International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011

Securing AODV Routing Protocol in MANET Based on Cryptographic Authentication Mechanism

Preeti Sachan and Pabitra Mohan Khilar

Department of Computer Science and Engineering
National Institute of Technology Rourkela, Odisha, India
preetischn@gmail.com, pmkhilar@nitrkl.ac.in

Abstract. *In mobile ad hoc wireless network (MANET), secure communication is more challenging task due to its fundamental characteristics like infrastructure less, wireless link, distributed cooperation, dynamic topology, lack of association, resource constrained and physical vulnerability of node. In MANET, attacks can be broadly classified in two categories: routing attacks and data forwarding attacks. Any action not following rules of routing protocols belongs to routing attacks. The main objective of routing attacks to mislead or disrupt normal functioning of network by advertising false routing updates. On the other hand data forwarding attacks include actions such as modification or dropping of data packet that does not disrupt routing protocol. In this thesis work, we proposed a method to secure ad hoc on-demand distance vector (AODV) routing protocol. The proposed method provides security for routing packets and can efficiently prevent the attacks such as black hole, modifying routing information and impersonation. The proposed method uses hashed message authentication code (HMAC) function which provides fast message verification and sender as well as intermediate nodes authentication. We simulate and compare the proposed method with original AODV and secure AODV (SAODV) protocol using network simulator tool (NS2). 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 performing black hole attack.*

Keywords: *Mobile ad hoc network (MANET), Routing attacks, AODV, Black hole, Impersonation, HMAC, Authentication.*

1 Introduction

A Mobile ad hoc network (MANET) is an autonomous system of wireless mobile nodes that can be dynamically setup anywhere and anytime. MANET differs from cellular networks or conventional wired networks as there is no centralized access point [11, 17]. MANET allows multi-hop communication among nodes that are not in direct transmission range through intermediate nodes. Nodes are free to move randomly thus form arbitrary network topology. The network size changes as a node can join or leave network at any time. MANET can be either connected to large internet or can be operated in a standalone fashion. MANET is an emerging research area because of their self configuration and self maintenance capabilities. Such network finds application in personal area networking, meeting rooms and conferences, emergency operation, disaster relief and military operation. Other applications include robot data acquisition, vehicular ad hoc networks (VANETS), wireless mesh and sensor networks, collaborative and distributed computing. However, MANET is more vulnerable to security

DOI : 10.5121/ijnsa.2011.3518

attacks than conventional wired and wireless networks due to its fundamental characteristics of open medium, dynamic topology, absence of centralized access point, distributed cooperation, lack of association [26]. Authorized and malicious nodes both can access the wireless channel. As a result, there is no clear line of security in MANETs from the outside world. Nodes are portable devices that make them vulnerable to compromises or physical capture. Routing algorithm needs mutual trust between nodes and absence of centralized access point prevents use of monitoring agent in the system. The limitation of wireless network and mobile nodes such as bandwidth of wireless channel, frequent disconnection of link, partition of network, short battery life time and limited computation capability poses an important challenge for implementation of cryptographic algorithms for providing security to these networks.

Routing security is an important issue in MANET [6, 7]. In MANET, two types of messages are used: data messages and routing or control messages. Data messages need end to end authentication and can be secured using point to point security mechanism. Routing messages are used for the route establishment and route maintenance. Routing messages are processed by intermediate nodes during their propagation therefore securing routing messages is more challenging compared to data messages. A malicious node can perform many types of routing attacks such as routing table overflow, routing table and cache poisoning. Routing protocols must be robust against routing attack in order to establish correct and efficient route between pair of nodes. The existing work for securing AODV protocol uses public key cryptography. The asymmetric key cryptography algorithm is slow and requires more CPU processing powers and battery power which is not feasible in MANET as nodes have limited memory, battery power and CPU computation power. So we proposed a method that is based on keyed hash message authentication code. The method can be easily implemented and requires little CPU processing capacity and battery power.

The rest of the paper is organized as follows. Section 2 discusses network security attacks and related works in MANET. Section 3 summarizes the basic operations of AODV routing protocol and its security flaws. In section 4, we propose a security mechanism to protect routing messages in AODV protocol. Section 5 discusses different mechanism to set up shared secret keys. Section 6 discusses simulation results of proposed method. Finally, we conclude in section 7.

2 Security Attacks and Related Work

Many researchers have surveyed on security attacks and their solutions in the recent past years [4, 14, 18, and 29]. The security attacks in mobile ad hoc network fall into two categories: passive attacks and active attacks. In passive attack, malicious node does not affect the normal operation of data so it is very difficult to detect. It includes traffic analysis, monitoring and eavesdropping. Encryption algorithms are used to prevent passive attacks. In active attack, malicious node disrupts the normal functioning of system by performing either external attacks or internal attacks. External attacks are from malicious nodes that do not belong to network. External attacks can be prevented by using cryptography techniques such as encryption. Internal attacks are from either compromised or hijacked nodes which attempt to disrupt the normal routing function in order to consume the network resources. Internal attacks include modification, impersonation, jamming, sleep deprivation and denial of service attacks which are very difficult to prevent. We need to address these five major security services in order to prevent the security attacks: Availability, Confidentiality, Authentication, Integrity and Non-repudiation [2, 16]. However ad hoc network routing protocols do not need *confidentiality* as intermediate nodes process routing messages before forwarding in the network. The security mechanism based on cryptography is useful for preventing external attacks. It cannot prevent the internal attacks if it is from compromised or hijacked nodes as adversary can get secret

information such as private keys of other nodes. We need intrusion detection system to prevent such type of attacks. Moreover security mechanism based on asymmetric key cryptography is not efficient. The asymmetric key algorithm is very slow and consumes more CPU processing power and battery power which is not feasible as nodes in MANET is resource constrained.

Hu, Johnson and Perrig proposed secure efficient ad hoc distance vector (SEAD) [9] protocol that is based on the design of DSDV [20]. SEAD is designed to prevent attacks such as DoS and resource consumption attacks. SEAD uses one way hash function for authenticating the updates that are received from malicious nodes and non-malicious nodes. This protocol is very efficient and can be easily implemented. However the protocol is robust against multiple uncoordinated attacks but is not able to prevent the attackers from broadcasting the routing message having same metric and sequence number which were used by the recent update message. Ariadne [10], by the same authors, is based on basic operation of DSR [13]. Ariadne is a secure on-demand routing protocol and uses only high efficient symmetric cryptographic operations. Ariadne provides security against one compromised node and also prevents many types of denial-of-service attacks. Ariadne uses message authentication code (MAC) and secret key shared between two parties to ensures point-to-point authentication of a routing message. However, it relies on the TESLA [22] broadcast authentication protocol for secure authentication of a routing message which requires loose time synchronization. Security-aware routing (SAR) [15] is an on demand routing protocol based on AODV [21]. SAR defines level of trust as a metric for routing. Nodes distribute key with those nodes having equal level of trust or higher level of trust. Thus an encrypted packet can be decrypted only by the nodes of the same or higher levels of trust. The main drawback of SAR is that during the path discovery process, encryption and decryption is done at each hop which increases the power consumption. The protocol also requires different keys for different level of security which leads to increase in number of keys required when the number of security levels used increases. K. Sanzgiri et al [24] developed authenticated routing for ad hoc networks (ARAN), which is based on AODV. In ARAN, each node has a certificate signed by a trusted server whose public key is known to all legal nodes in the network. The ARAN ensures secure route establishment by end-to-end route authentication process. ARAN provides authentication, non repudiation and message integrity but needs a small amount of prior security coordination among nodes. The keys are generated a priory and distributed to all the nodes by the server. The ARAN prevents unauthorized participation, message modification attacks but prone to replay attacks if nodes do not have time synchronization. The ARAN uses asymmetric cryptography computation which causes higher cost for route discovery. Zapata and Asokan [28] proposed Secure AODV (SAODV), another protocol designed to secure AODV. The idea behind SAODV is to use a digital signature to authenticate the non-mutable fields of messages and hash chains to secure the hop count information. The SAODV described two methods to secure routing: Single Signature Extension and Double Signature Extension. When a node receives any message such as RREQ or RREP, it first verifies the signature before creating or updating a reverse route to that host. The SAODV is based on asymmetric key cryptographic operation therefore the nodes in MANET are unable to verify the digital signatures quickly enough as they have limited battery life as well as processing power. Moreover if a malicious node floods messages with invalid signatures then verification can be very expensive.

3 Ad-hoc On-Demand Distance Vector Routing (AODV) protocol

3.1 Overview

AODV is an on-demand routing protocol designed for operation of mobile ad hoc network. Protocol provides self starting, dynamic, loops free, multihop routing [19, 21]. Protocol allows

mobile nodes to establish routes quickly for new destinations as well as to respond to changes in network topology and link failures as only affected set of nodes are notified. Nodes do not maintain routes to the destinations that are not in active communication. New routes are created on demand. It means control packets are broadcast when needed and hence eliminate the need for periodic broadcast of routing updates. AODV protocol works in two phases a) route discovery process and b) route maintenance process.

Route discovery process uses Route Request (RREQs) and Route Reply (RREPs) messages. The routing messages contain information only about the source and the destination. When a route to destination is needed, the node broadcasts a route request (RREQ) packet to its neighbors to find the optimal path. RREQ message 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, loop prevention and faster convergence. When a node sends any type of routing control message like RREQ/RREP, it increases its own sequence number. Every node should include the latest sequence number for the nodes in the network in its routing table. It is updated whenever a node receives RREQ, RREP or RRER related to a specific node. Hop count represents the distance in hops from the source to destination. Each node receiving the RREQ message sets up reverse path back to the sender of the request so that RREP message can be unicast to that sender node from the destination or any intermediate node that satisfy the request conditions. Upon receiving the route request message, the intermediate node forwards the RREQ message until a node is found that is the destination itself or it has an active route to the destination with destination sequence number greater than or equal to that of RREQ. This node replies back to the source node with a route reply message RREP and discards the RREQ. If the intermediate node receives RREQ with 'G' flag set, it must also unicast gratuitous RREP to the destination node. RREP contains Destination IP Address, Destination Sequence Number, Originator IP Address and Lifetime. Forward links are setup when RREP 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 forward path set-up.

Route maintenance is performed with two additional messages: Hello and RRER messages. Each node broadcast Hello messages periodically to inform neighbors about its connectivity. The receiving of Hello message proves that there is an active route towards the originator. When a node does not receive HELLO message within time period from a neighbor node then it detects that a link to that neighbor node has broken then it generates route error message (RERR). RRER message indicates those destinations that are unreachable, their IP address and destination sequence number. In order to inform the link failure information, each node maintains a precursor list for each routing table entry containing the IP address of set of neighboring nodes that are likely to use it as a next hop towards each destination. On receiving this RRER, each predecessor node, in turn, forwards the RERR to its own set of predecessors, thus effectively erasing all routes using the broken link. In addition to these routing messages, the route reply acknowledgment (RREP-ACK) message must be sent by sender node of RREQ in response to a RREP message with the 'A' bit set. This provides assurance to the sender of RREP that the link is bidirectional.

3.2 Security Issues of AODV

AODV routing protocol does not provide any security mechanisms to guard against attack. The major vulnerabilities present in AODV protocol are:

- Attacker can impersonate a source node S by forging a RREQ with its IP address as IP address of source node S.
- Attacker can impersonate a destination node D by forging a RREP with its IP address as IP address of the destination node D.

- Decreasing hop count in RREQ/RREP.
- Increasing sequence number in RREQ/RREP.
- Forging the RRER message.

AODV routing protocol requires at least two security services: Data origin authentication at each receiving node and routing message integrity. Message integrity is of the most concern in AODV routing. A malicious node or compromised node may change sequence number or hop count fields in RREQ /RREP messages or impersonate the sender of routing packets. Modification of routing information may lead to inconsistency in network. Routing table may contain false information about network topology. Change in sequence number may result in routing loops etc.

4 Proposals of Authentication Mechanisms

4.1 Assumption and Notation

The proposed method is based on shared secret key technology. We assume a mechanism to set up pair wise secret keys. A total number of $n.\ (n - 1)/2$ pair wise secret keys will be maintained in the network; if n is the number of nodes in the network. Both source and destination nodes are not compromised. AODV assumes bidirectional link it means if a node A is able to receive packet transmitted directly by some node B, then B is also able to receive packet transmitted directly by A. The following notation is used to describe cryptography operations:

- S and D are source node and destination node respectively.
- K_{SD} ($or\ K_{DS}$) denotes the secret key shared between nodes S and D.
- Each node holds the HMAC (hashed message authentication code) algorithm [1].
- MACm defined by $HMAC\ (K_{SD},\ M)$ denotes the computation of the message authentication code of message M using secret key K_{SD} between nodes S and D.

4.2 Proposed Method

The proposed method is based on AODV routing protocol and uses shared secret key technology. In AODV protocol, routing messages RREQ or RREP have two types of information: Mutable and Non Mutable. The hop count is only mutable field as intermediate nodes increment the hop count field while forwarding the RREQ. The rest fields such as sequence number or IP address are non mutable fields as they remain unchanged. The proposed method uses two mechanisms to secure the AODV messages: $HMAC\ (K_{SD},\ M)$ is used to authenticate the non-mutable fields of the routing message M and one way HMAC key chain is used to secure the hop count information i.e. only mutable information. We assume that HMAC function takes a variable number of arguments by simply concatenating 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 1. The propagation of the RREQ and RREP messages is described in Figure 2, where * denotes a local broadcast and $HMAC_{KX}$ (.) denotes HMAC code generated using shared secret key K_X . The message P is extended RREQ containing the following fields : < RREQ, MAC_m , HMAC chain, intermediate node list >, where RREQ is original route request message. Here RREQ is extended (denoted as message P) to hold three more fields MACm, HMAC chain and intermediate node list. The sender node first compute $MAC_m = HMAC_{KSD}\ (RREQ)$ using secret key K_{SD} 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

message and computes message authentication code MACm by simply concatenating them. The sender node computes $h0 = HMAC_{KSD}$ (S, N) and initializes the intermediate node list to empty list. Here S is source IP address and N is time varying component known as nonce. Nonce is used to prevent replay attack. We can use route request broadcast id or source sequence number as nonce since each time a source node broadcasts a new route request message, it monotonically increases its RREQ broadcast id

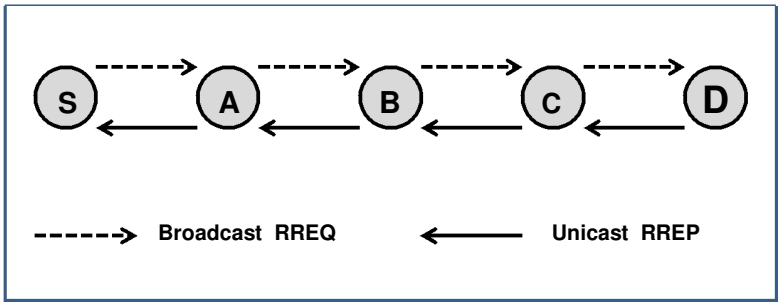

Fig. 1. The routing message exchange in AODV

or source sequence number. When any intermediate node for example node A receives a packet P it modifies packet P by appending IP address of previous node S (from which it receives the packet P) to the intermediate node list and replacing the HMAC chain field $h0$ with $h1 = HMAC_{KAD}$ $(A, h0)$ where K_{AD} is secret key between intermediate node A and destination node D. In the proposed method, the intermediate node only forwards the route request packet P by broadcasting it and does not send the route reply packet to the source node S. For the destination node D, if a packet is received, it checks the following three conditions:

- **Condition 1:** Check $MAC_m == HMAC_{KSD}$ $(RREQ)$.

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

- **Condition 2:** Check $h_3 == HMAC_{KCD}$ $(C, HMAC_{KBD}$ $(B, HMAC_{KAD}$ $(A, HMAC_{KSD}$ $(S, N))))$.

Destination node obtains intermediate node list (S, A, B, C) containing the IP address of intermediate nodes. It computes HMAC chain using intermediate node list and verify h3. If h3 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.

- **Condition 3:** Check the hop count field i.e. Number of intermediate nodes in node list (including source node) = = Hop count value in RREQ message.

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

source node can authenticate the destination node as well as can check integrity of RREP message. The whole procedure is same for securing RREP message.

4.3 Security Analysis

In MANET, the internal attacks are typically more severe, since malicious node already belongs to the network. To prevent internal attacks, we need to authenticate the unique identity of each node. Our proposed scheme provides an efficient way to verify the message authentication and message integrity. The receiver node can authenticate the sender of message as well as intermediate nodes using the shared secret key. Since a one-way hash function prevents a member node from removing IP address of intermediate node from intermediate node list, the receiver node can verify the hop count field in RREQ or RREP message using the intermediate node list. In proposed method, only HMAC is used to protect the integrity of message so computation is very efficient, and even affordable for low-end devices such as small sensor nodes. However, an HMAC can be verified only by the intended receiver, therefore we cannot apply this technique to verify and authenticate broadcast message such as RRER message. In the proposed method, only the destination node is permitted to initiate route reply message therefore the delay involved in the route discovery process increases as the size of the network increases. Moreover with increased in network size, a node needs more memory space to store secret keys. Besides, the proposed method uses pair wise secret key, so establishing the secret key between any two nodes is an expensive operation.

The RREQ process is illustrated below:

S : $\mathbf{MAC_m = HMAC_{K_{SD}}(RREQ)}$, $\mathbf{h_0 = HMAC_{K_{SD}}(S, N)}$
$\mathbf{P =< RREQ, MAC_m, h_0, () >}$
S ->*: P
A: $\mathbf{h_1 = HMAC_{K_{AD}}(A, h_0)}$, $\mathbf{P =< RREQ, MAC_m, h_1, (S) >}$
A ->*: P
B: $\mathbf{h_2 = HMAC_{K_{BD}}(B, h_1)}$, $\mathbf{P =< RREQ, MAC_m, h_2, (S, A) >}$
B ->*: P
C: $\mathbf{h_3 = HMAC_{K_{CD}}(C, h_2)}$, $\mathbf{P =< RREQ, MAC_m, h_3, (S, A, B) >}$
C ->*: P
D: receives $\mathbf{P =< RREQ, MAC_m, h_3, (S, A, B, C) >}$
D: verifies RREQ message integrity and hop count

The RREP process is illustrated below:

D: $\mathbf{MAC_m = HMAC_{K_{SD}}(RREP)}$, $\mathbf{h = HMAC_{K_{DC}}(MAC_m)}$
$\mathbf{h_0 = HMAC_{K_{SD}}(D, N)}$, $\mathbf{P =< RREP, MAC_m, h, h_0, () >}$
D ->*: P
C: verifies: $\mathbf{h == HMAC_{K_{CD}}(MAC_m)}$, $\mathbf{h = HMAC_{K_{CB}}(MAC_m)}$
C: $\mathbf{h_1 = HMAC_{K_{CS}}(C, h_0)}$, $\mathbf{P =< RREP, MAC_m, h, h_1, (D) >}$
C ->B: P
B: verifies: $\mathbf{h == HMAC_{K_{BC}}(MAC_m)}$, $\mathbf{h = HMAC_{K_{BA}}(MAC_m)}$
B: $\mathbf{h_2 = HMAC_{K_{BS}}(B, h1)}$, $\mathbf{P =< RREP, MAC_m, h, h_2, (D, C) >}$
B ->A: P
A: verifies: $\mathbf{h == HMAC_{K_{AB}}(MAC_m)}$, $\mathbf{h = HMAC_{K_{AS}}(MAC_m)}$
A: $\mathbf{h_3 = HMAC_{K_{AS}}(A, h_2)}$, $\mathbf{P =< RREP, MAC_m, h, h_3, (D, C, B) >}$
A -> S: P
S: receives $\mathbf{P =< RREP, MAC_m, h, h_3, (D, C, B, A) >}$
S: verifies previous hop, RREP message integrity and hop count

Fig. 2. The sequence of secure routing message exchange in proposed method

5 Key Setup

Key Management is essential for providing confidentiality, message integrity and authentication but key management in MANET is challenging issue as MANET has no centralized infrastructure or administrator. Key management includes key generation, key distribution and key maintenance. Key management protocol can be divided into two categories: Private Key Management and Public Key Management [5]. Private key management protocol establishes private key or secret key that is used in symmetric-key cryptography. The public key management protocol provides a pair of keys (private/public) used for asymmetric key cryptography. Symmetric-key cryptography is more efficient than asymmetric key cryptography however it needs a shared secret key between two communicating nodes. We need to set up n. (n-1)/2 shared secret keys if n is the size of network. Every node must have a mechanism to securely store the shared secret for each other nodes in the network. Since nodes in the ad hoc network are resource constrained, key setup is an expensive operation. A variety of mechanisms can be used to set up shared secret key between two nodes [2, 6]. For example, shared secret keys can be pre-loaded between all the interested parties before the start of communication possibly through physical contact. A trusted third party also known as key-distribution center (KDC) can be used. Key distribution center first shares a secret key with each node and then sets up secret key between two parties. If public key infrastructure (PKI) is present, the key can be encrypted with each participant's public key and transported to them. The two communicating party can create a secret key between themselves using symmetric key agreement schemes. The most common popular key agreement schemes use Diffie-Hellman exchange, an asymmetric key algorithm based on discrete logarithms [25].

6 Simulation Results and Analysis

We used standard simulator tool NS2 for simulation [8, 12]. Network simulator (NS2) is an event driven simulator tool and designed specifically to study the dynamic nature of wireless communication networks. To evaluate the performance of proposed method, we compared it with original AODV and secure AODV (SAODV) protocol in the presence of black hole attack [7]. A black hole attack is a kind of denial of service attack in which a malicious node assigns small hop count and high sequence number to the route reply message (RREP) and absorbs all packets by simply dropping it without forwarding them to the destination node. SAODV is implemented as an extension to original AODV protocol in NS2. Although SAODV has proposed two alternatives to send RREP message but we used first alternative for implementation in which only destination node can send RREP message [27]. We used SHA hash algorithm to secure hop count and RSA algorithm for digital signature [3, 23]. Network traffic and scenario are configured according to Table 1.

6.1 Performance Metrics

In simulation, we considered two scenarios to analyze the simulation results. In first scenario, pause time is varied from 0 seconds to 600 seconds in order to analyze the effect of mobility. Before moving to random destination each node remains stationary for the time equal to pause time seconds. When pause time is 0 seconds then mobility is high. Each node moves continuously. A pause time equal to length of simulation (in this simulation we took 600 seconds) corresponds to no motion. In second scenario, number of malicious nodes is varied for pause time of 0 seconds. We consider the following performance metrics to evaluate the performance of proposed method.

Table 1. Simulation Parameters

Simulator	NS2 (v-2.34)
Simulation Time	600 sec
Number of nodes	50
Area Size	1000m * 1000m
Transmission Range	250m
Maximum Speed	0-20 m/s
Maximum Number of Connection	20
Application Traffic	CBR
Packet Size	512 bytes
Traffic Rate	4 packets/sec
Node Mobility Model	Random Way-point Model

Packet Delivery Ratio Packet Delivery Ratio = Total Packets Received / Total Packets Sent. The ratio of the number of data packets successfully delivered to the destinations to those generated by CBR sources. Figure 3 shows the impact of mobility of nodes on packet delivery ratio when there are no malicious nodes in the network. It is clear that packet delivery ratio increases with increase in pause time as the packet loss rate at such a highly change in network topology is much high. AODV performs better in the absence of malicious nodes in network. Packet delivery ratio decreases with increase in malicious nodes as shown in Figure 4. 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 the destination node. In SAODV protocol, source node and intermediate node both verify signature before updating their routing table. A malicious node can impersonate a destination node but cannot generate signature of destination node. Similarly in proposed method, malicious node does not know the secret key shared between destination node and others node. The source node or intermediate node discards RREP packets coming from malicious node and hence does not establish route through malicious node. Therefore in proposed method and SAODV protocol, packet delivery ratio remains almost constant when numbers of malicious nodes is increased.

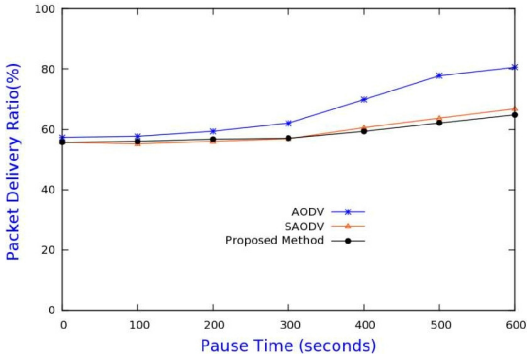

Fig. 3. Pause Time vs Packet Delivery Ratio

Figure 4 illustrates the impact of malicious nodes on packet delivery ratio.

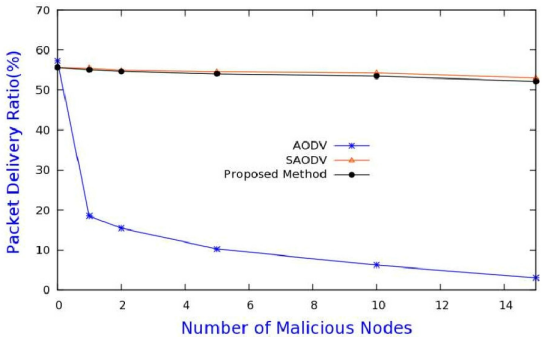

Fig. 4. Number of Malicious Nodes vs Packet Delivery Ratio

Time Delay Time delay of data packet is the difference between the time when the first data packet is received by the destination node and the time when the source node broadcasts a RREQ message. Figure 5 shows the impact of mobility on time delay. Time delay depends on both mobility and position of nodes. 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 SAODV protocol and the proposed method, the time delay is more due to delay in establishing particular route as only destination node can send route reply message. Moreover the SAODV protocol has larger time delay in compared to both because SAODV uses asymmetric key cryptography so it requires significant processing time to compute or verify signatures and hashes at each node. Figure 6 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.

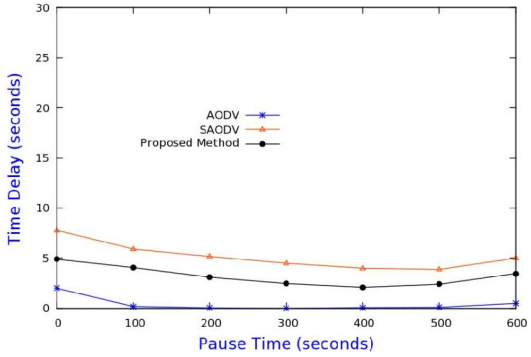

Fig. 5. Pause Time vs Time Delay

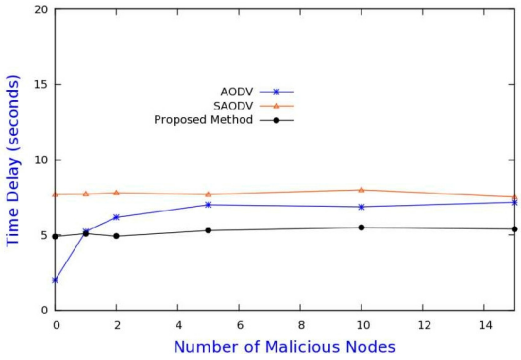

Fig. 6. Number of Malicious Nodes vs Time Delay

In SAODV and proposed method, source node does not establish route through malicious node therefore time delay remains almost same irrespective of number of malicious nodes.

Normalized Control Packet Overhead Normalized Control Packet Overhead = (Routing Packets Sent * Size of Routing Packet) / (Received Data Packets * Size of Data Packet).

Figure 7 shows the impact of the mobility of nodes on control packet overhead. The overhead increases with increase in mobility as higher speed of node leads to more link failures which results in more route discoveries thus increases the routing packet overhead. In proposed method, routing or control packets use extra bytes to store hashes and intermediate node addresses. Similarly in SAODV protocol, control packets contain extra bytes to store digital signatures and hashes for providing security therefore overhead is more in compared to AODV protocol. Figure 8 shows the impact of malicious nodes on normalized 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 normalized control packet overhead increases with increase in malicious nodes. In SAODV and proposed method, number of routing packets decreases with increase in malicious nodes but number of received data packets vary slightly therefore overall normalized control packet overhead decreases.

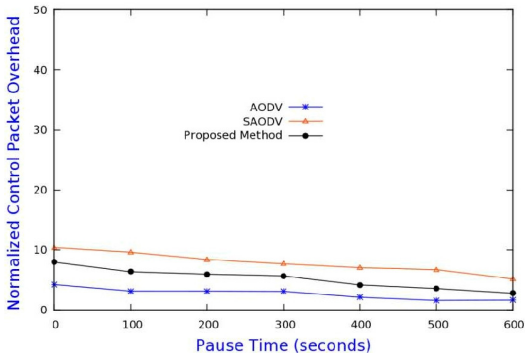

Fig. 7. Pause Time vs Normalized Control Packet Overhead

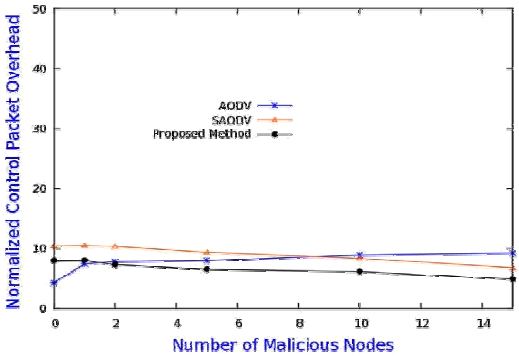

Fig. 8. Number of Malicious Nodes vs Normalized Control Packet Overhead

7 Conclusion

Routing security is an important issue in MANET. We need to consider a better tradeoff between higher security and network performance while designing of secure routing protocol. We propose a method to secure AODV protocol. The proposed method uses hashed message authentication algorithm. It does not involve any asymmetric key cryptographic operation and thus provides fast message verification, message authentication and intermediate nodes authentication. We compare proposed method with SAODV protocol. The simulation result shows that proposed method minimizes the time delay and network control packet overhead involved in computation and verification of security fields during route discovery process. The proposed method uses pair wise shared secret key for providing network services such as message authentication and message integrity. In MANET, establishing the secret key between any two nodes is an expensive operation. Moreover the proposed method cannot verify and authenticate RRER message.

References

[1] Fips pub 198, the keyed-hash message authentication code.

[2] W. stallings, cryptography and network security: Principles and practices, 3rd edition, prentice hall, 2003.

[3] Nist: Secure hash standard, fips 180-1, national institute of standards and technology, u.s. department of commerce (May 1994).

[4] et al., B.W.: A survey of attacks and countermeasures in mobile ad hoc networks. Wireless Network Security Springer, 17 (2006).

[5] Aziz, B., Nourdine, E., Mohamed, E.K.: A recent survey on key management schemes in manet. 3rd International Conference on ICTTA pp. 1-6 (April 2008).

[6] D.Djenouri, L.Khelladi, N.Badache: A survey of security issues in mobile ad hoc and sensor networks. IEEE Communications Surveys and Tutorials Journal 7(4), 2-29 (December 2005).

[7] Deng, H., Li, W., Agrawal, D.P.: Routing security in wireless ad hoc networks. IEEE Communications Magazine 40(10), 70-75 (October 2002).

[8] Fall, K., Varadhan, K.: Ns-2, the ns manual (formally known as ns documentation) available at http: //www. isi.edu/nsnam/ns/doc.

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

[10] Hu, Y.C., Johnson, D.B., Perrig, A.: Ariadne: A secure on-demand routing protocol for ad hoc networks. Proc. 8th Ann. Intl Conf. Mobile Computing and Networking (MobiCom 2002), ACM Press pp. 12-23 (September 2002).

[11] Hu, Y.C., Perrig, A.: A survey of secure wireless ad hoc routing. IEEE Security and Privacy 2(3), 28-39 (May-June 2004).

[12] Issariyakul, T., Hossain, E.: Introduction to network simulator ns2 (July 2008).

[13] Johnson, D.B., Maltz, D.A.: The dynamic source routing protocol in ad hoc wireless networks. In: Mobile Computing, Kluwer Academic Publishers. vol. 353, pp. 153-181 (1996).

[14] Kannhavong, B., Nakayama, H., Nemoto, Y., Kato, N.: a survey of routing attacks in mobile ad hoc networks. IEEE Wireless Communications pp. 85-91 (October 2007).

[15] Kravets, R., Yi, S., Naldurg, P.: A security-aware routing protocol for wireless ad hoc networks. In: Proceedings of ACM MOBIHOC 2001. pp. 299-302 (October 2001).

[16] Menezes, A.J., Oorschot, P.V., Vanstone, S.: Handbook of applied cryptography, crc press, 1996.

[17] Murthy, C.S.R., Manoj, B.: Ad hoc wireless networks: Architectures and protocols, prentice hall (2004).

[18] Papadimitratos, P., Haas, Z.J.: Secure routing for mobile ad hoc networks. In: Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002). pp. 1-13 (January 2002).

[19] Perkins, C., Belding-Royer, E., Das, S.: Ad-hoc on-demand distance vector (aodv) routing, rfc-3561, network working group (July 2003).

[20] Perkins, C.E., Bhagwat, P.: Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers. In: Proceeding of ACM SIG-COMM. vol. 24, pp. 234-244 (August 1994).

[21] Perkins, C.E., Royer, E.M.: Ad hoc on-demand distance vector (aodv) routing. In: Proceeding of IEEE Workshop on Mobile Computing system and applications. pp. 90-100 (February 1999).

[22] Perrig, A., Canetti, R., Song, D., Tygar, D.: Efficient and secure source authentication for multicast. In Network and Distributed System Security Symposium (NDSS01) (February 2001).

[23] Rivest, R., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. In: Communications of the ACM. vol. 21 (February 2002).

[24] Sanzgiri, K., Dahill, B., Levine, B.N., Shields, C., Royer, E.M.B.: A secure routing protocol for ad hoc networks. In: Proceedings of IEEE ICNP. pp. 78-87 (November 2002).

[25] Steiner, M., Tsudik, G., Waidner, M.: Diffie hellman key distribution extended to group communication. ACM Conf. Comp. and Commun. Security pp. 31-37 (1996).

[26] Yang, H., Luo, H., Ye, F., Lu, S., Zhang, L.: security in mobile ad hoc networks: challenges and solutions. Wireless Communications, IEEE 11, 38-47 (February 2004).

[27] Zapata, M.G.: Secure ad hoc on-demand distance vector (saodv) routing, internet-draft draft-guerrero-manet-saodv-00.txt (October 2002).

[28] Zapata, M.G., Asokan, N.: Securing ad hoc routing protocols. Proc. ACM Workshop on Wireless Security (WiSe), ACM Press pp. 1-10 (2002).

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