Trust Based Secure On-Demand Multipath Routing Scheme in MANET

Hetal Gevariya[1], Dhaval Parikh[2]

[1]*Student, Computer Department, L D College of Engineering, Ahmedabad, Gujarat, India*
[2]*Associate Professor, Computer Department, L D College of Engineering, Ahmedabad, Gujarat, India*

Abstract*— Mobile Ad-hoc Network (MANET) of wireless nodes is a temporarily formed network, created, operated and managed by the nodes themselves. It is also often termed as an infrastructure-less or self-organized network. Nodes assist each other by passing data and control packets from one node to another, often beyond the wireless range of the original sender. The execution and survival of an ad-hoc network is solely dependent upon the cooperative and trusting nature of its nodes. However, this naïve dependency on the intermediate nodes makes the ad-hoc network vulnerable to passive and active attacks by the malicious nodes. Generally cryptographic mechanisms are used in the routing protocols to secure the routing information from tampering it by the attacker, but this approach can't be deployed in real MANET network because of high computational cost and it can't identify the attacker nodes. Recently many trust-based routing protocols have been introduced but each has its own advantages and disadvantages. In MANETs, trust is a challenging task and it is imperative for the nodes to work in a trusted and cooperative way. We propose a trust- based secure on-demand multipath routing scheme which considers the behaviour of nodes and computes trust and accordingly sets the trustworthiness of the nodes in an ad- hoc network to decrease the hazards from malicious nodes. Our propose scheme considers two parameters for computing the trust which are control packet forwarding ratio and data packet forwarding ratio. The primary goal of our proposed scheme is to mitigate nodes performing packet dropping and maximizes Packet Delivery Ratio, Throughput and minimizes End-to-End Delay performance parameters. Performance comparison of S_AOMDV and exist AOMDV shows that S_AOMDV is able to achieve a remarkable improvement in packet delivery ratio, throughput, end-to-end delay parameters and to reduce black-hole attack.

I. INTRODUCTION

The recent trends in wireless communications have changed the lives of the human beings. The new wireless technologies create a tremendous potential for the next generation Mobile Ad-hoc Networks (MANETs) and applications. The arrival of wireless technologies such as Bluetooth and Wi-Fi increases the scope of the ad hoc networking and enables potential applications in the personal and local area networking, Military battlefield scenarios. Due to the ubiquitous handling, it is a challenging task to attain proficient wireless intercommunication over mobile devices. The MANET is a multi-hop distributed communication network comprising of a collection of mobile nodes that operate in a dynamic and self organized manner [1]. The network connectivity changes dynamically due to the random mobility of mobile nodes in the absence of access point or any predefined infrastructure. Each mobile node performs the data forwarding only through single or multi-hop communication due to the limited transmission range [2] [3]. The design of routing protocols is used to find a suitable path to route the data packet from the source to the destination. The routing process has to evolve efficiently and enhance the efficiency of the routing process in the presence of dynamic network conditions, unpredictable mobility, limited energy, autonomous architecture, and resource constrained environment. The short communication range and lack of infrastructure are the major reasons for collaborative communication model. In a MANET, the mobile node forming dynamic network topology and the nodes located within the transmission range of a node are called neighbors. The neighbors transmit the data packets directly to the other nodes within the communications range. However, a node transmits the data through a sequence of multiple hops, with intermediate nodes, when it wants to send the data packet to a non-neighboring node or a distant node [2]. The diversity of potential applications in the MANET promotes a broad range of routing protocols to fulfill the requirements. The major focus of the routing is the performance and the efficiency of the protocol in the presence of a dynamic network environment. The routing protocol has to overcome the security pitfalls to utilize the potentials of the MANET. A secure routing is challenging due to the security vulnerabilities present in the network.

The structure of the paper is organized as follows: section 2 presents the various proposed techniques describing the related work of preventing and detecting the black hole attack related work. Section 3 discussed about need for security. Section 4 presents the problem statement. Section 5 discussed about proposed work. Section 6 presents the performance evaluation. Finally, concluded in last section with future work.

II. RELATED WORK

Jyoti Rani et al. (2013) [3] present improving AOMDV protocol for blackhole detection. They did modification in RREQ and RREP. They have implement a legitimacy table which contains field named selection and success. One more additional packet used in this approach which is route change

packet. They also did modification in routing table for better performance MANET.

Biswas et al. (2014) [4] proposed a solution for detect and prevent blackhole attacks for both single and co-operative nodes with ensuring secure packet transmission. In the network each node have three parameter for checking its trust

(1) Rank, (2) Remaining Battery power and (3) Stability factor. If the rank of the node is falls 0 then consider it as blackhole node. This proposed scheme applied after route discovery phase and minimum rank consideration is 1.

K.Selvavinayaki et.al (2015) [5] presents the security oriented solution to prevent the black hole attack using the digital certificates to authenticate the routes selected during the route discovery process.

Muhammad Imran et.al (2015) [6] proposed a Detection and Prevention System (DPS) to detect black hole attack in MANETs. It works on the basic principle that, "the black hole node never broadcasts route requests as compared to the normal nodes". This detection and prevention system has three different types of nodes, Normal Nodes, Malicious (Black hole) Nodes and DPS Nodes.

Sumaiya Vhora et.al (2015) [7] proposed a solution based on Rank Based Data Routing (RBDR) record to identify malicious behavior in network. The RBDR is created with field of routing details to analysis the behavior of network for detecting the malicious paths. After getting RREPs from all possible path, a source again propagate RREQ with a higher number of destination sequence number that is greater than all received destination sequence number. If any route claims greater value than previous destination sequence number, then it is clear that particular route having malicious node. According to lower hop count and constant unchanged destination sequence number assign ranks to every route which is in RBDR record.

Abrar Omar Alkhamisi et.al (2016) [8] proposed a protocol in which the IDS attached with each node, performs packet forwarding statistics of the neighbors during the data forwarding phase and then measured statistics is incorporated into trust values for selecting the most trusted path to improve the performance of TS-AOMDV.

III. NEED FOR SECURITY IN ROUTING PROTOCOLS

The node co-operation is an essential requirement in multi-hop routing. The non-co-operation of nodes leads to selfish and malicious behavior resulting in routing attacks. The misbehaving nodes drop some of the packets or all the other packets passing through it. The lack of centralized administration and resource constraint is the key issue that causes dishonest and non-co-operative nodes. Therefore, MANET is vulnerable to serious attacks [10][11][12][13]. Some of the usual routing attacks are a wormhole, black hole, grey hole, and rushing attack [9][14][15]. The MANET needs to provide reliable and secure routing over mission-critical environments like healthcare and military applications. When the attackers interrupt the routing services and the flow of information, the observation and determination of critical activities, i.e., in an incident of enemy tracking and a case of heart attack jeopardize human lives. Moreover, this kind of applications forward the most sensitive information among soldiers or patients, and it is paramount to protect the information from unauthorized parties. Due to lack of infrastructure, security in MANET is a challenging task, especially in multipath MANET [16]. The availability ensures the possibility of service access at any time and the network needs to provide a reliable service that guarantees the data delivery even in the face of attacks. The requirements of resilience and self-healing are interrelated to the availability. The term resilience refers to attack tolerance and ability to offer continuously uninterrupted services to the users even in the presence of attacks. The self-healing is the capability to recover the network from security threats and to isolate the source of the attack. The usage of single path routing is highly vulnerable to the security threats because it easily compromises with the requirement security factors such as availability, reliability, resilience, and reliability of the service over MANET[17][18][19]. An attack can easily prevent data forwarding by breaking the wireless links among any mobile nodes located in the routing path, and the destination does not continuously receive the packets as the data packets are sent over a single path between source and destination. The conventional routing techniques initiate the route discovery phase to determine new routes to the destination from the source in case of route failure. However, this is a time and energy consuming problem over a battery constrained mobile nodes in MANET. It is unacceptable in mission-critical applications because they are required to monitor the environment continuously for supporting the timely decision making. Owing to the availability of disjoint paths, the multipath routing protocol is resilient to routing attacks compared to single path routing.

IV. PROBLEM STATEMENT

The MANET needs to provide a reliable and secure routing over mission-critical environments like healthcare and military applications. Several routing techniques have been proposed in the mobile ad-hoc networks. These protocols work well in benign environments, where the mobile nodes are highly trusted. Therefore, it is necessary to modify these protocols substantially if they are used in a hostile network environment. The MANET maximizes throughput by using all available nodes for routing and forwarding. Stimulating cooperation among the nodes in the network is the one of the key issues in MANETs. It makes use of all nodes in the network for broadcasting and routing if nodes are co-operative and well behaving. The major challenge in designing such a self- organized network is the detection of the routing attacks. The steady increase of attacking nodes will severely degrade the routing

performance. The attacking nodes must be detected and eliminated effectively to improve the performance of the network. Another important problem of wireless communication over infrastructure-less networks is the unpredictable node mobility. The node mobility leads to frequent link failures in single path routing, resulting in poor network throughput. Thus, to balance the network throughput and reliable data delivery, it is essential to incorporate multipath routing and an efficient trust evaluation model in hostile environments. The security issues in multipath routing are not considered in the conventional routing techniques. In other words, the existing multipath routing protocols are not designed with the aim of provisioning security in mind [14]. The most important factors to include in the security provision are the availability, reliability, resiliency, and self-healing. Have a trusted path in multipath routing which prevents black hole attack is a challenge.

V. THE PROPOSE ARCHITECTURE

The proposed S_AOMDV aims to identify and isolate the black hole attack in a MANET. With the aid of a trust-based routing, the attack identification and isolation are carried out. The sender places itself in promiscuous mode after the transmission of any packet so as to overhear the retransmission by the forwarding node. Using this method, a node can know whether the packet which has been sent to a neighbor for forwarding is indeed forwarded or not. Each node derives trust value from packet forwarding ratio. During trust computation, a weighted sum method is used to estimate the overall trust in a node according to trust factors, and a minimal value method is used to compute a path's trust. Trust application including trust-based route discovery and route selection like in ad-hoc networks on battlefield or business applications or many more.

In this area, we presented the choice of most secure and reliable route by establishing the trust between the nodes. We have carried out two mechanisms as: Trust model and Trust-based secure on-demand multipath routing protocol.

1. Trust Model

The trust model essentially performs the function of trust derivation, computation, and application. In our model, each node derives trust value from packet forwarding ratio. During trust computation, a weighted sum method is used to estimate the overall trust in a node according to trust factors, and a minimal value method is used to compute a path's trust. Trust application including trust-based route discovery and route selection like in ad-hoc networks on battlefield or business applications or many more.

A. Trust Derivation

No matter what kind of trust models, two types of evolutions, direct trust and indirect trust, are available. Direct trust is first- hand information for neighbors and easy to obtain. In order to simplify trust model, we only use the history of direct interactions among nodes to compute trust. Packet dropping is always due to poor wireless communication quality or heavy traffic or black-hole attack or gray-hole attack. Thus we use packet forwarding ratio to evaluate the quality of forwarding.

Packet Forwarding Ratio (*FR*) is the ratio between the forwarded packets count and the received packets count.

In MANETs, packets can be classified into two groups: control packets and data packets. The accuracy of control packets plays a vital role in establishment of accurate routes throughout the network. So packet forwarding ratio is divided into two parts: Control packet Forwarding Ratio (CFR) and Data packet Forwarding Ratio (DFR).

B. Node's Trust Computation

The trust of a node *j* to another node *k* is a measure of ensuring that packets which have been sent to node *k* by node *j* for forwarding have actually been forwarded by node *k*. Trust values from the two trust factors (CFR and DFR) are assigned weights in order to determine the overall trust level for a particular node. The direct trust of node *k* by node *j* is represented as T_{JK} and is given by the following equation:

$$T_{JK}(t_i) = w1 \times (\textit{No. of RREQ forwarded/No. of RREQ received})_{JK} + w2 \times (\textit{No. of DP forwarded/No. of DP Received})_{JK}(t_i)$$

(Where $0 < w1$ and $w2 < 1$ and $w1 + w2 = 1$)

Here w1 and w2 represent the weight factors. The parameters *w*1 and *w*2 reflect the weights assigned to *(No. of RREQ forwarded/No. of RREQ received*) and (*No. of DP forwarded/No. of DP Received*), represent the control packet forwarding ratio and data packet forwarding ratio respectively observed by node *j* for forwarding node *k* at time t_i. Initially we take value of w1 as 0.3 and w2 as 0.7 and threshold value as 0.7 for trust calculation.

Table 1 Trust levels of nodes

Level	Trust Value	Meaning
1	T < 0.7	Malicious
2	T >= 0.7	Trustworthy

In our trust model, trust values are limited in a continuous range from 0 to 1. A trust value of 0 signifies complete distrust while a value of 1 implies absolute trust. The trust levels of nodes are listed in Table 1.

The sender places itself in promiscuous mode after the transmission of any packet so as to overhear the retransmission by the forwarding node. Using this method, a node can know whether the packet which has been sent to a neighbor for forwarding is indeed forwarded or not.

C. Path's Trust Computation

When a source discovers a path to the destination with the help of forwarding nodes, the trust value of the path is able to be computed through the trust values of nodes among the path.

The trust of a path *P* (denoted by *TP (ti))* is equal to the minimal one of the node's values in the path like,

$$TP(t_i) = \min(\{T_{jk}(t_i) n_j, n_k \in P \text{ and } n_j \rightarrow n_k\})$$

Where nj and nk are any two adjacent nodes among the path *P* and nj → nk means that nk *is* the next-hop node of node nj.

2. Trust-based secure on-demand Multipath Routing Protocol

We describe on-demand routing mechanism for ad-hoc network based on proposed trust model. The progressions of most incipient scheme is characterizes as underneath. At first, the structures of routing table and trust record list are depicted. Then, the procedures of route discovery and routing maintain are discussed. Finally a sequence number method is presented to avoid the routing loop.

A. Routing Table

Routing table stores the routes to various nodes in an ad-hoc network. Each node maintains a route table composed of multiple routing entries. AOMDV adopts hop-by-hop routing mechanism, in which the source is not expected to have all the information about how to get to the destination; it is sufficient for the source to know only how to get to the next hop. So when a data packet is going to a particular node, it then refers to local routing table to find the address of next hop (named node *j*) to the destination. Once it reaches the node *j*, it again refers to the *j*'s routing table for the address of next hop and so on, until it reaches the final destination.

The routing table in any node *j*, only stores the destinations' routes and reverse routes to the sources interacted with node *j* recently, not all nodes' route in history. This is because the topology of MANET changes dynamically, i.e., the mobile nodes might join or quit the network for some reasons.

Table 2 Structure of routing table entry

Destination node IP address
Sequence Number
Expiration Time
Route List { (NextHop1, HopCount1, PathTrust1), (NextHop2, HopCount2, PathTrust2), (NextHop3, HopCount3, PathTrust3) …}

B. Trust Record List

To remember trust information, we introduce a trust table. Each node will also maintain a trust record for every neighbor which has been sent packets to for forwarding.

Table 3: Structure of a trust table

Node ID
RREQR and RREQF for control packets
DPR and DPF for data packets
Trust

A trust record listed in Table 3 comprises a node ID, two counters for control packets, two counters for data packets and a trust value of that node.

C. Route Strategy

As shown in Figure 1, the overall procedure of proposed S_AOMDV routing is given as follows:

(1) Initialize all neighbor nodes trust value with 1 initially.

(2) Initialize time and RREQF, RREQR, DPF and DPR of all neighbor nodes as 0 initially.

(3) All the nodes are connected in MANET.

(4) When a source node s wants to send a data packet to another node d, then the source node s first tries to look up destination d in its route table. If no such route, it will initiate a route discovery for d and update RREQR and RREQF for the neighbor nodes. If one or more paths to the destination are found after the on-demand route discovery, all paths information will be inserted into the route table.

(5) Node s selects a trusted route to the destination d with the greater path trust value and then node s sends the data packets to node n.

(6) After sending, s overhears the channel and checks whether the data packet will be forwarded or dropped by that next hop n and update DPR and DPF according to that.

(7) After data forwarding process, if the time is equal to session time then all the nodes update their neighbor node's trust value based on TJK(ti)= w1×(RREQF/RREQR)JK (ti) + w2 ×(DPF/DFR)JK (ti) observation.

(8) If the trust value of neighbor node is less than threshold then that node can be detected as malicious node otherwise the node is trusted node.

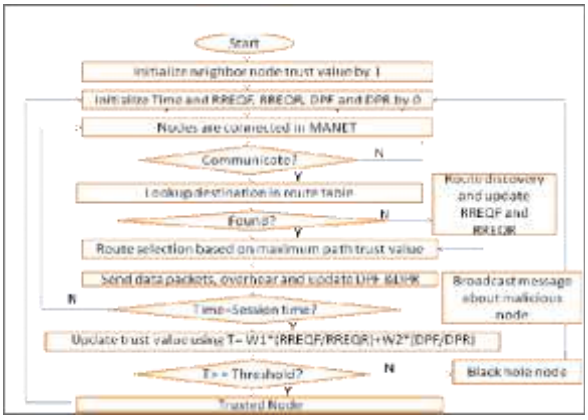

Figure 1: Proposed workflow

If one neighbor's trust value is lower than a threshold, then it will be regarded as a malicious node, and then deleted from the neighbor set, finally added into the black list. That is, it will be ultimately denied by the whole network.

The proposed S_AOMDV is a multipath on-demand routing protocol, which tries to alleviate route discovery attempts in

dynamic networks by computing multiple paths in a single route discovery round. Multiple paths could be formed at both source node and intermediate nodes. New route discovery is needed only when all paths break or fail. Multiple paths can also be used to balance load by forwarding data packets on multiple paths at same time.

D. Route discovery and Path Selection

The route discovery process is initiated whenever a source node *s* needs to communicate with another node *d* for which nodes has no routing information in its routing table. Every node maintains two independent counters: a node sequence number and a broadcast ID. The source node initiates a network-wide flood by broadcasting a route request (RREQ) packet and waits for a route reply (RREP) packet.

1) Route Request

A RREQ packet contains the following fields:

<BroadcastID, SourceAddr, SourceSequenceNo, DestAddr, DestSequenceNo, HopCounter, PathTrust>

The *PathTrust* denotes the minimal one of trust values of nodes that the RREQ has passed by during the route discovery process. And it is initialized to 1 by the source. During the flood, *PathTrust* varies with the transmission of RREQ packet.

2) Route Reply

The intermediate node can reply only when it has a route with a sequence number that is greater than or equal to that contained in the RREQ. If it does have a fresh route to the destination, and if the RREQ has not been processed previously, the node unicast a route reply (RREP) packet back to its neighbor from which it received the RREQ. A RREP packet contains the following information:

<SourceAddr, SourceSequenceNo, DestAddr, DestSequenceNo, HopCounter, LifeTime, PathTrust>

The PathTrust have same meaning to the ones in RREQ. The Path*Trust in* RREP denotes the minimal one of trust values of nodes that the RREP passed by during route reply. And it is initialized to 1 by the destination. If an intermediate node receives a RREQ from a neighbor, and if it has multiple paths to the destination, it will reply two copy of RREP, in which one has the smallest hop count and the other has the greatest trust value. If the destination receives multiple copies of RREQ, it will reply the first *k* trusted paths at most. After a RREQ packet arrives at a node, a reverse path is established to the source of the RREQ. The RREP travels back to the source, each node along the path sets up a forwarding route to the destination from which the RREP came, updates its timeout information for route entries to the source and destination, and records the latest destination sequence number for the requested destination. The parameter *k* is used to control the number of RREPs and to prevent a RREP storm.

3) Route Maintenance and Loop Freedom

The route maintenance in proposed S_AOMDV is similar to that in AOMDV, i.e., nodes maintain and update route table when receiving a RREQ, RREP or route error (RERR) packet. When a link failure is detected (by a link layer feedback, for example), a RERR is send back to all sources using that failed link via separately maintained predecessor links. Routes are erased by the RERR along its way. When a node receives a RERR, it initiates a new route discovery to fix the link if the route is still needed. Unused routes in the routing table are expired using a timer-based technique.

VI. PERFORMANCE EVALUATION

The Proposed protocol is resistant to black hole attack. The performance of the S_AOMDV protocol is evaluated using Network Simulator (NS2) in terms of packet delivery ratio, throughput and end to end delay.

A. Experimental Setup

NS-2 simulator was used to evaluate the performance of routing protocols in different conditions. The Distributed Coordination Function (DCF) of IEEE 802.11 for wireless LANs is used as the MAC layer protocol. An UDP is used to transmit the data packets and route packets. The trust threshold is set to 0.7, which means the node with trust value less than 0.7 will be regarded as a malicious node and added into the black list. That is, packet forwarding ratio is computed by the count of forwarding packets and the received packets. The transmission radius of every node in one hop is fixed at 150m.The node mobility uses the random waypoint model in which each packet starts its journey from a random location to a random destination with a randomly chosen speed. These fixed simulation parameters are listed in Table 4.

Table 4: Simulation Parameters

Parameters	Values
Simulator	Network Simulator 2.35
Topology	Random
Interface Type	Phy / WirelessPhy
Mac Type	IEEE 802.11
Queue Type	Droptail/Priority Queue
Queue Length	50 Packets
Antenna Type	Omni Antenna
Propagation Type	Two Ray Ground
Routing Protocol	AOMDV, S_AOMDV
Transport Agent	UDP
Application Agent	CBR
Network Area	500 * 500
Number Of Nodes	50,75,100
Mobility	10 m/s
Number Of Attackers	1,2,3
Number Of Connections	2,4,6

Weight w1 and w2	0.3 and 0.7
Simulation Time	40 seconds

B. Performance Metrics

The metrics such as packet delivery ratio and End-to-End delay are evaluated in the scenarios of varying number of nodes.

1) *Packet delivery ratio*: The fraction of the data packets received at the destination nodes to the data packets sent successfully by the source nodes is called packet delivery ratio (PDR).

PDR =∑ Number of packet receive / ∑ Number of packet sent

2) *End-to-End delay:* It measure the average delay time that is taken by the data packets from sources to destinations, including buffering delays during route discovery, queuing at the interface queue, retransmission delays at MAC layer and propagation time.

End to End Delay =∑ (Arrive time – Send time) / ∑ (No of connection)

3) *Throughput:* It refers to the total number of packets sent over one a second's time.

Throughput is sum of sizes (bits) or number (packets) of generated / sent/ forwarded/ received packets calculated at every time interval and divided by its length. Throughput (bits) is shown in bits. Throughput (packets) shows numbers of packets in every time interval. Time interval length is equal to one second by default.

Throughput= ∑ Number of packet sent successfully / time (second)

C. Experimental Results

The Simulation has been carried out in two aspects. In the first aspect, the algorithm is simulated by modifying the number of nodes. In the Second aspect the simulation is carried out by modifying the number of the attacker nodes.

Test 1: By Varying Number of nodes

The network varies the number of nodes from 50 to 75 to 100 with one attacker node and to study the impact of the network size on routing attack detection of S-AOMDV. The communication range assigned to the nodes is 150m. We generated the graph based on our simulation result. The graph is given below:

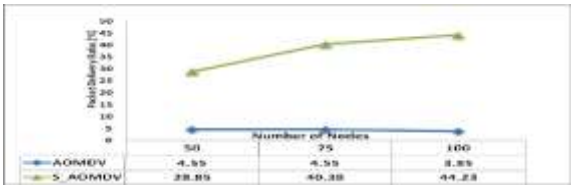

Figure 2: PDR vs. Number of nodes (under 1 attacker node)

Figure 2 illustrates the comparison of PDR with reference to number of nodes. The proposed S_AOMDV protocol provides high packet delivery ratio due to the fact that the data packets are transmitted only through the secured and reliable route. The security scheme obstruct the attacker activities and provide attacker free network. The packets successful transmission is improves the performance of network besides that the packet dropping is degrades the performance of network. The routing misbehavior through black hole attack is degrades the percentage of data receiving in node densities. The attacker is consuming whole data packets that are not forwarded to destination after positive route reply. The attacker has drop the most of the data packets by that the routing performance of AOMDV routing is degrades. The proposed security scheme improves the PDR performance in presence of attacker.

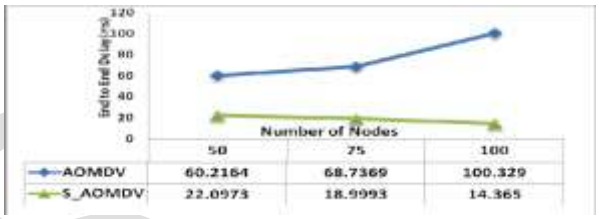

Figure 3: End-to-End Delay vs. Number of nodes (under 1 attacker node)

Figure 3 shows the comparison of End-to-End Delay with reference to number of nodes. The average end- to-end delay varies with reference to the number of nodes. As we start increasing the number of nodes, more number of control packets is transmitted to discover the routes. On-demand routing opposed to proactive routing is naturally adaptive to traffic diversity and therefore its end-to-end delay proportionately increases with increase in traffic diversity. So when the traffic diversity is low, on demand routing is relatively very efficient in terms of the control overhead regardless of relative node mobility.

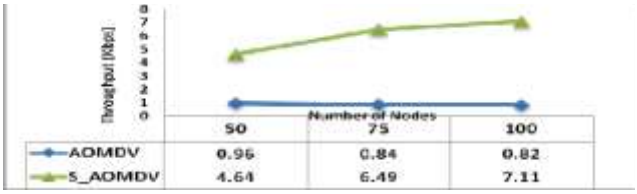

Figure 4: Throughput vs. Number of nodes (under 1 attacker node)

Figure 4 illustrates the graph of Throughput vs. Number of Nodes. The proposed S_AOMDV protocol provides high throughput due to the fact that the data packets are transmitted only through the secured and reliable route. The proposed security scheme improves the throughput in presence of attacker.

Test 2: By Varying Number of Attacker nodes

To evaluate the results; simulation is done with 75 nodes and by varying the number of malicious nodes from one to two and three malicious nodes respectively. In test 2, we evaluate the effects on these protocols under varying number of malicious nodes.

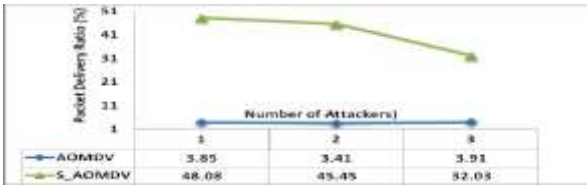

Figure 5: PDR vs. Number of attackers (No. of node: 75)

Figure 5 illustrates the comparison of PDR with respect to the number of attackers. The packet delivery ratio of protocols degrades sharply as malicious nodes increase. Lower packet delivery ratio means less network throughput. Malicious nodes essentially limit the interactions of nodes in the network. However, in S_AOMDV, intermediary nodes have several trusted routes to a destination so that when detecting black hole attacks, it can try alternate route to forward packets and thus improve the packet delivery ratio.

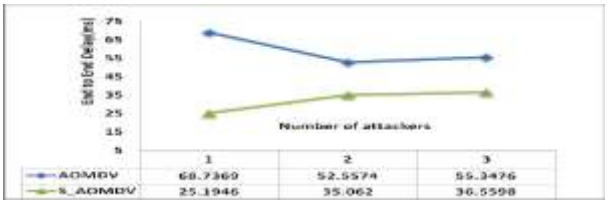

Figure 6: End-to-End Delay vs. Number of attackers (No of node: 75)

Figure 6 shows the comparison of Average End-to-End Delay with reference to number of attackers. As shown in Figure, the end-to-end delay of all protocols increases sharply as malicious nodes increase. Malicious nodes essentially limit the interactions of nodes in the network. However, in S_AOMDV, intermediary nodes have several trusted routes to a destination so that when detecting black hole attacks, they can try alternate route to forward packets and thus improve the end- to-end delay.

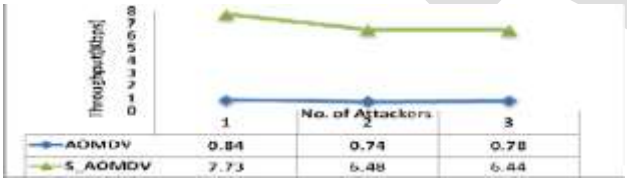

Figure 7: Throughput vs. Number of attackers (No of node: 75)

Figure 7 represents graph of Throughput vs. Number of Attackers. As shown in Figure, the throughput of all protocols degrades sharply as malicious nodes increase. Malicious nodes essentially limit the interactions of nodes in the network. However, in S_AOMDV, intermediary nodes have several trusted routes to a destination so that when detecting black hole attacks, they can try alternate route to forward packets and thus improve the throughput.

VII. CONCLUSION

In this research, a Trust-based Secured On-demand Multipath Distance Vector, S_AOMDV was clearly designed to achieve security in MANET. We have described a simple trust model based on packet forwarding ratio to evaluate neighbor's behaviors. Combined with the model, a multipath reactive routing protocol S_AOMDV is proposed to discover trustworthy forward paths and alleviate the black hole attack. In this protocol, a source can find multiple trusted paths to a destination in a single route discovery round. New route discovery is needed only when all paths break or fail to meet the trust requirement. Multiple paths can also be used to balance load by forwarding data packets on multiple paths at same time. Performance comparison of AOMDV and S_AOMDV routing protocols shows that S_AOMDV is able to achieve a remarkable improvement in the packet delivery ratio, Throughput, End to End delay and prevent most malicious black hole attack.

For future work, we plan to extend our trust model to other ad hoc network routing protocols like DSR, DSDV and TORA. We will also conduct a comprehensive performance evaluation to compare S_AOMDV with other trust-based routing protocols.

REFERENCES

[1]. Erciyes, K. "Distributed Graph Algorithms for Computer Networks", *Computer Communications and Networks*, London: Springer, pp. 259-275, 2013.

[2]. S. Abdel Hamid, H. Hassanein and G. Takahara, "Routing for Wireless Multi-Hop Networks: Unifying Features", *SpringerBriefs in Computer Science*, pp. 11-23, 2013.

[3]. Jyoti Rani, Naresh Kumar, "Improving AOMDV Protocol for Black Hole Detection in Mobile Ad hoc Network" International Conference on Control, Computing, Communication and Materials (ICCCCM), 2013.

[4]. Suparna Biswas, Tanumoy Nag, Sarmistha Neog, "Trust Based Energy Efficient Detection and Avoidance of Black Hole Attack to Ensure Secure Routing in MANET", Application and innovations in Mobile computing, 2014.

[5]. Selvavinayaki, K., Shankar, K. K. S., & Karthikeyan, E. (2010). Security Enhanced AOMDV Protocol to Prevent Black Hole Attack in MANET, International Journal of Engineering and Technology (IJET), Vol 6 No 6 Dec 2014-Jan 2015.

[6]. Muhammad Imran, Farrukh Aslam Khan (&), Haider Abbas and Mohsin Iftikhar, "Detection and Prevention of Black Hole Attacks in Mobile Ad hoc Networks", Springer-Verlag Berlin Heidelberg 2015, DOI: 10.1007/978-3- 662-46338-3_10

[7]. Sumaiya Vhora, Rajan Patel, Nimisha Patel, "Rank Base Data Routing (RBDR) Scheme using AOMDV: A Proposed Scheme for Packet Drop Attack Detection and Prevention in MANET", 978-1-4799-608S-9, IEEE (2015)

[8]. Abrar Omar, Alkhamisi, Seyed M Buhari, "Trusted Secure Adhoc On- demand Multipath Distance Vector Routing in MANET", *2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)*, 212–219. http://doi.org/10.1109/AINA.2016.105

[9]. Hamid, S. A., Hassanein, H., & Takahara, G., "Routing for Wireless Multi Hop Networks–Unifying and Distinguishing Features", School of Comp.— Queen's University, Canada, report 583, 2011.

[10]. Habib, S., Saleem, S., & Saqib, K. M., "Review on MANET routing protocols and challenges", *IEEE Student Conference on Research and Development SCOReD*, pp. 529-533, 2013.

[11]. A. Ahmed, K. Abu Bakar, M. Channa, K. Haseeb and A. Khan, "A survey on trust based detection and isolation of malicious nodes in adhoc and sensor networks", *Frontiers of Computer Science*, vol. 9, no. 2, pp. 280-296, 2015.

[12]. I. Abdel-Halim, H. Fahmy and A. Bahaa-Eldin, "Agent-based trusted on- demand routing protocol for mobile ad-hoc networks", *Wireless Netw*, vol. 21, no. 2, pp. 467-483, 2015.

[13]. Mahmoud, Mohamed MEA, and Xuemin Sherman Shen.

"Secure routing protocols." *Security for Multi-hop Wireless Networks. Springer International Publishing*, pp. 63-93, 2014.

[14]. Shanmuganathan, V., and T. Anand. "A Survey on Gray Hole Attack in MANET." *IRACST–International Journal of Computer Networks and Wireless Communications (IJCNWC)*, pp. 2250-3501, 2012.

[15]. Tayal, S., & Gupta, V., "A Survey of Attacks on Manet Routing Protocols", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 2, No.6, pp. 2280-2285, 2013.

[16]. Vaidya, Binod, et al. "Secure multipath routing scheme for mobile ad hoc network." *Third IEEE International Symposium on Dependable, Autonomic and Secure Computing*, pp. 163-171, 2007

[17]. C. Tachtatzis and D. Harle, "Performance evaluation of multi-path and single-path routing protocols for mobile ad-hoc networks", *Performance Evaluation of Computer and Telecommunication Systems, 2008. SPECTS2008. International Symposium on*, pp. 173-180, 2008.

[18]. K. Yu, C. Yu and S. Yan, "An Ad Hoc Routing Protocol with Multiple Backup Routes", *Wireless Personal Communication*, vol. 57, no. 4, pp. 533- 551, 2011.

[19]. Soundararajan, S., & Bhuvaneswaran, R. S., "Ant Based Multi-path Routing for Load Balancing and Congestion Control in MANETs", *Journal of Information & Computational Science*, 2012.

[20]. 802.11:"Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications 802.11", 1997

[21]. Stephen Mueller, Rose P. Tsang, and Dipak Ghosal. "Multipath Routing in Mobile Ad Hoc Networks:Issues and Challenges"

[22]. Perkins, Royer, Das. "Ad hoc On-Demand Distance Vector (AODV) Routing" Request for Comments: 3561