ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MULTIPATH TRUST BASED FRAMEWORK FOR PREVENTION OF BLACKHOLE ATTACK IN MANETS

[1]DILRAJ SINGH, [2]Dr. AMARDEEP SINGH

[1]Research Scholar, Department of Computer Engineering, Punjabi University, Patiala, India.

[2]Professor, Department of Computer Engineering, Punjabi University, Patiala, India.

E-mail: [1]dilraj@pbi.ac.in, [2]amardeep_dhiman@yahoo.com

ABSTRACT

Due to its self-organizing nature the Mobile Ad hoc Networks (MANETs) are successfully able to provide a great channel for communication anywhere, anytime in absence of any centralized infrastructure and have a huge potential in actual applications like, in the military, rescue and commercial fields. However, due to its dynamic nature the network they are susceptible to different type of attacks which can hinder smooth functioning of the network. The standard routing protocols for MANETs do not perform well in the presence of nodes that intentionally drop data packets, one such malevolent behavior is launched by blackhole nodes. In this paper, we propose a new protocol Enhanced Secure Trusted AODV (ESTA) to cope with the problem of presence of such nodes in network. ESTA is extension of on the broadly used reactive protocol Ad hoc On-demand Distance Vector (AODV). The proposed protocol is multiple path approach combined with the use of trust to eliminate the corrupt paths. The NS-3 based simulation results present that the proposed protocol is efficiently able to thwart the effect of the blackhole attack in different scenarios and proves to increase the ratio of successfully delivered data packets significantly.

Keywords: *Blackhole Attack, NS-3, Multipath, AODV, Trust.*

1. INTRODUCTION

A mobile ad hoc network (MANET) is formed by a set of nodes equipped wireless network interfaces, and are located in the transmission range of a subset of the others. The nodes acts both as a host and as a router to enable others to use their relaying capability to communicate with nodes that are out of their direct transmission range. Such a setup does not require the presence of any pre-existing infrastructure, due to which they have some unique characteristics, like unreliable wireless medium for communication, limited bandwidth and dynamic varying network topologies member nodes. Though these characteristics enhance flexibility in terms of setup for MANETs, but make the network more susceptible to security threats. The different types of attacks against MANETs can be categorized as Passive and Active attacks[1]. The key security issues for any network can be categorized as Authorization, Authentication, Non-Repudiation, Integrity and Confidentiality. Specifically in the case of MANETs due to dependability on peer nodes the Availability becomes a very important aspect.

In the case of MANETS the traditional routing and security schemes cannot be adapted as such. Due to its dynamic nature the route selection becomes a critical aspect in order provide efficient and secure transmission, which mainly depends upon the routing protocol. The routing protocols in MANETs are broadly classified as Proactive, Reactive and Hybrid routing protocols[2]. In case of proactive routing, every node always maintain routing information to the other nodes. The Destination Sequenced Distance Vector (DSDV) and Optimized Link State Routing (OLSR) belong to this category. Whereas in case of reactive protocols the route established as and when required by nodes, like Ad hoc On demand Distance Vector (AODV) and Dynamic Source Routing (DSR). Finally, the hybrid protocols are combination of the features from both the proactive and reactive routing protocols like Zone Routing Protocol (ZRP).

As the proposed solution is based on the AODV [3] routing protocol with certain enhancements to its existing control packets and introduction of couple of more control packets. The route formation is based on the principles of reactive protocols and creates multiple paths. In order to create loop free routing paths new control packet are introduced. Section-2 of the paper provides a brief overview about some of the existing approaches used for securing transmission. In Section-3 the problem statement is defined. In Section-4, the proposed solution details is elaborated. The Section-5 describes the simulation setup details and analysis based on the simulation results are provided. Finally, in Section-6 presents the conclusion along with the future scope.

2. PREVIOUS WORK

Due to its dynamic feature the MANETs and susceptibility to variety of attacks the area of security in MANETs garner a lot of attention from the research community. A variety of approaches has been proposed by different researchers solve these challenges. Many types of attacks have been proposed so far by various researchers like, rushing attack, packet alteration attack, blackhole attack, wormhole attack and spoofing attack, etc. A detailed overview of such attacks has been discussed by the authors in [4, 5, 6, 7, 8 & 16] . With the main focus on the Blackhole attack in this section, a very brief overview of some of the existing work related to various approaches proposed is discussed.

No study would be complete without reviewing the one of the first and widely known security enhancements for AODV is Secure AODV proposed by Zapata and Asokan [9]. Due to resource-limitation and dynamic nature of network nodes the SAODV does not depend upon any Certificate Authority (CA). The framework makes use of a digital signature and one-way hash chain to protect the packet to provide security. Asymmetric cryptographic is used in the SAODV, for every generated packet the node needs to add a signature and with every received routing message (even the intermediate node), the verification process has to executed. Although it helps in communicating nodes to find secure paths, but at a cost of heavy computations.

In [7] Eichler and Christian, proposed AODV-SEC a new secure routing protocol, which is based on AODV and SAODV. As per the proposal, digital certificates along with encryption keys are issued by trusted CA. A new type of digital certificate known as m-Cert is created, and contains only relevant information related to the certificate, due to which the overhead is reduced by 50 %. The m-Cert is x.509 standard compatible certificate. The route created by this approach may not be the shorted path to the destination.

Mishra et al., [10], proposed a mechanism to tackle the black hole attacks by discovering a safe path to destination. For this purpose a new table Data Routing Information (DRI) table with additional check bit is introduced in the AODV protocol. Simulation on NS2 was done and the new scheme showed results demonstrating effectiveness of mechanism to detect and eliminate attack and maximize network performance by reducing packet dropping ratio.

Tamilselvan and Sankaranarayanan [11] proposed an approach in which the source node await for the responses from neighboring nodes along with the details of next hop, for a predetermined time value. A table Collect Route Reply Table (CRRT) is used to store and cross check the if there is any recurrence of the next-hop-node details or not. Only paths with repetitive nodes in paths are used. Additional overhead and delay is added with this solution. The crux of solution is to find path via non-malicious nodes only, and it does not focus on the integrity and confidentiality of the data packets transmitted which at stake due to internal attack.

Tan and Kim [12] proposed Secure Route Discovery for AODV (SRD-AODV), which is an extension of AODV routing protocol. As per the proposed solution, a threshold value for the sequence number used by the control packets is defined, which would depends upon network environment and possible node density. In AODV the sequence number are used to maintain the fresh and loop free paths. When the sequence number reaches the threshold value, it is reset. This solution is able to defend the network from the blackhole node attack, but fails to counter any other form of attack.

Yerneni and Sarje, [13], proposed Secure-Ad hoc On demand Distance Vector(SAODV) by introducing Modified Request (MREQ) and Modified Reply (MREP) as an additional packets used to carry random numbers after RREP control packet. These random number remains same at each node but malicious node increments it and detected as blackhole node. Random numbers generation each time wastes memory and much delay especially in the presence of suspicious node.

In [14] Jalil, et. al., proposed a scheme named as Enhanced Route Discovery AODV (ERDA). In the scheme an additional RREP table is used to store received RREPs. The first RREP is ignored and second RREP is considered as legitimate entry. But if this RREP is also sent by any blackhole node then routing table is updated falsely.

Apart from above presented approaches various other approaches based on promiscuous monitoring, trust management, introduction of control packets and data structures have also been proposed by various researchers. But in the above reviewed approaches the additional overhead like prior knowledge of certificates, use of control packets to nail down bad nodes, suppression of first RREP of being possibly compromised or extra processing at nodes may degrade the network performance and could be still at stake.

3. PROBLEM STATEMENT

Belonging to the class of reactive protocols the AODV [3,15] starts the route formation whenever a source node has some data for transmission. It uses and maintains the same routing information for entire durations of transmission or until the route is stable. The Route Request (RREQ) packets are broadcasted to the destination or some intermediate node having fresh path to the destination. In either case a Route Reply (RREP) packet sent as unicast message to the source node. In AODV, the duplicate RREQs per ID are not processed by the intermediate and destination nodes, so formation multiple loop free paths is not possible. Therefore, in case of networks with high mobility nodes or sparsely populated networks, the route could be unstable due to frequent breakage, which leads to efficiency degradation. Therefore, for mission critical operations this may become a bottleneck and the basic purpose of the network formation could be defeated. Also, in presence of malicious nodes, the route formation may be effected as the malicious nodes can respond to the RREQ messages and successfully plant themselves in the route. This may affect the network performance adversely and could be a threat in terms of confidentiality, integrity of data packets and availability of network resources. The review of literature related to AODV suggests that with the use of a single path for transmission the delay and control data can be reduced ,but, in unfavorable network conditions, the working of the network could be affected. Hence, the question arises as to how handle situations like this. Likewise, in case the network is under attack how will be the working of the network safeguarded.

4. PROPOSED SOLUTION

Based on the review of the existing security enhancements available for MANETs environment, a trust based multiple path-based solution is proposed (Figure 1). In the proposed solution multiple loop free and disjoint paths are utilized for the data transmission. Further in this approach a combination of trust and asymmetric cryptography is used to phase out the non-performing paths. But in this paper we are highlighting limited use of cryptography in the approach, by just signing a newly added control packet. In case of non-performing paths they are suppressed and more RREQs are raised to maintain multiple paths. The complete process follow the a sequence of phases for secure data transmission, to start with is the basic route formation process, followed by data transmission and finally the path evaluation.

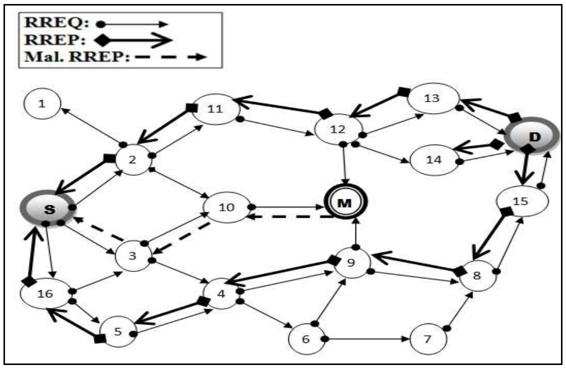

Figure 1. Sample Network Topology

4.1 Network Model

In the considered MANET all nodes have comparable features like transmission range, pause time and mobility. A unique-ID is assigned to all nodes for ease of identification. In the proposed solution the network does not contain any CA as taken in account by certain approaches, so all nodes perform extra functions such as trust evaluation and maintaining backup queues in order to ensure security and high performance. In case of networks with CA, they may become a single point of failure, also it defy the basic charter of the ad hoc networks. To demonstrate the attack, there may exist a varying number of blackhole nodes in the network at different locations, not necessarily the neighbor nodes.

4.2 Blackhole Attack

The blackhole node attack belongs to a category of active attacks. The blackhole node responds to the RREQ messages with a very high sequence number and claims to have the shortest path to the destination. The sequence number of a packet acts

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

as a form of time-stamping, and is a measure of the freshness of a route. Indeed, the node having the higher sequence number to reach the destination, will be considered as the one having most upto date path for the destination. So, on receipt of the RREQ packet, the attacker will simply set the sequence number to the higher possible value. Hence, this malicious node will be able to position itself on the path between the communicating nodes, and will be able to do anything once the data transmission starts through.

4.3 Route Formation

For the route formation phase in the proposed framework works to form multiple paths. So to support this functionality two new data structures are introduced 'LINK_TABLE' and 'LINK_INFO'. The 'LINK_TABLE' is used by the nodes to store information of the multiple RREQ packets received from neighboring nodes. RREP packs are propagated towards source node using information from this. After transmitting the RREP packet the intermediate node generates and broadcasts a control packet, 'LINK_INFO', in order to update the neighboring nodes about its and next used nodes non-availability to be part of any other path. Upon receiving this control packet, all neighbor nodes mark the entry of the sending node and its next used node as Invalid in their 'LINK_TABLE'. This feature ensures that the paths created are disjoint. Upon receiving the RREPs the source node save them in a newly defined route table which is capable of holding multiple entries for the same destination.

4.4 Data Transmission

Upon receiving the first RREP, a wait timer is initiated for '1s', so that multiple routes can be established before the transmission begins using paths formed by step 1. The transmission starts once the count of the minimum number of packets and valid route counts is achieved, Purpose of having minimum packet count is to ensure that all paths get a optimal share of data packets to be transferred through them, as shown by algorithm in *Table 1*. In order to do so the packets are divided on the basis of following formulas (1 & 2).

$$\boldsymbol{PR = N_{TQ} / VR} \qquad \textbf{-- (1)}$$

$$\mathbf{RP = N_{TQ}\ \%\ VR} \qquad \textbf{-- (2)}$$

Where:- ***PR*** = *Packets per Route*, ***RP*** = *Remaining Packets*, $\boldsymbol{N_{TQ}}$ = *Packets in Transmission Queue*, ***VR*** = *ValidRoute count.*

Table 1. Algorithm for ESTA Packet Transmission

BQ: ***Backup Queue;*** **TQ:** ***Transmission Queue;***
Minp : ***Minimum Packet Count;*** $\mathbf{P_X}$: ***PacketCount;***
PPR: ***Packets Per Route;*** **RP:** ***Remaining Packets;***
$\mathbf{P_{ID}}$: ***Packet ID;*** **GWStatus:** ***Gateway Node Status***

```
1: Enqueue Datapacket & Raise RREQ.
2: Process RREQ at ndoes.
3: Initialize Timers for Multiple Routes &
HelloProcessind at Source Node.
4: If Timer's set at Step5 > SetTime.
        {
5:          Fetch all valid routes validRouteCount().
6:          If validRouteCount  >= 1, then:
            {
7:            Append BQ to TQ.
8:            If  $P_x < Min_p$.
9:             then: wait till $P_x >= Min_p$
10:          Else.
             {
11:            Initialize PPR = $P_x$ / valid route count.
12:           Initialize RP = $P_x$ valid route count.
13:      For every route in valid route list repeat steps
14:            If $GW_{status}$ = 0 or $GW_{status}$ = 1, then:
15:                  continue.
16:             Else:
                {
17:               set count:= 0.
18:              While count <= PPR+RP.
19:                SendPacketFromQueue().
20:              Endwhile.
21:              set RP := 0.
               }
             }
           }
22: Else.
23:         Raise RREQ.
            }
24: Process packets RouteInput().
25: if DataPacket.
      {
26:   Initiate Timer for DeliveryInfo() broadcast.
27:  if Timer set at Step 28 > SetTime.
      SendDeliveryInfo().
      }
28: At source RecvDeliveryInfo().
29: Compare DeliveryInfo $P_{ID}$ with BQ $P_{ID}$.
30: Increment the $GW_{Status}$ for performing Gateway
nodes.
31: Clear BQ where $P_{ID}$ == BQ($P_{ID}$).
32: if TQ != 0 GOTO Step 3.
```

4.5 Trust Evaluation

Upon receiving the data packets at the destination node the details of the received packets are stored. This stored information is used for broadcasting a special time bound control packet 'SEND_DELIVERY_INFO'. The idea is to ensure maximum delivery, by notifying the source node about the packets it has received. This packet is signed with the private key of the destination node, so that the malicious nodes cannot manupulate the trust value by sending the fake delivery information packets. The missing packets are re-transmitted. This information helps the source node to evaluate the paths and assign them a trust value based on its direct experience.

A trust value referred as *GWStatus* is assigned to the gateway nodes of a path based on its performance. Let *GWStatusi(j)* represent the level of direct trust of node '*i*' on its neighbor '*j*'. Its values range from 0 ≤ GWStatusi(j) ≤ 3. In *Table 2*, the trust values and definitions are listed. Every new Gateway node is assigned a trust value of '2' by default. The trust value is manipulated on the basis of the control packet, 'SEND_DELIVERY_INFO'; for every successful report, the value is incremented and, in case of failure, it's decremented. Fixed interval timers, t and t' , are used to perform this check on the trust value for nodes, as shown in (3) & (4). In the case of the trust value of node being 1, it's under observation and no packets are transmitted through this Gateway node, but it's not yet marked for blacklisting. Some extra time is given to this node as the delivery reports may be delayed. Once it is assigned the value 0, it is marked for blacklisting and any new RREP from this Gateway node is barred from entry into the new routing table at the source node.

$$t > NetTraversalTime : GWStatus = 1 \quad \text{--(3)}$$
$$t' > 2 + NetTRaversalTime : GWStatus = 0 \quad \text{-- (4)}$$

Table 2. Trust values for Gateway Nodes

Trust Value	Definition
0	Absolutely No Trust
1	Partially Trusted
2	Default Trust
3	Full trust

In the proposed solution, the HELLO packet processing phase at source node performs an extra task in addition to neighbor discovery, i.e. processing the packets existing in the transmission queue. At this stage, if multiple routes still do not exist, the current packets in the transmission queue are sent using a single path only; in the presence of multiple paths, the load is divided among the paths. With this approach, the focus is to achieve maximum efficiency in the case of mission critical operation where the entire information should reach the destination, albeit maybe with some minor delay.

5. SIMULATIONS AND RESULT ANALYSIS

For simulation purposes, the NS-3.19 simulator is used. We designed and programmed the modules described above using C++ and implemented the various classes to work with existing NS-3.19 modules. In order to analyze the efficiency and other important aspects of the proposed solution, is compared with the standard AODV protocol. Also, to emphasize the effect of trust among the nodes in the network, a simulation was conducted with and without use of trust value ESTA and ESTA-NT respectively in proposed solution.

Table 3. Simulation Parameters

Parameter	Value
Topology Dimension	1000m*1000m
Simulation Time	60s
No of Nodes	50(if not specified)
Node Speed	2m/s (SM) & 10m/s (HM)
Pause Time	0s (if not specified)
Transmission Range	250m
Traffic Model	CBR; 4pkts/s
No. of source nodes	3
No. of malicious nodes	0% & 10%

Based on the simulation results the parameters that are compared are:

- **Average Packet Delivery Fraction (PDF):** This is the ratio of data packets received at the destination to those generated at the CBR sources.
- **Average End-to-End Delay:** The difference in terms of delivery time of the first data packet at destination node to the time it was transmitted by the source node.
- **Average Routing Overhead:** The total number of RREQ and RREP packets generated by the source and destination.
- **Average Packet Drop Fraction:** This is ratio of data packets dropped by blackhole node to those generated at the CBR sources.

5.1 Results and Analysis

In order to analyze the performance of the proposed solution two type of scenarios are taken into consideration i.e. based on pause time and node density. In both the cases the effect of Node Mobility is varied between slow mobility and high mobility.

5.1.1 Average Packet Delivery Fraction

Fist, the PDF of AODV, ESTA and ESTA-NT with different pause times is studied and varying node mobility. The results captured in Figure-2 show that with slow mobility, in the absence of any malicious node, the performance the is high. However, there is a slight reduction in the performance of AODV for a pause time of 2 seconds, but the proposed solution works fine with or without trust. With the introduction of malicious nodes in the network the PDF reduces drastically for AODV and ESTA-NT, but ESTA still performs better even in presence of high number of malicious nodes. Likewise in case of high mobility in absence of malicious nodes the performance of the network is very good, as shown in Figure-3. The ESTA and AODV performs almost in a similar fashion. But, upon introduction of malicious nodes the PDF of the network degrades, with high variation. However, the PDF for AODV reduces considerably. The main reason for variation is due to the high mobility of the nodes and reformation of routes.

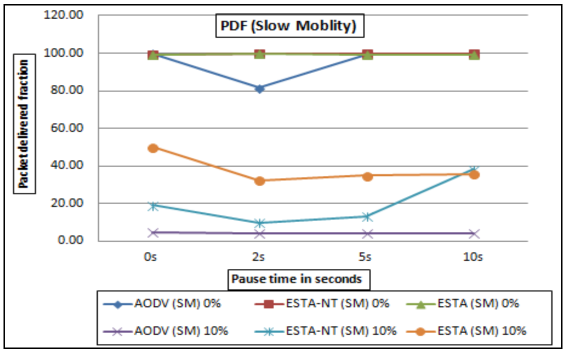

Figure 2. PDF vs Pause Time at slow mobility

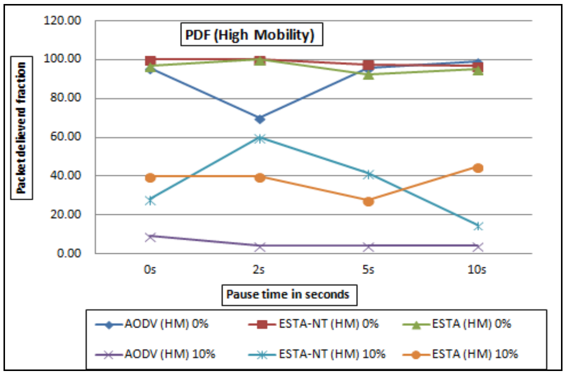

Figure 3. PDF vs Pause Time at high mobility

Secondly, the PDF of AODV, ESTA, ESTA-NT is studied with different Node densities and varying node mobility i.e. slow and high mobility. As shown in Figure-4 with nodes at slow mobility and in absence of malicious nodes the network behavior is normal. But once the malicious nodes gets activated the performance in terms of PDF starts degrading, due to varying node density there is a strong variation. Still, in all cases the proposed solutions is successfully able to prevent the blackhole effect in contrast to AODV considerable. In case of 90 nodes the performance of all 3 cases is almost similar due to the fact that malicious nodes were not able to become the successfully due to continuous movement of the nodes and route reformations. But with high node density the AODV fails to perform whereas the proposed solution performs due to formation of multiple paths. Similarly when node mobility is high the performance of the network in absence of malicious nodes is acceptable but with introduction of malicious nodes there is a variation, Figure-5. The performance of the ESTA is quite high in case of 70 nodes, where as in case of 90 nodes it reduces to same level as in case of slow mobility. But AODV fails drastically in this case with no variations at any node density.

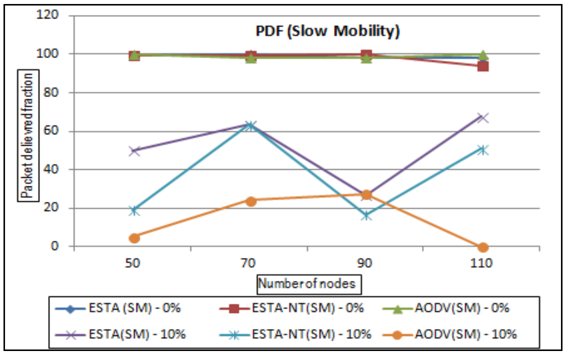

Figure 4. PDF vs Node Density at slow mobility

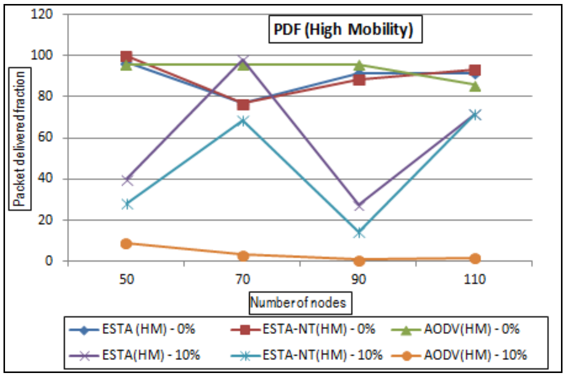

Figure 5. PDF vs Node Density at high mobility

5.1.2 Average Packet Drop Fraction

In order to analyze the Packet Drop Fraction we are considering case of 10% malicious nodes. The results in Figure 6 display the percentage of packets dropped at slow and high mobility for varying node pause time. Based on the simulation results AODV drops almost all the packets, but in case of the packet droppage is very high. Still with this high value of droppage the packet delivery fraction as shown in Figure 2 & 3 is quite high. This happens due to the re-transmission feature added in the ESTA.

Similarly in Figure-7 the packet drop fraction results are plotted based on the node density with varying speed. In this case also the packet droppage of AODV is low but the PDF as shown in Figure 4 & 5 is low. Whereas, for the ESTA and ESTA-NT the droppage is quite high still the PDF is considerably high.

Another factor to be considered here is that in case of ESTA and ESTA-NT the droppage in case of ESTA-NT is more than ESTA case. The reason is use of trust and avoiding non-performing nodes.

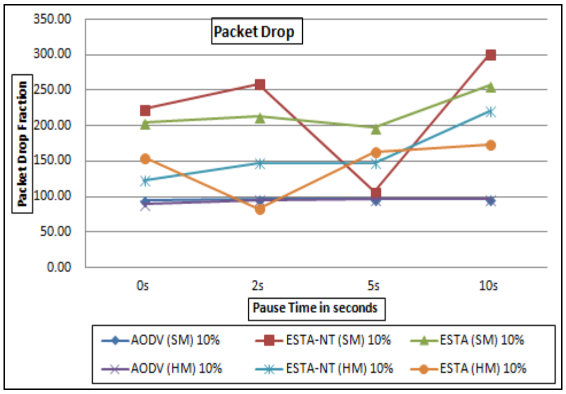

Figure 6. Packet Drop Fraction vs Pause Time

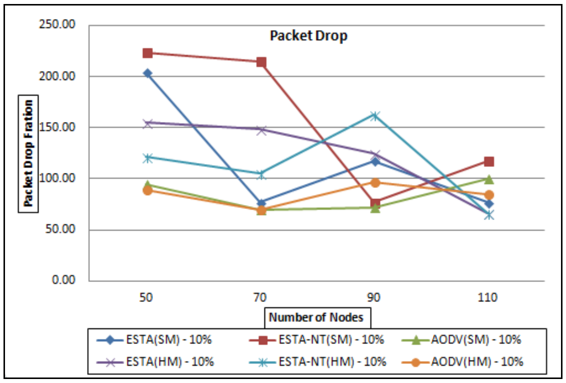

Figure 7.Packet Drop Fraction vs Node Density

5.1.3 Average End-to-End Delay

First, for this scenario the average end-to-end delay for the first data packet delivery is studied for varying node mobility at different pause times. Results captured in Figure- 8 show that the delay in the case of AODV is always lower than the ESTA and ESTA-NT in absence of malicious nodes. The slightly high delay for ESTA and ESTA-NT is due to a wait time feature upon receiving the first RREP so as to gather more than one route before the transmission begins. Once the network comes under attack the delay of AODV increases considerably because for some pair of transmissions the packets are never received at destination so it is not possible to measure their delay. So the simulation time is considered as delay. Whereas, in case of ESTA and ESTA-NT delay increases with pause time due to slow mobility and less number of nodes which means added delay in formation of multiple paths. As shown in Figure-9, in case of high mobility of nodes the delay of AODV with and without attack is similar as in case of slow mobility. But, for the ESTA and ESTA-NT cases delay in case of normal network is low which increase with introduction of the blackhole nodes.

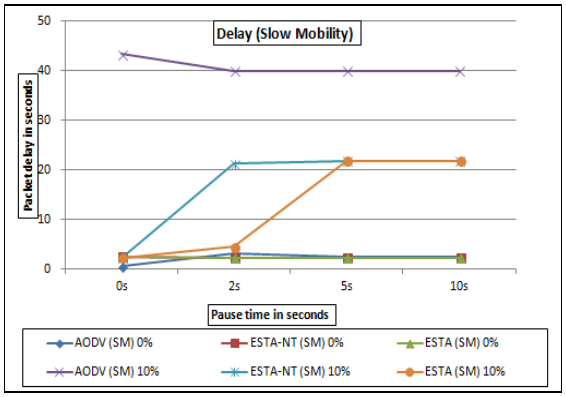

Figure 8.Delay vs Pause Time at slow mobility

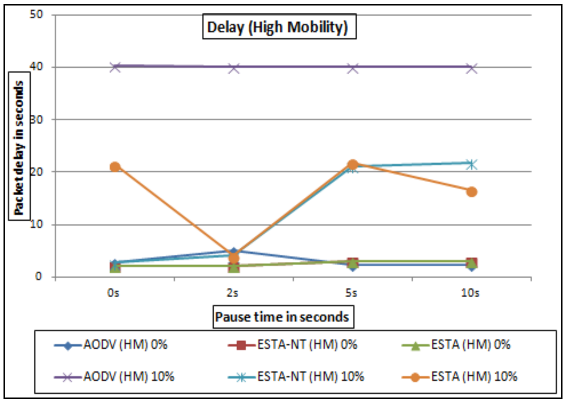

Figure 9. Delay vs Pause Time at high mobility

Second, the focus is the average end-to-end time delay in the delivery of the first data packet for different node densities. The results shown in Figure-10 the AODV, ESTA and ESTA-NT without malicious nodes has very low delay compared to results with malicious nodes presence. As stated above in case of AODV under attack for some transmission pairs no packets are received so the delay turns out to be quite high. In ESTA, the time delay is high with an increasing number of blackhole nodes and it re-transmits the packets to ensure maximum performance. Therefore, the packets dropped due to the formation of corrupt paths because of malicious nodes are also re-transmitted, which adds to the delay for the first packet of applications. Likewise, in Figure-11 at high mobility the delay is almost similar for cases with no malicious nodes. But in case of malicious presence the results vary du to the fact that with high node density and mobility the path formation is more stable.

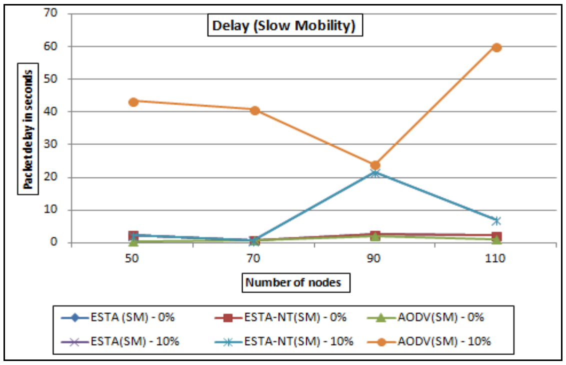

Figure 10. Delay vs Node Density at slow mobility

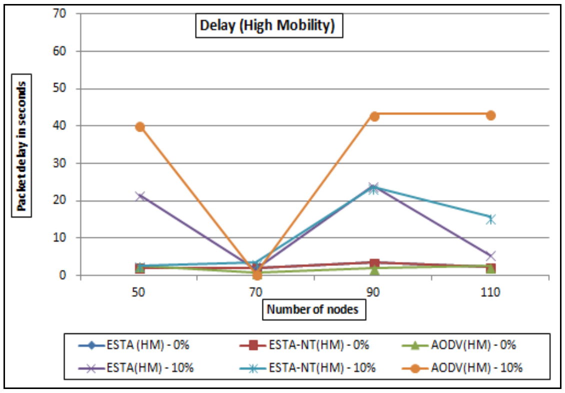

Figure 11 . Delay vs Node Density at high mobility

5.1.4 Average Routing Overhead

For this analysis the total number of control packets specifically RREQ and RREP are taken into consideration at the source and destination nodes of the communication pairs. For the first analysis shown in Figures-12 and 13 node mobility and varying pause time are used for analysis. In both cases of slow and high mobility in absence of malicious nodes the Routing overhead is for AODV is quite low. While for the ESTA & ESTA-NT cases the routing overhead is more because in order to create multiple routes all intermediate nodes process the duplicate RREQs received. Similarly the destination node reply with multiple RREPs. In case of attack situation the routing overhead increases because in order to have high efficiency the corrupt paths are neglected and more path creations processes are executed. With increase in mobility this overhead increases due to path instability and under performance.

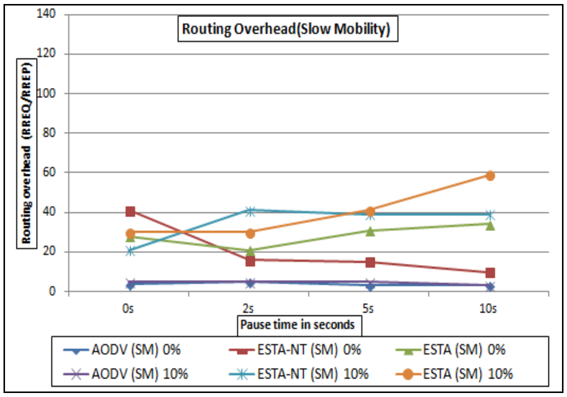

Figure 12.Routing Overhead vs Pause Time at slow mobility

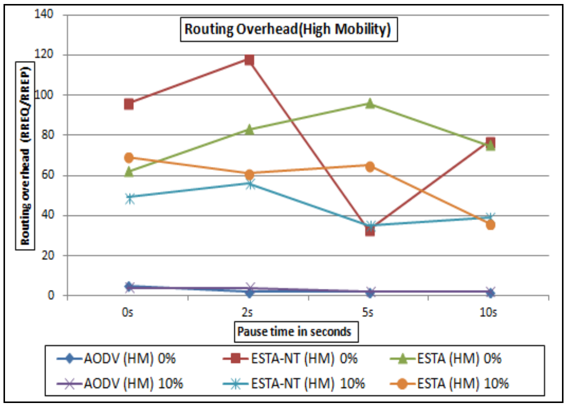

Figure 13. Routing Overhead vs Pause Time at high mobility

Secondly, the effect of node density is studied at varying node mobility. In Figures- 14 & 15 the AODV cases have low routing overhead again due to inherent nature of the protocol to suppress the duplicate RREQs and send single RREP in presence or absence of malicious nodes. But for the ESTA and ESTA-NT cases the routing over head is again high due to the fact that multiple path creation is done so multiple RREQs packets are processed and multiple RREPs are being sent. For ESTA and ESTA-NT cases at slow mobility the number of control packets are more at low density but increasing density the count reduces. But for cases with high mobility density the count is comparatively low to fact that shorter routes were created due to which path breakage is less.

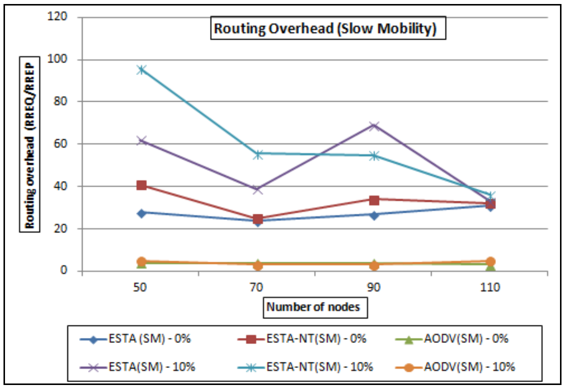

Figure 14. Routing Overhead vs Node Density at slow mobility

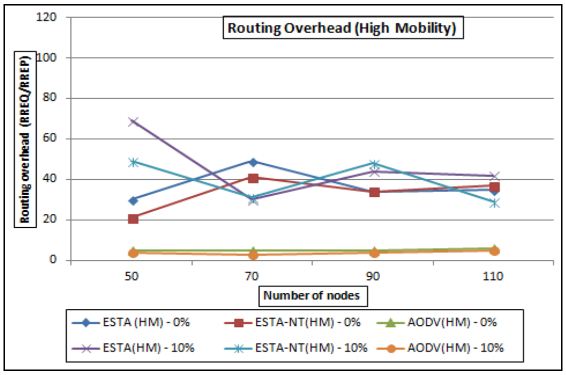

Figure 15. Routing Overhead vs Node Density at high mobility

6. CONCLUSION AND FUTURE WORK

In this paper, the proposed protocol ESTA and its variation with No-Trust ESTA-NT are evaluated in presence of blackhole node attack in a MANET . Multiple paths are used for data transmission in the proposed solution. A combination of trust and asymmetric cryptography to ensure integrity of the data and control packets, while maintaining the high delivery ratio for data packets. The route formation process is not computationally heavy but it is successfully able to suppress the non-performing paths. Based on the simulation results, it can concluded that, under different conditions, the performance of ESTA is better than AODV, but at a cost of additional delay to provide security. The trustworthiness of the paths is helpful in reducing the delay, packet droppage and routing overhead. In future, we would extend the approach to introduce IDS mechanism and shall focus to reduce and optimize the extra delay introduced in the protocol.

REFERENCES:

[1] Hu, Yih-Chun, and Adrian Perrig. "A survey of secure wireless ad hoc routing."*IEEE Security & Privacy* 3 (2004): pp- 28-39..

[2] Sen, Jaydip, Sripad Koilakonda, and Arijit Ukil. "A mechanism for detection of cooperative black hole attack in mobile ad hoc networks." In *Intelligent Systems, Modelling and Simulation (ISMS), 2011 Second International Conference on*, IEEE, 2011, pp. 338-343.

[3] Royer, Elizabeth M., and Charles E. Perkins. "An implementation study of the AODV routing protocol." In *Wireless Communications and Networking Conference, 2000. WCNC. 2000 IEEE*, vol. 3, IEEE, 2000, pp. 1003-1008.

[4] Deng, Hongmei, Wei Li, and Dharma P. Agrawal. "Routing security in wireless ad hoc networks." *Communications Magazine, IEEE* 40.10 (2002): pp- 70-75.

[5] Gupte, Siddhartha, and Mukesh Singhal. "Secure routing in mobile wireless ad hoc networks." *Ad Hoc Networks* 1.1 (2003): pp - 151-174.

[6] Amara korba Abdelaziz, Mehdi Nafaa, and Ghanemi Salim. "Analysis of Security Attacks In AODV." (2014), pp. 752-756.

[7] Eichler, Stephan, and Christian Roman. "Challenges of secure routing in MANETs: A simulative approach using AODV-SEC." In *Mobile Adhoc and Sensor Systems (MASS), 2006 IEEE International Conference on*, IEEE, 2006, pp. 481-484.

[8] Abdelshafy, Mohamed, and Peter SB King. "Analysis of security attacks on AODV routing." In *Internet Technology and Secured Transactions (ICITST), 2013 8th International Conference for*, IEEE, 2013, pp. 290-295.

[9] Zapata, Manel Guerrero, and Nadarajah Asokan. "Securing ad hoc routing protocols." In *Proceedings of the 1st ACM workshop on Wireless security*,. ACM, 2002, pp. 1-10.

[10] Mishra, Anadi, Ranjeet Jaiswal, and Shantanu Sharma. "A novel approach for detecting and eliminating cooperative black hole attack using advanced DRI table in Ad hoc Network." In *Advance Computing Conference (IACC), 2013 IEEE 3rd International*, IEEE, 2013, pp. 499-504.

[11] Tamilselvan, Latha, and V. Sankaranarayanan. "Prevention of blackhole attack in MANET." In *Wireless Broadband and Ultra Wideband Communications, 2007. AusWireless 2007. The*

2nd International Conference on, IEEE, 2007, pp. 21-21.

[12] Tan, Siew-Chong, and Keecheon Kim. "Secure Route Discovery for preventing black hole attacks on AODV-based MANETs." In *ICT Convergence (ICTC), 2013 International Conference on*, IEEE, 2013, pp. 21-21.

[13] Yerneni, Rajesh, and Anil K. Sarje. "Enhancing performance of AODV against Black hole Attack." In *Proceedings of the CUBE International Information Technology Conference,* ACM, 2012, pp. 857-862

[14] Jalil, Kamarularifin Abd, Zaid Ahmad, and Jamalul-lail Ab Manan. "Securing Routing Table update in AODV routing protocol." In *Open Systems (ICOS), 2011 IEEE Conference on,* IEEE, 2011, pp. 116-121.

[15] Cerri, Davide, and Alessandro Ghioni. "Securing AODV: the A-SAODV secure routing prototype." *Communications Magazine, IEEE* 46, no. 2 (2008): pp- 120-125.

[16] Chang, Jian-Ming, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai. "Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach." *Systems Journal, IEEE* 9, no. 1 (2015): pp- 65-75.