International Journal of MC Square Scientific Research Vol.8, No.1 Nov 2016

DETECTION AND ISOLATION OF ATTACKS IN MANET USING TS-AOMDV

Rajesh. D,
Assistant Professor, Department of Computer Science and Engineering,
Universal College of Engineering and Technology, Vallioor, Tamil Nadu, India
Email- rajeshd936@gmail.com

Keiser Jahana S,
UG Scholar, Department of Computer Science and Engineering,
Universal College of Engineering and Technology, Vallioor, Tamil Nadu, India
Email- hasana999@gmail.com

Sivakalai R,
UG Scholar, Department of Computer Science and Engineering,
Universal College of Engineering and Technology, Vallioor, Tamil Nadu, India
Email- rsivakalai1992@gmail.com

Jasmin Meera Banu P,
UG Scholar, Department of Computer Science and Engineering,
Universal College of Engineering and Technology, Vallioor, Tamil Nadu, India
Email- yasminmeera17@gmail.com

Abstract— A mobile ad hoc network (MANET) is a collection of wireless nodes, which works well only if those mobile nodes are good and behave cooperatively. The lack of infrastructure support and resource constraint is the key issue that causes dishonest and non-co-operative nodes. Therefore, MANET is vulnerable to serious attacks. To reduce the hazards from such nodes and enhance the security of the network, this paper extends an Ad hoc On- Demand Multipath Distance Vector (AOMDV) Routing protocol, named as Trust-based Secured Adhoc On-demand Multipath Distance Vector (TS-AOMDV), which is based on the nodes' routing behavior. The proposed TSAOMDV aims at identifying and isolating the attacks such as flooding, black hole, and gray hole attacks in MANET. With the help of Intrusion Detection System (IDS) and trust-based routing, attack identification and isolation are carried out in two phases ofrouting such as route discovery and data forwarding phase. IDS facilitates complete routing security by observing both control packets and data packets that are involved in the route identification and the data forwarding phases. To improve the routing performance, the IDS integrates the measured statistics into the AOMDV routing protocol for the detection of attackers. This facilitates the TS-AOMDV to provide better routing performance and security in MANET. Finally, the Trust based Secured AOMDV, TS-AOMDV is compared with the existing AOMDV through the NS2 based simulation model. The performance evaluation reveals that the proposed TS-AOMDV improves the performance in terms of throughput by 57.1% more than

that of an AOMDV under adversary scenario. The simulated results show that the TS-AOMDV outperforms the AOMDV routing protocol.

Keywords— Mobile Ad-hoc Network; Intrusion Detection System; Trust; Attack Identification and Isolation

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 WiFi increases the scope of the ad hoc networking and enables potential applications in the personal and local area networking 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 selforganized 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.

II. NEED FOR SECURITY IN ROUTING PROTOCOLS

The node co-operation is an essential requirement in multihop 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 [4][5][6][7]. Some of the usual routing attacks are a wormhole, black hole, stealthy, and rushing attack [3][8][9]. 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 212incident 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 [10]. The most important factors to be included in the security provisioning are the availability, reliability, resiliency, and self-healing. 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[11][12][13]. 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 multi-pathrouting protocol is resilient to routing attacks compared to

single path routing

III. 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 wellbehaving. The major challenge in designing such a selforganized 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.

IV. THE PROPOSAL ARCHITECTURE

The proposed TS-AOMDV aims to identify and isolate the attacks such as flooding, black hole, and a gray hole in a MANET. With the aid of an IDS and a trust-based routing, theattack identification and isolation are carried out in two phases of routing such as route discovery phase and data forwarding phase. In the route discovery phase, an attacker launches the route request flooding attack, in which it floods the routing packet with the nonexistent destination address in the network. An IDS monitors the packet generation rate of the source and assigns an inversely proportional value of the request packet count as the 'source-trust value' of the corresponding source. When the trust value of the source reaches the threshold, the route request packet from the attacker source is dropped. In data forwarding phase, an attacker that involves as a router drops the packet instead of forwarding. The IDS monitors the packet forwarding activity of the router and assigns the 'routertrust value' as the ratio between the forwarded packet count and the received packet count. When the trust value of the router reaches the threshold, it selects an alternate path from the multiple available paths that are stored in the routing table and resumes the data transmission through it.

1. Attack Identification with IDS on Network Layer in TSAOMDV

In TS-AOMDV, the IDS runs on each node, and it monitors the neighboring nodes' routing activities at the network layer to detect the routing attackers[15][16][17]. It performs continuous data monitoring to identify the behavior of the nodes and to measure the routing packet generation rate and determine data forwarding statistics. An IDS facilitates a complete routing security by observing both the control packets and data packets that involve in the route identification and the data forwarding phases. The measured statistics are integrated into the AOMDV routing protocol for the detection of attackers. To improve the routing performance, the IDS converts the measured statistics into trust values that are used in the route discovery and data forwarding phases of TS-AOMDV. It facilitates the TS-AOMDV to provide better routing performance and security in MANET. The architecture of TSAOMDV is shown in Figure 1.

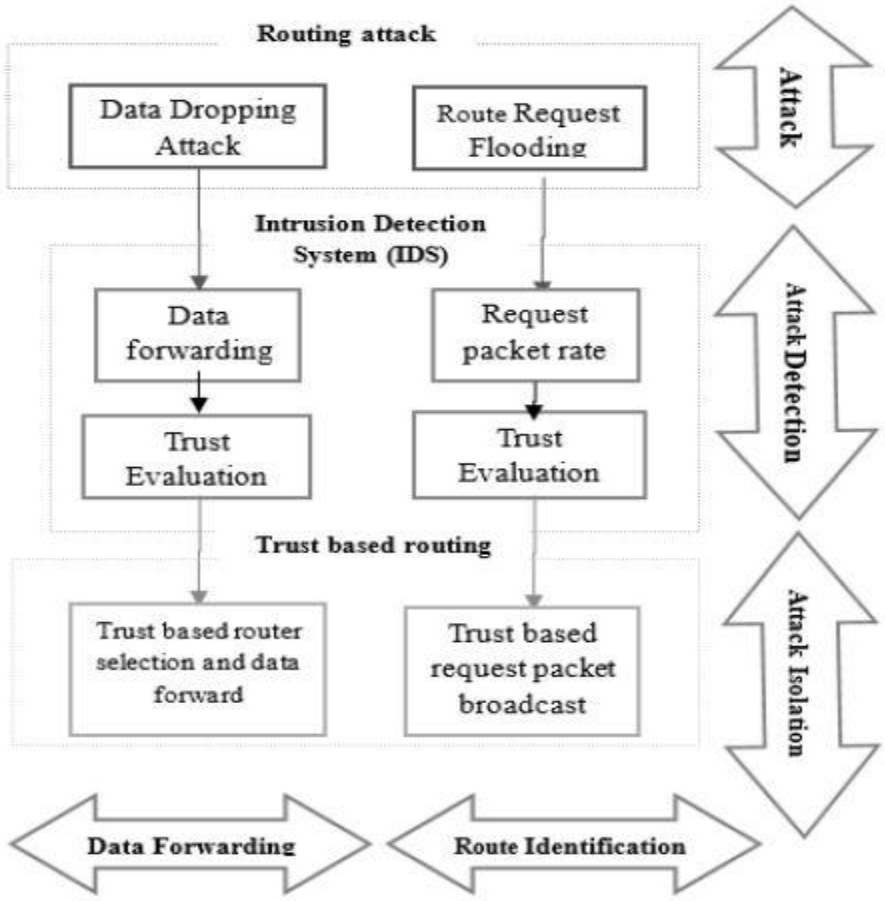

Fig. 1. The Architecture for TS-AOMDV.

A. Measuring threshold for Routing Packet Generation Rate in Network Layer

The flooding attackers disseminate massive RREQ packets violating the routing rule. Moreover, they adopt fraudulent IP addresses for the destination nodes to broadcast the bogus route discoveries. To verify the behavior of the source node during route discovery phase before forwarding the packet, the TSAOMDV count the generated packets by the source node that is measured at each node that receives the RREQ packet. On receiving the RREQ packet, the IDS extracts the ID of the originating node from the packet and increments the RREQ count of the corresponding source. The packet generation rate per node should not be more than the threshold. According to the TS-AOMDV, the IDS on the network layer of each node separately maintain the count of RREQ flooded from the source nodes. If it exceeds the threshold of the routing packet generation rate, the IDS sends a notification message to the network layer.

B. Monitoring Packet Drop of Neighboring Nodes

In the data forwarding phase, the attacker that involved as a router drops the packet instead of forwarding. The black hole and gray hole attacks continuously and partially drop the data packets respectively. The IDS observes the data transmission activity of the neighbors to

detect black hole and gray hole attack during the data forwarding phase. It measures the number of received packets, and the number of forwarded packets of the neighbor to decide the trust value. The IDS assigns the router-trust value as the ratio between the forwarded packet count and the received packet count and notifies the network layer.

C. Direct Trust Evaluation

The IDS identifies the attacker after a certain number of routing activities. It converts the forwarding statistics of a node into trust value. The threshold for routing packet generation and data forwarding are varied based on the network traffic. In high network traffic, the threshold range is minimized. In such cases, the IDS spends more time to identify the attackers. If a node has no knowledge about the IDS activities, it frequently selects the attacker for data forwarding. It impacts the performance of routing in TS-AOMDV. With the aim of improving the routing performance, the IDS on each node measures the source and the router-trust value of the node as the inverse proportion of the RREQ count, the ratio between the forwarded packet count and the received packet count respectively. The trust value of attackers is reduced for every routing activity compared to others, and thus they are immediately excluded from the routing activities. These trust values are stored in the trust table, and the router-trust is used to select the most trusted routers for data forwarding. The source-trust is used to decide about propagating RREQ packet of the particular source node. Themaintenance of source trust is not limited to the neighboring nodes since the RREQ packet with the nonexistent destination id is flooded into the network after identifying it as an attacker by the neighboring nodes. A node identifies the attackers when the trust value of the source or router exceeds the threshold and isolates the attacker from the neighbor list. Moreover, it removes all the routes that have an isolated attacker from the routing table.

2. TS-AOMDV routing process

With the help of IDS and trust-based routing, the attack identification and isolation in TS-AOMDV are carried out in two phases of routing such as route discovery phase and data forwarding phase. The trust obtained from IDS is applied in the routing decision-making about propagating RREQ packet of the source and selecting the trust based router for data forwarding.

A. Trust Based Route Discovery Process

Initially, each node assigns the trust value as ‘one’ to its neighboring nodes. According to the routing activities of these nodes, the IDS measures the original trust value and informs the network layer. The route discovery process is carried out based on the trust value to isolate the flooding attacker activity. Prior to rebroadcasting the received RREQ packet to theneighbors, every node checks for the trust value of the source that has broadcasted the RREQ packet. If the trust value is lesser than the threshold, then the RREQ packet from the corresponding source is dropped to block the flooding activity of the attacker. For instance, in figure 2 the trust value of the source node is maintained by its neighboring nodes such as A, B, and C. The trust value of the source node is different in various neighboring nodes due to the network collisions. The 214 trust value of the source node is very less, so these nodes do not forward the RREQ packet of the source node into the network.

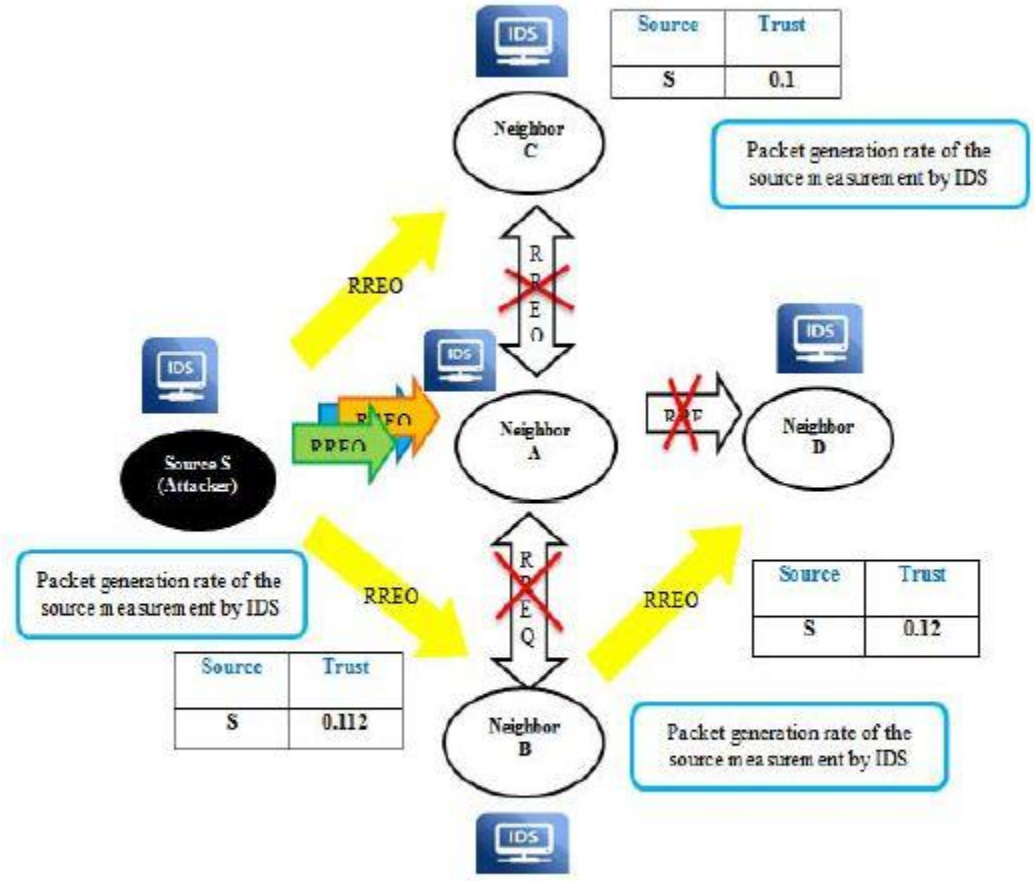

Fig. 2. Route Identification Phase: Route Request Flooding Attack Detection and Isolation.

B. Trust Based Data Forwarding Process

Data forwarding process is carried out based on the trust value to isolate the activity of black hole and the gray hole attacker. Prior to forwarding the data packet to the router, every node checks for the trust value of the router. The trust value of the router indicates the reliability of data delivery through it. If the trust value is low, the current data transmission through the malicious router is blocked. Subsequently, the trusted router from the routing table is accessed to resume data transmission through it. For instance, the trust value of the node B is higher than node A, and so the source node selects router B for further data forwarding. Thus, the IDS and the trust based TS-AOMDV protocol improves the routing performance and security in MANET.

V. EXPERIMENTAL EVALUATION

The Proposed protocol is resistant to two types of routing attacks launched over data packets and control packets such as data dropping attack (gray hole and black hole) and a request

packet flooding attack. The IDS attached with each node performs operations in both the route discovery and the data forwarding phases. The performance of the TS-AOMDV protocol is evaluated using Network Simulator (NS2) in terms of route selection time, throughput, Trust non-utilization factor, overhead, and energy Consumption.

1. Experimental Setup

The NS2 simulation is employed to evaluate the performance of proposed TS-AOMDV routing protocol. The application and transport agent are Constant Bit Rate (CBR) and User Datagram Protocol (UDP) respectively. In NS2 simulation, the CBR generates the data in the network, and the UDP configures the transport layer. The propagation model used is TwoRayGround model. This model is appropriate for long distance communication. The simulation model consists of 50 to 90 deployed nodes within the square network area of 600m x 600m to transmit data packets of 1024 bytes. The node communication range is 250m, and it is capable of communicating directly with others in the range of 250m. The network is simulated for 30 seconds. The performance of the proposed TS-AOMDV is evaluated and compared with the existing AOMDV. To obtain the accurate simulation results, this work runs the TS-AOMDV algorithm for ten times and measures the performance metrics for each simulation. The average value of the metrics are taken as resultant values and are plotted in the graphs.

2. Performance Metrics

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

i) Route selection time

Route selection time is defined as the total time required to select a path set for routing.

ii) Trust Non-Utilization Factor

T he trust non-utilization factor is defined as the attacker involvement in the routing even after its trust level gets reduced below the threshold.

Flooding Attack: Trust Non-Utilization Factor is measured as the number of control packets a node fetches from source node even after the trust level of the source node gets reduced below the threshold.

Data Dropping Attack: Trust Non-Utilization Factor is measured as the number of data packets forwarded to the router even after its trust value has reduced below the threshold.

iii) Overhead

Communication overhead refers to the number of control messages involved in the routing process.

iv) Energy Consumption

It refers to the total amount of energy consumed to perform successfully the communication over the entire network.

3. Experimental Results

The simulated results discuss the different simulation models employed. To facilitate the performance of the proposed TS-AOMDV routing protocol, various performance metrics are evaluated.

A. Detection of Blackhole and Gray hole Attacks The communication model is initiated from source 0 to destination 1 for a specific duration. Through a basic AOMDV routing process, the nodes involved in the routing path are computed. One of the nodes is configured as an attacker at

the specific time in such a way that it drops the packets forwarded through it. An IDS is embedded with every node. Hence, a neighbor node of each router is enabled to monitor the packet forwarding activity of the router. The neighbor node applies the
IDS and computes the trust value for each router as the ratio of the number of packets forwarded to the number of packets received. All the nodes are initialized to the high trust value that is 1, and it varies between 0 and 1 based on their behavior. Moreover, the threshold for the router-trust is fixed as 0.8 according to the traffic level. If it goes below the threshold, then the node is detected as a router-attacker and as an alternative highly trusted router is selected for further data transmission. To evaluate the performance of TS-AOMDV protocol in the detection of a black hole and gray hole attacks, the metrics such as Route selection time, Throughput, and Trust Non-Utilization Factor are evaluated by varying the number of nodes.

1) Varying the Number of Nodes

The network varies the number of nodes from 50 to 90 to study the impact of the network size on routing attack detection of TS-AOMDV. The communication range assigned to the nodes is 250m.

2) Route selection time

The simulation results of the TS-AOMDV with Black-hole and Gray-Hole attack and The simulation is conducted by varying the number of nodes from 50 to 90. From the results, it is observed that the route selection time increases with the number of nodes. With a sufficient density of nodes in the network, both the TSAOMDV and the AOMDV discover the routes in less time. With increased number of nodes, the minimum hop count between the source and the destination is high resulting in time consuming route selection.

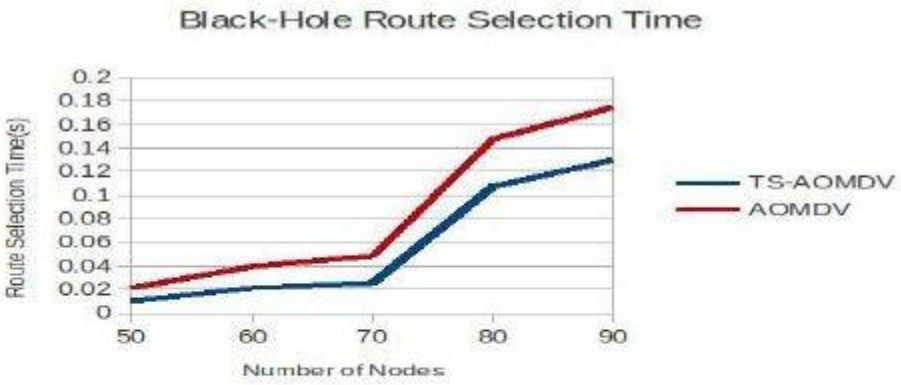

Fig. 3. Number of Nodes Vs Route Selection Time for Black-Hole Attack.

For instance, the route selection time of TS-AOMDV with black-hole attacks is 0.021 Sec at the point of 50 nodes, and increases to 0.184 Sec when the number of nodes is 90. However, the selection of routers with the knowledge of trust on routing activities increases the minimum hop

count and the route selection time. It increases the route selection time by 38.4% compared to the existing AOMDV.

3) Throughput

It is observed that the throughput increases with the rise in the node density or the number of nodes. The substantial node density in MANET ensures the availability of alternative path and the reliability of packet delivery. For instance, 6, 0.0285 Mbps of network traffic are delivered per second at the point of 50 nodes, but it increases to 0.040Mbps with nodes of 90 numbers. At the same time, the network throughput on TS-AOMDV is increased more than the AOMDV. The reliable packet delivery with the black-hole/gray hole attack is not possible since the gray hole attacker drops the data packets either continuously or partially.

The IDS based TS-AOMDV converts the measured statistics into trust values which is used in the route discovery phase and establishes the most trusted paths to the destination. This improves the network throughput of TS-AOMDV to 0.036 Mbps at the point of 50 nodes when compared to AOMDV.

4) Trust Non-Utilization Factor

The simulation is conducted by varying the number of nodes from 50 to 90 with the communication range of 250m in the network area of 600x600m. The TS-AOMDV achieves better performance compared to AOMDV, as the proposed work measures the trust of neighboring nodes continuously and eliminate the nodes which behave selfishly in the network. For instance, two packets are forwarded to the router after its trust value is reduced below the threshold, but in AOMDV it is increased to 25 packets. Moreover, in both the protocols the Trust Non-Utilization Factor does not increase while increasing the number of nodes since the network traffic applied is the same in all the cases.

5) Overhead

The comparative results of overhead between the proposed TS-AOMDV and AOMDV with a black hole and gray hole attacks. The simulation is conducted by varying the number of nodes from 50 to 90 nodes with the same network traffic in the specific simulation area of 600m x 600m. Both the protocols escalate the routing overhead while increasing the number of nodes. As TS-AOMDV uses no additional packets for routing, the routing overhead of TS-AOMDV is similar to that of AOMDV. It is observed that both the protocols have similar overhead. For instance, the overhead of both the protocols is 1500 at the point of 50 nodes, but it increases to 2700 when the number of nodes is 90.

B. Detection of Flooding Attacks

The route request flooding attack is created when a node acts as a Flooding attacker. It broadcasts the route request packet every 0.01 Sec. An IDS is embedded with every node. Each node monitors its neighbor node about its route request packet generating activity. If the number of generating route request packets is higher than the threshold, then the node is detected as a flooding attacker. Each node applies the IDS and computes the trust value for the request packet generating node. The Trust is computed as the reciprocal of its total
request packet count. The threshold is fixed as 0.2 for trust. If it goes beyond the threshold, then the node is detected as a flooding attacker and the packets received from it are discarded.

1) Varying the Number of Nodes

To study the impact of network size on the flooding attack detection in TS-AOMDV routing protocol, the number of nodes is varied from 50 to 90 with the communication range of 250m.

2) Trust Non-Utilization Factor

The simulation is conducted by varying the number of nodes from 50 to 90 in the network area of 600x600m. The TSAOMDV achieves a better performance when compared to AOMDV, as the proposed work eliminates the nodes that continuously flood the routing packets into the network. For instance, packets are forwarded to the router after its trust value is reduced below the threshold, but with 90 nodes it is increased to 28 packets. Compared to TS-AOMDV, the Trust Non-Utilization Factor of AOMDV is increased to 62 packets, when the number of nodes is 90.

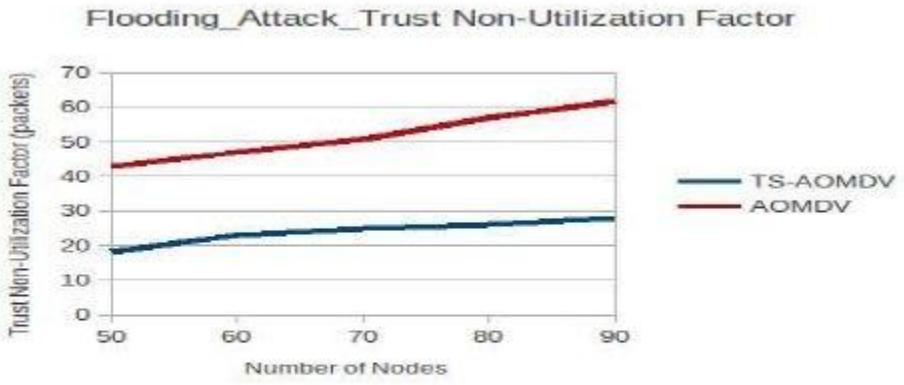

Fig. 4 . Number of Nodes Vs Trust Non-Utilization Factor for Flooding Attack.

3) Energy Consumption

The energy consumption of TS-AOMDV is compared with AOMDV, by varying the nodes from 50 to 90 on 600 x 600 m area with the same network traffic. Figure 12 illustrates energy consumption for flooding attack. TS-AOMDV shows moderate variations in the energy consumption while increasing the number of nodes. The trustbased routing protocol refuses to forward the routing packets of flooding attackers into the network. This saves the overall energy in the network. For example, TS-AOMDV consumes 8.52 joules at the point of 50 nodes but increases to 19.17 Joules with 90 nodes. However, in AOMDV the energy consumption is increased from 52.8 joules to 91.38 joules while increasing the number of nodes from 50 to 90.

4) Overhead

The simulation is conducted by varying the number of nodes from 50 to 90 nodes with the same network traffic in a particular simulation area of 600m x 600m. The AOMDV escalates the routing overhead while increasing the number of nodes, but the TS-AOMDV shows only a marginal variation in the overhead. TS-AOMDV measures the forwarding statistics using the IDS and convert it into a trust value to propagate the RREQ packet of the particular source node.

it is observed that the AOMDV with no awareness about the flooding attackers blindly propagate the routing packets into the network, creating a huge overhead. For instance, the overhead of TS-AOMDV is 434 at the point of 50 nodes, but in AOMDV it spurts up to 4156 packets.

VI. CONCLUSION

A Trust-based Secured Ad hoc Ondemand Multipath Distance Vector, TS-AOMDV was clearly designed to achieve security in MANET. The proposed protocol is resilient and combative with two types of routing attacks launched over data packets and control packets, such as gray hole and black hole, and request packet flooding

attack. The IDS attached with each node, performs two operations such as measuring the route request generation rate of the source, and packet forwarding statistics of the neighbors during the route discovery and data forwarding phase respectively. By comparing these values with the threshold, the IDS easily captures the different types of attackers in various routing phases. The measured statistics is incorporated into trust values for selecting the most trusted path to improve the performance of TS-AOMDV. Moreover, the performance of the proposed protocol is simulated using NS2. The proposed Trust based Secured AOMDV (TS-AOMDV) is compared with the existing AOMDV in terms of throughput, route selection time, trust non-utilization factor, energy consumption and overhead through the simulation model. The simulated results show the superiority of the proposed protocol in various scenarios.

REFERENCES

[1] Erciyes, K. "Distributed Graph Algorithms for Computer Networks", *Computer Communications and Networkss* , 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] 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.

[4] 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.

[5] 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.

[6] 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.

[7] Mahmoud, Mohamed MEA, and Xuemin Sherman Shen. "Secure routing protocols." *Security for Multi-hop Wireless Networks. Springer International Publishing*, pp. 63-93, 2014.

[8] 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.

[9] 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.
[10] 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
[11] 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. SPECTS 2008. International Symposium on*, pp. 173-180, 2008.
[12] 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.
[13] Soundararajan, S., & Bhuvaneswaran, R. S., "Ant Based Multi-path Routing for Load Balancing and Congestion Control in MANETs", *Journal of Information & Computational Science*, 2012.
[14] Eliana Stavrou, Andreas Pitsillides,"survey on secure multipath routing protocols in WSNs," *Computer Networks*, vol. 54, no.13,pp 2215–2238, 2010.
[15] Mitchell, R., & Chen, R, "A survey of intrusion detection in wireless network applications", *Computer Communication*s, vol.42, pp. 1-23, 2014.
[16] Mitchell, R.; Chen, I.-R., "Behavior Rule Specification-Based Intrusion Detection for Safety Critical Medical Cyber Physical Systems," *in Dependable and Secure Computing, IEEE Transactions on* , vol.12, no.1, pp.16-30, 2015.
[17] Mitchell, R., & Chen, I. R., "Specification based intrusion detection for unmanned aircraft systems", *Proceedings of the first ACM MobiHoc workshop on Airborne Networks and Communications*, pp. 31-36, 2012.