Asian Journal of Information Technology 15 (23): 4711-4718, 2016
ISSN: 1682-3915

Cross-Layer Architecture for Secure Multipath Routing in MANET

[1]J. Srinivasan and [2]G. Tholkappia Arasu
[1]Department of Electronics Communication Engineeing,
Jayam College of Engineering and Technology, Dharmapuri, India
[2]AVS Engineering College, Salem, India

Abstract: Mobile Adhoc Network (MANET) is a wireless network with nodes linked to each other without any infrastructure and the nodes are capable of entering and leaving the network independently. Due to this feature of the MANET, this network is highly susceptible to attacks by malicious nodes which can be minor or major. Also, since all the nodes in the network are continuously mobile, the path between any two distant nodes keep changing and so there is a need to determine paths effectively. So in this study, we have developed a secure multipath routing technique which checks the network to identify every malicious node within the network and then determines an efficient path from the source node to the destination node.

Key words: Mobile Adhoc Network (MANET), multipath routing, destination node, infrastructure, susceptible

INTRODUCTION

Mobile Ad hoc Network (MANET): Mobile Ad hoc Network (MANET) is a self configuring network with nodes that communicates wirelessly. When the nodes are within the communication range of one another then they communicate directly and also determine all the nodes within its communicating range. When a node intends to communicate with another node which is not within its communication range, then it transfers the data through the intermediate node which behave as routers in forwarding the data to the destination node (Hoebeke *et al*., 2004). MANET consists of a group of mobile nodes which commune with one another in a wireless topology since the topology does not consist any infrastructure. In MANET, every node works as a router and also as a host (Bakshi *et al*., 2013).

Multipath routing in MANET: Node mobility is an essential feature that has to be considered while performing routing in MANETs. In multipath routing, several paths are created from the source to the destination. Multipath routing technique helps in increasing the data reliability during data transmission and also performs load balancing. In MANET, load balancing is critical due to the restricted bandwidth between the nodes in this network (Mueller *et al*., 2004). There exists numerous protocols related to multipath routing in MANET. A few have been listed:

Split Multi-path Routing (SMR): This routing protocol estimates the number of link disjoint path and node disjoint paths. The maximum possible path is initially set to two. Thus the source node has complete information about the path to the destination node.

Ad Hoc on Demand Multi-path Distance Vector (AOMDV) routing: This protocol configures the maximum possible paths and also determines the difference in the hop count between the shortest path and the possible alternate routes between the source and the destination. This protocol also estimates the number of link disjoint paths and the node disjoint paths.

Ad hoc on-demand Distance Vector (AODV) multipath: This protocol is responsible for establishing the node disjoint paths. Any number of paths can be created between the source and the destination (Parissidis *et al*., 2006).

Characteristics of MANET: MANET faces several security related threats due to several reasons. Some of the major causes of this problem are its predominant features such as:

- Lack of secure boundaries
- Threats from compromised nodes inside the network lack of centralized management facility
- Restricted power supply
- Scalability (Li and Joshi, 2008)

Corresponding Author: J. Srinivasan, Department of Electronics and Communication Engineeing,
Jayam College of Engineering and Technology, Dharmapuri, India

Objectives and proposed contribution: The previous research defined a cross-layer based architecture for defense against selfish attacks in MANET. It consists of data collection and monitoring agents. At each layer, the monitoring agent monitors each neighbor and computes time, traffic and topology statistics and passes these feature values to the data collection agent. The data collection agent maintains separate tables for each layer to store the collected values. The data collection agent collects data from network, MAC and physical layers. A combined trust value is then estimated by each node which is a fusion of various metrics from the collected information from all layers. Then the routing table is updated for the routing process.

In this research, if any node is captured or isolated, the data collection agent cannot able to collect any layer information from that node so that trust value cannot be updated. Hence node capture attacks need to be detected before estimating the trust values. Also a secure routing protocol should be developed computed trust value. Hence, in this study a cross-layer based architecture for secure multipath routing is proposed in which node capturing attacks are detected and isolated.

Literatire review: A Rajaram and colleagues have proposed a cross layer based Secure multipath Neighbour routing protocol in MANET. The cross layer described in this work extends the lifetime of the network. In this research, the secure multipath routing is used in order to avoid the link failures and path failures and also to offer security to the network from the intruders. In order to decrease the attacker's effect in the network, the secret sharing mechanism is used for authentication. The simulation results describes that this work delivers good performance, and also attains higher connectivity, lifetime, reduced overhead increased rate of reliability in the path and energy consumption.

Sivamani and Visalakshi (2014) have proposed a cross layer enhanced secure routing scheme for authentication and fault tolerant that attains the integrity and confidentiality between the mobile agents. Based on the simulation results, it is seen that this CLSRS mechanism attains good authentication rate, packet delivery ratio, fault tolerant rate, network lifetime, low delay and overhead when compared with the conventional mechanisms such as CCRVC and HCSLR but the mobility, time, simulation time, pause time and speed keeps varying in this mechanism. As a further extension to this work, secure secret sharing mechanism can be used to achieve better security and data integrity.

Obaidat *et al*. (2013) have proposed a QoS-Aware Multipath Routing Protocol (QMRP). This is a node disjoint protocol which takes into account the channel condition during the development of the multipath from the source node to the destination node in the wireless adhoc networks so as to overcome the problems faced by the remaining single paths as in AODV. In QMRP, the EPD is considered as an important factor in selecting the path which takes into account the SNR at the physical layer and also the correct data rate from the MAC layer along with the average queuing delay of the nodes in order to determine the quality of the link and rate of utilization of the medium near the node.

Babu and Sekharaiah (2014) have proposed a cross layer based detection and authentication mechanism for secure multi-path routing. In this research, the cross layer scheme for dropping the malicious packet is improved by using the authentication and routing attack detection modules. Regular checking of the RTS, CTS and RREQ counts is performed to identify the packet dropping attacks. When a data packet or a RREQ packet has to be sent by the source node, then the authentication method creates a hash value and then encrypts the hash value along with the path by utilizing the shared symmetric key of the destination node. The next hop in the present path is noted by all the nodes in the black or gray hole detection technique. This research aids in determining the malicious nodes which are the result of packet dropping and link breaking in the network.

Conti *et al*. (2009) have proposed a distributed solution to one of the major security threat in MANETs which is the node capture attack. The main idea behind this work is that the node mobility along with local node corporation can be used to develop security protocols which are highly efficient and energy proficient. When the nodes cooperate with each other at a higher rate then the information flow throughout the network becomes very much faster but with higher usage of energy. The results indicate that increasing the node mobility and node cooperation aids in the development of the good protocols. Also, to overcome the disadvantages of the conventional protocols, it is important for this protocol to increase the information flow rate.

MATERIALS AND METHODS

Cross layer architecture for secure multipath routing

Overview: In this study, a cross-layer architecture for secure multipath routing is developed. It consists of node capture attack detection and secure routing establishment phases.

In node capture attack detection, if a node is absent for a specific period of time, it is considered as captured. For that, node meeting time is estimated and a node

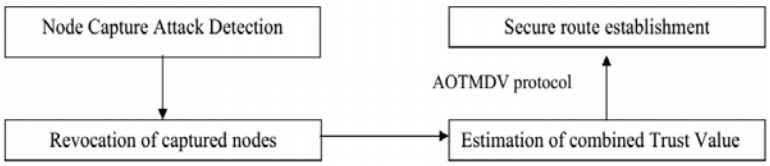

Fig. 1: Block diagram of cross-layer architecture

Table 1: Network layer values

Time	Network layer					
t1	Pr(f)			NN_{net}		NO_RREQ
MAC layer values						
t1	NN_{mac}	D_{tr}	N_{atr}	N_{rtr}	NO_RTS	NO_CTS
Physical layer values						
t1	PI					

Table 2: Trust table

Trust table	Metrics	Trust value
Node i	x	0
Node j	y	1

re-meeting timer is triggered. If the re-meeting timer is expired, an alarm will be flooded to the network by the tracked node. If the node's absence is confirmed within a specified interval, it is revoked from the network. The data collection agent then collects the information from non-revoked nodes only and estimates the combined trust value as described in our previous study.

For secure route establishment, Ad Hoc On-demand Trusted Multi-path Distance Vector routing (AOTMDV) protocol (Xia *et al*., 2013) is implemented based on the updated trust value. Figure 1 presents the block diagram of the proposed architecture.

Node capture attack detection: In this study initially the nodes are validated so as to ensure that the network is secure and free of malicious nodes. This is attained by the use of the node capture detection technique (Conti *et al*., 2009). This technique selects and validates the nodes in the network based on the meeting time. Then the nodes that do not satisfy this criterion are rechecked by the remaining nodes based on the alarm message. If the node doesn't get validated even after this, then the node is revoked by the network. The node capturing attack detection technique is described in Algorithm 1.

Algorithm 1:

1. When a node, x detects the presence of a specific set of nodes, Set_{nodes} within its communication range, it sets a time out for each node in that set with a specific time out period, α.
2. Nodes which are tracked by both the node, x and also $y \in Set_{nodes}$ are called as the meeting nodes.
3. The meeting nodes cooperate and exchange information during the meeting time with the nodes of interests.
4. If the node, x and y do not meet again within the time out period, α, then x broadcasts an alarm message in the network.
5. All the nodes that receive the alarm message checks the trust value of the node x.
6. If the trust value is low, then the alarm is ignored by all the nodes in the network
7. If the trust value is high, then it sets a new time interval to check the possibility of node detection again.
8. If any node in the node set does not meet the node x within a new predefined time period, β then that particular node of the node set is revoked by the network.

Estimation of combined trust value: Data Collection Agent (DCA) collects data from mobile nodes and maintains separate tables for each layer to store the collected values. The format of the data tables maintained at DCA is shown in Table 1.

From the stored information at the data Table 1a combined trust value for each node is estimated by DC which is a fusion of various metrics. These metrics includes the data from the data collection module and from the monitoring agent (time, traffic, statistical topology). The trust value between node i and node j is built in the form of a trust Table 2. The overall combined trust value is given by:

$$Tr = \frac{\alpha Pr(f) + \beta.N_{atr} + \gamma PI}{\delta D_{tr} + \lambda N_{rtr}} \quad (1)$$

where, α, β, γ, δ, λ are normalized weight values between 0 and 1. Afterwards, the routing table is updated proactively using the above estimated trust values. With the help of updation the trusted nodes can participate in the routing process.

Secure route establishment using AOTMDV protocol: Once the network is effectively validated, then when data packet has to be transmitted from a source node to any destination, an efficient path is selected between these two nodes (Xia *et al*., 2013) selected based on the trust value of the path and the hop count. In this study, AOTMDV routing technique is used for routing the data packet from the source to the destination node. The AOTMDV routing strategy is described in Algorithm 2.

Algorithm 2:

When a source node, s wants to send a data packet to a destination node, d then it is sent through a route that has a specific Path Trust, Trust $_{Path}$
If there does not exist any path that has the required Trust $_{Path}$ value, then the route discovery process as shown in Fig. .2 is used to determine a suitable path with the Trust $_{Path}$ value.
In the route discovery process, a node, m sends a RREQ message to its neighboring node.

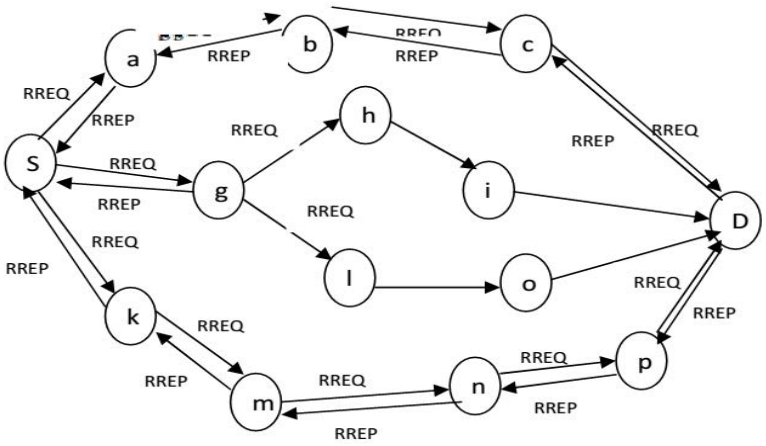

Fig. 2: Oute discovery process

Type	J	R	G	D	U	Reserved	Hop Count
RREQ ID							
Destination IP Address							
Destination Sequence Number							
Originator IP Address							
Originator Sequence Number							
Required Trust	Actual Trust		Hash Function				
Hash							

Fig. 3: REQ message format

The RREQ format and its field are shown in Fig. 3.
The receiving node, n updates the route entry of node m in its routing table if it was not present initially and then a predefined trust value is assigned to it.
Then a reverse path is created from n to m, if it is trustworthy which is calculated according to the technique in study 3.3.
Next node, n sends a RREP message to the node, m. Thus, creating a path between node m to n. The RREP message format and its field is shown in Fig. 4.
In this way, all possible paths between the source node, s and destination node, d is created such that the Trust $_{Path}$ is met.
If there exists q paths between s and d that satisfies the then the node's selects the path with minimum hopcount.
If more than one path has the minimum hopcount then the path with the highest trust value is selected by source node, s for data transmission.
Nodes with very low trust value are detected as malicious nodes.
Then the data packet is transmitted from the source node, s to the destination node, d through the path selected by s according to trust value and hop count.

In Fig. 2, the source node, S wants to send data packet to destination node, D. It determines the route by sending the RREQ message to all its intermediate nodes. The capable node replies with the RREP message. Then based on the hop count route S-a-b-c-e-D is selected to deliver the data packet.

Figure 3 depicts the RREQ format. In the RREQ message, the frame is divided into several fields. The field J denotes the join flag and it is reserved for multicast.

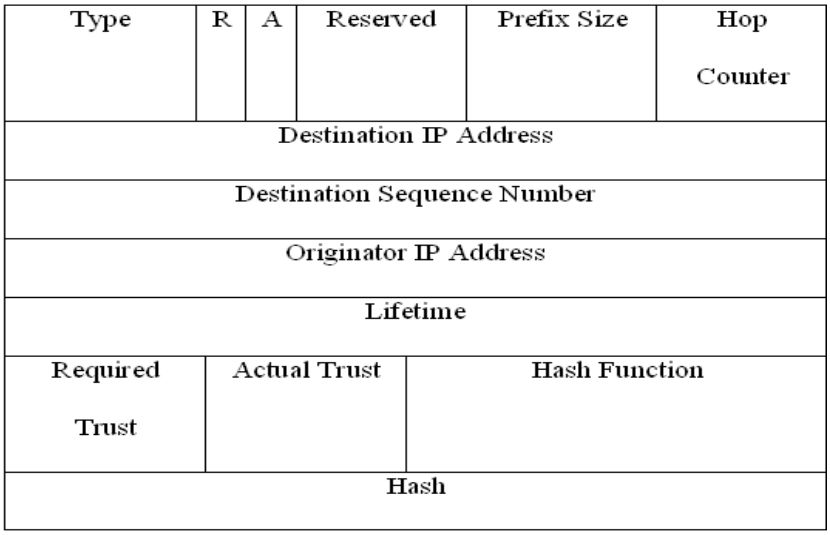

Fig. 4: RREP message format

Field R denotes repair flag, reserved for multicast. G denotes for Gratuitous RREP flag and indicates whether a gratuitous RREP should be unicast to the node specified in the destination IP address field. D denotes destination only flag and indicates only the destination may respond to this RREQ. U denotes Unknown sequence number and indicates the destination sequence number is unknown. If the source does not have a route to the destination, dest-sequence no is set to 0. If the source has a route but its trust value is smaller than the trust requirement, the source will set destSequence no of the RREQ to dest sequence no in its routing table. Four new fields Required Trust (RT), Actual Trust (AT), Hash function and hash. Required Trust (RT) represents the path trust requirement of data packet transmission which is determined by the source node and remains unchanged during the flood. The field Actual Trust (AT) denotes the continued product of intermediate node's trust values on this path that the RREQ has passed. It is initialized to 1 by the source and varies with the transmission of the packet. The Message Authentication Code (MAC) mechanism protects the two new important fields, 'RT' and 'AT' and use MD5 algorithm for the 'Hash Function'. The hash value filed 'Hash' is described as tag a = MACK (m), K is the secret key shared between the monitoring node and monitored node pairs, m is the 'RT' and 'AT' simply joining together value.

Figure 4 depicts the RREP format. In the format, R denotes Repair flag and is used for multicast. A denotes Acknowledgment required. The new added field Required Trust (RT) is equal to the RT in the RREQ. And the new field Actual Trust (AT) in an RREP denotes for the continued product of the intermediate nodes' trust values on the path that the RREP has passed in route reply and is initialized to 1 by the destination. The fields 'Hash Function' and 'Hash' have the same meaning with RREQ. If the destination receives multiple copies of RREQ, it will reply the first k paths at most whose path trust values are greater than or equal to the required trust of the RREQ and which come from different neighbors of the destination.

RESULTS AND DISCUSSOIN

Simulation parameters: We use NS2 [ ] to simulate our proposed Cross-layer Architecture for Secure Multipath Routing (CSMR) protocol. We use the IEEE 802.11 for MANETs as the MAC layer protocol. It has the functionality to notify the network layer about link breakage. In our simulation, the packet sending rate is varied as 10, 30, 50, 70 and 90 Kb. The area size is 1000×1000 m^2 region for 50 sec simulation time. The simulated traffic is Constant Bit Rate (CBR). Our simulation settings and parameters are summarized in Table 3.

Performance metrics: We evaluate performance of the new protocol mainly according to the following parameters. We compare the AOTMDV protocol with our proposed CASMR protocol.

Average packet delivery ratio: It is the ratio of the number of packets received successfully and the total number of packets transmitted.

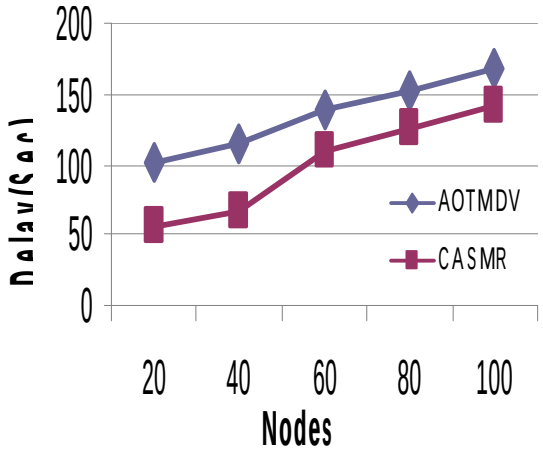

Fig. 5: Nodes vs delay

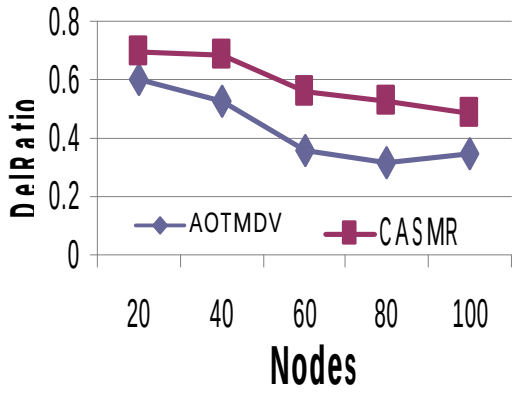

Fig. 6: Nodes vs delivery ratio

Average end-to-end delay: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

Overhead: It is the number of router packets received by the receiver during the data transmission

Results and Analysis

Effect of increasing number of nodes: To analyze the effect of both the techniques by increasing the number of nodes, the network size is varied from 20-100 keeping 10% of the total nodes as attackers.

Figure 5 shows the results of end-to-end delay for both AOTMDV and CASMR when the number of nodes is increased. It is evident that when the nodes are increased, the number of malicious nodes are also increased, leading to more number of validations and routing table updations. Hence, the delay is linearly increased as depicted by the figure. However CASMR attains 27% less delay when compared to AOTMDV,

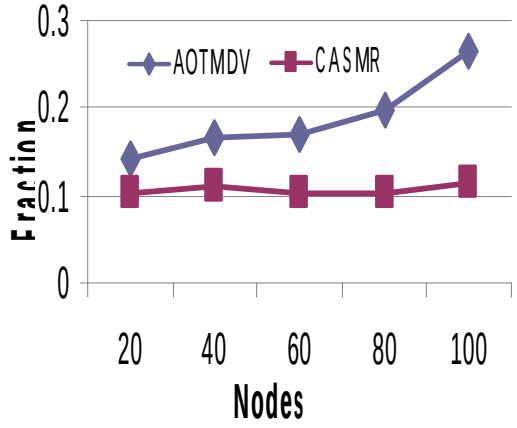

Fig. 7: Nodes vs compromised communications

Table 3: Trust table simulation parameters

No. of nodes	20,40,60,80 and 100
Area	1000×1000
MAC	802.11
Simulation time	50 sec
Traffic source	CBR
Rate	100 kb
Propagation	Twr ray ground
Antenna	Omni antenna

since it eliminates node capture attacks before selecting the trusted path. Figure 6 shows the results of packet delivery ratio for both AOTMDV and CASMR when the number of nodes is increased. Since malicious are increased when the number nodes are increased, more packets are dropped leading to decrease in packet delivery ratio. The cross-layer based trusting mechanism of CASMR filters attacks from all the layers, the routing table involves only legitimate nodes. Hence, the packet delivery ratio of CASMR is 28% more when compared to AOTMDV.

Figure 7 shows the results of fraction of compromised communications for both AOTMDV and CASMR when the number of nodes is increased. Since, malicious nodes are increased when the number nodes are increased, there will be more number of compromised communications. Since, CASMR has the node capture attack detection mechanism in addition to the secure routing protocol, it reduces the fraction of compromised communications by 41% when compared to AOTMDV.

Effect of increasing malicious nodes: To analyze the effect of both the techniques by increasing the malicious nodes, the number of malicious nodes is varied from 2-10 among 100 nodes.

Figure 8 shows the results of end-to-end delay for both AOTMDV and CASMR when the number of malicious nodes is increased. It is evident that when the malicious nodes are increased, there will be more number

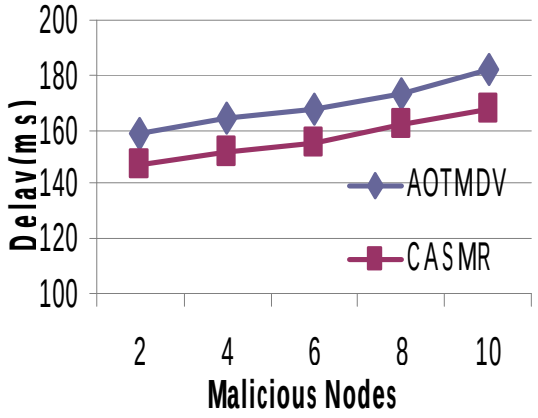

Fig. 8: Malicious nodes vs Delay

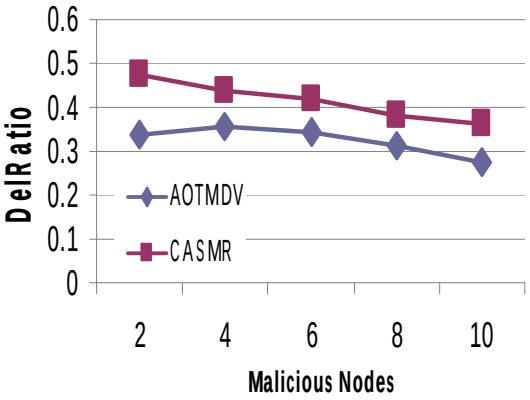

Fig. 9: Malicious nodes vs delivery ratio

of validations and routing table updations. Hence, the delay is linearly increased as depicted by the figure. However CASMR attains 8% less delay when compared to AOTMDV since it eliminates node capture attacks before selecting the trusted path. Figure 9 shows the results of packet delivery ratio for both AOTMDV and CASMR when the number of is increased Since, malicious nodes are increased, more packets are dropped leading to decrease in packet delivery ratio. The cross-layer based trusting mechanism of CASMR filters attacks from all the layers, the routing table involves only legitimate nodes. Hence, the packet delivery ratio of CASMR is 21% more when compared to AOTMDV.

Figure 10 shows the results of fraction of compromised communications for both AOTMDV and CASMR when the number of malicious nodes is increased. Since, malicious nodes are increased, there will be more number of compromised communications. Since, CASMR has the node capture attack detection mechanism in addition to the secure routing protocol, it reduces the fraction of compromised communications by 31% when compared to AOTMDV.

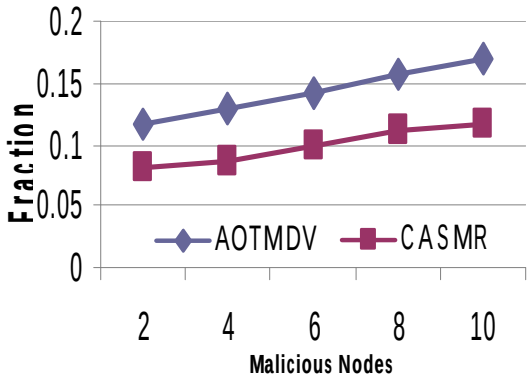

Fig. 10: Malicious nodes vs compromised communications

CONCLUSION

In this study, we have proposed a cross-layer architecture for secure multipath routing in MANET. This work ensures successful routing process in MANET. In this mechanism initially, the network is validated so that all the nodes are non malicious nodes through the node capturing technique. In this technique, the trust value of every node is estimated and updated in the routing table for further purposes. Next when a data packet has to be transmitted from the source node to the destination node, then the AOTMDV routing technique is employed. This technique determines the most efficient path from the source to the destination based on the path trust value and hop count. Once the most efficient path is selected, then the data packet is transmitted through this path ensuring data delivery at the destination. Simulation results show that the proposed architecture provides better delivery ratio and reduces the compromised communications.

REFERENCES

Babu, K.S. and K.C. Sekharaiah, 2014. CLDASR: Cross layer based detection and authentication in secure routing in MANET. IRACST. Int. J. Comput. Networks Wirel. Commun., 4: 2250-3501.

Bakshi, A., A.K. Sharma and A. Mishra, 2013. Significance of Mobile Ad-Hoc Networks (MANETs). Intl. J. Innovative Technol. Exploring Eng., 2: 2278-3075.

Conti, M., R.D. Pietro, L.V. Mancini and A. Mei, 2009. Mobility and cooperation to thwart node capture attacks in manets. EURASIP. J. Wirel. Commun. Networking, 2009: 1-13.

Hoebeke, J., I. Moerman, B. Dhoedt and P. Demeester, 2004. An overview of mobile ad hoc networks: Applications and challenges. J. Commun. Netw., 3: 60-66.

Li, W. and A. Joshi, 2008. Security issues in mobile ad hoc networks-A survey. Department Comput. Sci. Electr. Eng. Univ. Maryland Baltimore County, 1: 1-23.

Mueller, S., R.P. Tsang and D. Ghosal, 2004. Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges. In: Performance Tools and Applications to Networked Systems, Calzarossa, M.C. and E. Gelenbe, Springer, New York, ISBN: 9783540219453, pp: 209-234.

Obaidat, M., M. Ali, I. Shahwan, M.S. Obaidat and S. Obeidat, 2013. QoS-Aware multipath communications over MANETs. J. Netw., 8: 26-36.

Parissidis, G., V. Lenders, M. May and B. Plattner, 2006. Multi-Path Routing Protocols in Wireless Mobile Ad Hoc Networks: A Quantitative Comparison. In: International Conference on Next Generation Wired/Wireless Networking. Koucheryavy, Y., J. Harju and V.B. Iversen (Eds.). Springer Berlin Heidelberg, Berlin, Germany, ISBN: 978-3-540-34430-8, pp: 313-326.

Sivamani, C. and P. Visalakshi, 2014. CROSS layer enhanced secure routing scheme for authentication in mobile ad hoc networks. J. Theor. Appl. Inf. Technol., 68: 2005-2014.

Xia, H., Z. Jia, L. Ju, X. Li and E.H.M. Sha, 2013. Impact of trust model on on-demand multi-path routing in mobile ad hoc networks. Comput. Commun., 36: 1078-1093.