ISSN 2278-3091
Volume 9, No.3, May - June 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcs227932020.pdf
https://doi.org/10.30534/ijatcse/2020/227932020

Prevention of Routing Attacks using Trust-Based Multipath Protocol

S. Ananthakumaran[1], M. Sathishkumar[2], R. Bhavani[3], R. Ravinder Reddy[4]
[1,2] Associate Professor, Department of Computer Science Engineering, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India, [1] bhashkumaran@gmail.com, [2] sathishkumarmani17@gmail.com
[3]Assistant Professor (Senior Grade), Department of Electrical and Electronics Engineering, Mepco Schlenk Engineering College, Sivakasi, Tamil Nadu, India, bavanir@mepcoeng.ac.in
[4] Associate Professor, Department of Computer Science Engineering, Chaitanya Bharathi Institute of Technology, Hyderabad, Telangana, India, ravi.ramasani@gmail.com

ABSTRACT: In order to provide secure data transmissions, the neighbour nodes must recognize different types of attacks and their effects on the Mobile Ad Hoc Networks (MANET). To perform routing in the traditional protocol the number of hops is used to select the route. To measure the neighbour's behaviour, to forward the packets, and to reduce the effect of malicious node trust model is used in MANET. In this paper, Trusted Path-based ad hoc on-demand multipath distance vector (TAOMDV) routing protocol is proposed. It is used to discover trustworthy forward paths and can prevent the blackhole, wormhole, flooding and misrouting attacks. The highest trusted path is selected to send the data. The above said attacks are prevented, by the TAOMDV, using passive acknowledgement. The simulation result shows that TAOMDV protocol achieves high packet delivery ratio (PDR), reduces the packet overhead and end to end delay of packet. It provides higher detection ratio of the attacker. But the throughput is achieved little lower while more attackers presents in the network.

Key words: Blackhole, Wormhole, Flooding, Misrouting and Passive Acknowledgement.

1. INTRODUCTION

As the communication is through wireless medium, it is possible for the intruder to intercept and modify the message or can even prevent the routing information (RI). However, many applications run in untrusted environments, requiring secure routing and communication.

Therefore it is mandatory to preserve all the security principles, confidentiality, integrity, availability, authentication and non-repudiation, so that the entire network operation should not get disturbed. There are two primary motivations associated with trust management in MANETs. Firstly, trust evaluation helps to identify malicious entities. Secondly, trust management offers a prediction of one's future behaviours and improves network performance.

The general routing protocols for ad hoc networks cope well with dynamically changing topology but are not designed to accommodate defense against malicious attackers and to detect the compromised nodes through RI. Routing protocols for ad hoc networks must handle the outdated RI to accommodate dynamic changing topology. False RI generated by compromised nodes can also be regarded as outdated RI. As long as there are sufficient numbers of valid nodes, the routing protocols should be able to bypass the compromised nodes or make use of an alternate route.

The malicious node(s) can attack the MANET using different ways, such as sending fake messages several times, fake RI, and advertising fake links to disrupt routing operations. A black hole attack is a type of routing attack in which malicious node advertise itself as having shortest path to the destination in a network by sending fake route reply to the source node. It can be treated as Denial of Service (DoS) by dropping the received packets. In the flooding attack, the attacker broadcast many useless packets per time interval with the IP address which does not exist in the network. Attack such as gray hole, where the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behaviour. In wormhole attack, severe threats to MANET, the attacker records packets at one location in the network and tunnels them to another location. This tunnel between two colluding attackers is referred as a wormhole. The wormhole and blackhole attacks disclose the confidential security service and flooding attacks reduce the availability of the network service.

The traditional routing protocols only care about the number of hops but not addressing the security. A secure routing protocol is unable to prevent malicious or compromised nodes from doing misbehaviours, which are authorised as participants in the network. There are two trust models used in ad hoc network [10] such as direct trust and indirect trust. To find the neighbour's behaviour and to forward the packet to the destination, the trust model is used in MANET. It monitors only a node's own packet forwarding requests. If malicious node moves to a new sub-network, it will be recorded as a normal node with initial trust value.

In this paper, a protocol named trusted path based ad hoc on-demand multipath distance vector (TAOMDV) is proposed to discover secure path. It is based on the ad hoc on demand distance vector protocol (AODV) and the multipath routing protocol [7].

2. RELATED WORKS

Some solutions work well in the presence of one malicious node, but they might not be applicable in the presence of multiple colluding attackers. A routing protocol is designed like intrusion detection system (IDS) to provide solution for detecting and preventing nodes from security threats in [16]. It observes the network traffics and tries to examine the misbehaviour activities of nodes.

An efficient method to detect and avoid wormhole attacks in the OLSR protocol is discussed in [8]. A timing-based countermeasure against the wormhole attack is discussed in [2]. In this, a statistical approach, uses the relative frequency of each link, on multi-path routing is discussed. In [9], a trust-based scheme for identifying and isolating the nodes that create a wormhole in the network, without engaging any cryptographic technique is presented.

An anomaly-detection scheme based on a dynamic learning process and IDS is used in [13], allows the training data to be updated at particular time interval is used. The flooding attack prevention (FAP) suggested a defense system using path cut-off against either RREQ or data flooding attacks. This limitation of FAP is eliminated by [1] threshold prevention. A period-based defense mechanism (PDM) [4] against data flooding attacks is used to enhance the throughput of burst traffic. In [13], the scheme based on their relationship with the neighbouring node and categorised the node in three categories such as stranger, acquaintance and friend.

In [5], [12], the blackhole attack is analysed and a mechanism based on Packet Drop Ratio (PDRR) [14] is used to detect the blackhole attack in MANET with AODV protocol. The analysis of network survivability in the presence of node misbehaviours and failures is discussed in [19]. A topology transform-based trust model [18] is used to relieve the malicious effects on the accuracy of trust. Secure routing against collusion (SRAC) [20] is used by a node to make a routing decision based on its trust of its neighbouring nodes against the Byzantine attacks. A secure routing protocol (SRP) with quality of service (QoS) support, called Trustworthiness-based Quality of Service (TQOS) routing is used.

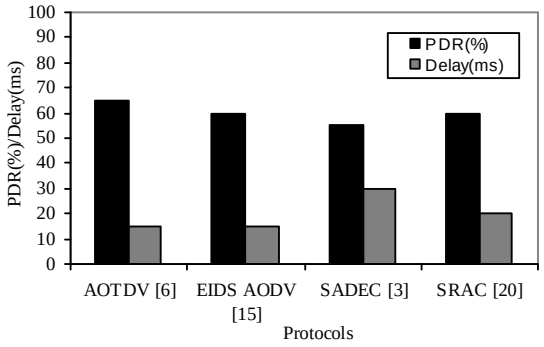


Figure. 1: Comparison of Packet Delivery Ratio and Delay of Packets

Multicast Ad hoc On Demand Distance Vector protocol (MAODV) is a multicast routing protocol which is used to identify the routing attacks like black hole, wormhole and flooding. A trust based approach in which each node maintains a record of success and failure rate of packet transmissions and then used to determine the trust values to reduce the black hole and the wormhole attacks. A method, to detect and remove blackhole and grayhole attack, is discussed in [17]. In [11], the survey of trust based protocols and some techniques on trust management in MANETs are presented and also the various trust models are discussed.

Figure 1 shows the comparison of various protocol of packet delivery ratio and end to end delay of the packets against the routing attacks.

3. PROPOSED WORK

In MANETs each node has to send packets for other nodes. Due to this, nodes may act as selfish or malicious nodes to capture the data and thus needs a secure communication to transfer the packets. Trust levels can be computed based on the battery consumption, packets forwarding or dropping. A trust model is based on experiences and can monitor the behaviour of the nodes and also can identify the attacks.

Figure 2 shows the system design. Here the multipath protocol is used to discover and select the route. Trust model is based on the trust value of the path and is incorporated in the routing to select the secure path. After sending the packets the sender will observe for any irrelevant packet and monitor the node for any malicious activities. When there is any change in the behaviour of any node then it will update the trust value of the nodes and detect the attack node accordingly.

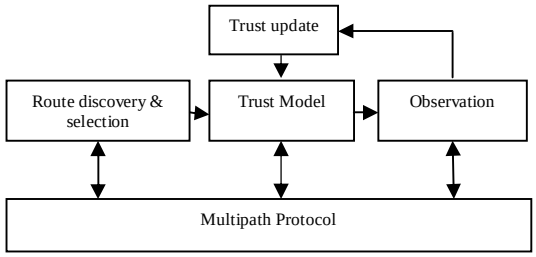


Figure. 2: System Design

a. Trusted Path-based on-demand multipath routing protocol

This protocol discovers multiple loop free paths and used to find multiple paths in one route discovery. Each node maintains a routing table which is composed of multiple routing entries to other node. TAOMDV protocol is a hop-by-hop routing method, in which the source is not capable to know all the nodes in the path to a destination but it is enough for the source to recognize which neighbour is the next hop. When a node *i* need to transmit data packet to a destination, it checks the local routing table to find the next hop node *j* based on the highest path trust value. This process will continue until it reaches the destination. An unused route to a destination after a particular period is marked as invalid and will be removed from the routing table. The main difference between AODV and AOMDV [7] protocol is that path trust is added to the route list. A routing table entry in TAOMDV contains such as destination and its sequence number, next hop, hop count and path trust, and expiration

timeout (ET). The hop count and path trust metrics contain an evaluation vector of a path from the source to the destination. AODV and AOMDV protocols are using only the hop count for the route selection, but this protocol uses the hop count and the path trust value for routing selection.

b. Route discovery and Path selection

A route discovery is initiated only when trusted routes does not exist. Initially, the source node will initiate a route request (RREQ) packet by broadcasting to all the neighbours and will wait for route reply (RREP) packets. Every node maintains two increasing counters such as a sequence number and a broadcast ID. Sequence number is used to maintain the fresh route. Broadcast ID is incremented each time the source issues a new RREQ, Route Update (RUPD) or Route Error (RERR) packet.

The Source Trust (ST) and Path Trust (PT) fields are also added with each node. ST is used to represent the PT value required by the data packet, which is initialised by the source and does not change during the route discovery. The field PT contains the continued product of trust values of nodes that the RREQ has travelled in the route discovery. It is initialised to 1 by the source and changes when the transmission of the packet occurs.

If an intermediate node has a route entry for the desired destination node, it checks whether the route is fresh by comparing the destination sequence number in its own route entry with the one in the RREQ. If the RREQ's sequence number for the destination is greater than or equal to that in the route entry, the intermediate node should not use its recorded routes to respond to the RREQ. Instead, it rebroadcasts the RREQ. The intermediate node replies to an RREQ only when it has a route with a sequence number that is greater than in the RREQ. If it does have a fresh route to the destination and the RREQ has not been processed previously, the node unicasts a route reply (RREP) packet back to its neighbour from which it received the RREQ.

When the destination *d* receives an RREQ, it will compare the destination sequence number in the RREQ and the sequence number (*Sd*) maintained in node *d*. If destination sequence number is equal to *Sd*, the destination will increase *Sd* by 1. If destination sequence number is smaller than *Sd*, the destination will not modify *Sd* and then the destination makes a decision to send back a route reply packet to the source according to the condition.

If an intermediate node has multiple paths to the destination, it will reply two copies of RREP at most, one of which has the smallest hop count and the other has the large trust value. 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 ST of the RREQ and which come from each neighbours of the destination. If several path trust values are smaller than the ST, the destination will reply at most *k* of the shortest paths from different neighbours. The RREP contains the latest sequence number of the destination. The parameter *k* is used to reduce the number of RREP packet and can prevent an RREP flood.

If an intermediate node receives an RREP, it will unicast the RREP through the route whose PT is not less than the ST of the RREP and whose HopCount is the minimum in all paths to the source. As the RREP travels back to the source, each node along the path sets up a forwarding route to the destination and refills its ET for routes to the source and the destination. When the RREP packet reaches the source node, the most secure path is selected by the source. It calculates the PT based on the trust values of paths received in the RREP packet and the number of nodes in the path. The path selected is the one which has the maximum path trust and the minimum number of nodes in the path. If valid route could not be found then it will send RERR back to the source. RERR packet specifies the route to the source and the destination does not exist due to link may be broken or the intermediate node may be maliciously attacked.

c. Trust Model

The trust manager stores trust information of all known nodes during the transmission, and make to query for information about stored trust values. The direct interactions between the nodes are used to compute trust. If the distance between source and destination is beyond one hop, packets might be dropped by intermediate nodes because of unexpected causes such as heavy traffic or malicious attacks. Trust evaluation in a routing procedure is a measurement of behaviours of neighbours after forwarding a packet. For example, a node *j* will give a trust value to its neighbour *k* after the node *k* transmits a packet which is sent by node *j*.

Forwarding ratio, is the proportion of the number of packets have been forwarded correctly to the total number of packets forwarded, is used to evaluate the quality of forwarding. The forwarding ratio FR is calculated as,

$$FR = \frac{CPF}{TPF}$$

where CPF is the packets that are correctly forwarded by the neighbour node and TPF denotes the total packets that are forwarded by the source.

Correct forwarding means the forwarding node not only transmits the packets to its next hop node but also forwards correctly without modification. For instance, when a malicious neighbour node forwards a data packet after corrupting the data, it is not considered as correct forwarding. If the sender monitors this illegal modification, the forwarding ratio of the neighbour will be decreased.

C.1 Node Trust

The trust of a node *j* in another node *k* is a measure to make sure that packets sent by node *j* have actually been forwarded by node *k*. After each interaction, node *j* checks whether the neighbour *k* forwards the packet correctly. If so, the trust value increases otherwise it decreases. The node trust value for node *j* in node *i* is calculated as follows,

$$Tij = \sum_{k}^{n} \left[Wk \times FR \right]$$

where W_k is the weight assigned to the k^{th} trust category and *FR* is the correct forwarding ratio of the packets. The sum of the weights should be equal to 1 and the value should be between 0 and 1.

When the trust value is 0 then it is complete distrust whereas the trust value is 1 then it is complete trust. Trust levels of nodes are listed in Table 1.

C.2 Path Trust

When a source discovers a path to the destination with the help of neighbouring nodes, the trust value of the path is computed according to the trust values of intermediate nodes along the path. The trust of a path, TP, is equal to the continued product of node trust values in the path,

$$TP = \prod_{i} Ti$$

where T_i is the node trust value of all intermediate nodes in the path.

Table 1: Different Trust Level

Trust value	Type
0-h	Malicious Node
h-0.75	Suspicious Node
0.75-0.9	Less trustworthy Node
0.9-1	Trustworthy Node

The destination node, *d*, need not forward the packets to itself, so it need not to compute the path trust to node *d*. If the destination node *d* is a neighbour of the source node *s*, the path trust is equal to 1 because it is assumed that all packets would be transmitted in one hop.

d. Monitoring and Detection

In trust model, passive acknowledgement is used to evaluate the trust. Passive acknowledgement uses promiscuous mode to monitor the neighbour's behaviours in the wireless communication channel. It is used to detect the nodes which are passing the packets irrelevant to the destination within the communication range.

The sender node places itself in promiscuous mode after the transmission of packets so as to listen the retransmission by the forwarding node. Using this method, a node comes to know that whether the packet has been sent to a neighbour is certainly forwarded or not. The circular packet buffer is used to record all packets sent recently. It contains the node id, trust value of the node and the packet that is recently forwarded by the particular node. The packet is stored in the packet buffer after the transmission and will wait for acknowledgement. A retry counter, RetryCnt, is used to remember the number of retransmitted packets and also used to avoid the flooding. If the sender is in the promiscuous mode then it is monitoring the packets for correct forwarding. If the packet is correctly forwarded then it will be removed from the packet buffer and the corresponding counter of correct forwarding is incremented by 1. The sender will update the node trust for the neighbour when the packet is forwarded correctly. Passive acknowledgement is used to recognize the black hole attack and also monitors the correct forwarding to the next hop that can avoid the misrouting of the nodes.

In the malicious node detection, if the trust value of a neighbour node is smaller than black-list threshold value, it will be marked as a malicious node. The malicious node will then be moved into a black list and can not participate in the routing for further. It will find an alternate path in the routing table if any other route exists. If the valid route does not exist in the routing entry then the node will start the route discovery procedure to find the valid route.

Here the black-list trust threshold *h* is initialised as 0.6 by the source. In particular, every node maintains a local black list. The packets from a malicious node will not be forwarded by the neighbour; at the same time the neighbour will not send packets to the malicious node. If a node is evaluated very low by all its neighbours, any reply it gives to route requests is discarded, and any request that initiated is ignored.

4. SIMULATION AND RESULT ANALYSIS

The experimental setup and the fixed simulation parameters for proposed work are listed in Table 2.

Table 2: Experimental Setup

Parameter	Value
Simulator	NS-2
Simulation Time	250 Sec
Number of Nodes Area	50 1000 x 1000m
MAC	802.11
Transmission Protocol	TCP
Application Type	CBR
Mobility Model	Random Way Point
Packet Size	512 bytes
Transmission radius	250m
No. of Malicious Node	0-20
Routing Protocol	AOMDV
Type of attacks	Blackhole, Wormhole, Flooding and Misrouting.

The five network parameters are used to evaluate the performance of the proposed technique. They are Packet Delivery Ratio (PDR), average end to end delay, packet overhead, throughput and detection ratio. Each parameter is used in two different scenarios such as by varying the number of attacker node and the simulation time. The protocol used in the simulation is trusted path based ad hoc on-demand multipath distance vector (TAOMDV). The various attacks used to analyse the performance are blackhole, wormhole, flooding and misrouting attacks.

Packet Delivery Ratio (PDR) is defined as the number of the packets received at the destination node to the number of packets sent by source node. Figure 3 shows the simulation result of the PDR with respect to the number of attackers. In this network when there is no attacker node, the PDR achieves up to 98.48%. When the number of attacker node increases the PDR is decreasing. In the presence of 20 blackhole attackers, the number of packets sent by the source is 2765 and the number of packets received by destination is 2203. The

proposed method achieves the PDR up to 79.6% for blackhole attack whereas in [6] it achieves only 55%. The 77% of PDR is achieved while wormhole attack is present. This is low when compared to other attacks. In the presence of the misrouting attack the 82% of PDR is achieved which is high when compared to other attacks in the network.

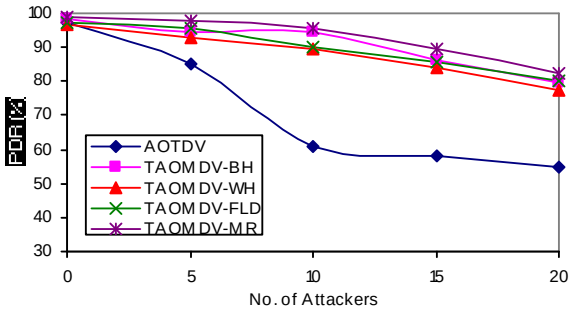


Figure. 3: Packet Delivery Ratio vs No. of Attacks

Figure 4 shows the simulation result of PDR with respect to time. The simulation time is set from 25 to 250 seconds. Initially the PDR of the proposed method achieves up to 93%, 90%, 92% and 94% for blackhole, wormhole, flooding and misrouting attacks respectively. With the time increases the PDR also increased. In the presence of 20 attackers, the total number of packets generated by the source is 3612 and the total number of packets received correctly at the destination is 3549.

In the blackhole and wormhole prevention technique of our previous work shows the PDR is 96% and 99% respectively. The proposed method of the blackhole attack achieves up to 98% of PDR. In the presence of the wormhole, flooding and misrouting attacks the PDR is 99%, 98.8% and 99.5% respectively. Thus in the presence of the misrouting attack higher PDR is achieved than the other attacks.

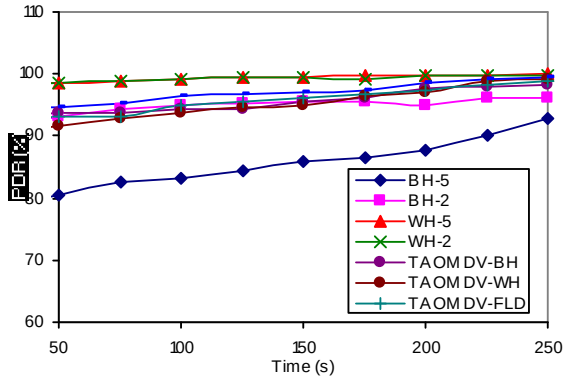


Figure. 4: Packet Delivery Ratio vs Time

The packet overhead is defined as the total number of control packets to the total number of data packets received and the simulation results with respect to the number of attacker is shown in figure 5. The control packets are used for route request, route reply, route error and route update. The control packets are generated when the routes are discovered and selected, and also when any error occurs in the network. While there is no attacker node, then the less number of control packets are generated. When the attacker nodes are increased then the control packets are increased automatically. In [6], it generates up to 3.5 packet overhead whereas in the proposed method, the overhead is 3 in the presence of blackhole attack. In the presence of wormhole, flooding and misrouting attacks, the packet overhead is 3.3, 3 and 2.9 respectively. In the proposed work, in the presence of wormhole attack the packet overhead is high than the other attack and the misrouting attack presents the low packet overhead when compare to other attacks. Thus the proposed method reduces the packet overhead.

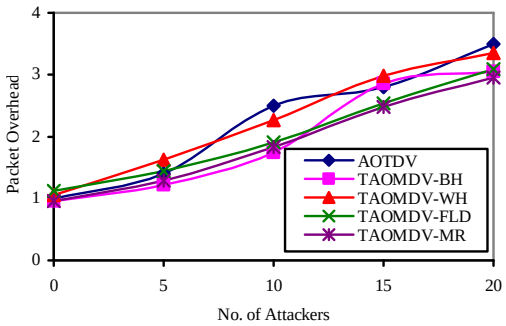
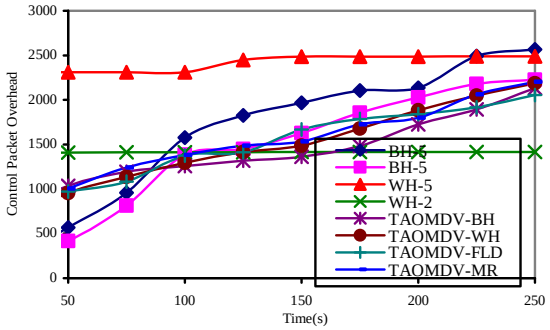


Figure 5: Packet Overhead vs No. of Attacks

Figure 6 shows the control packet overhead with the variation with respect to time. The control packets are used to find the routes to the destination and also used to update the routes if any error occurs. The control packets increase when the simulation time increases. In the previous work of the blackhole and wormhole prevention technique, generated control packets are 2567 and 2488 respectively. The control packets generated in the proposed system for the blackhole and wormhole attacks are up to 2131 and 2187 packets respectively with the increase in the simulation time. The high numbers of control packets are generated in the presence of the misrouting attack and less in the presence of the flooding attack. When compared to our previous work, the proposed scheme generates less number of control packets and reduces the overhead.

Figure 7 shows the throughput of the sent and the received packets with respect to time. Throughput is defined as the average number of packets delivered successfully from source to the destination per unit time.

In our previous work, the throughput is generated up to 69895 and 1785 respectively. With the increase in the simulation time the throughput of the network increases. The throughput achieved is 1677 in the presence of the blackhole attack. In the presence of the flooding attack it achieves high throughput when compared to other attacks present in the network. In the proposed method, the throughput of the network increases slowly but our previous work provides good results



. Figure. 6. Control Packet Overhead vs Time

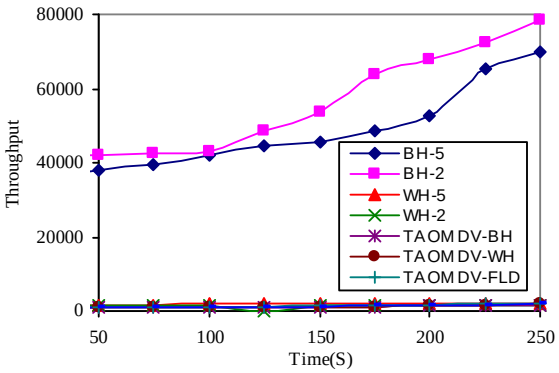


Figure. 7: Throughput vs Time

Figure 8 shows the simulation result of the throughput with respect to number of attackers. When there is less number of attackers the throughput is high and when the attackers increase, the throughput decreases. The throughputs in the presence of blackhole, wormhole, flooding and misrouting attacks are 1496.67, 1057.06, 1364.32 and 1231.33 respectively. In the presence of the blackhole attack the throughput achieves high and when the wormhole attack is present, it has low throughput when compared to other attacks.

End to End delay is the average time taken by the data packets from source node to destination node and also includes the delay in the queue. Figure 9 shows the simulation result of the average end to end delay of packets between the source and the destination with the variation of the number of attackers and the data is shown in Table 9. The delay is low when there is less number of attacks. The average delay increases when there is increase in the attacker node. The highest delay obtained in the proposed method is 0.2074ms for wormhole attack but in [6], the delay of packets to reach the destination is 0.23ms. In [6], average delay of packet is 0.2ms and the proposed system has the delay of 0.15125ms in the presence of 20 blackhole attacker nodes. The delay of the flooding and misrouting attacks in this network is 0.1804ms and 0.1915ms respectively. In the presence of the wormhole attack the average delay of packet is high.

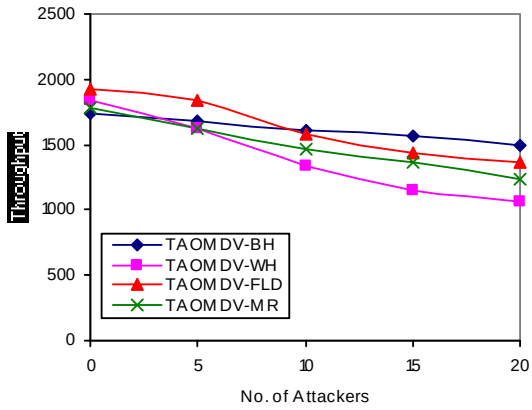


Figure 8: Throughput vs No. of Attacks

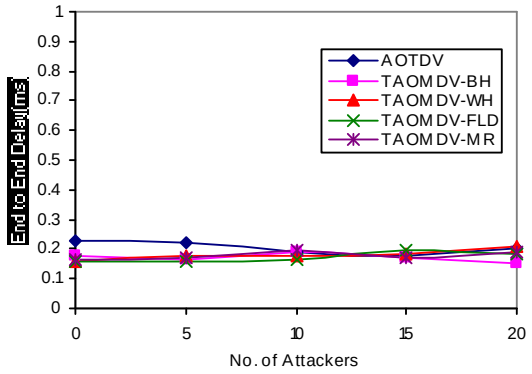


Figure 9: End to End Delay

Detection ratio is the ratio of the number of nodes whose behaviour is identified correctly to the actual total number of nodes in the network. The behaviour is used to detect the normal and the abnormal node. Figure 10 shows the simulation result of the detection ratio with respect to the number of attacker node its data is tabulated in Table 10. The detection ratio declines when there is increase in the number of attacker node.

The detection ratio of the normal node in the proposed method achieves up to 82% whereas in [7], it achieves only up to 75% of the nodes behaviour can be correctly detected and the detection of the blackhole node achieves up to 82% and but in [6], it can detect 81% of the nodes correctly. The detection ratio of the wormhole, flooding and misrouting attacks is 84%, 86% and 87% respectively. Here the detection ratio is high for the misrouting attack and wormhole attack is low in the network.

TAOMDV protocol is able to detect the attacker node in a high ratio. If the malicious node is detected correctly then it will find the other trustworthy path to the destination. The availability of multiple routing entries reduces the delay of packets to reach the destination and also it reduces the control packet overhead. Due to the presence of the alternative routes the PDR and throughput are also improved.

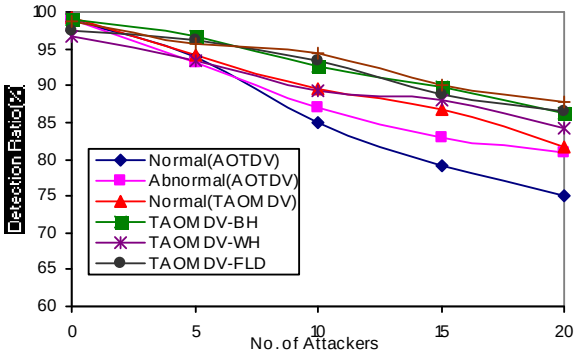


Figure 10: Detection Ratio

Thus the result has been analyzed in two different scenarios such as by varying the number of attacker nodes and simulation time. In the presence of 4 types of attacks, this network performance is analyzed. Thus the simulation results show that the TAOMDV protocol achieves high packet delivery ratio, detection ratio of malicious nodes and reduces the delay of packets to reach the destination, reduces the packet overhead. Also it produces good throughput result.

5. CONCLUSION

A multipath reactive routing protocol TAOMDV is proposed, in this paper, to discover trustworthy forward paths and can prevent the blackhole, wormhole, flooding and misrouting attacks. The highest trusted path is selected to send the data from the source to the destination. Forwarding ratio is used to evaluate a trust value and a continued product of node trusts is used to compute a path trust. A route discovery is started only when all paths become error or does not meet the trust requirements of data packets. Using this it is able to protect the network effectively against the different attacks. The above said attacks are prevented, by the TAOMDV, using passive acknowledgement to monitor the neighbour node. The simulation result shows that the throughput is achieved little lower since there is more number of attacks in the network. However, TAOMDV protocol achieves high PDR, reduces the packet overhead and also average end to end delay of packet is reduced. It also has the high detection ratio of the attack node. This work achieved good results and provides multipath routing.

REFERENCES

1. Chouhan N. S. and Yadav S., **Flooding Attacks Prevention in MANET**, International Journal of Computer Technology and Electronics Engineering (IJCTEE), vol. 1, no. 3, pp. 68-72, 2011.
2. Khabbazian M., Mercier H. and Bhargava V. K., Severity **Analysis and Countermeasure for the Wormhole Attack in Wireless Ad Hoc Networks**, IEEE Transactions on Wireless Communications, vol. 8, no. 2, pp. 736-745, 2009. https://doi.org/10.1109/TWC.2009.070536
3. Khalil I. and Bagchi S., **Stealthy Attacks in Wireless Ad Hoc Networks: Detection and Countermeasure**, IEEE Transactions on Mobile Computing, vol.10, no. 8, pp. 1096-1112, 2011. https://doi.org/10.1109/TMC.2010.249
4. Kim H., Chitti R. B, and Song J., **Novel Defense Mechanism against Data Flooding Attacks in Wireless Ad Hoc Networks**, IEEE Transactions on Consumer Electronics, vol. 56, no. 2, pp. 579-582, May. 2010.
5. Kurosawa S., Nakayama H., Kato N., and et. al, **Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method**, International Journal of Network Security, vol. 5, no. 3, pp. 338-346, Nov. 2007.
6. Li X., Jia Z., Zhang P., and et. al, **Trust-based on-demand multipath routing in mobile ad hoc networks**, IET Information Security, vol. 4, no. 4, pp. 212-232, Apr. 2010. https://doi.org/10.1049/iet-ifs.2009.0140
7. Marinam K. and Das S.R., **On-demand multipath distance vector routing for ad hoc networks**, Proc. Int. Conf. on Network Protocols, Riverside, CA, USA., pp. 14-23, Nov. 2001.
8. Nait-Abdesselam F., Bensaou B., and Taleb T., **Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Networks**, IEEE Communication Magazine, vol. 46, no. 4, pp. 127-133, 2008.
9. Pirzada A. A. and McDonald C., **Detecting and Evading Wormholes in Mobile Ad-hoc Wireless Networks**, International Journal of Network Security, vol. 3, no. 2, pp. 191-202, Sep. 2006.
10. Pirzada A.A. and Mcdonald C., **Trust Establishment in Pure Ad-hoc Networks**, International Journal on Wireless Personal Communications, vol. 37, no. 1, pp. 139-168, 2006. https://doi.org/10.1007/s11277-006-1574-5
11. Ramana K. S., Chari A. A. and Kasiviswanth N., **A Survey on Trust Management for Mobile Ad Hoc Networks**, International Journal of Network Security & Its Applications (IJNSA), vol. 2, no. 2, pp. 75-85, Apr. 2010.
12. Saini A. and Kumar H., **Effect of Black Hole Attack On AODV Routing Protocol In MANET**, International Journal of Computer Science and Technology, vol. 1, no. 2, pp. 57-60, Dec. 2010.
13. Shandilya S. K. and Sahu S., **A Trust Based Security Scheme for RREQ Flooding Attack in MANET**, International Journal of Computer Applications, vol. 5, no. 12, pp. 4-8, Aug. 2010.
14. Tandan S. and Saurabh P., **A PDRR based detection technique for blackhole attack in MANET**, International Journal of Computer Science and Information Technologies, vol. 2, no. 4, pp. 1513-1516, 2011.
15. Umang S., Reddy B. V. R and Hoda M. N, **Enhanced intrusion detection system for malicious node detection in ad hoc routing protocols using minimal energy consumption**, IET Communication, vol. 4, no. 17, pp. 2084–2094, Jun. 2010. https://doi.org/10.1049/iet-com.2009.0616

16. Vani A. and Rao S. D., **Providing of Secure Routing against Attacks in MANETs**, International Journal of Computer Applications, vol. 24, no. 8, pp. 16-25, 2011.
17. Vishnu K. and Paul A. J., **Detection and Removal of Cooperative Black/Gray hole attack in Mobile AdHoc Networks**, International Journal of Computer Applications, vol. 1, no. 22, pp. 38-42, 2010.
18. Wang K. and Wu M., **Cooperative communications based on trust model for mobile ad hoc networks**, IET Information Security, vol. 4, no. 2, pp. 68–79, 2010.
19. Xing F. and Wang W., **On the Survivability of Wireless Ad Hoc Networks with Node Misbehaviors and Failures**, IEEE Transactions on Dependable and Secure Computing, vol. 7, no. 3, pp. 284-299, 2010. https://doi.org/10.1109/TDSC.2008.71
20. Yu M., Zhou M. and Su W., **A Secure Routing Protocol against Byzantine Attacks for MANETs in Adversarial Environments**, IEEE Transactions on Vehicular Technology, vol. 58, no. 1, pp. 449-460, 2009.
21. Lei Xu, Nengqiang He, Zhu Han and Abderrahim Benslimane, **Trust-Based Collaborative Privacy management in Online Social Networks**, IEEE Transactions on Information Forensics and Security, Vol. 14, No. 1, January 2019.
22. Jun Du and et al., **Peer Prediction-Based Trustworthiness Evaluation and Trustworthy Service Rating in Social Networks**, IEEE Transactions on Information Forensics and Security, Vol. 14, No. 6, June 2019. https://doi.org/10.1109/TIFS.2018.2883000
23. S. Sundeep Desai and Manisha J. Nene, **Node-Level Trust Evaluation in Wireless Sensor Networks**, IEEE Transactions on Information Forensics and Security, Vol. 14, No. 8, August 2019. https://doi.org/10.1109/TIFS.2019.2894027