small size key [10]. This key is exchanged between the nodes. For transmission of packets from one node to other, the node exchanges the key. If the key matches then only further data transmission takes place if not there is no establishment of secure path between the nodes for data transmission. Hence, ECDH security scheme checks for the attacked node [8] and thus neglects the transmission of data from it. As a result data is transmitted smoothly.

The delay in proposed method is minimized upto an extent. Also it has been proved that ECDH has less weightage and can share secret data over an insecure channel at high security strength.

As from the graph, we can conclude that the delay in the transmission of data packets is less as compared with the existing system. As in the Proposed system we have used ECDH protocol, enabling the common key sharing between the nodes within the elliptic curve. Elliptic Curve consists of finite points which enables the key sharing between the nodes depending upon the field parameters.

The graph below shows the comparison of transmission of data packets at the time of attack between the proposed system and the existing system. In existing system the packets transmission drops down to zero once attack occurs. In proposed system the data transmission is carried out smoothly which is clearly shown [10].

CONCLUSION

As we know that, Security is the challenging issue in the wireless communication network arena for the safety as well as non safety applications. WiMAX is emerging broadband wireless technology aimed at providing high-speed Internet of 100 Mb/s at a vehicular speed of up to 350 km/h. The security of the network is upgraded by using high bandwidth without affecting the quality of service. Thus considering quality of service of the wireless network, security architecture is proposed, in which we are using ECDH Protocol ie Elliptic Curve Diffie Hellman protocol which generates the key which is smaller in key size with easy computation as well as providing comparable security with larger key size. The advantage of using ECDH Protocol is that, the nodes forms an elliptic curve within themselves forming a field having finite field points parameters depending upon which the key is generated. The nodes which do not have common key are discarded and thus, providing the security. The attacker attacks the server of the node, by using ECDH Protocol, the attacker can only detect the signal but cannot see the data within it. In this Paper, we are implementing ECDH Protocol by using NS2 Software. We are showing the simulation by using NAM window and the graph showing the comparison between the existing trend and the proposed trend by using XGRAPH window of the version 10.04.The advantage of using NS2 Software is that, it provides accurate and precise result. Thus, by seeing the simulation, graph and result, we can conclude that ECDH Protocol is the better option for providing security without degrading the quality of service (QOS) as it provides less delay and faster transmission of data packets in comparison with other protocols used by the researchers by keeping mobile node in consideration.

REFERENCES

1. Maccari, L., M. Paoli and R. Fantacci, 2007. Security Analysis of IEEE 802.16 communicatins.
2. Kwon, B. and J. Copeland, 2007. Security Scheme for centralized Scheduling in IEEE 802.16 Mesh Networks.
3. Rengaraju, P., C.H. Lung and A. Srinivasan, 2011. Measuring and Analyzing WIMAX security and QOS, IEEE ICC.
4. Kolias, C., G. kambouakis and S. Gritzalis, 2013. Attacks and Countermeasures on 802.16 IEEE Common Surveys.
5. Naseer, S., M. Younus and A. Ahmed, 2008. vulnerabilities exposing IEEE 802.16e networks to Dos attacks.
6. Ibikunle, F., 2009. Security issues in Mobile WiMAX 802.16ein Proc IEEE Mobile WiMAX.
7. WiMAX end-to-end Network System Architecture release, 2008 1, WiMAX Forum, Clackamas, OR, USA, 1.3.0
8. Kim, Y., H.K. Lim and S. Bahk, 2008. share authentication information for preventing DDoS attacks in mobile WiMAX networks, in Proc. 5th IEEE Conference Consum. Comm. Netw.
9. Kumar, S., M. Girimondo, A. Weimerskirch, C. Paar, A. Patel and A.S. Wander, 2003. Embedded end-to-end wireless security with ECDH key exchange, in Proc. IEEE midwest Symp., Circuits system.
10. Purkhiabani, M. and A. Salahi, 2011. enhanced authentication and key aggrement procedure of next gen. evolved mobile networks, in Proc. 3rd Int. Conf. Commun. Softw. Netw.