Advances in Wireless and Mobile Communications.
ISSN 0973-6972 Volume 10, Number 5 (2017), pp. 969-984

http://www.ripublication.com

Symmetric Key Cryptography based Secure AODV Routing in Mobile Adhoc Networks

Awadhesh Kumar[1] and R. R. Tewari[2]

[1, 2:] *Department of Electronics and Communications, University of Allahabad, India.*

Abstract

Due to routing attacks secure routing in a mobile adhoc network is a one of the most challenging research areas in computer science. Any exploit not follow the rules of routing protocol belongs to routing attack. In a mobile adhoc network, attacks are classified in two broad categories named as routing attacks and data forwarding attacks. Routing attacks are the attacks which mislead or interrupt normal functioning of network by advertising false routing updates and data forwarding attacks include actions such as modification or dropping of data packet that does not disrupt routing protocols. In this paper we propose a symmetric 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. The proposed method provides fast message verification and maintained the authentication and integrity principle of security. We use symmetric key based AODV approach instead of asymmetric key based cryptographic approach because in asymmetric key based approach block of message are encrypted and compute digital signature of each block, this will take a long time for computation, transmission and required more storage. We simulate and compare the proposed secure AODV protocol with original AODV protocol in the network simulator OMNeT++. Simulation result shows that proposed method minimizes the time delay and network routing load involved in computation and verification of security fields during route discovery process and performs better than the original AODV protocol in the presence of malicious nodes.

Keywords: Mobile Adhoc Networks, AODV Protocols, Symmetric Key Cryptography, MAC, HMAC.

1. INTRODUCTION:

In the current decade, Mobile Adhoc Network (MANET) is one of the most popular research areas in computer science. MANET is an emerging technology in which node acts as router as well as host to communicate each other in peer to peer manner in multi-hope fashion without existing any infrastructure [1]. This means, it is also known as infrastructure less network in which there is no need of any base station or access point which is required in infrastructure based networks [2]. In MANET, the data packet is routed among the nodes directly or indirectly. There are currently two kinds of mobile wireless networks, namely, infrastructure based and infrastructure less network. In MANETs, all nodes are dynamically and arbitrarily located, and are required to relay packets for other nodes in order to supply data across the network. The dynamic nodes in mobile adhoc network follow the property of "Anywhere Anytime".

There are some applications in which MANETs are most useful like in Military vehicles on a battlefield with no existing infrastructure, in a fleet of ships at sea, in flooding areas, in an earthquake and in gathering of people. Routing in wireless adhoc network is much more complicated than wired network because MANET faces several challenges such as open medium, dynamically changing network topology, routing, centralized monitoring, energy conservation and security issues [3, 4]. Secure routing is one of the big security issue in MANET because several types of attack occurs in MANET during the establishment of route from source node to destination node. Routing protocols in MANET are subdivided as being Proactive (or table-driven), Reactive (or on demand), or Hybrid protocols [5]. Proactive algorithms employ classical routing strategies such as distance-vector or link-state routing, and any change in the link connections is updated periodically throughout the network. Reactive protocols use an approach in which nodes only discover routes to the destinations when demanded [5]. Hybrid protocols combine local proactive and global reactive routings in order to achieve a higher level of efficiency and scalability. In this paper we propose a Secure AODV routing protocol that establish a route from source node to destination node only when demanded and uses a symmetric key cryptography based approach of hash function and hashed message authentication code (HMAC) for fast verification of message and maintaining the authentication and integrity principle of security. The symmetric key cryptography uses same key for both encryption and decryption of message. The different kinds of routing attacks occurs during the establishment of route through AODV protocol and procedure of hash value and HMAC computation are described below:

2. ATTACKS ON AODV:

Adhoc networks are vulnerable to variety of attacks that attempt to compromise the network's operation and the data that networks nodes generate. Basically attacks are

classified as passive attack and active attack. Passive attack refers to the reception of message by an unauthorized individual which can be prevented using confidentiality measure. Active attacks refer to a situation where an unauthorized individuals or system positions itself between the sender and receiver such that the sender message are intercepted, modified and retransmitted to the receiver [6]. During the route establishment through AODV protocol, different kinds of attacks occurs that are described as follows:

Modification Attack: In a modification attack, shoddy nodes can cause redirection of network traffic and denial of service (DoS) attacks by altering control message fields or by forwarding routing messages with falsified values.

Redirection by modified route sequence numbers: In AODV protocol Route are established by assigning monotonically increasing sequence number to route towards specific destination [2]. Any node may divert traffic through itself by advertising a route to a node with a destination sequence number greater than the authentic value. Consider an example given in figure 1, when source node 'S' initiate a route discovery to destination node 'D', firstly node 'S' broadcasting RREQ message to its neighbor node 'A' then node 'A' broadcast RREQ to its neighbor 'B' but shoddy node 'M' receive a RREQ broadcasted by 'A' and 'M' redirect traffic towards itself by unicasting RREP to 'A' containing much higher sequence number than the last value advertised by 'D' and at that point 'A' receive a false RREP message from 'M' and thinking that RREP is from 'A' and unicast to 'S' for valid route but 'A' and source node 'S' receive a false RREP from node 'M'.

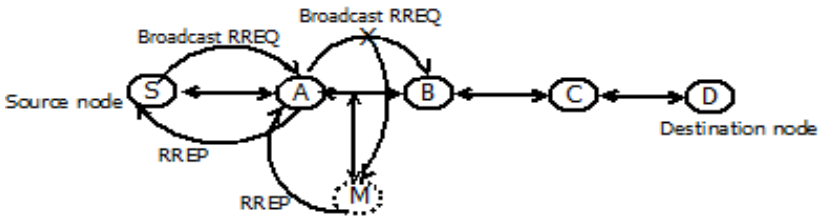

Figure 1: Redirection by modified route sequence numbers

Redirection of traffic with modified hop counts: A redirection attack is possible by modification of the hop count field in route discovery messages. When routing decisions cannot be made by other metrics, AODV uses the hop count field to determine a shortest path. In AODV, malicious nodes increase the chances that they are included on a newly created route by resetting the hop count field of the RREQ to zero. Similarly, by setting the hop count field of the RREQ to infinity, created routes will tend to not include the malicious node. Such an attack is most threatening when combined with

spoofing [7].

Wormhole Attack: In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and retransmits them into the network. The wormhole attack can form a serious threat in wireless networks, especially against many ad hoc network routing protocols and location-based wireless security systems [4]. Figure 2 shows an example of the wormhole attack against an AODV routing protocol. In the figure, we assume that nodes 'A1' and 'A2' are two colluding attackers and that node 'S' is the target node to be attacked. During the attack, when source node 'S' broadcasts an RREQ to find a route to a destination node 'D', its neighbors nodes 'X' and 'P' forward the RREQ as usual. However, node 'A1', which receives the RREQ forwarded by node 'X', records and tunnels the RREQ to its colluding partner 'A2'. Then, node 'A2' rebroadcasts this RREQ to its neighbor node 'Y'. Since this RREQ passed through a high-speed channel, this RREQ will reach node 'D' first. Therefore, node D will choose route D-Y-X-S to unicast RREP to the source node 'S'.

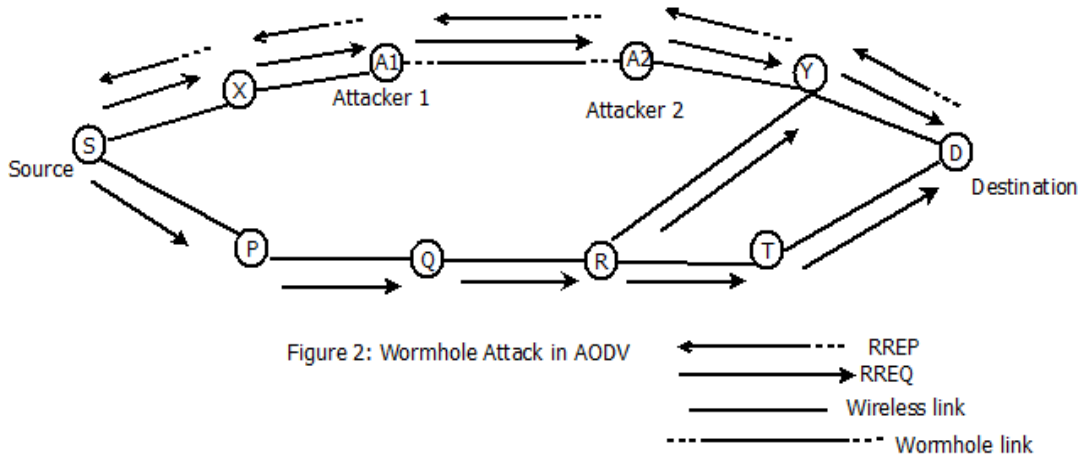

Figure 2: Wormhole Attack in AODV

Impersonation Attack such as Forming Loop by Spoofing: Spoofing occurs when a node misrepresents its identity in the network, such as by altering its MAC or IP address in outgoing packets, and is readily combined with modification attacks. The example illustrated in Figure 3, showing how impersonation attacks works on AODV. According to the example node ' A' can hear nodes 'B' and 'D', node 'B' can hear nodes 'A' and 'C', node 'D' can hear nodes 'A' and 'C', node 'C' can hear nodes 'D', 'B' and 'E', node 'M' can hear nodes 'A','B','C' and 'D' and node 'E' can hear node 'C' and next hope on the path towards node 'X'. During the route discovery attacker can learn this topology by listening to the exchange of RREQ/RREP. Malicious node M can then form a routing loop so none of the four nodes can reach to the destination.

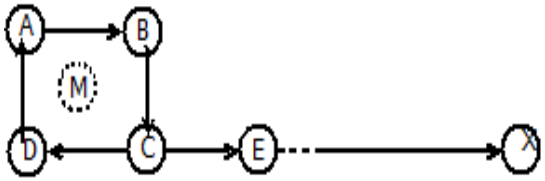

Fig. 3: Impersonation Attack

Fabrication attack: Generation of false routing message can be classified fabrication attack and such attack can be classified as falsifying routing error in AODV, DSR and route cache poisoning in DSR. Here we discuss the falsifying routing error in AODV.

Falsifying routing error in AODV: when node moves through broadcasting, AODV implement path maintenance to recover broken links. If the destination node or intermediate node along an active path moves the node upstream of the link breakage then it broadcast the route error message to all active upstream neighbors. The source node also invalidate the route for this particular destination in its routing table. The vulnerability here is that, a route attack can be launched by sending false route error message. Consider an example illustrated in figure 1, there is an route between source node 'S' to destination node 'D' via nodes 'A','B','C' and shoddy node 'M' can launch denial of service(DoS) attack against destination node 'D' by continuously sending route error message to node 'A' as link breakage between spoofed node 'B' and node 'D' . Node 'A' received a spoofed error message thinking that message is come from node 'B', deleting its routing table entry for 'D' and forward the route error message to next upstream node which also deletes it routing table entry for 'D' and continue using this process in chain system forward the route error message to source node 'S' and source node deleted routing table entry for destination node 'D' from its routing table and reinitiate the route discovery process. In this process of establishing a route from source node 'S' to destination node 'D' , shoddy node 'M' listen and can broadcast route error message to prevent communication between 'S' and 'D'.

2.1 Security requirement in Adhoc network routing: In a MANETs several types of routing attacks occurs during the path establishment from source node to destination node for communication through AODV routing protocol. Proposed Secure AODV Routing algorithm must prevent most of the attack discussed above by using the symmetric key cryptography based hash value and hashed message authentication code (HMAC) computation for verification and maintaining the authenticity and integrity of the message during communication. In an adhoc networks, protecting the route establishment from source node to destination node, secure routing algorithms can satisfied following properties [8]:

- Route signaling cannot be spoofed

- Fabricated routing message cannot be injected into the network
- Routing message cannot be altered in transit, except to the normal functionality of routing protocol.
- Loops in the route cannot form through malicious node.
- Route cannot be redirected from the shortest path through malicious node.
- Unauthorized nodes should be excluded from route computation and discovery.

Since adhoc network is an open medium environment then above requirement comprises the needs of security. We use symmetric key based cryptography approach for secure routing communication because public key encryption and digital signature takes more time for doing the complex computation and more storage space required.

2.2 Hash Function and Message Authentication Code:

Securing a message during transmission, cryptography algorithms are used. Public key cryptography such as RSA used for encrypting the plaintext message into cipher text message by dividing the plaintext message in a block of fix size as 1024 bit or 2024 bit and convert each block of plaintext message into cipher text block . When the size of plaintext message is large such as 1 MB then it is divided into 1024 block of 1024 bit each. By using RSA encryption scheme for encrypting and signing the message requires 1024 block of 1024 bit each for cipher text and 1024 block each block of size 1024 bit for digital signature, since each block compute a separate cipher text and separate digital signature. Hence 1 MB space required for cipher text and 1MB for digital signature i.e. 2 MB sent by sender to receiver. This process of authentication takes much time as well as energy consumption. Hash function solve the above stated problem and it compute the message digest of hash value of message at once and sign it. Hash function has the following characteristics [9]:

- Hash value can be computed for any arbitrary length of message.
- It function produces fixed output length and computation is relatively easy
- It is Preimage resistance i.e. for a given output z, it is impossible to find any input x such that $h(x) = z$, i.e. $h(x)$ is one-way.
- It is Second preimage resistance i.e. for given x1, and thus $h(x1)$, it is computationally infeasible to find any x2 such that $h(x1) = h(x2)$.
- It has Collision resistance i.e. It is computationally infeasible to find any pairs $x1 \neq x2$ such that $h(x1) = h(x2)$.

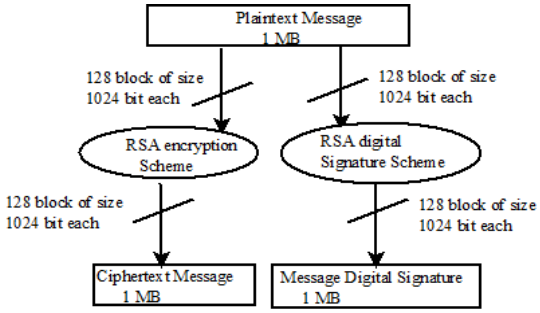

Fig. 4 (a) Computation of Digital Signature and Encryption through RSA

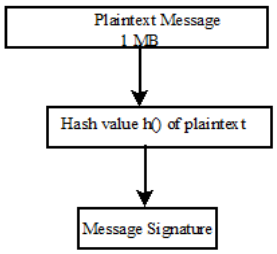

Fig. 4 (b): computation of digital signature through hash function

Message Authentication code(MAC), also known as key based hash function or cryptographic checksum[9]. MAC uses symmetric key encryption scheme for genrating the authentication tag and verifying it and they do not provide non repudiation. It provides message authentication and message Integrity. MAC is much faster than digital signature since they are based on hash function[9]. A MAC 'm' is a function of the symmetric key k and the message x.

$$m = MAC(x, k), where\ x\ is\ a\ message\ and\ k\ is\ a\ symmetric\ key$$

3. INTRODUCTION TO AODV:

AODV routing protocol is basically a combination of DSDV and Data Source Routing (DSR) protocols [10, 11]. It borrows the basic on-demand mechanism of route discovery and route maintenance from DSR, plus the use of hop-by-hop routing, sequence numbers, and periodic beacons from DSDV. AODV routing algorithm minimizes the number of required broadcasts by creating routes only on-demand basis and enables dynamic, self-starting and multi-hop routing between participating mobile nodes by wishing to establish and maintain an ad hoc network [5]. The routing messages in AODV do not contain information about the complete route path, but only about the source and the destination. The message types defined by AODV are Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs) [12]. AODV discovers routes as and when necessary and it does not maintain routes from every node to every other. Every node maintains its monotonically increasing sequence number. Sequence number increases every time the node notices change in the neighbourhood topology. AODV utilizes routing tables to store routing information. The route table stores information in the form : < destination address, next-hope address, destination sequence number, life time>. AODV relies on a broadcast discovery mechanism and route maintenance. For example, sender 'S' broadcast a message to all its neighbours, each node receiving the message from 'S' forwards message to its own neighbours. Message reaches destination 'D' provided that 'D' is reachable from sender 'S'. This process of sending message from source node 'S' to destination node 'D', Continues in

a chain system, till the message is reached at the final destination 'D'. Node 'D' sets up a reverse route reply (RREP) for the source node 'S' in its route table.

Route Maintenance in AODV: 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 to the destination along the path. Once the source stops sending data packets, the links will be time out and eventually be deleted from the intermediate node routing tables [13]. If a link break occurs while the route is active, the node upstream of the break propagates a route error (RERR) message to the source node to inform regarding the unreachable destinations [14]. After receiving the RERR, if the source node still desires the route, it can reinitiate route discovery.

4. PROPOSED CRYPTOGRAPHY BASED AODV ROUTING METHODS:

The proposed secure AODV routing protocol uses a cryptography based symmetric shared secrtet key technology for encrypting and signing the message during communication.We Adopt a mechenism to setup pair wise secret keys. If n is the number of nodes in the network, total n(n-1)/2 pair wise secret key will be maintained. following notations describes the cryptographic operation in AODV.

- 'S' and 'D' are the source and destination nodes in the networks
- K_{SD} or K_{DS} denotes the shared secret key betweensource node 'S' and Destination node 'D'.
- Each nodes holds the Hashed Message Authentication Code (HMAC) Algotithms
- MAC_m defined by $HMAC(K_{SD}$, M) denotes the computation of message authentication code of message M between source node 'S' and Destination node 'D'

Proposed Method:

Proposed Secure AODV routing protocol uses private or shared key cryptography techniques for securing the message and routing path during the communication. Route discovery in AODV uses Route Request (RREQ) and Route Reply(RREP), Containing two types of information fields named as Mutable and Non Mutable. Hope count is the only mutable field as intermidiate nodes increment the hope count field while forwarding the RREQ and the rest of fields such as IP address, Sequence Number are nonmutable fields as they remain unchanged. the proposed AODV uses two mechenism to secure routing in MANETs

i) for authenticating the non mutable field of routing message M, use HMAC (K_{SD} , M)

ii) For authenticating the mutable field i.e. hope count information , one way $HMAC$ key chain is used

HMAC takes a variable number of arguments by simply concatenating them and compute the message authentication code. Consider the fiure 5, showing the source node 'S' uses AODV routing Protocol to connect from the destination node 'D' through intermidiate nodes A,B,and C or X, Y and C. RREQ and RREP message are dipicted in the figure 6. Message P extended route request containg the following fields: $< RREQ, MAC_m, HMAC\ chain, List\ of\ Intermidiate\ nodes >$. Sender node 'S' first compute $MAC_m = HMAC(K_{SD}, M) = HMAC_{K_{SD}}(RREQ)$ then uses non mutable field <Sequence Nmber, IP address of Source and destination > and compute the message authentication codes by simply concatenating them such as $h_0 = HMAC_{K_{SD}}(S, N)$ and initialize intermidiate node to empty list where S denotes the source node IP address and N is the time varing component named as nonce. Nonce are used to prevent reply attacks. RREQ broadcast ID or source sequence number are used as nonce since each time source node S broadcast a new RREQ message , it monotonically incresing its RREQ broadcast ID or Source Sequence Number, when any intermidiate node receives a packet P by appending IP address of previous node 'S' to intermidiate node list and replacing the HMAC chain field h_0 with h_1 and $h_1 = HMAC_{K_{AD}}(A, h_0)$ where K_{AD} is the secret key between A and D. when any intermidiate node such as node 'A' receives a packet P , it modifies packet P by appending IP address of the previous node 'S' (from which it receives the packet P) to the intermidiate node list and replacing the HMAC chain field h0 with $h1 = HMAC_{K_{AD}}(A, h0)$, Where K_{AD} is the secret key between intermidate node 'A' and Destination node 'D'. In the proposed method intermidate node only forward the RREQ packet P by broadcasting it and does not sent route Reply Back to the sender S. When Destination node 'D' receives the Message it checks the following three conditions

i) For Intigrity of Received RREQ message computes $MAC_m = HMAC_{K_{SD}}(RREQ)$

ii) Computes HMAC chains and verify it. According to the figure 5 the process is

$$h_4 = HMAC_{K_{ED}}(E, HMAC_{K_{CD}}(C, HMAC_{K_{BD}}(B, HMAC_{K_{BD}}(A, HMAC_{K_{SD}}(S, N)))))$$

$i.e.\ destination\ node\ obtain\ the\ intermidiate\ list\ (S, A, B, C)$ containing IP addresss of each.

iii) verify the hope count field by counting the intrmidiate node in the node list and hope count value in RREQ Message

If all the above stated coditions are satisfied, the received message is regarded as a valid message and destination nodes 'D' floods the reverse route reply (RRREP) of packet P to find the source node S and the process of reverese route reply(RRREP) is same as the process of route discovery because this process of

RRREP uses multicast route reply instead of using unicast route reply used by simple AODV. when source nodes receives an RRREP message , data packet transmiision started immidiately. In this process of our study to increse the posibility of establishing routing path with less RREQ message than other protocol have on topology changed by nodes mobility in uniast RREP. the Route Request initiated from source node S to destinataion node D are shown in the following figure 6.

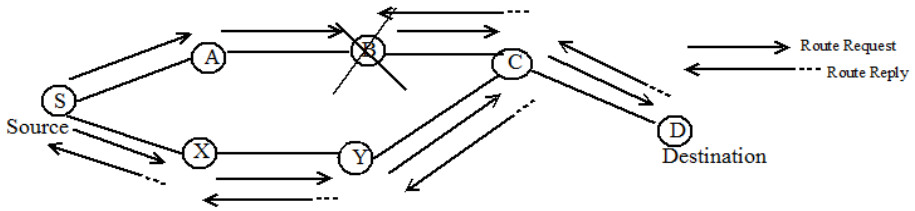

Figure 5 : Exchange of Routing Message in AODV

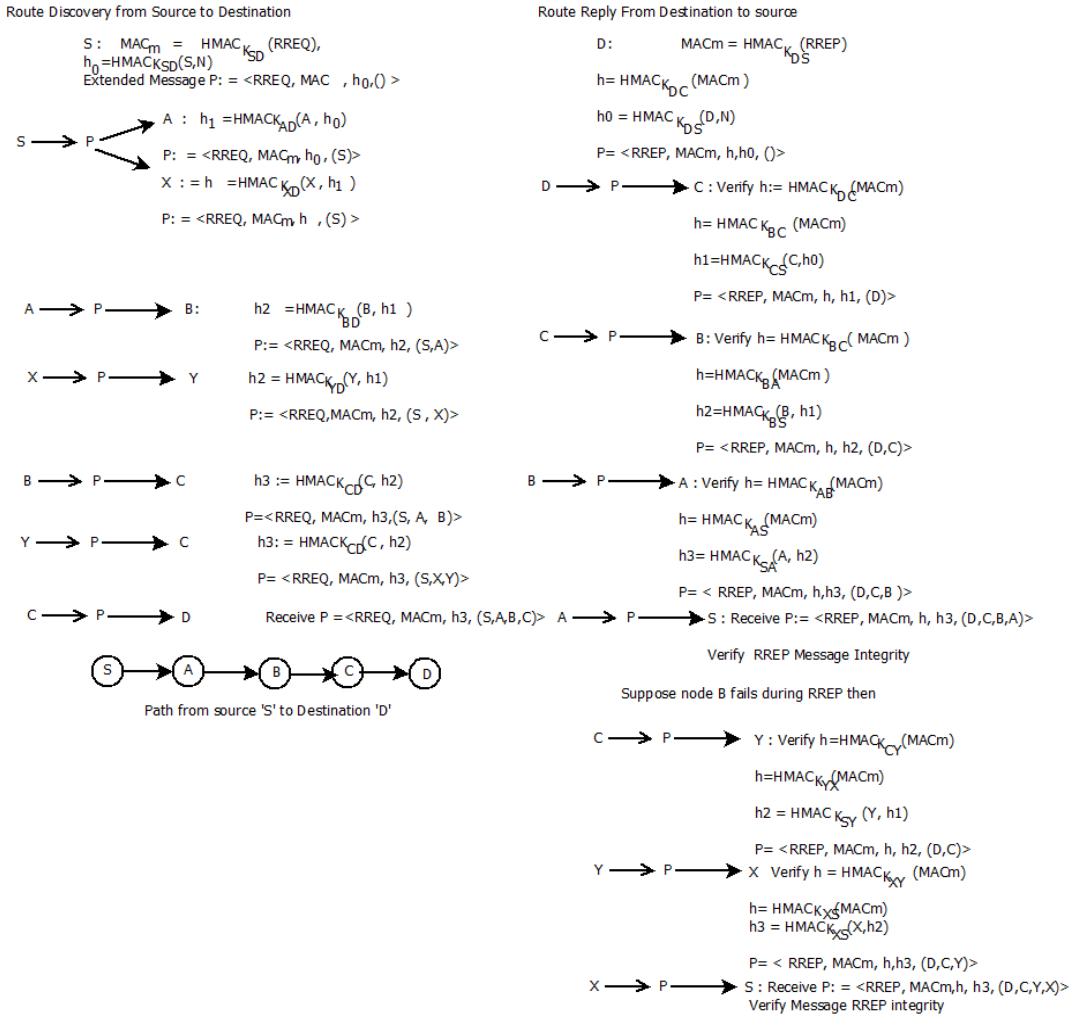

Figure 6 : Route Discovery and Route Reply in Secure AODV

5. SIMULATION AND RESULT ANALYSIS:

For simulating this work we use network simulator OMNeT++ which is an extensible, component based C++ simulation library framework. INET framework is an open source model library for the OMNeT++ simulation environment. The INET Framework supports wireless and mobile simulations as well. Support for mobility and wireless communication has been derived from the Mobility Framework. The simulation is setup in 1000 m × 1000 m playground with varies number of mobile nodes. The OMNeT++ Simulation Environment is setup as follows

Play Ground Dimension	1000m X 1000m
Number of nodes	50
Max. Channel Power	2.0 mW
Radio Tx. Power	2.0 mW
Radio Bitrate	54 Mbps
Broadcast Delay	0 to 0.008s
Simulation Time	600s
Start Time	0 s
Message Length	512B
Message Frequency	0.2s
Routing Protocol	AODV, Proposed Secure AODV

5.1 Performance Matrices and Results: To evaluate performance of above mentioned protocols, we compared them for the following matrices as a function of pause time and malicious nodes**.**

5.1.1 Packet Delivery Ratio: this is the ratio of number of packet successfully sent to destination to those genrated by source.

$$Packet\ Delivery\ Ratio = \frac{Total\ pakets\ received\ by\ the\ destination}{Total\ packets\ sent\ from\ the\ source}$$

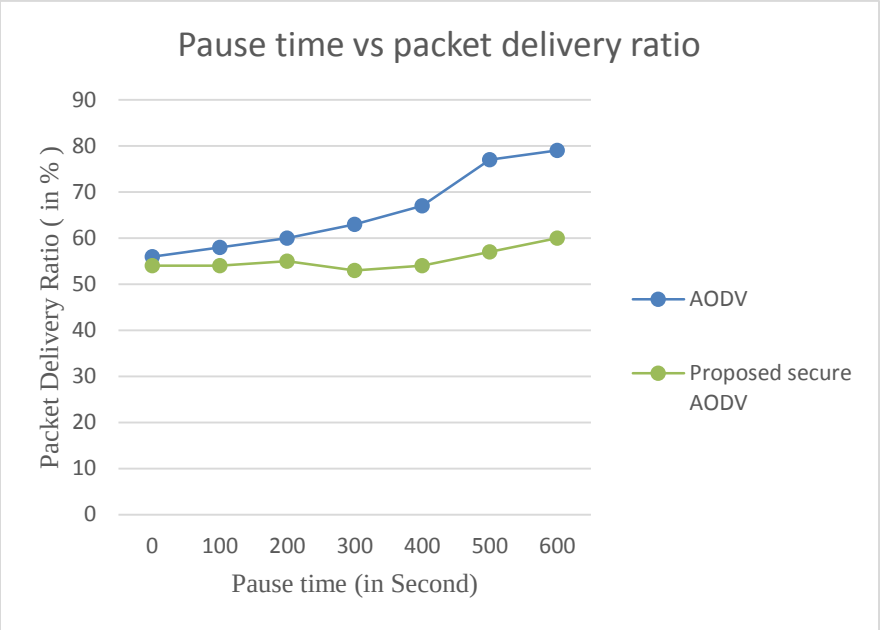

Figure 7: Pause Time Versus Packet Delivery Ratio

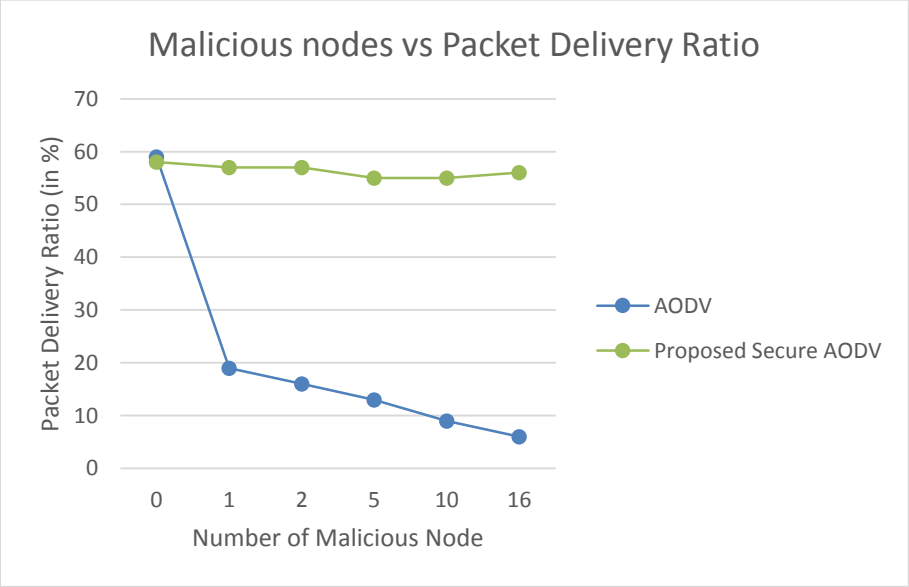

Figure 8: Packet delivery ratio with incresing Malicious node

The figure 7 shows the mobility of nodes on packet delivery ratio when no malicious nodes present in the networks and we found that packet delivery ratio increases with increase in pause time but packet loss rate is high due to change in network topology. AODV performs better in the absence of malicious nodes in network as compared to

Proposed Secure AODV because AODV uses unicast route reply.

From figure 8, we found that Packet delivery ratio decreases as malicious nodes increases in the network. In case of AODV protocol, packet delivery ratio decreases with increase in malicious node as AODV protocol has no security mechanism to guard against malicious attacks so very few of data packets reach to the destination node. In Proposed Secure AODV protocol having much better packet delivery ratio as compared to AODV because proposed protocol uses secure symmetric cryptographic technique for securing message.

5.1.2 Time Delay: Time delay is the difference between the time when first data packet is received by the destination node and the time when source node broadcast a Route Request (RREQ) message. it depends on both position and mobility of the nodes.

$$Time\ Delay = time\ when\ destination\ node\ receive\ first\ data\ packet - time\ when\ source\ node\ broad\ cast\ RREQ\ Message$$

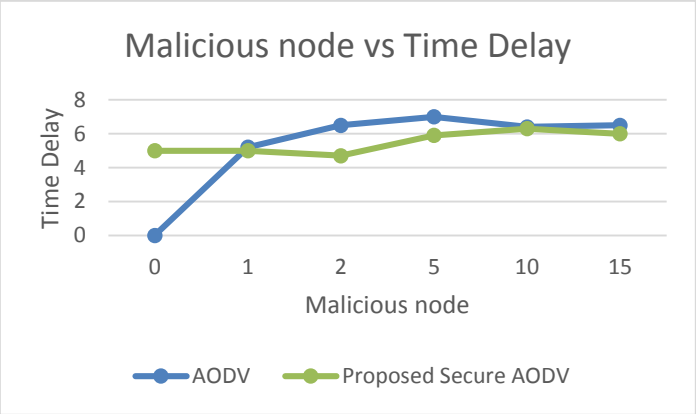

Figure 9: Pause time versus Time Delay

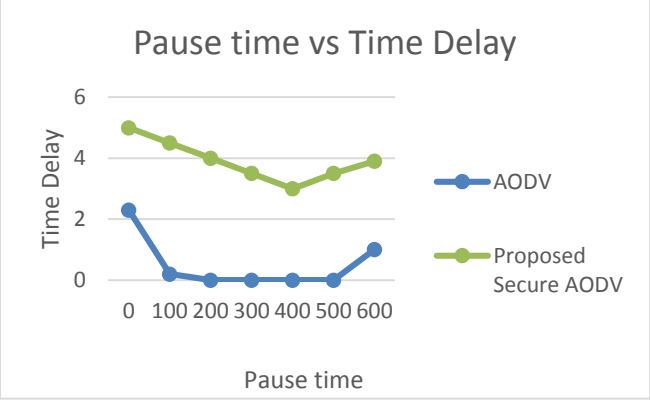

Figure 10: Time Delay with incresing Malicious node

Figure 9 shows the impact of mobility on time delay. When mobility is high, the network topology changes frequently which causes frequent link failures. So time delay is more due to increased communication overhead. In case of the proposed secure AODV protocol, the time delay is more because proposed method uses symmetric key cryptography so it requires significant processing time to compute or verify HMAC and hashes at each node.

Figure 10 illustrates the impact of malicious nodes on time delay. In AODV protocol, time delay increases with increase in malicious nodes because in the presence of malicious nodes, more time is required to deliver data packet to destination node. When compare both, time delay is less in case of Proposed Secure AODV as compared to AODV.

5.1.3 Control Packet overhead: this is the ratio between the packet sent multiplied by paket size and received data paket multiplied by received packet size.

$$Control\ Packet\ overhead = \frac{Routing\ Packet\ sent * Size\ of\ Routing\ Packets}{Received\ data\ packets * Size\ of\ received\ data\ packets}$$

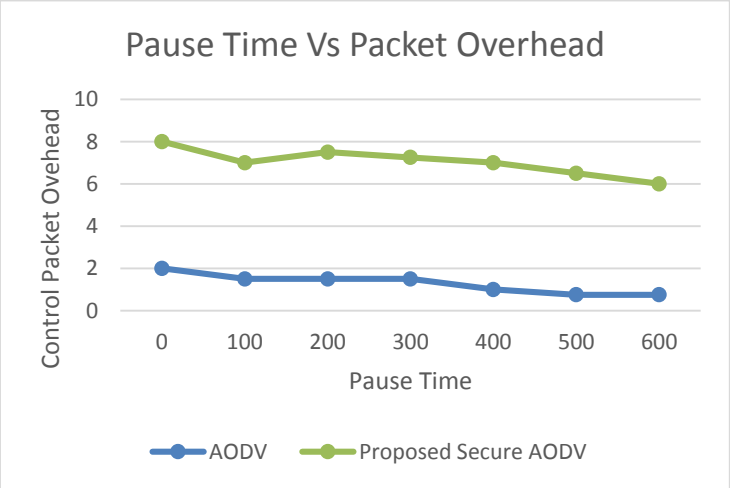

Figure11: Control Packet overhead with increasing Mobility

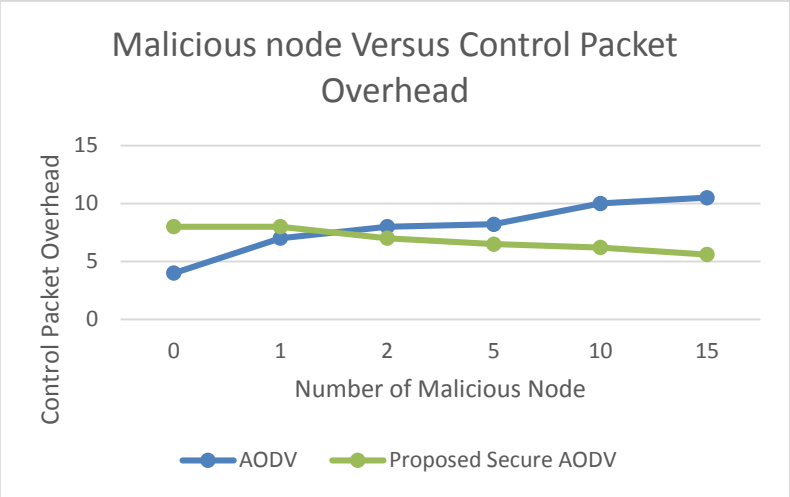

Figure 12: Control Packet overhead with increasing malicious node

Figure 11 shows the impact of the mobility of nodes on control packet overhead. . In proposed secure AODV method, routing or control packets use extra bytes to store hashes and intermediate node addresses hence packet control overhead is more as compared to simple AODV protocol.

Figure 12 shows the impact of malicious nodes on control packet overhead. In AODV protocol, the number of routing packets and data packets delivered to destination nodes both decrease with increase in malicious nodes but decrements in received data packets is more in comparison to decrements in routing packets therefore control packet overhead increases with increase in malicious nodes. In Proposed secure AODV method, number of routing packets overhead decreases with increase in malicious nodes but number of received data packets vary slightly therefore overall control packet overhead decreases.

CONCLUSIONS:

Secure routing is one of the issues in MANET. For providing better performance, AODV routing of MANETs uses hashed based message authentication code during the establishment of secure route between source node and destination node. In the proposed secure AODV approach pairs of node share a symmetric key and through this key message is encrypted and secure communication between intermediate node by signing and verifying the RREQ message during traveling from one node to other nodes. The simulation result concludes that secure AODV method minimizes the time delay and network control packet overhead involved in computation and verification of security fields during route discovery process. we also found that proposed secure AODV routing perform much better than the normal AODV routing when number of

malicious nodes present in the network because normal AODV does not have any security mechanism while proposed secure AODV uses hashed message authentication code for providing authentication and integrity of the message.

REFERENCES:

[1] Johnson, D. B. et al. (2003). The dynamic source routing protocol for mobile adhoc networks (DSR). INTERNET DRAFT, MANET working group.

[2] Routing Protocols for Ad-Hoc Mobile Wireless Networks, IEEE Personal Communications Magazine, April 1999, pp. 46-55.

[3] 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.

[4] B.C. Lesiuk, Routing in Ad Hoc Networks of Mobile Hosts, Available Online: http://phantom.me.uvic.ca/clesiuk/thesis/reports/adhoc/ adhoc.html

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

[6] Hu, Y., Johnson, D.B., Perrig, A. (2002b). Sead: Secure efficient distance vector routing for mobile wireless ad hoc networks. *Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications (WMCSA)*,3-13

[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] Cordeiro, C.M., & Agrawal, D.P.(2014). Adhoc and Sensor Networks: Theory and Applications(2 Ed.). USA:World Scientific Publication

[9] Paar, C., & Pelzl, J. (2010). Understanding Cryptography: A Textbook for Students and Practitioners. Newyork, Springer

[10] Abdalla, A.M et. al.(2011): Misbehavior Nodes Detection and Isolation for MANETs OLSR Protocol". *Procedia Computer Science*, PP. 115–122.

[11] Perkins, C.E., & Bhagwat, P. (1994). Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. Proceeding of ACM SIG-COMM. 24, 234-244.

[12] Andrea Goldsmith, Wireless Communications; Cambridge University Press, 2005.

[13] Karloff,C., and Wagner,D. (2003). Secure routing in wireless sensor networks: attacks and countermeasures "springer journal of Ad Hoc Networks. University of California, Berkeley, pp. 293–315

[14] Shree, R. & Khan R. J. (2014). Wormhole Attacks in Wireless sensor Networks. International Journal of Computer Networks and Communications Security. 2(1), pp. 22–26