An Efficient Secure Routing in Mobile Ad-hoc Networks Using HMAC

[1] CH. Anusha, [2] K. Chinnaiah
[1]M.Tech Scholar, Department of Computer Science and System Engineering,
Andhra University College of Engineering (A), Visakhapatnam, AP, India.
[2]Department of Computer Science and System Engineering,
Andhra University College of Engineering (A), Visakhapatnam, AP, India

Abstract: Now-a-days security is a major challenging problem in mobile ad-hoc networks because the nodes in mobile ad-hoc networks are moving from one place to another due to this the structure of the network changes frequently. The topology changes may cause "routing modification attack" problem that can easily be exploited against the MANETs. The main goal of routing attacks is to disrupt normal functioning of network by advertising false routing updates. On the other hand data communication attacks include modification or dropping of data packet that does not disrupt routing protocol. In this thesis work, this could be achieved by adding some extensions for secure routing. These extensions include integrity which means the message modification is not allowed and authentication which means the node validation (identification) is done. This protection is provided by a hashed message authentication code function which provides fast message verification and information about sender as well as intermediate node authentication. We obtained acceptable results by using network simulator tool (NS2) depending on the performance of metrics such as packet deliver ratio, packet drop, delay analysis and throughput. The average of delay and packet drop is decreased when we used a secured protocol and also it increases the packet delivery ratio and throughput.

Key words: mobile ad-hoc networks, routing attacks, authentication, integrity, network simulator tool.

1. INTRODUCTION

Present day's mobility is becoming increasingly important for users of computing systems. As a result users can ability to exchange information and maintain connectivity while roaming through a wide area. The necessity support for mobile computing is being provided in some areas by installing base stations and access points. Mobile system users can maintain their connectivity by accessing this type infrastructure from office, home or while on the road [5]. Mobile ad-hoc networks (MANET's) are sometimes called a wireless ad hoc network or a wireless mesh network of mobile nodes, comprises of mobile computing devices (nodes) that uses wireless communication without the presence of any established infrastructure or centralized authority such as an access point in wireless local area network. The nodes which are free to move randomly and organize arbitrarily; thus, the topology of the wireless network may change rapidly and unpredictably. So, in mobile ad hoc network each node acts both host as well as router hence such networks sometime call as multi-hop wireless ad hoc networks. Below Figure 1 shows an example of mobile ad hoc network and its communication technology.

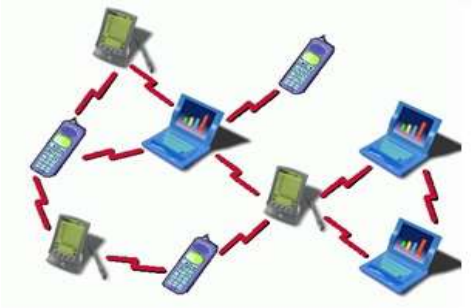

Figure 1: A Typical Mobile Ad Hoc Network

Routing in wireless ad hoc network is much more complicated than wired network because MANET faces several challenges such as open medium, dynamically changing network topology, routing, centralized monitoring and security issues[3]. Secure routing is one of the security issues in MANET because several types of attack occur in MANET during the establishment of route from source node to destination node. Routing protocols must be robust against routing attack in order to establish correct and efficient route between each pair of nodes. The importance of cryptography and trust in secure MANET routing is outlined with relevant security extensions of existing routing protocols for MANETs described [6]. In this paper we propose a shared key cryptography based AODV approach that uses hash function and hashed message authentication code to secure route discovery and route reply process of communication among the nodes in a networks [16]. The proposed method provides efficient message verification and maintained the authentication, integrity principle of security.

2. OVERVIEW OF AD-HOC ON-DEMAND DISTANCE VECTOR ROUTING (AODV) PROTOCOL

AODV is a reactive routing protocol designed for operation of mobile ad hoc network. Protocol provides self starting, dynamic, loops free, multi hop routing. The routing in AODV does not contain information about the complete route path, but only about the source and the destination. The AODV protocol contains message types are Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs)[6]. The routing messages contain information only about the source and the destination. When a route to destination is needed, the node sends a route request (RREQ) packet to its neighbors to find the optimal path. RREQ packet contains route request broadcast ID, Destination IP Address, Destination Sequence Number, Source IP Address, Source Sequence Number and Hop Count. Sequence number is used for route freshness and loop prevention. When a node sends any type of routing control message like RREQ/RREP, it increases its sequence number. The routing table should include latest sequence number for the nodes in the network. This is updated whenever a node receives RREQ, RREP or RRER related to a specific node. Hop count represents the distance between source node to destination node. Each node receiving the RREQ packet sets up reverse path back to the sender of the request so that RREP packet can be unicast to a sender node from the destination or any intermediate node that satisfy the route request conditions. Upon receiving the route request message, the intermediate node forwards the RREQ until a node is found that is the destination itself or it has an active route to the destination with destination sequence number more than or equal to that of RREQ. This node replies back to the source node with a route reply message RREP and remove the RREQ. RREP packet contains Destination IP Address, Destination Sequence Number, Originator IP Address and Lifetime. Forward links are setup when RREP packet travels along the reverse path. Once the source node receives the route reply, it establishes a route to the destination and sends data packet along optimal path set-up.

Route Maintenance in AODV protocol: As long as the route remains active, it will continue to be maintained. A route is considered as active as long as data packets periodically are travelling from the source node to the destination node along the shortest path. Once the source stops sending data packets, the links will be time out and eventually be discarded from the intermediate node routing tables[5,7,14]. If a link failure occurs while the route is active, the node sends a route error (RERR) packet to the source node to inform regarding the unreachable destinations. After receiving the RERR packet, if the source node still desires the route, it can resume route discovery.

2.1. SECURITY ISSUES OF AODV

The major vulnerabilities present in AODV routing protocol are:

- Attacker can masquerade as a source node S by forging a RREQ with its IP address as IP address of source node.
- Attacker can masquerade as a destination node D by forging a RREP with its IP address as IP address of the destination node.
- The hop count is decreasing in RREQ/RREP.
- The sequence number is increasing in RREQ/RREP.

3. CRYPTOGRAPHIC BASED AODV

The proposed method uses a cryptography based symmetric shared secret key technology for encrypting and signing the message during communication. We use a mechanism to setup pair wise secret keys[15]. Following notations describes the cryptographic operation in AODV.

- Let 'S' and 'D' are the source and destination nodes in the networks.
- KSD or KDS denotes the shared secret key between source node 'S' and Destination node 'D'
- Each node holds the Hashed Message Authentication Code (HMAC) Algorithms.
- $MACm$ defined by $HMAC(KSD$, M) represents the computation of message authentication code of message M between source node 'S' and Destination node 'D'.

3.1. PROPOSED METHOD

Proposed AODV routing protocol uses private or shared key cryptography technique for securing the message and routing path during the communication[15]. Route discovery in AODV uses Route Request (RREQ) and Route Reply (RREP), containing two mechanisms to secure routing in MANETs

i) For authenticating the non mutable field include sequence number or IP address of routing message M, use HMAC (KSD,M)

ii) For authenticating the mutable field which contains hope count information , one way $HMAC$ key chain is used

The mutable field contains only hop count information as intermediate nodes increment the hop count field while forwarding the RREQ. The rest of the fields such as sequence number or IP address are related to non mutable fields as they remain unchanged [9]. The following is the steps of algorithms that are used in this research to secure routing:

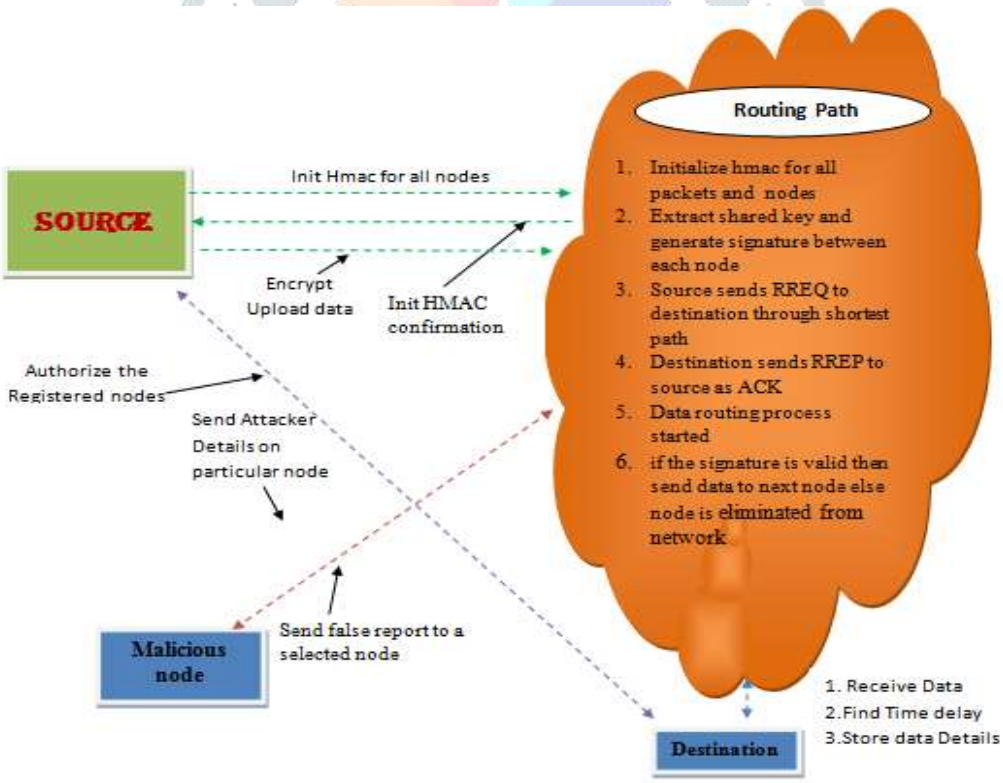

Figure 2: Architecture of proposed work

i.*Algorithm.* *Calculate Security Value for each node*

Begin

Step1. Initialize hmac chain.

Step2. Generate hmac chain.

Step3. Max hop count.

Step4. Define hash function.

Step5. Generate hash based on Source address.

Step6. Extract secret key.

Step7. Generate signature.

End

ii. ***Algorithm.*** *Check signature integrity and verify the hop count*

Begin

Step1. IF the signature is invalid

THEN simply eliminate node from network.

ELSE send data to next hop.

Step2. IF verify hop count is invalid

THEN destroy the packet

ELSE recalculate hash field

End

HMAC function takes a variable number of arguments by simply merging them and computes the message authentication code. The source node S uses AODV routing protocol to connect to the destination node D through three intermediate nodes A, B, and C as shown in Figure 3. The message RREQ containing the following fields : < RREQ, *MACm*, HMAC chain, intermediate node list >, where RREQ is original route request message. Here RREQ is extended to hold three more fields MACm, HMAC chain and intermediate node list. First the sender node compute *MACm* = *HMACKSD* (*RREQ*) using secret key *KSD* shared between itself and destination node D. The source node uses non mutable fields such as sequence number, source and destination IP address except the hop count of RREQ packet and computes message authentication code MACm by simply concatenating them[3,8,12,14]. The sender node calculates h0 = *HMACKSD* (*S, N*) and initializes the intermediate node list to empty list. We can use source sequence number as nonce since each time a source node broadcasts a new route request message, it monotonically increases its RREQ broadcast id or source sequence number.

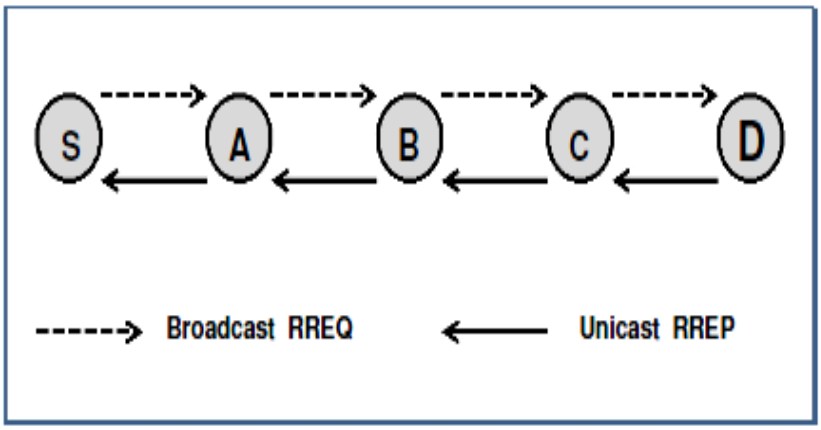

Figure 3: The routing message exchange in AODV

When any intermediate node for example node A receives a packet modifies packet by appending IP address of previous node S to the intermediate node list and replacing the HMAC chain field *h*0 with *h*1 and *h1 = HMACKAD* (*A*, *h*0) where *KAD* is secret key between intermediate node A and destination node D. once destination node D receives the packet it checks the following three conditions:

- Check *MACm* == *HMACKSD* (*RREQ*).

Destination node D checks integrity of received RREQ packet and initially computes message authentication code using non mutable fields of RREQ message and then verifies with received MACm.

- Check *h*2 == *HMACKCD* (*C*, *HMACKBD* (*B*, *HMACKAD* (*A*, *HMACKSD* (*S*, *N*)))).

Destination node gets intermediate node list (S, A, B, C) and containing the IP address of intermediate nodes. It computes HMAC chain using intermediate node list and verify h2. If h2 is verified it means that received node list (S, A, B, C) is correct and malicious node has not removed any intermediate node from node list.

- Check the hop count field i.e. Number of intermediate nodes in node list

If the above three conditions are satisfied, then received RREQ message is regarded as a valid message. If the destination node determines that the RREQ message is valid, it sends acknowledgement as route reply packet back along the reverse path to the source node. The route reply packet contains one extra field i.e. h. Each hop verifies the value h in order to authenticate the previous hop from which it has received packet. In same way source node can authenticate the destination node as well as can check integrity of RREP message.

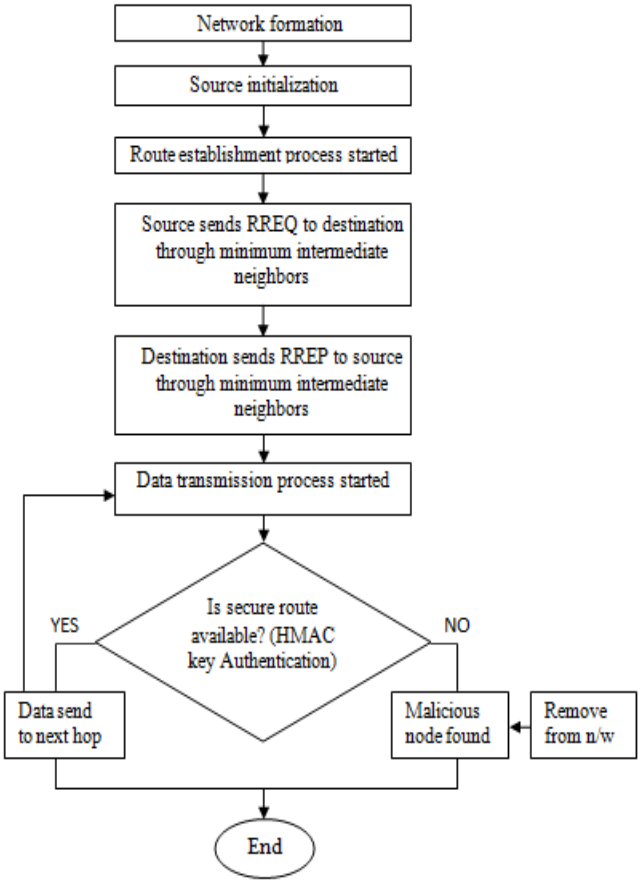

Figure 4: Flow diagram of proposed work

4. SIMULATION RESULTS

For simulating this work we use network simulator Network Simulator Version 2, widely known as NS2, is an event driven simulation tool that is useful in studying the dynamic nature of wireless communication networks .The network simulator is

written in C++ and a script language called OTcl2. Ns2 use an Otcl interpreter towards the user. The OTcl script is used by ns during the simulations. The result of the simulations is an output trace file that can be used to do data processing (calculate delay, throughput etc) and to visualize the simulation with a program called NAM (Network Animator). The graphs below have been generated to show the performance of new cryptographic AODV. Graphs are generated to show Packet Delivery Ratio, Average end-to-end delay, throughput and packet drop of the network.

a) PACKET DELIVERY RATIO:

Packet delivery ratio is the ratio of number of packets received by the destination to number of packets sent by the sender. Packet delivery ratio is higher in cryptographic AODV because data communication starts after, only when nodes are properly authenticated.i.e, there is lesser chance of dropping or missing packets. Reliability is also achieved, in this solution. So a high packet delivery ratio can be archived.

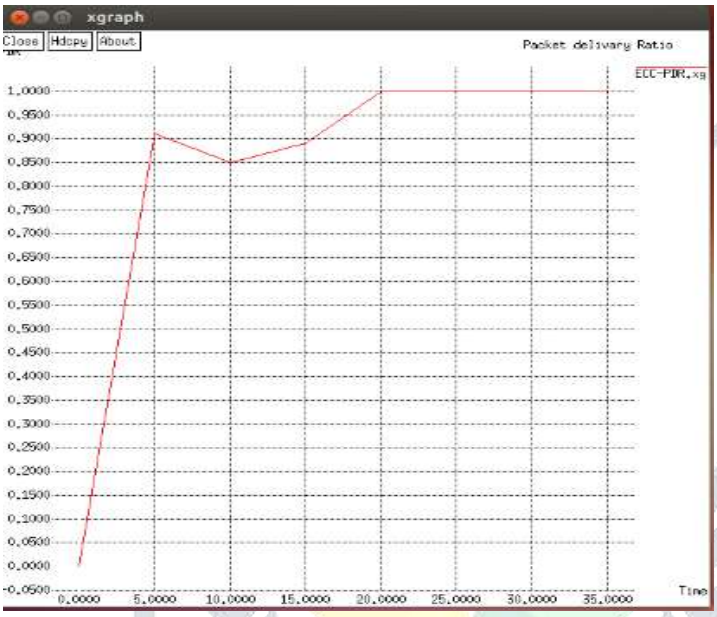

Figure 5: Packet Delivery Ratio Analysis

b) THROUGHPUT

Throughput is defined as how much data can be transferred from one location to another in a given amount of time. Below graph shows the throughput behalf of simulation time. In this graph x axis show the simulation time and y axis show the throughput. When the simulation time increases, the throughput of cryptographic AODV also increases.

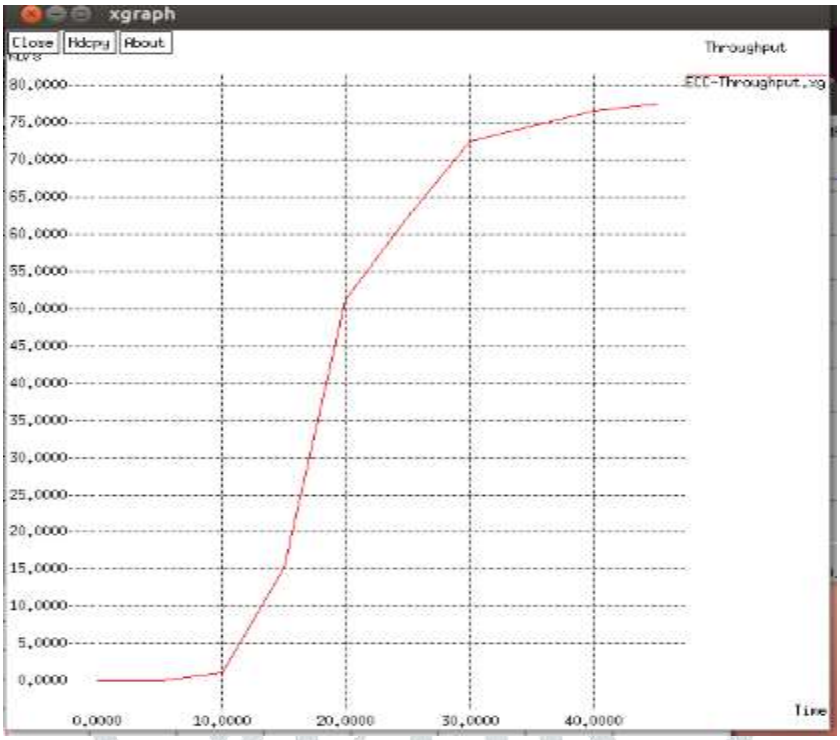

Figure 6: Throughput Analysis

c) PACKET DROP

Packet drop also known as packet loss which is occurs when one or more packets of data travelling across a network fail to reach their destination.

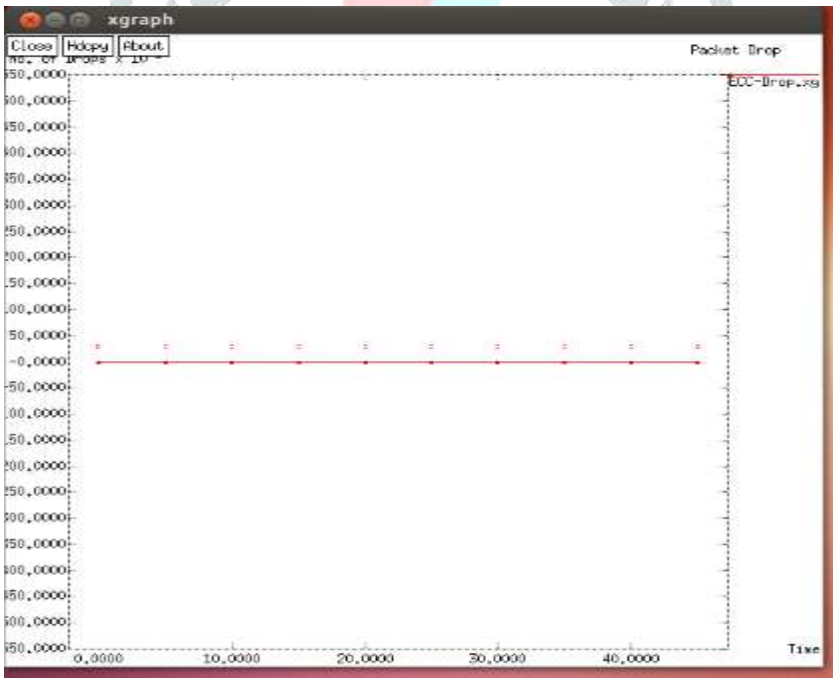

Figure 6: packet Drop Analysis

In AODV with HMAC cryptographic algorithm the packet-loss is zero because data dispatch after node authentication.

d) DELAY ANALYSIS

The delay of a network specifies how long it takes for a bit of data to travel across the network from one node to another. In Authenticated AODV protocol, time delay less with increase in security level.

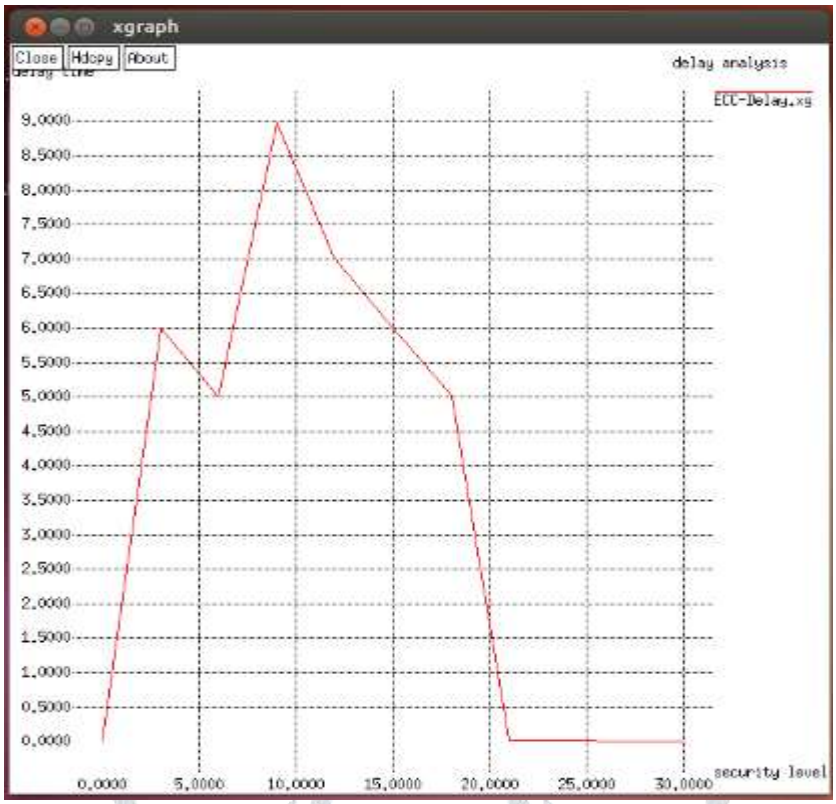

Figure 6: delay Analysis

5. CONCLUSION

Secure routing is one of the most challenging security issues in mobile ad hoc networks. In this paper we provided a higher security and network performance while designing of secure routing protocol. The proposed method uses cryptography based symmetric shared secret key algorithm hashed based message authentication code for establishing a secure optimal route between source node and destination node. In a cryptographic AODV We use a mechanism to setup pair wise secret key between intermediate node by certification and verifying the RREQ message during traveling from one node to other nodes. The proposed method providing both authentication and integrity of the message. The simulation results of cryptographic AODV minimizes the time delay, packet drop and maximize the packet delivery ratio, throughput involved in computation and verification of security during route discovery process.

6. References:

[1]. Abusalah, L., Khokhar, A., & Guizani, M. (2008). A survey of secure mobile ad hoc routing protocols. *IEEE Communications Surveys & Tutorial, 10*(4), 78-93.

[2]. Goyal, T., Batra, S., & Singh, A. (2010). A literature review of security attack in mobile ad-hoc networks. *International Journal of Computer Applications, 9*(12), 11-15.

[3].I. D. Chakeres and E. M. Belding-Royer, "Aodv routing protocol implementation design," in Proc. 24th Int. Conf. Distrib. Comput. Syst. Workshops, 2004, pp. 698–703.

[4]. H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: Challenges and solutions," IEEE Wireless Commun., vol. 11, no. 1, pp. 38–47, Feb. 2004.

[5]. Murthy, C.S.R., & Manoj, B. (2004). Ad hoc Wireless Networks: Architectures and Protocols. Prentice Hall.

[6]. Royer, E.M., & Perkins C.E. (2010). An Implementation Study of the AODV Routing Protocol, Proceedings of the IEEE Wireless Communications and Networking Conference, Chicago .

[7]. Sanzgiri, K. et al. (2002) . A Secure Routing Protocol for Ad Hoc Networks. Computer Science Department Faculty Publication Series. 49. http://scholarworks.umass.edu/cs_faculty_pubs/49

[8]. Garg, N., & Mahapatra, R. P. (2009). MANET security issues. *IJCSNS International Journal of Computer Science and Network Security*, *9*(8).

[9]. Cordasco, J., & Wetzel, S. (2007). Cryptographic vs. trust-based methods for MANET routing security. *Electronic Notes in Theoretical Computer Science, Elsevier*, *197*(2), 131-140. Retrieved December 11,

[10]. Darren Hurley-Smith, Jodie Wetherall and Andrew Adekunle, "SUPERMAN: Security Using Pre-ExistingRouting for Mobile Ad hoc Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING, 2017.

[11]. M. Bouhorma, H. Bentaouit and A. Boudhir, "Performance comparison of ad-hoc routing protocols AODV and DSR," International Conference on Multimedia Computing and Systems, ICMCS '09, Pages511 - 514, 2009.

[12]. Zhou, L., Haas, Z.J.: Securing ad hoc networks. IEEE Network 13(6), 24-30 (November/December).

[13]. Buchegger, S., & Boudec, J.-Y.L. (2002). Cooperation of nodes fairness in dynamic ad-hoc networks. *Pro-ceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC)*.

[14]. Abusalah, L., Khokhar, A., & Guizani, M. (2008). A survey of secure mobile ad hoc routing protocols. *IEEE Communications Surveys & Tutorial*, *10*(4), 78-93.

[15]. H. Krawczyk and P. Eronen, "Hmac-based extract-and-expand key derivation function (HKDF)," RFC 5869, May 2010, Doi: 10.17487/RFC5869.

[16].A. Adekunle and S. Woodhead, "An aead cryptographic framework and tinyaead construct for secure wsn communication," in Proc. Wireless Adv., 2012, pp. 1–5.