Journal of Computer Science, 9 (4): 439-448, 2013
ISSN 1549-3636

doi:10.3844/jcssp.2013.439.448 Published Online 9 (4) 2013 (http://www.thescipub.com/jcs.toc)

SECURED ROUTING WITH AUTHENTICATION IN MOBILE AD HOC NETWORKS

[1]Guru Baskar, T. and [2]D. Manimegalai

[1]Department of Applied Sciences, Sethu Institute of Technology, Tamilnadu, India
[2]Department of Information Technology, National Engineering College, Tamilnadu, India

Received 2012-06-26, Revised 2012-09-07; Accepted 2013-05-09

ABSTRACT

A Mobile Ad hoc Network (MANET) is a collection of wireless mobile nodes that dynamically forms a temporary network without any fixed infrastructure. Each node participates in the ad hoc routing protocol that helps it to discover multi-hop paths through the network to any node. Security challenges have become a primary concern for these networks due to their characteristics such as open medium, dynamic topology, distributed collaboration and other various constraints like battery power and low bandwidth. An Authentication mechanism is certainly needed to prevent the various possible attacks by any malicious node. In this study, we propose an efficient authentication protocol, named CAODV for a MANET with the aid of cryptographic certificates. We implemented this CAODV protocol using the network simulator NS-2 and the simulation results reveal that this mechanism is highly effective even in the presence of large number of malicious nodes. Despite a considerable increase in the routing overhead, it is minimal and outweighed by the increased security services provided by our proposed CAODV protocol for MANET.

Keywords: Mobile Ad hoc Network (MANET), Authenticated Routing for Ad hoc Networks (ARAN), Top Hash (TH), Packet Delivery Fraction (PDF)

1. INTRODUCTION

A Mobile Ad hoc Network (MANET) is a collection of wireless mobile nodes that dynamically forms a temporary network without any fixed infrastructure. Each mobile node acts not only as a host but also as a router (Russell *et al*., 2011) to determine the optimal path to forward the information for the other nodes that may not be within the direct transmission range of each other in the network. Each node participates in the ad hoc routing protocol that helps it to discover multi-hop paths through the network to any other node. The major requirements of a routing protocol in MANET (Perkins and Bhagwat, 1994) include minimum route acquisition delay, loop-free routing, minimum control overhead and scalability in establishing the route between the communicating nodes before the transmission of data packets. MANET is one of the recent vibrant fields and many researches are going on in the study of routing protocols because of their self-configuration and self-maintenance capabilities. The applications of MANET range from the defense sector to commercial area and will be more helpful during disaster recovery.

But, MANET is particularly vulnerable due to its fundamental characteristics such as insecure operational environment, dynamic topology, distributed cooperation, limited resource availability and physical vulnerability (Murthy and Manoj, 2004). Since MANET has the capability to form a temporary network quickly, security challenges have become a primary concern. There are several active/passive attacks possible in MANET like spoofing, denial of service, masquerading, eavesdropping, resource consumption and host impersonation. External attackers can inject erroneous routing information, replay old routing information, or distort routing information, thus partition a network or introduce excessive traffic load into the network by causing retransmission and inefficient routing. Another

Corresponding Author: Guru Baskar, T., Department of Applied Sciences, Sethu Institute of Technology, Tamilnadu, India

severe attack can be launched from the compromised nodes, which might advertise incorrect routing information to the other nodes in the network.

There are quite a number of ad hoc routing protocols (Johnson *et al*., 2007) available, but none of them are secure enough to prevent all types of attacks. These protocols are insecure because the attackers can gain the network topology information easier as the routing messages are transmitted in clear text. Thus the attacker can be aware of the network structure by analyzing the received routing messages and may tamper the information in it to disrupt the network. Hence, a complete security solution is needed to thwart such attacks in the network. The routing protocol should also be secure enough while establishing the route for the source node. Such secure routing protocols should encapsulate an essential set of security mechanisms such as confidentiality, integrity, authentication, availability and non-repudiation to prevent, detect and respond to the attacks from malicious nodes and guarantee the correct route discovery.

1.1. Security Issues

There exists several proactive and reactive ad hoc routing protocols but reactive protocols like AODV are preferred over the proactive routing protocols like DSDV due to the resource limitations of mobile nodes in an ad hoc environment. The existing routing protocols for MANET cope well with the dynamic topology but are not designed to provide security mechanisms against the malicious attackers and hence they are highly vulnerable to routing attacks. Since AODV is one of the standard reactive protocols for MANET and its vulnerabilities are similar with the other familiar routing protocols, we are considering its vulnerabilities that lead to the possible attacks.

The Ad hoc On-demand Distance Vector (AODV) protocol is an on-demand routing protocol that allows mobile nodes to find routes quickly for new destinations and does not require nodes to maintain routes to destinations that are not in active communication (Perkins *et al*., 2002). The advantage of this protocol is low connection setup delay and the disadvantage is more number of control overheads due to many route reply messages for single route request. AODV performs better in case of packet delivery ratio when it is compared with the other standard routing protocols (Manickam *et al*., 2011). In this protocol, the attacker may launch several attacks by advertising a false route with some modifications in the routing message and invalidate all the routing updates from other nodes. Such attacks can be classified into major categories such as message modification, message fabrication and node impersonation.

1.2. Message Modification

In AODV protocol, the fresh enough route will be selected based on the destination sequence number and the optimal route is selected on the basis of the smaller hop count metric during the route discovery. Since these fields in the routing message are not protected, the malicious node may announce better routes than the existing valid route by modifying the destination sequence number and the hop count fields. In general, the malicious node would set the value zero in the hop count field to ensure the smallest hop count so that the route through this malicious node will always be chosen.

1.3. Message Fabrication

The AODV protocol allows the mobile nodes to react to the link breakages by sending the route error messages to intimate the neighbor nodes so that they are able to invalidate the routes using the lost link. The malicious node may cause a denial of service attack by spoofing the identity of any node and send error messages to the other nodes. This attack can isolate any node in the network. The malicious node may also launch the routing table overflow attack by sending routing messages to the non-existent nodes in the network.

1.4. Node Impersonation

The node impersonation attack is also called as Spoofing in which a malicious node uses the address of an another node as there is no authentication of messages in the existing protocols and can launch many attacks in the network by masquerading as another node. This attack allows the malicious node to alter the network topology as per its desire.

In this study, it is proposed to implement the authentication protocol, CAODV using the digital certificates which provides secured routing with authentication and non-repudiation security services.

1.5. Related Works

Due to the significance attached to the applications of MANET, security in MANET is an active research area and considerable research is already done in this field. Zhou and Haas (1999) proposed several secured routing protocols with the help of cryptographic mechanisms and reliable certification authority in an ad hoc network. A good overview on the secure routing

protocols such as SAODV, ARAN and SEAD with their limitations was presented by Abusalah *et al*. (2008).

Hu *et al*. (2002a) proposed a ARIADNE, an on-demand secure ad hoc routing protocol based on DSR that provides security by using symmetric cryptography. The routing message is authenticated with the Message Authentication Code (MAC) by having the shared key between the two nodes. This protocol makes use of a broadcast authentication protocol called TESLA which requires low synchronization time and high key setup overhead of using pair-wise shared secret keys. This protocol has a higher complexity in assuming clock synchronization between the nodes in the network.

Hu *et al*. (2002b) presented a protocol, SEAD which extends the proactive protocol DSDV by providing security that prevents the modification of routing message with the help of one-way hash chains. The one-way nature of hash chains prevents any node from advertising a route with the higher sequence number than the original sequence number of the source node. This protocol protects only against the modification of the routing messages and does not allow any node to authenticate the source.

Zapata (2006) proposed a SAODV protocol, an extension of the AODV routing protocol which uses digital signature to authenticate the non-mutable fields of the control packets and uses hash chains to secure the only mutable information, the hop count during the route discovery process with security features like integrity and authentication. It also provides an end-to-end authentication and node-to-node verification of the routing messages. SAODV uses hash chain mechanism to authenticate the hop count in the routing message which allows every intermediate and destination node to verify the number of hops so that they know that the hop count has not been decremented by any attacking node. The main vulnerability of the SAODV protocol is that it does not prevent a malicious node from spoofing the identity of another node. Moreover, it does not provide node-to-node authentication for the routing messages in which the intermediate nodes just forward the routing message after verifying the originating node's signature.

Kush and Hwang (2009) proposed hash key chain mechanism that uses symmetric cryptography and hash functions to secure the on-demand routing protocols with the inclusion of security parameter in the routing message. As hash key chain is configured as a recursive chain, these keys are noted in the routing tables which ultimately increase the memory requirements. Burmester and Medeiros (2009) presented the various flaws of ARIADNE and endairA which is a variant of ARIADNE and several secure route discovery challenges were presented. Saxena *et al*. (2009) proposed a secure and fully non-interactive admission protocol which is constructed by using secret sharing techniques based on bivariate polynomials for temporary MANETs.

Sanzgiri *et al*. (2005) proposed the Authenticated Routing for Ad hoc Networks (ARAN) protocol, which is an on-demand routing protocol that detects and protects against malicious actions by employing cryptographic certificates. The entire routing message is protected with the help of the digital signatures of originating and intermediate nodes and provides both end-to-end authentication and node-to-node authentication of the routing messages. The limitation of the ARAN protocol is the exclusion of the hop count field in the routing message and hence, the better route with the shortest hop count cannot be selected.

2. MATERIALS AND METHODS

The proposed protocol CAODV (AODV with Certificates) extends AODV with authentication by using digital certificates to prevent many attacks from the malicious nodes. The preliminary phase of CAODV begins with certificate distribution followed by route establishment phase. It guarantees both node-to-node and end-to-end authentication during route establishment phase. The third phase is route maintenance phase which is also secured with authentication. Since every node possesses its own certificate, its identity is verified by its neighbors whenever that node is involved in any process at any time. Only authorized nodes are allowed to participate in the route discovery and route maintenance phases. The notations used in this study are summarized in the **Table 1**.

2.1. Certificate Distribution

In CAODV protocol, a certificate is absolutely necessary for a node to participate in MANET. A node needs to acquire its certificate from the Certificate Server (CS) before joining into the network. Hence, CAODV requires a trusted server to distribute the certificate to the requesting node after getting the credentials of a node such as the IP address (IP_a) and its generated public key (KA_{pub}).

Table 1. List of notations used

Notation	Description
IP_a	IP address of the node A
$SEQNO_a$	Sequence number of the node A
Ts	timestamp when the message was created
E	Expiration time of the certificate
KA_{pub}	Public key of the node A
KA_{pri}	Private key of the node A
S_{cs}	Signature of the Certificate Server
S_a	Signature of the node A
$Cert_a$	Certificate of the node A
REQ_{id}	Route Request id
h(x)	Hash value for the value x

Before getting the certificate from the CS, every node must generate its own key pair (private key, public key) itself. Then, the node passes its credentials to CS to obtain the certificate. The server will sign the node's credentials with its private key and put its signature (S_{cs}) within the certificate before sending it to the requesting node. Every node must know the public key of CS to verify the certificate of any node since the certificate is signed by the private key of CS. One of the major challenges of this protocol is the distribution of the certificates of the participating nodes in the network. In this protocol, the nodes distribute their certificates to their respective neighbors through the Hello messages at fixed intervals of time. After receiving the Hello messages, the nodes update the details of their neighbors with their certificates which are utilized during the route computation process.

2.2. Route Establishment

Before transmitting any data packet, the source node must find the route to reach the destination through the routing protocol. The intermediate nodes also involve in establishing the route between the source and destination. The Source node (S) broadcasts the Route Request (RREQ) message to its neighbors to begin the route discovery process to find the route to the Destination node (D). The fields within the RREQ message are specified in the **Table 2**.

Every route request is uniquely identified with its REQ_{id} which is generated by the corresponding source node. The RREQ also contains the IP addresses and Sequence numbers of both the source and destination nodes for which the route is required. The Sequence number is maintained by each node and it is used to determine the freshness of the information originated from a node. HC is the hop count field, which is incremented whenever the RREQ message traverses along the intermediate nodes. Hash chain mechanism is employed in the CAODV protocol to protect this hop count field with the computation of Top Hash (TH) and the Hash value (h (HC)) for the hop count using the hash function.

Table 2. Fields in RREQ message

Field	Description
REQ_{id}	Route Request id
IP_s	IP address of the source node
$SEQNO_s$	Sequence no. of the source node
IP_d	IP address of the destination node
$SEQNO_d$	Sequence no. of the destination node
HC	Hop count
TH	Top hash
h(HC)	Hash value of the hop count
ts	Time stamp
$Cert_s$	Certificate of the source node
S_s	Signature of the source node
S_h	Hop signature

It also contains the timestamp (t_s) to represent the time at which the RREQ message is generated. The source node includes its certificate ($Cert_s$) in the RREQ message to prove its identity. Finally, the entire RREQ message is signed by the private key (KS_{pri}) of the node S and the RREQ message is broadcasted with the signature of the source node (S_s). S_h is the hop signature signed by every intermediate node which provides node-to-node authentication and it will be the same as that of S_s after generating the RREQ message in the source node.

After receiving the RREQ message, the intermediate node verifies RREQ message as shown in the Algorithm 1.

Algorithm 1: RREQ Verification by a node:

Step 1: If RREQ is already received, then drop the RREQ
Step 2: If IP_s in RREQ <> IP_s in $Cert_s$ then drop the RREQ and exit
Step 3: If $Cert_s$ is invalid, then drop the RREQ and exit
Step 4: If h(HC) is invalid, then drop the RREQ and exit
Step 5: If S_s in RREQ is invalid, then drop the RREQ and exit
Step 6: If S_h in RREQ is invalid, then drop the RREQ and exit
Step 7: Set up the reverse route to the source node S
Step 8: If the intermediate node is the destination, then send RREP to the source and exit
Step 9: Increase the hop count (HC) in RREQ
Step 10: Calculate the hash value (h (HC)) and update it in RREQ
Step 11: Replace the S_h in RREQ by its own signature
Step 12: Forward the RREQ
Step 13: Exit

At first, the intermediate node verifies whether the received RREQ message is already processed and matches the IP addresses of the source node in RREQ and $Cert_s$. Then, it validates the identity of the node S by verifying the certificate ($Cert_s$) in RREQ. After its validation, the

hash of the hop count is verified with the top hash value to check whether the hop count is falsely advertised or not. Then, the signature S_s of the source node in the RREQ is verified with the public key of the source node S which can be extracted from the certificate $Cert_s$. The final verification is done on Hop signature (S_h) using the public key of the respective neighbor which is known through the Hello messages.

After all these verifications are performed, the intermediate node sets up the reverse route back to the node S by adding an entry in the routing table with the neighbor (the node that transmits RREQ) as the next hop. This route will be helpful for the intermediate node to forward the Route Reply message to the node S from the destination D. If the receiving node is the destination itself, then it generates the Route Reply message (RREP) and unicasts it towards the source node S. The processing of RREP message is exactly similar to that of processing of RREQ message. In CAODV protocol, the destination alone can send the RREP to the source in order to prevent the attacks of a malicious node sending the invalid route reply.

The CAODV protocol ensures secured routing within the network fulfilling several security requirements such as authentication and integrity. A mobile node should have the ability to detect forged routing messages and should recognize if the message is originated or forwarded from a malicious node. To accomplish these security mechanisms, this protocol uses mechanisms of both asymmetric cryptography and hash algorithms. Digital signatures ensure the authenticity and the integrity of the routing messages while the hash chain mechanism protects the Hop Count of those messages.

2.3. Route Maintenance

All the participating nodes monitor the operation of the active routes and inform the respective source nodes by sending the Route Error messages (RERR) whenever their routes are lost due to link failure. If the node A within an active route detects the link failure for the destination node (IP_d), then it broadcasts the RERR message to the affected neighbor nodes which are using this route and its content is as shown in **Table 3**.

The Destcount field in the RERR message indicates the number of the destination nodes for which the routes are lost. IP_d and $SEQNO_d$ represent the IP address and Sequence number of the affected destinations. The certificate of the node A ($Cert_a$) is stored in RERR message so that any malicious node cannot masquerade as another node and its signature (S_a) is also placed in it after the entire message is signed by its private key.

Table 3. Fields in RERR message

Field	Description
DestCount	No. of the destination nodes
IP_d	IP address of the destination node
$SEQNO_d$	Sequence no. of the destination node
$Cert_a$	Certificate of the node A
S_a	Signature of the node A

All the intermediate nodes which contain the routes for the enlisted destinations in the RERR message deactivate them after verifying the certificate and the signature within the RERR message. Then the intermediate nodes forward the RERR message without any modification and it reaches the source node. The source node initiates a new route discovery process for the same destination upon receiving such RERR messages. Though it is difficult to detect whether the route is actually broken or lost, the Signature (S_a) in the RERR message prevents both the impersonation attack and the modification of error messages.

3. RESULTS AND DISCUSSION

3.1. Experimental Results

We have simulated our CAODV protocol in the widely used NS-2 simulator (version 2.34) (Fall and Varadha, 2010) by including the cryptographic mechanisms from the openssl library of version 0.9.8r. The performance of CAODV is evaluated and compared with the verified version of AODV in NS-2.

3.2. Simulation Model and Parameters

The simulation scenario used is 30 nodes distributed over 670×670 m area and the node mobility was simulated as per the Random waypoint mobility model. The simulation was performed by varying the speeds as 0, 1, 5, 10 and 15 m sec^{-1} with the fixed pause time of 30 sec and the total duration of simulation was 120 sec. During each simulation, five CBR sessions were established with the packet size of 512 bytes and each session generated a maximum of 400 data packets at the rate of 4 packets per second. The average of ten simulation runs is considered for each configuration.

3.3. Performance Metrics and Simulation Analysis

The performance of our proposed protocol, CAODV is compared with the AODV protocol with the following metrics.

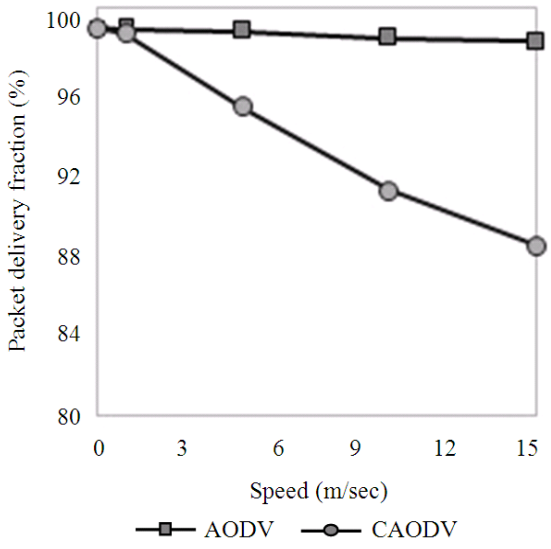

Fig. 1. Packet delivery fraction

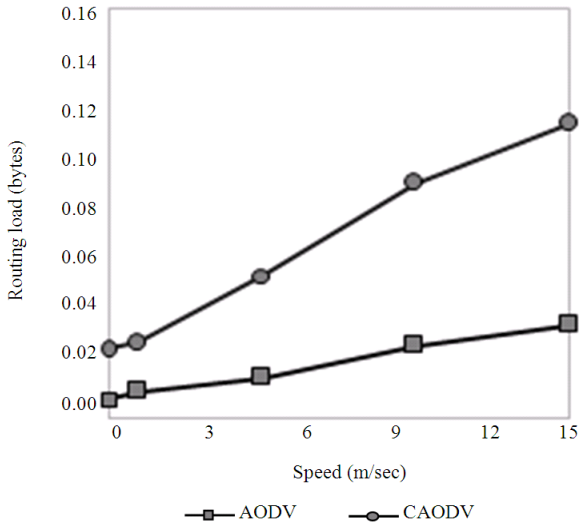

Fig. 2. Routing load (bytes)

3.4. Packet Delivery Fraction (PDF)

It is the ratio of the number of packets received at the destination node and the number of packets transmitted by the source node (Issariyakul and Hossain, 2012). It measures the loss rate as seen by transport protocols and as such, it characterizes both the correctness and efficiency of ad hoc routing protocols. A higher packet delivery ratio is desired in any network. **Figure 1** depicts the PDF values obtained for both the AODV and CAODV protocols. As the node movement speed increases, the PDF of CAODV decreases and the PDF of CAODV is 88% even when the nodes are moving at the speed of 15 m sec^{-1}. Hence, CAODV is more effective in establishing the authenticated route even with high node mobility.

3.5. Routing Load

It is the number of the overhead bytes transmitted per delivered data bytes at the destination. The control messages such as RREQ, RREP and RERR transmitted at each hop are considered as overhead bytes. Routing load in terms of bytes is represented for the AODV and CAODV protocols in **Fig. 2**. The routing load for CAODV is three times bigger than AODV at all the node movement speeds due to the inclusion of certificates, signatures and hash values within the routing messages. But, the number of control packets sent is almost equal for these two protocols.

3.6. Average Route Acquisition Delay

It is the average time taken by the source node to establish a route to the destination. **Figure 3** shows that the route acquisition delays for the CAODV protocol are more than AODV due to the involved process of signing and verification of digital signatures with the computation of hash values for the hop count during the route discovery.

3.7. Average End-to-End Delay

It is the average time that a packet takes to reach the destination. This is the time from the generation of the packet in the sender up to its reception at the destination's application layer and it is measured in seconds. It therefore includes all the delays in the network such as buffer queues, transmission time, route acquisition delays and MAC control exchanges.

The average end-to-end delay results for both the AODV and CAODV protocols are presented in the **Figure 4**. This illustrates that the end-to-end delays of CAODV are almost identical with AODV though the route acquisition delays of CAODV are considerably more. This shows that the effect of route acquisition delay is less and the processing of data packets are almost same for these two protocols.

3.8. Performance Evaluation with Malicious Nodes

The above simulation results are obtained when all the nodes in the network perform in good spirit for both the AODV and CAODV protocols.

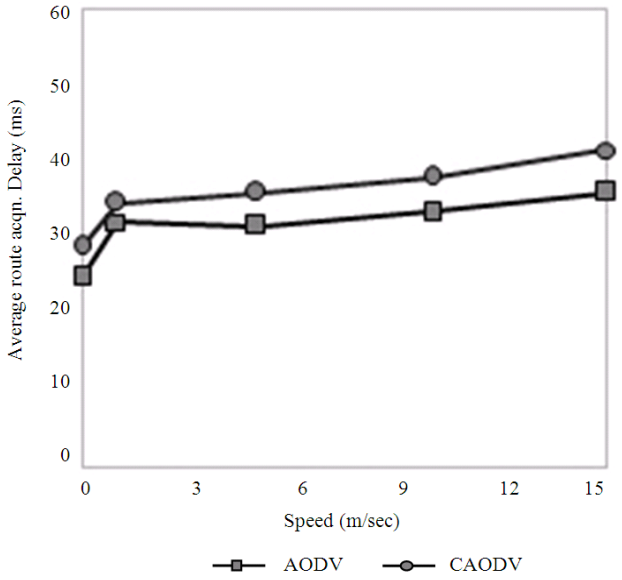

Fig. 3. Average route acquisition delay

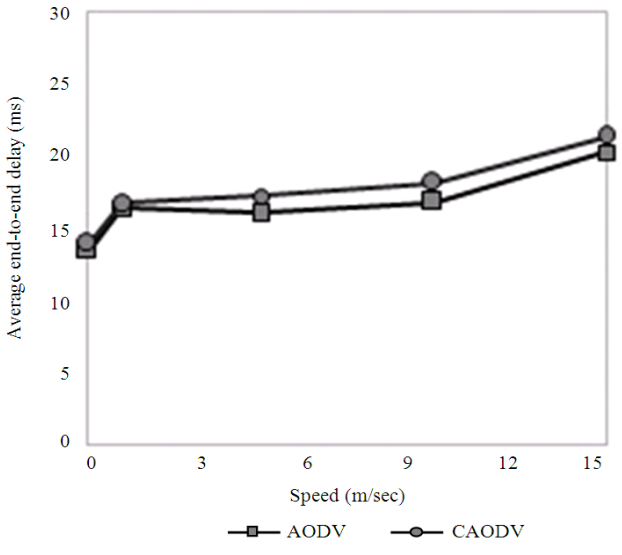

Fig. 4. Average end-to-end delay

It is important to analyze how these protocols behave when there are malicious nodes operating within the network. Hence, we introduced the malicious nodes (3, 6 and 9 malicious nodes to represent 10, 20 and 30% of total number of nodes) in the simulation scenario, which always reset the hop count in the routing message to zero before forwarding it to the neighbor nodes to observe the effect of malicious nodes.

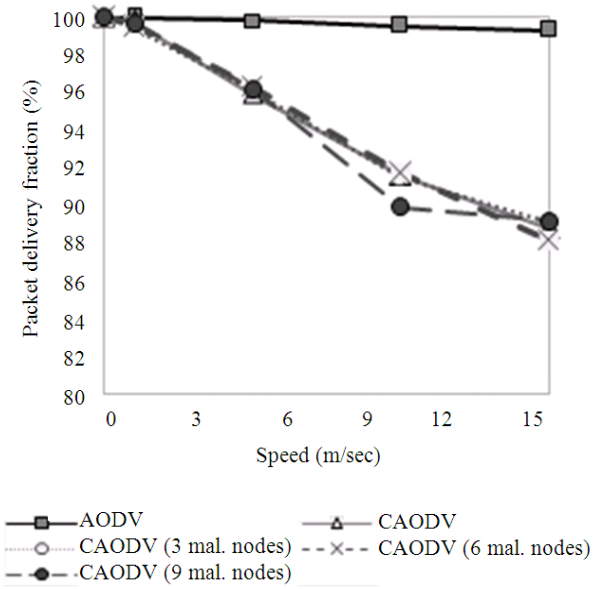

Fig. 5. Packet delivery fraction

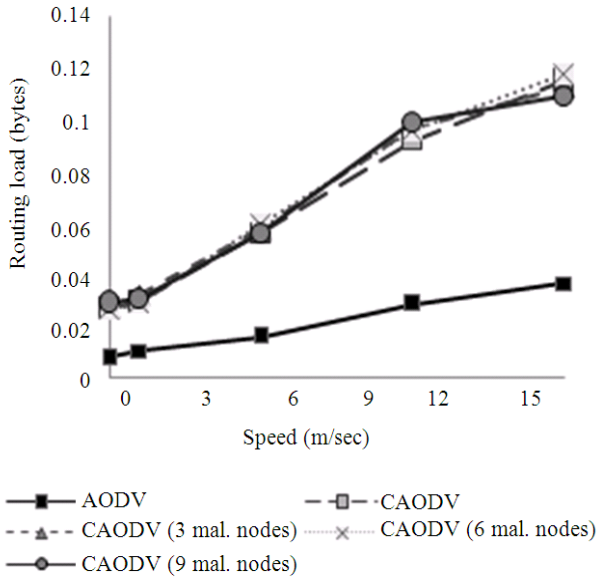

Fig. 6. Routing load (bytes)

Figure 5-8 demonstrate the simulation results of packet delivery fraction, routing load, average route acquisition delay and average end-to-end delay of AODV and CAODV protocols respectively in the presence of malicious nodes.

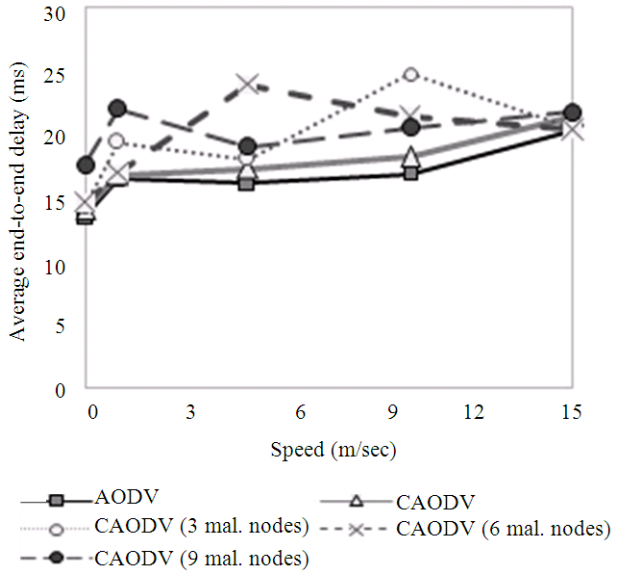

Fig. 7. Average end-to-end delay

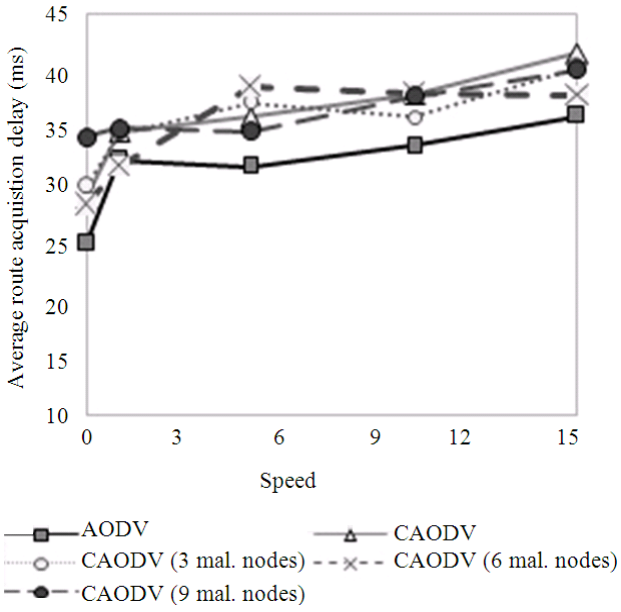

Fig. 8. Average route acquisition delay

Packet delivery fractions and Routing Loads of CAODV are almost same even in the presence of 30% malicious nodes in the network. The average end-to-end delay and the route acquisition delays of the CAODV protocol vary slightly because it has to find the valid routes avoiding the routes with malicious nodes.

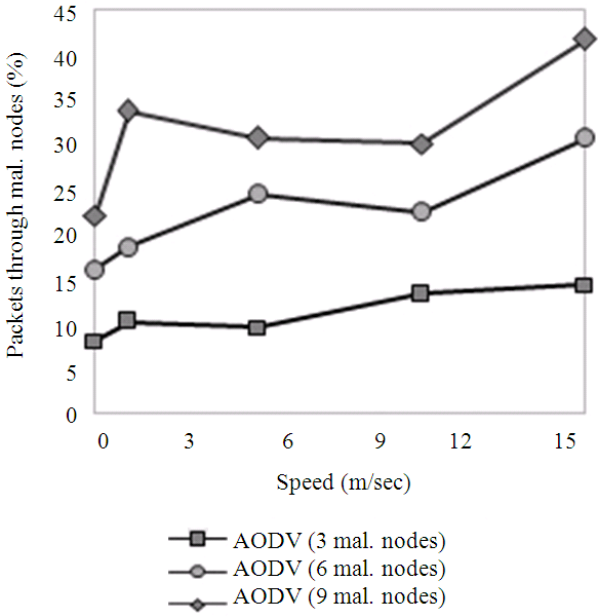

Fig. 9. Packets through malicious nodes

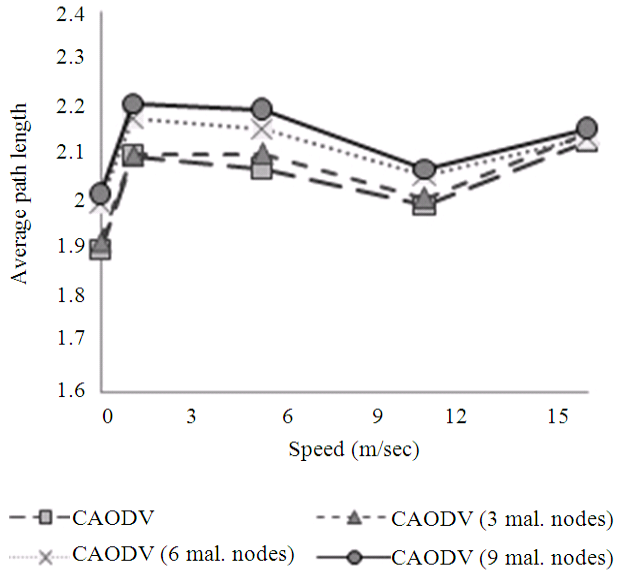

Fig. 10. Average path length

The route acquisition delay of CAODV with 30% malicious nodes is slightly higher due to the presence of more number of malicious nodes. The end-to-end delays of both AODV and CAODV protocols are almost equal at the node speed 15 even in the presence of malicious nodes.

3.9. Fraction of Data Packets through Malicious Nodes

It is the ratio of the number of data packets passed through malicious nodes to the total number of received packets at the destination. This metric reveals the quantity of data packets that can be tampered or dropped by the malicious nodes. **Figure 9** shows the percentage of data packets passed through malicious nodes in AODV protocol. It is obvious that the number of packets traversed through malicious nodes increases considerably with the presence of more number of malicious nodes in the network. On the other hand, none of the data packets is transmitted through the malicious nodes in the CAODV protocol since the routes with the malicious nodes are not selected.

3.10. Average Path Length

It is the metric that indicates the average number of hops traversed by each data packet to reach the destination. This is an important metric since longer routes increase the routing overhead and data packet latencies. This metric would be identical for the AODV and CAODV protocols like the above metrics when there are no malicious nodes in the network. In **Fig. 10**, the average path length of CAODV protocol with 30% of malicious nodes is approximately higher because of the rejection of more number of routes with the increased numbers of malicious nodes and it is almost equal for CAODV with 10, 20 and 30% malicious nodes at the node movement speed of 15 m sec^{-1}. Hence, the presence of malicious nodes does not affect much the performance of CAODV protocol in terms of this metric with the high node mobility.

4. CONCLUSION

In this study, an authentication protocol, CAODV for MANETs is proposed which provides secured routing with authentication and non-repudiation security services. It guarantees both node-to-node authentication and end-to-end authentication during route discovery and route maintenance that withstand many attacks launched by any number of malicious nodes in the network. The simulation results show that CAODV is as effective as AODV in discovering and maintaining routes and it performs consistently even in the presence of more number of malicious nodes by discarding all the routes through them. Though there is a considerable increase in the routing overhead, it is minimal and outweighed by the increased security services provided by this protocol.

5. REFERENCES

Abusalah, L., A. Khokhar and M. Guizani, 2008. A survey of secure mobile ad hoc routing protocols. IEEE Commun. Surveys Tutorials, 10: 78-93. DOI: 10.1109/SURV.2008.080407

Burmester, M. and B. Medeiros, 2009. On the security of route discovery in MANETs. IEEE Trans. Mobile Comput., 8: 1180-1188. DOI:10.1109/TMC.2009.13

Fall, K. and K. Varadha, 2010. The ns Manual (formerly ns Notes and Documentation). The VINT project.

Hu, Y.C., A. Perrig and D.B. Johnson, 2002a. ARIADNE: A secure on-demand routing protocol for ad hoc networks. Wireless Netw., 11: 21-38. DOI: 10.1007/s11276-004-4744-y

Hu, Y.C., D.B. Johnson and A. Perrig, 2002b. SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications, IEEE Computer Society Washington, DC, USA., pp: 3-13.

Issariyakul, T. and E. Hossain, 2012. An Introduction to Network Simulator NS2. 2nd Edn., Springer, New York, ISBN: 1461414067, pp: 510.

Johnson, D., Y. Hu and D. Maltz, 2007. The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4. The IETF Trust.

Kush, A. and C.J. Hwang, 2009. Proposed protocol for secured routing in ad hoc networks. Proceedings of the International Association of Computer Science and Information Technology-Spring Conference, Apr. 17-20, IEEE Xplroe Press, Singapore, pp: 76-81. DOI: 10.1109/IACSIT-SC.2009.28

Manickam, P., T.G. Baskar, M. Girija and D. Manimegalai, 2011. Performance comparisons of routing protocols in mobile ad hoc networks. Int. J. Wireless Mobile Netw., 3: 98-106. DOI: 10.5121/ijwmn.2011.3109

Murthy, C.S.R. and B.S. Manoj, 2004. Ad Hoc Wireless Networks: Architectures and Protocols. Pearson Education, ISBN-10: 0132465698, pp: 879.

Perkins, C., E. Belding-Royer and S. Das, 2002. Ad hoc On-Demand Distance Vector (AODV) Routing. The Internet Society.

Perkins, C.E. and P. Bhagwat, 1994. Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers. Proceedings of the Conference on Communications Architectures, Protocols and Applications, Aug. 31-Sept. 02, ACM New York, USA., pp: 234-244. DOI: 10.1145/190314.190336

Russell, B., M.L. Littman and W. Trappe, 2011. Integrating machine learning in ad hoc routing: A wireless adaptive routing protocol. Int. J. Commun. Syst., 24: 950-966. DOI: 10.1002/dac.1202

Sanzgiri, K., D. LaFlamme, B. Dahill, B.N. Levine and C. Shields *et al*., 2005. Authenticated routing for ad hoc networks. IEEE J. Selected Areas Commun., 23: 598-610. DOI: 10.1109/JSAC.2004.842547

Saxena, N., G. Tsudik and J.H. Yi, 2009. Efficient node admission and certificateless secure communication in short-lived MANETs. IEEE Trans. Parall. Distrib. Syst., 20: 158-170. DOI: 10.1109/TPDS.2008.77

Zapata, M.G., 2006. Secure Ad hoc On-Demand Distance Vector (SAODV) Routing. Internet Engineering Task Force (IETF).

Zhou, L. and Z.J. Haas, 1999. Securing Ad hoc networks. IEEE Netw., 13: 24-30. DOI: 10.1109/65.806983