Future Internet **2015**, *7*, 342-362; doi:10.3390/fi7030342

OPEN ACCESS

future internet

ISSN 1999-5903

www.mdpi.com/journal/futureinternet

Article

Enhanced Secure Trusted AODV (ESTA) Protocol to Mitigate Blackhole Attack in Mobile *Ad Hoc* Networks

Dilraj Singh * and Amardeep Singh

Department of Computer Engineering, Punjabi University, Patiala 147002, Punjab, India;
E-Mail: amardeep_dhiman@yahoo.com

* Author to whom correspondence should be addressed; E-Mail: dilraj@pbi.ac.in;
Tel.: +91-781-456-6122.

Academic Editor: Andrew Hudson-Smith

Received: 15 July 2015 / Accepted: 14 September 2015 / Published: 23 September 2015

Abstract: The self-organizing nature of the Mobile *Ad hoc* Networks (MANETs) provide a communication channel anywhere, anytime without any pre-existing network infrastructure. However, it is exposed to various vulnerabilities that may be exploited by the malicious nodes. One such malicious behavior is introduced by blackhole nodes, which can be easily introduced in the network and, in turn, such nodes try to crumble the working of the network by dropping the maximum data under transmission. In this paper, a new protocol is proposed which is based on the widely used *Ad hoc* On-Demand Distance Vector (AODV) protocol, Enhanced Secure Trusted AODV (ESTA), which makes use of multiple paths along with use of trust and asymmetric cryptography to ensure data security. The results, based on NS-3 simulation, reveal that the proposed protocol is effectively able to counter the blackhole nodes in three different scenarios.

Keywords: AODV; Multipath ROUTING; encryption; blackhole attack; trust

---

1. Introduction

A Mobile *Ad hoc* Network (MANET) is a collection of wireless mobile nodes that can be deployed rapidly as a multi-hop packet radio network without the presence of any or existing infrastructure [1]. Such networks can be used to enable next generation network applications like battlefield operations, emergency rescue, commercial or personal usage in terms of resource or information sharing. As the MANETs belong to a category of infrastructure-free networks, they have some special characteristics,

like limited bandwidth and unreliable wireless medium for communication, dynamic network topologies and constantly changing member nodes. While these characteristics provide flexibility in terms of deployment of MANETs, they also introduce certain security concerns that are absent or less prevalent in infrastructure-based networks. Thus, traditional routing and security schemes cannot be adapted as such for MANET scenarios. The main security issues for any network can be classified as Authentication, Authorization, Non-Repudiation, Integrity and Confidentiality, but, in the case of an *ad hoc* network, there exists another aspect that is quite important, *i.e.*, Availability. The attacks that happen in MANETs for various reasons can be broadly classified as Passive and Active attacks [2].

The security-related aspects in MANETs are interesting and an emerging area of research among researchers. One particular area of focus is secure transmission of data in MANETs. In order to have secure transmission, a critical and basic aspect is route selection, which depends upon the routing protocol being used. The routing protocols in MANETs are classified as Proactive, Reactive and Hybrid routing protocols [1]. In proactive routing protocols, each node maintains predetermined routing information to the destination. The Optimized Link State Routing (OLSR) and Destination Sequenced Distance Vector (DSDV) belong to this category. The reactive routing protocols, however, start the route established whenever it is required, such as *Ad hoc* On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR). The hybrid protocols contain the features of both proactive and reactive routing protocols like Zone Routing Protocol (ZRP).

In this paper, a solution is proposed for secure data transmission by extending the AODV routing protocol and making use of trusted multiple routes and asymmetric key encryption. In order to provide loop free routing, special control packets are introduced. Section 2 of the paper provides an insight into some of the existing security solutions. Section 3 highlights the problem and security needs. In Section 4, the details of the proposed solution are described. For analysis purposes, the simulation setup details and results are provided in Sections 5 and 6. In Section 7, a comparative analysis is presented between the reviewed and proposed solution. Section 8 highlights certain limitations of the proposal along with future scope. Finally, in Section 9, the conclusion is presented.

2. Related Work

The topic of MANET security and secure routing has been a focus of the research community for quite some time. One of the important reasons that attract this focus is the variety of attacks that have been defined. The work of different researchers has tried to solve these challenges. Many different types of attacks have been proposed so far, among them blackhole attack, wormhole attack, rushing attack, packet alteration attack and spoofing attack, *etc*. The authors in [2–8] have provided a detailed overview of various attacks. In this section, a brief overview of some of the existing work is presented and will focus on various attempts that have been published in the literature to mitigate and counter blackhole attacks and the use of cryptography.

Zapata and Asokan [9] proposed Secure AODV (SAODV), one of the widely known security enhancements for AODV. SAODV takes into account the resource-limitation and dynamic nature of network nodes and does not depend upon any Certificate Authority (CA). For security purposes, it makes use of a digital signature and one-way hash chain to protect the packet. As suggested by the author, if the digital certificates are not used, an impersonation attack could happen. Therefore, the Route

Reply (RREP) messages can only be generated by destination nodes; in the case of intermediate nodes replying to some RREQ, then it has to perform the activity of signing the packet twice; this process is known as double signature and adds an extra processing load. SAODV uses a hash chain to protect mutable fields like hop count. It further requires all the nodes of the network to have knowledge of the public certificates of other nodes. SAODV messages are significantly heavy due to the presence of digital signatures. As the SAODV uses an asymmetric cryptographic, each packet generated by the node requires a signature and every time it receives a routing message (even an intermediate node), it has to execute the verification process. Although it helps in communicating nodes to find secure paths, it is computationally heavy.

Tamilselvan and Sankaranarayanan [10] proposed an approach in which the route requesting node waits for the responses from neighboring nodes, which includes the next hop details, for a predetermined time value. After the wait period is complete, the entries in the Collect Route Reply Table (CRRT) are cross checked to see if there is any repetition of the next-hop-node details or not. If any such information is found in the reply paths, it assumes the paths are correct or the chance of malicious paths is limited. The solution adds a delay and the process of finding a repeated next hop is an additional overhead. In addition, the focus here is to find non-malicious nodes only, and it does not focus on the integrity and confidentiality of the data packets transmitted.

Tan and Kim [11] proposed an extension of AODV routing protocols known as Secure Route Discovery for AODV (SRD-AODV) to mitigate the effect of the blackhole attacks. In the proposed solution, depending upon network environment and possible node density, a threshold value for the Sequence number is defined, as AODV makes use of a Sequence number to maintain the fresh and loop free paths. In SRD-AODV, upon receiving the RREQ, the destination node compares the Sequence number present in the packet and its routing table. If the value is higher, the sequence number in the destinations routing table is updated, otherwise the higher value present in the table is used. When the sequence number reaches the threshold value, it is reset. Similarly, a check of the same nature is performed at the requesting node, but, if the sequence number is high, it ignores the RREP, assuming it to be sent by some malicious node. This solution counters the blackhole node attack but fails to counter any other form of attack.

In [12], authors proposed a secure routing protocol, Authenticated Routing for *Ad hoc* Networks (ARAN). ARAN provides security against external attacks by introducing authentication, message integrity and non-repudiation. Every node in ARAN has a certificate from a trusted server; therefore, it becomes difficult for malicious nodes to participate in the routing process. Processing in ARAN is divided into three stages: a preliminary certification process, a mandatory end-to-end authentication stage and an optional stage providing a secure shortest path. ARAN doesn't record the entire route information and also doesn't consider the total number of hops in the route discovery. As it makes use of public key cryptography to protect routing process, the time delay of signature generation and verification is significant. In general, significant time delay at each hop causes unacceptable route acquisition latency.

Deng, Li and Agrawal [13] have suggested a mechanism to counter the blackhole attack that could be initiated by the malicious node present in *ad hoc* networks. In their proposed scheme, they have modified the RREP packet by adding an extra field that carries information about the one-hop next node. After the RouteReply packet is received from an intermediate node, a special RREQ is generated for the one-hop next node of the replying node. This is to ensure that the path conveyed by RREP exists from

the intermediate node to the destination node or not. If the reply is sent by that node, the route is considered to be safe and free of blackhole nodes. While this scheme is successful in eliminating the blackhole attack by a single attacker, it fails completely in identifying a cooperative blackhole attack involving multiple malicious nodes or other forms of passive attacks.

In [14], techniques based on symmetric encryption to protect the network from external attacks are used. All the nodes in the network have to obtain a one-time public and private key pair from a Certification Authority (CA), along with a CA key, which have to be used while exchanging the session keys by the communicating nodes. These session keys are used to encrypt both routing and data packets. Although this solution is capable of protecting the routing information and possible external attacks, maintaining a group secret for a one-hop neighbor all the time consumes a significant bandwidth. Even after using such a computationally heavy approach, it cannot counter the impersonating nodes because node authentication and data integrity are not guaranteed inside the group.

In [15], a new secure routing protocol, AODV-SEC, was proposed. This protocol is based on AODV and considers the main features of SAODV. As per the proposal, a trusted CA issues digital certificates along with encryption keys. This digital certificate is a new type of certificate, known as m-Cert, and contains only relevant information related to the certificate. This, in turn, reduces the overhead by 50%. This m-Cert is X.509 standard compatible. With this approach, the path that is formed may not be the shortest.

Yi, Naldurg and Kravets [16] proposed Security Aware ad hoc Routing (SAR) protocol. This takes into consideration the trust level of intermediate nodes during the route formation phase. In most protocols, the length of the route is the only metric used. The required trust level is specified in the modified RREQ packets. When intermediate nodes receive an RREQ packet with a particular trust level, the node can only process the packet or forward it if it can provide the required trust level. However, limited security is achieved at the cost of performance degradation in terms of latency time and, in certain cases, the route formation even fails.

The authors of [17,18] has raised a very critical aspect related to the research being done in the field of MANETs specially related to the use of simulation tools. In a survey [17], it was concluded that most of the research articles related this field used simulation for experimentation and random waypoint models was used by 64% of simulations. The basic idea for use of simulators is justified by the fact that deployment of real networks and gathering performance metrics is cumbersome, time consuming and economically not feasible for most of cases. Thus, the use of simulators provides ease of setting up and modifying network scenarios easily, and monitoring becomes more manageable. Furthermore, [18] have revealed the inherent limitations the simulation tools have in modeling the Media Access Control (MAC) and physical layer aspects of the network. It signifies that the results from a simulation tool are only good for approximation of the performance parameters. In this study, the use of multiple paths is also suggested as one of the possible ways to counter a security threat. In addition, there is a lack of consistency between the results of the same protocol being run on different simulation tools.

In addition to the brief overview of different approaches presented above, a variety of other approaches have been proposed by researchers based on promiscuous monitoring of packets, trust based proposal, by introducing new control packets, and data structures, *etc*. On the basis of the reviewed schemes above, it was observed that additional overhead is being incurred by the approaches like prior knowledge of certificates, extra processing by intermediate nodes, use of additional control packets to nail down bad nodes, or dependence on the CAs. Trust among the entities plays a vital role. Thus, in the

case of MANETs transmission through trusted parts can also save a lot of resources and provide a secure transmission, but trust alone is not sufficient to ensure the integrity and authenticity of the transmission. Thus, a new security framework is being proposed which does not depend upon any CA, saves resources of the participating peer nodes and does not require any knowledge about the network topology and density. It uses a combination of trust and cryptographic approach is used to safeguard of the data packets. As the cryptographic based computations are being done at the communication end, only so no additional load is incurred on the intermediate nodes, details are provided in Section 4.

3. Problem Statement

The AODV [19], being a reactive protocol, starts the route formation when the source node has some data for transmission. The AODV maintains and uses the same routing information as long as the transmission lasts or the route remains stable. It makes use of broadcasted RREQ messages to form paths and, upon receiving these RREQs, the intermediate nodes can forward them further or respond on behalf of the destination, in the case of them having a fresh path to the destination node, with an RREP message. The RREP is sent as a unicast message to the source node using information gathered by intermediate nodes. This process also helps the intermediate nodes to learn about the forward and reverse path between the communicating nodes. Other than using this information for data transmission, it could also be used for transmitting error notifications in the form of an RERR message. This approach helps in reducing the control traffic in the network, which, in turn, gives it an edge over proactive routing protocols used by MANETs.

In AODV, the intermediate nodes and destination node process the RREQs only once per request ID, so formation multiple routes are not taken into consideration. In the case of high node mobility of intermediate nodes or sparsely populated networks, the route breakage could be frequent, which can lead to loss of control packets or data packets. Therefore, in the case of mission critical operations, the basic purpose of the network formation could be defeated. In addition, if malicious nodes are present in the network, they could respond to the RREQ messages and successfully become part of the transmission path. 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. Relatively recent AODV literature suggests that the use of a single path for transmission reduces the delay and excessive control data, but, in adverse network conditions, this could make the network crumble. Hence, the question arises as to how such situations should be dealt with. It is equally important that the confidentiality and integrity of the transmission should be upheld, for which there is no inbuilt mechanism available in AODV. The protocol should be capable of scaling up without much dependency on the presence of CAs or key management systems for the authorization of joining nodes.

In reference to existing literature, the existing solutions for secure routing are based on the assumptions of the existing trusted server, CAs for key management, or prior knowledge of security secrets of nodes that contradict the basic character of the MANETs. If the dynamic nature of intermediate nodes is taken into consideration during the routing phase, an extra computational load is imposed on the nodes. As in Figure 1, there are different multi paths available, but most of the protocols take only the shortest one as final. So, if a node is tampered with or overpowered to perform malicious activities, the transmission task can be hijacked. Taking into consideration such weaknesses of current techniques,

the aim is to design a solution that makes use of multiple paths to perform better in adverse environments and do end-to-end message authentication.

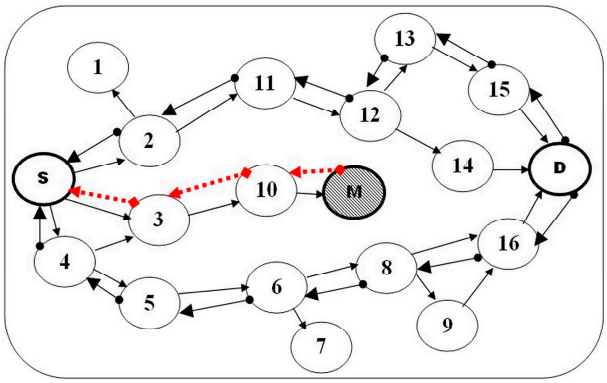

Figure 1. Sample Network Topology.

4. Proposed Solution

Based on the review of the existing security enhancements available for MANETs' environment, a multiple path-based solution is proposed (Figure 1). In the proposed solution for the data transmission, multiple loop free and disjoint paths are utilized. Due to the absence of any CA or heavy computations-based processes during the route establishment phase, it becomes important that integrity and confidentiality of the data transmission should remain intact. So, to fulfill this aspect, the use of asymmetric cryptography and trust of paths is based on direct observations of the source node.

4.1. Network Model

The considered MANET consists of nodes having similar features such as transmission range, pause time and mobility in terms of m/s. The nodes can roam randomly or remain stationary in a location for an arbitrary period of time. The nodes perform in a cooperative fashion using peer-to-peer communication over the shared bandwidth-constrained and error-prone wireless channel. All the nodes in the network have bi-directional links. In order to have ease of identification, all nodes are assumed to have a unique non-zero node ID. Unlike some existing security frameworks, in the proposed solution, the network does not contain any CA, but all nodes perform extra functions such as key sharing and maintaining backup queues in order to ensure security and high performance. With the presence of a CA, the network may have a single point of failure. To demonstrate the attack, there may exist a varying number of blackhole nodes in the network at different locations.

4.2. Blackhole Attack

The blackhole node attack belongs to a category of active attacks. In this case, the blackhole node responds to the RREQ messages with a very high sequence number and claims to have the shortest path to the destination. As it responds with a very high sequence number, it replaces any route entry present in the source nodes routing table. Once the data transmission starts through, it silently drops all the data packets.

4.3. Route Formation

For the route establishment phase, two new structures are introduced "LINK_TABLE" and "LINK_INFO". The "LINK_TABLE" is used by the nodes to store the multiple RREQ details they receive from neighboring nodes (Table 1). Information from this table is used by nodes to propagate RREP packets to source nodes. Once an intermediate node becomes part of a path, it generates and broadcasts a control packet, "LINK_INFO" (Figure 2), to update its and the next used node's availability in the "LINK_TABLE" of neighboring nodes. 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.

Table 1. Link table.

Sender IP	Timestamp	Request ID	Origin IP	Destination IP	Flag
10.10.1.15	+1286351.0ns	1	10.10.1.32	10.10.1.32	-
10.10.1.2	+9034998.0ns	1	10.10.1.32	10.10.1.32	-
10.10.1.40	+16931601.0ns	1	10.10.1.32	10.10.1.32	-
10.10.1.28	+23828591.0ns	1	10.10.1.32	10.10.1.32	-

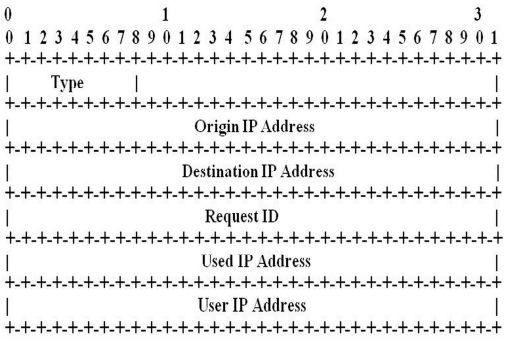

Figure 2. Link info control packet.

4.4. Packet Transmission at Source Node

When the source nodes start receiving the RREP packets, they are stored in a newly defined route table that is capable of holding multiple entries for the same destination nodes, unlike the routing table in AODV (Table 2).

Table 2. New routing table.

Destination IP	Gateway IP	Interface IP	Flag	Expire	Hops
10.10.1.27	10.10.1.1	10.10.1.32	DOWN	−1.58	4
10.10.1.27	10.10.1.42	10.10.1.32	DOWN	1.95	5
10.10.1.27	10.10.1.9	10.10.1.32	UP	8.50	4
10.10.1.27	10.10.1.6	10.10.1.32	UP	9.87	6
10.10.1.27	10.10.1.42	10.10.1.32	UP	11.20	7

As per algorithms defined in Algorithm 1, upon receiving the first RREP, a timer is initiated for "1 s", so that multiple routes can be established. The transmission starts once the count of the minimum number

of packets and valid route counts is achieved; the assumed values are four and two, respectively. The transmission is always done via the queue only. The purpose of using the queue is to perform the encryption on every data packet that is transmitted. Another important consideration for using the queue is to divide the packets based on the number of available routes, using the following formula 1 & 2:

$$PR = N_{TQ}/VR \quad (1)$$

$$RP = \text{mod}\ (N_{TQ}, VR) \quad (2)$$

where:

PR = Packets per Route, *RP* = Remaining Packets, N_{TQ} = Packets in Transmission Queue, *VR* = Valid Route count.

Algorithm 1. Enhanced Secure Trusted *Ad Hoc* On-Demand distance vector (ESTA) packet transmission.

```
1: InitializeNodes() & GenerateCertificates().
2: GenerateData() for transmission.
3: Enqueue Datapacket & Raise RREQ.
4: Process RREQ RecvRequest().
5: Initialize Timers for Multiple Routes & HelloProcessing.
6: If Timer's set at Step5 > SetTime.
        {
7:      Fetch all valid routes validRouteCount().
8:      If validRouteCount >= 1, then:
                {
9:              Append BQ to TQ.
10:             If Px < 4.
11:                     then: wait till Px ≥ 4
12:             Else.
                        {
13:                     Initialize PPR = Px/valid route count.
14:                     Initialize RP = Px valid route count.
15:             For every route in valid route list repeat steps
16:                     If GWstatus = 0 or GWstatus = 1, then:
17:                             continue.
18:                     Else:
                                {
19:                             set count: = 0.
20:                             While count ≤ PPR + RP.
21:                             SendPacketFromQueue().
22:                             Endwhile.
23:                             set RP: = 0.
                                }
                        }
                }
```

Algorithm 1. *Cont.*

24: Else.
25: Raise RREQ.
}
26: Process packets RouteInput().
27: if DataPacket.
{
28: Decrypt () & initiate Timer for DeliveryInfo() broadcast.
29: if Timer set at Step 28 > SetTime.
SendDeliveryInfo().
}
30: At source RecvDeliveryInfo().
31: Compare DeliveryInfo P_{ID} with BQ P_{ID}.
32: Increment the GW_{Status} for performing Gateway nodes.
33: Clear BQ where P_{ID} == $BQ(P_{ID})$.
34: if TQ ! = 0 GOTO Step 3.

Where:

BQ: Backup Queue; *TQ*: Transmission Queue; P_x: Packet Count; *PPR*: Packets Per Route; *RP*: Remaining Packets; *PID*: Packet ID; GW_{Status}: Gateway Node Status.

In order to ensure end-to-end security of transmission, in terms of the confidentiality, authenticity and integrity, the Rivest-Shamir-Adleman (RSA) based asymmetric encryption is being used in the proposed solution. The RREQ and RREP packet are modified to carry Public Keys, (Figures 3 and 4, respectively).

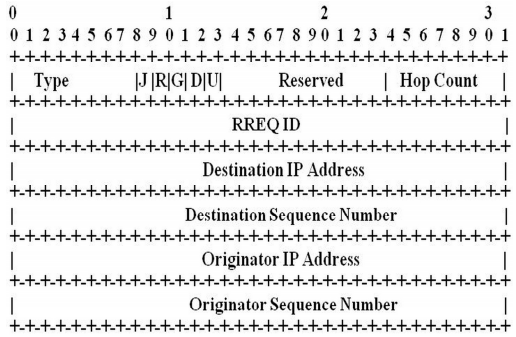

Figure 3. Modified RREQ.

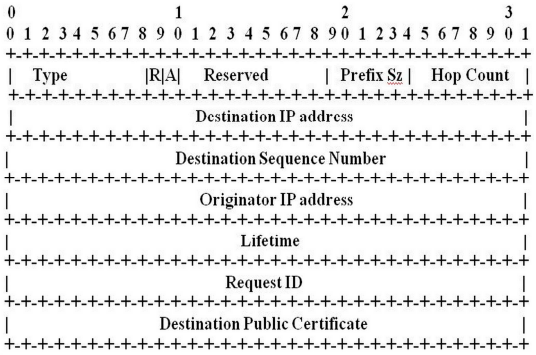

Figure 4. Modified RREP.

In order to satisfy the authenticity of packets being sent by the genuine source, they are enhanced to carry node ID and timestamp value encrypted by the Private Key (EPiS) of source node *t′*. Meanwhile, to ensure the confidentiality and integrity of data, the encryption of the payload is done with the Public Key (EPD) of the destination node M_e. The encryption process at source end is as follows:

$$M_e = E_{PD} \text{ (Payload)} \tag{3}$$

$$t' = E_{PiS}(\text{NodeID,TIMESTAMP}) \tag{4}$$

$$\text{Data Packet} = \{(\{M_e\},)\ t'\} \tag{5}$$

4.5. Packet Processing at Destination

At the destination node, upon receiving the data packet, first, the *t′* is decrypted using the Public Key, EPS, of the source node. Upon successful execution of this step, the payload part is decrypted using the Private Key, EPiD, of the destination node.

In order to ensure maximum delivery, the destination node broadcasts a time bound delivery report of the packets it received. To perform this action, a new control packet was created "SEND_DELIVERY_INFO" (Figure 5)

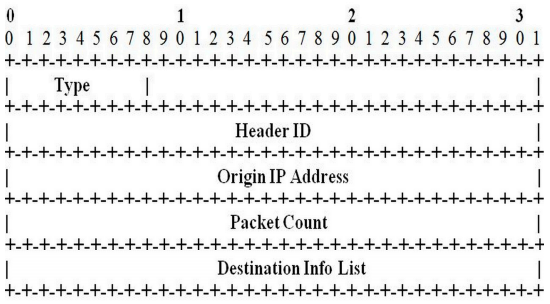

Figure 5. Delivery info control packet.

4.6. Trust Evaluation of Paths

To ensure the trustworthiness of the paths created, the direct observation mode is used by the source nodes. In order to record the trust values, a new data structure, "SOURCEINFO", is used. Based on the performance of the path, its Gateway node is assigned a trust value known as GWStatus. Let GWStatus(i, j) denote the level of direct trust of node "i" on its neighbor "j". Its values range from $0 \leq \text{GWStatus}(i, j) \leq 3$. In Table 3, the trust values and definitions are listed. By default, every new Gateway node is assigned a value of two.

Table 3. Trust values for Gateway Nodes.

Trust value	Definition
0	Absolute no trust
1	Partially trusted
2	Default trust
3	Full trust

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 is decremented. Fixed interval timers, t and t', are used to perform this check on the trust value for nodes, as shown in Equations (6) and (7). In the case of the trust value of node being 1, it is under observation and no packets are transmitted through this Gateway node, but it is 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.

$$t > \text{NetTraversalTime: } GW_{Status} = 1 \quad (6)$$

$$t' > 2 + \text{NetTraversalTime: } GW_{Status} = 0 \quad (7)$$

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. The complete process is depicted in the flowchart in Figure 6.

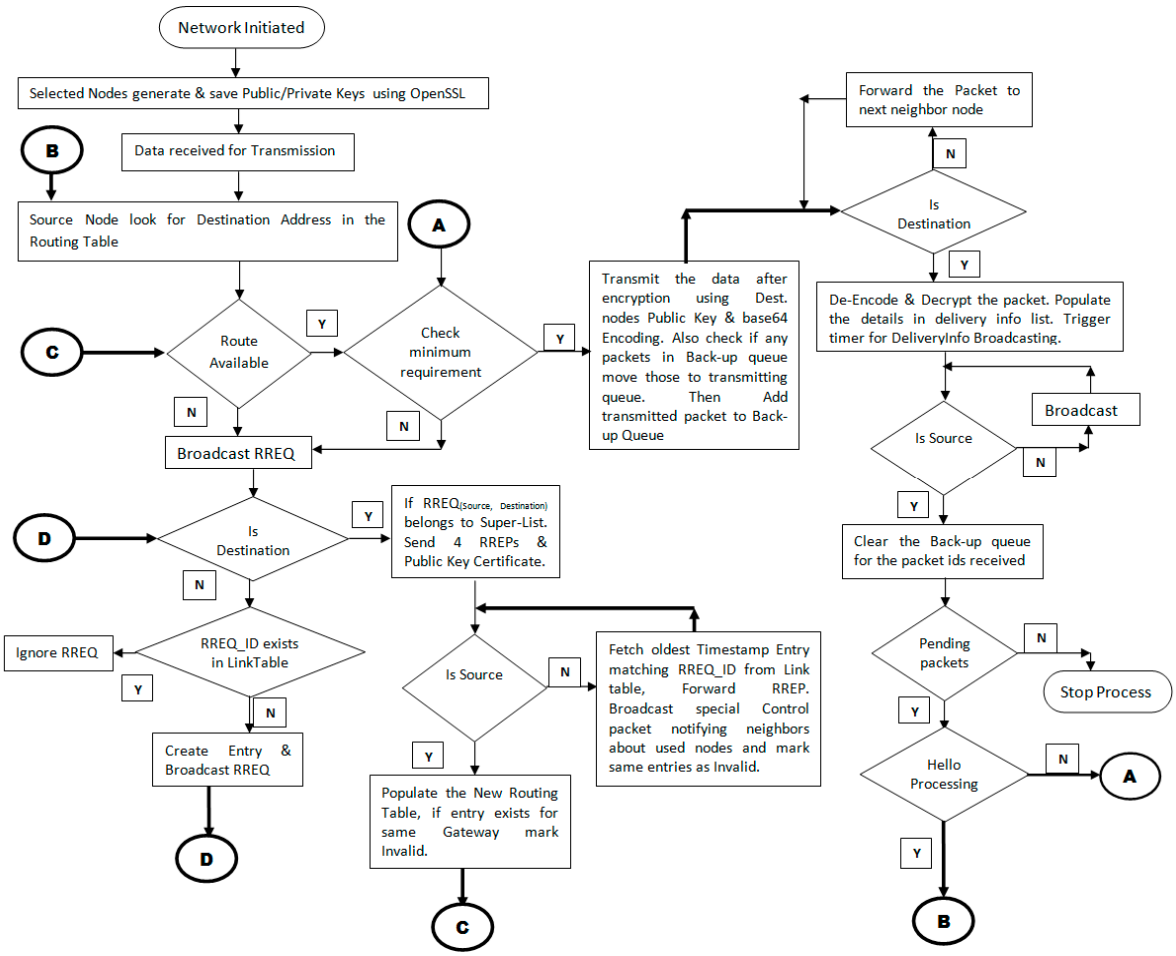

Figure 6. Flowchart for the ESTA processing.

5. Implementation and Simulations

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. Several modifications were also carried out on existing NS-3.19 modules to incorporate the various required node behaviors and the overall functionality of the proposed algorithm. In order to analyze the efficiency and other important aspects of the proposed solution ESTA is compared with the standard AODV protocol. In addition, to emphasize the effect of trust among the nodes in the network, a simulation was conducted with and without use of trust value in proposed solution.

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. The PDR is calculated using the Formula (8).

$$PDF = \frac{1}{n}\sum_{A=0}^{n}\frac{(Pr*100)}{Ps} \quad (8)$$

where:

Pr: Packets received at destination.

Ps: Packets transmitted from source.

A: application ID.

n: total applications.

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. The Formula (9) used for calculating the average value.

$$E = \frac{1}{n}\sum_{A=0}^{n}(tr - ts) \quad (9)$$

where:

tr: Time of first received packet at destination.

ts: Time of first received packet at source.

A: application ID.

n: total applications.

Average Throughput: The number of data bits delivered at the destination node in unit time. Its measure is bits per second (bps). The Formula (10) is used for the average throughput calculation:

$$T = \frac{1}{n}\sum_{A=0}^{n}\frac{(N*1024*8)}{Transmission\ Time} \quad (10)$$

where:

A: application ID.

N: total number of packets delivered.

n: total applications.

6. Results and Analysis

In order to study the effect of Area, Node Mobility, and varying number of Malicious nodes, different scenarios are taken into consideration with variation in node mobility, number of nodes and variation in malicious nodes numbers.

6.1. Scenario A

This scenario considers an area of 1000 m × 1000 m, 50 nodes with a transmission range of 250 m each. Seven CBR-based traffic generating applications are used which produce four packets/sec of size 1024 bytes. A fixed node mobility of 2 m/s is applied with varying pause time of 0, 5, 10, 15 and 20 s. In this case, a single blackhole node is being considered with its position strategically defined to interrupt possibly all traffic taken into consideration for simulation. In order to display the effect of trust among nodes in this scenario, a simulation was done by stopping the trust implementation in the proposed algorithm.

First, the PDF of AODV, ESTA and ESTA (no-Trust) with different pause times was studied. The results captured in Figure 7 show that, in the absence of any malicious node, the performance of all the nodes is high. However, there is a slight improvement with increase in the pause time. In this case, the performance of ESTA (no-Trust) is higher than ESTA. This happens due to the absence of any check mechanism on the performance of the gateway nodes, which do have connectivity to the destination, but, due to possibly longer paths, the delivery reports are taking more time to reach source nodes. So, due to this delay, the trust value is getting reduced and these gateways are not being in a trusted version. With the introduction of a blackhole node, the performance decreases overall. A unique feature noticed in this case is that, with no pause time and a moderate node speed, the performance of the ESTA is very high. If trust mechanism is not implemented, the performance of ESTA (no-Trust) is lower, but still much better than AODV.

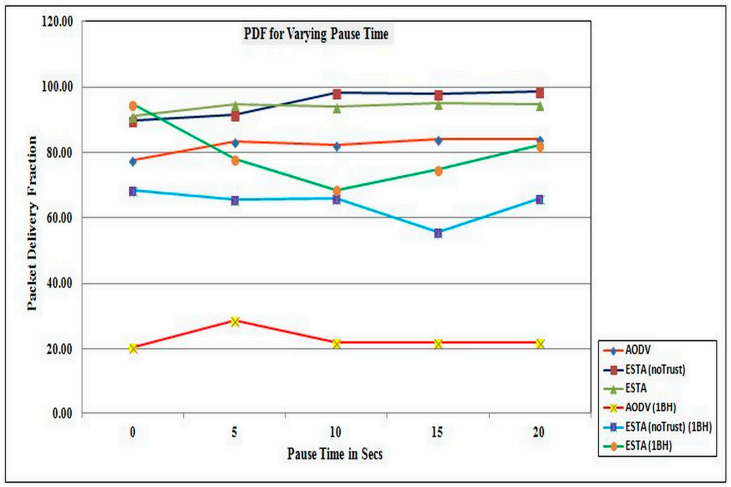

Figure 7. PDF for varying Pause Time.

Second, for this scenario, the average end-to-end delay for the first data packet delivery is studied. Results captured in Figure 8 show that the delay in the case of AODV is always lower than the ESTA and ESTA (no-Trust). This is due to a wait time feature upon receiving the first RREP, so as to gather more than one route before the transmission begins. In the case of ESTA, in the absence of any malicious nodes, the delay for the first packet is quite high in the case of no pause on the node mobility, whereas, in the presence of the malicious node and more pause time, the delay is higher for the first packet delay. This is due to the fact that, with fast mobility, the nodes are able to form more routes as and when required, whereas, with more pause time, the non-performing nodes still exist in the same area, causing delays.

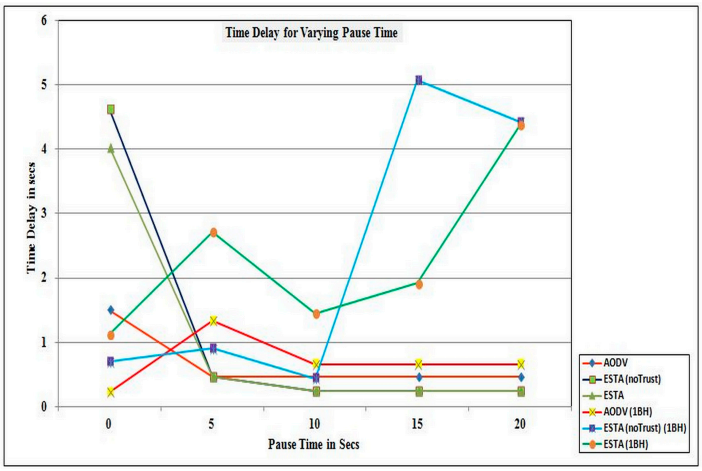

Figure 8. Time delay for varying pause time.

Third, the throughput of the AODV, ESTA (no-Trust) and ESTA, captured in Figure 9. The throughput of the AODV and ESTA variants are high in the absence of blackhole nodes. However, if a blackhole node enters the network, the performance of AODV degrades substantially, whereas the ESTA variants perform fairly. The performance of ESTA is good, both at 0 pause time and high pause time. The reason for this behavior is the formation of new paths due to node mobility or malicious paths being suppressed, respectively, in case some of the paths do not perform well.

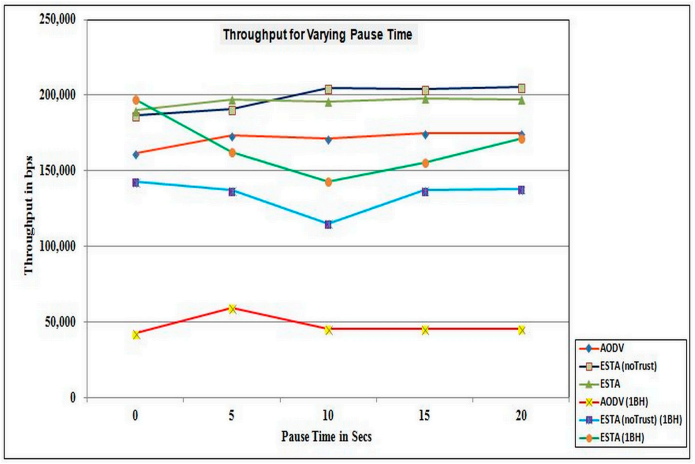

Figure 9. Throughput for varying pause time.

6.2. Scenario B

In this scenario, the area of network is 1000 m × 1000 m, 50 nodes with a transmission range of 250 m each. A CBR-based traffic generating application is used which produces four packets/sec of 1024 bytes; in total seven applications are used. Two different node mobility speeds are simulated, (a) Slow Mobility (SM) with node speed of 2 m/s and a pause time of 5 s; (b) High Mobility (HM) with node speed of 20 m/s and pause time of 2 s. Varying percentages of malicious nodes, 0%, 1%, 5%, 10%, 15% and 20% are introduced in both cases.

First, the study is focused on the PDF of AODV and ESTA in the presence of a varying number of blackhole nodes, comparing their performance in varying mobility as well. As seen in results captured

in Figure 10, the AODV performs well when the node mobility is low and in the absence of blackhole nodes, but, with an increasing number of blackhole nodes, the performance degrades drastically and, in the case of high mobility, it reaches almost to 0%. Whereas the ESTA performs well when the node mobility is low, but, with high mobility and an increasing number of blackhole nodes, its performance also degrades. However, it still performs far better than AODV in an adverse environment.

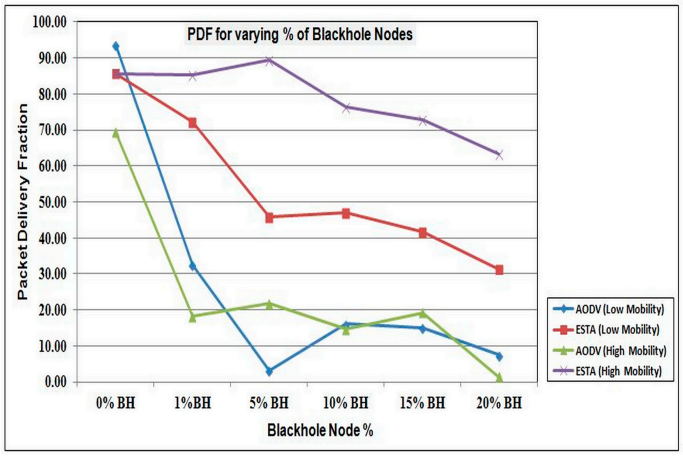

Figure 10. PDF for varying % of blackhole nodes and mobility.

Second, the focus is the average end-to-end time delay in the delivery of the first data packet. The results shown in Figure 11 illustrate that AODV has very low delay compared to ESTA; this is due to the fact that PDF in AODV is very low and a few applications are only able to partially perform transmissions. 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.

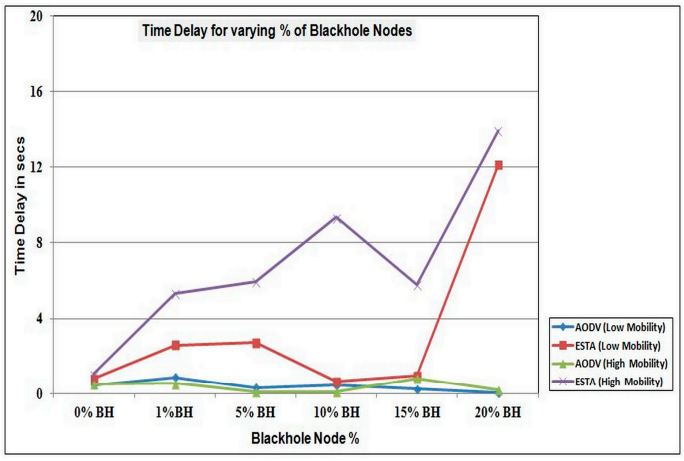

Figure 11. Time delay for varying % of blackhole nodes and mobility.

Third, the throughput of AODV and ESTA, and the results are captured in Figure 12. As in the case of PDF, the performance of the ESTA, in terms of throughput, is quite higher than standard AODV. However, with slow mobility, even if the blackhole node percentage is high, it performs fairly.

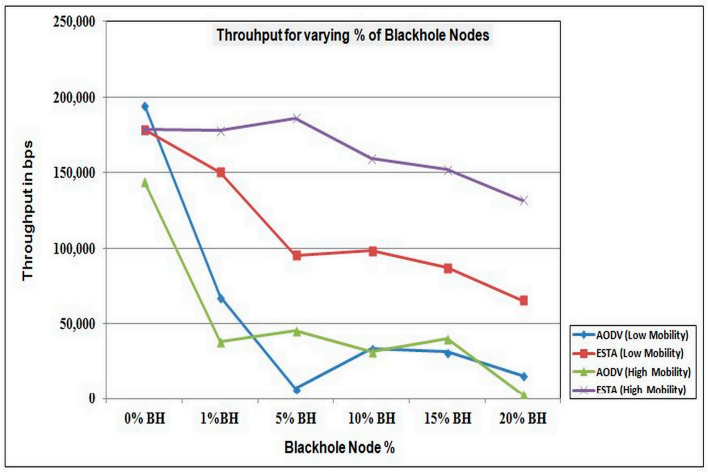

Figure 12. Throughput for varying % of Blackhole nodes and mobility.

6.3. Scenario C

In this scenario, the focus is the effect of the network area and a varying number of nodes. The two different networks taken into consideration are 1000 m × 1000 m and 1500 m × 1500 m, with varying number of nodes 50, 70, 90, 110 and 130. The transmission range of nodes is 250 m each and seven CBR-based traffic generating applications are used, which produce four packets/sec with size of 1024 bytes. A fixed node mobility of 5 s pause time and node speed of 10 m/s is applied. A strategically placed single blackhole node is considered to possibly interrupt all traffic taken into consideration for simulation.

First, the PDF of AODV and ESTA in the presence of a varying number of nodes and different network sizes is analyzed. Based on the results captured in Figures 13 and 14, in a small area, apparently due to high density of the nodes, the performance of ESTA is almost equal to the AODV. However, with the introduction of a blackhole node, the PDF of ESTA remains almost stable, while the AODV PDF decreases considerably. Likewise, the same trend is visible in a large area, with the exception that, with low node density, the performance is comparatively bad. This happens because route formation is not successful in AODV or ESTA.

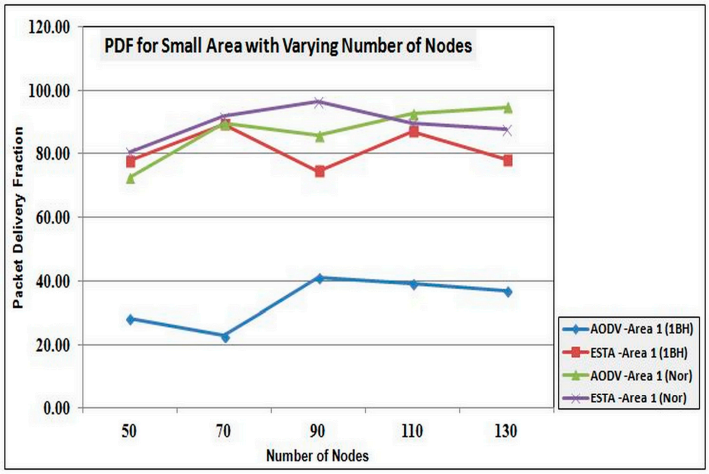

Figure 13. PDF for varying nodes in a small area.

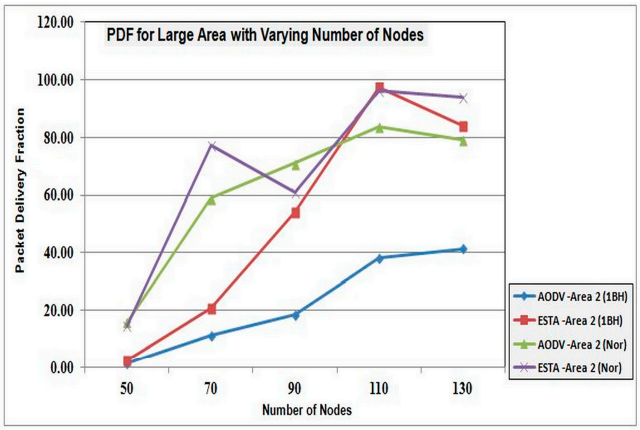

Figure 14. PDF for varying nodes in a large area.

Second, for this scenario the focus is average end-to-end delay for the first data packet delivery. Results in Figures 15 and 16 shows that the delay in the case of AODV is always lower than the ESTA, irrespective of the network area or the number of nodes. However, the ESTA shows exceptional behavior in a particular case where the network is attacked by a strategically placed blackhole node. Similar behavior was noticed for ESTA in a bigger network area with no malicious node having exceptionally high delay and exceptionally low delay in the presence of blackhole nodes. Likewise, the delay in the case of ESTA is also high due to the inclusion of a wait period for the multiple route gather phase.

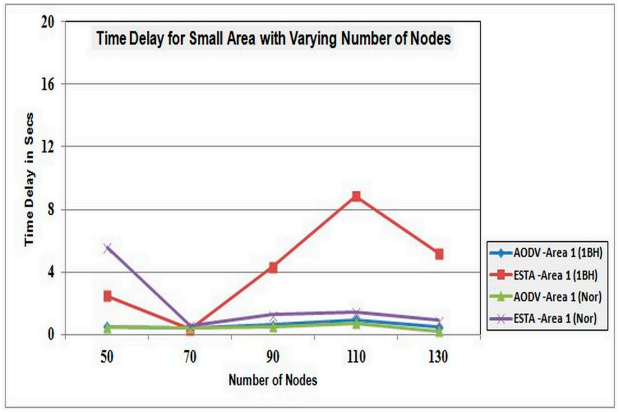

Figure 15. Time delay for varying nodes in a small area.

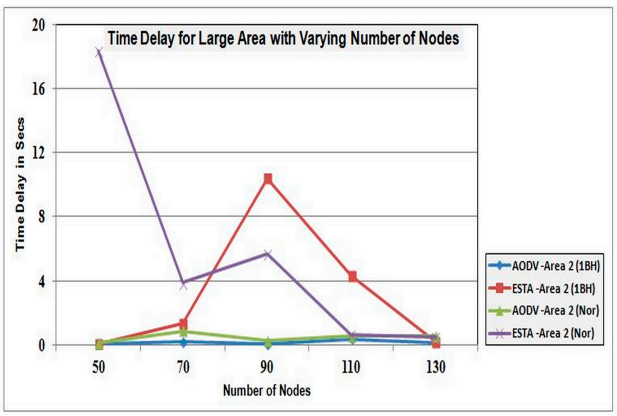

Figure 16. Time delay for varying nodes in a large area.

Third, the throughput of AODV and ESTA, and the results are captured in Figures 17 and 18. In the case of a small area and a good node density, the throughput of AODV and ESTA is quite high, but, in the case of AODV with the inclusion of a blackhole node, the performance degraded. Similarly, for a larger network area and good node density, the performance is good. However, with low node density, the throughput for both protocols is very low.

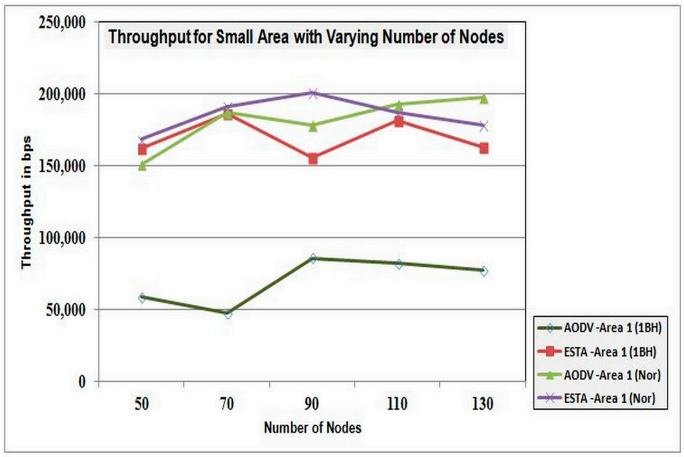

Figure 17. Throughput for varying nodes in a small area.

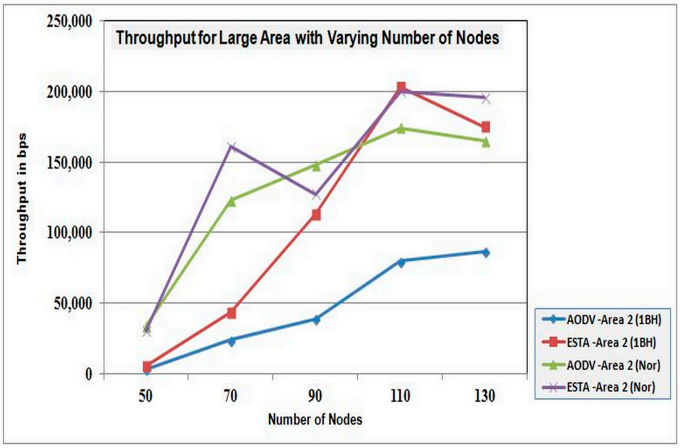

Figure 18. Throughput for varying nodes in a large area.

7. Comparative Analysis

Based on the simulation results presented above, the proposed solution performs well in different scenarios with varying conditions and in presence of malicious nodes. Though it is not possible to perform a simulation based comparison of the proposed solution with other existing security framework as their implementation for NS-3 simulator are not available. But, based on the review of the existing works and results of the simulation of proposed framework a comparative analysis is presented. As compared to SAODV [9] the proposed ESTA does need to have prior knowledge of all public certificates of the participating nodes, only the communicating nodes need to exchange the certificates as and when required, which saves a lot of memory and saves resources that would be required to handle the certificates in case of bigger networks. Furthermore, during the route formation phase, the additional

computations being done by the nodes, though, provide a safe path but consumes a lot of resources. Whereas, in ESTA, no precautions are taken into consideration during this phase, which saves the resources of the intermediate nodes but at a cost of delay and some certain amount of performance degradation due to selection of corrupt path having malicious nodes which are anyways routed out later due to their non-performance, which leads to trust value degradation. In [10], the approach proposed by the authors depends upon multiple route replies, which ESTA also relies on, but in the approach of [10], the intermediate nodes can also reply, which is prohibited in ESTA. In addition, no comparison of the common nodes is done in ESTA as the routes formed are dis-joint paths. Even after introducing delay to ensure correctness of the path, the multiple path transmission is not done which could help in load balancing. In addition, the integrity of the data packets cannot be ensured in case of passive attacks, which ESTA can handle. The solution proposed by Tan and Kim [11] is based on a consideration of network size and density which defines the maximum value for the sequence number. In the true sense of MANETs, it is not possible to judge these parameters until it is a pre-defined network defying the charter of the *ad hoc* networks. Whereas ESTA does not depend upon any such considerations, it can scale well as the network size and density grows as shown in the simulation results. In the approaches of [12,14,15], the use of CA is taken into consideration, which ensures that authentic nodes are able to join the networks, but this can make the network susceptible as a single point of failure and also defies the true nature of *ad hoc* networks. ESTA, in contrast, make use of trust values rather than Certificate Authority which helps in evaluating which helps in evaluating the goodness of the paths used and excludes the non-performs paths. Finally, it can be summarized that ESTA does not make use of CA or extra processing at intermediate nodes in terms of computations and still performs well in a variety of scenarios. The basic concern around the approach is the additional delay added along with a certain amount of overhead introduced by the new control packets.

8. Limitations and Future Work

In the current form of the proposed solution, use of a data structure with the name of SuperList is being used, which would be generalized in future research tasks. The use of trust in the current form is based on the direct observation that we would extend its scope by gathering the trust information from other peer nodes. Then, a generalized trust value would be assigned to the nodes. This will also help the approach to isolate the malicious non-performing nodes. Further, in the future, the focus would be to reduce and optimize the extra delay introduced in the protocol and add the Intrusion Detection Scheme (IDS) mechanism to nail down the actual malicious node.

9. Conclusions

In this paper, a new protocol ESTA for secure transmission of data in the case of a blackhole node attack in a MANET is proposed and evaluated. The proposed protocol makes use of multiple paths for data transmission and this process of route formation is not computationally heavy. Still, it is successfully able to suppress the non-performing paths. It makes use of a combination of trust and asymmetric cryptography to ensure integrity and authenticity of the data packets. Based on the simulation results, it can be concluded that, in various scenarios, the performance of ESTA is better than AODV, but it also introduced an additional delay at the cost of security.

Author Contributions

This paper is the result of research conducted by authors on a topic for fulfillment of a Ph.D. The main idea was proposed by Dilraj Singh and further refined by Amardeep Singh. Dilraj Singh was mainly involved in developing the proposed protocol. Extensive simulations for testing, verifying, and getting the results for the analysis of the proposed model was carried out by Dilraj Singh under the guidance of Amardeep Singh. The authors have read and approved the final version of the manuscript.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Sen, J.; Koilakonda, S.; Ukil, A. A mechanism for detection of cooperative black hole attack in mobile *ad hoc* networks. In Proceedings of the Second International Conference on Intelligent Systems, Modelling and Simulation (ISMS), Kuala Lumpur, Malaysia and Phnom Penh, Cambodia, 24–28 January 2011; pp. 338–343.
2. Gupte, S.; Singhal, M. Secure routing in mobile wireless ad hoc networks. *Ad Hoc Netw.* **2003**, *1*, 151–174.
3. Karlof, C.; Wagner, D. Secure routing in wireless sensor networks: Attacks and countermeasures. *Ad Hoc Netw.* **2003**, *1*, 293–315.
4. Hu, Y.C.; Perrig, A. A survey of secure wireless ad hoc routing. *IEEE Secur. Priv.* **2004**, *2*, 28–39.
5. Sharma, N.; Sharma, A. The black-hole node attack in MANET. In Proceedings of the 2012 Second International Conference on Advanced Computing & Communication Technologies (ACCT), Rohtak, India, 7–8 January 2012; pp. 546–550.
6. Abdelshafy, M.A.; King, P.J. Analysis of security attacks on AODV routing. In Proceedings of the International Conference on Information Science and Technology (ICIST), Yangzhou, China, 23–25 March 2013; pp. 290–295.
7. Nafaa, M.; Ghanemi, S. Analysis of security attacks in AODV. In Proceedings of the 2014 International Conference on Multimedia Computing and Systems (ICMCS), Marrakech, Morocco, 14–16 April 2014; pp. 752–756.
8. Chang, J.M.; Tsou, P.C.; Woungang, I.; Chao, H.C.; Lai, C.F. Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach. *IEEE Syst. J.* **2015**, *9*, 65–75.
9. Zapata, M.G.; Asokan, N. Securing ad hoc routing protocols. In Proceedings of the 1st ACM Workshop on Wireless Security, Atlanta, GA, USA, 28 September 2002; pp. 1–10.
10. Tamilselvan, L.; Sankaranarayanan, V. Prevention of blackhole attack in MANET. In Proceedings of the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, AusWireless, Sdyney, Australia, 27–30 August 2007; p. 21.
11. Tan, S.; Kim, K. Secure Route Discovery for preventing black hole attacks on AODV-based MANETs. In Proceedings of the ICT Convergence (ICTC), Jeju, Korea, 14–16 October 2013; pp. 1027–1032.

12. Sanzgiri, K.; Dahill, B.; Levine, B.N.; Shields, C.; Belding-Royer, E.M. A secure routing protocol for ad hoc networks. In Proceedings of the 10th IEEE International Conference on Network Protocols, Paris, France, 12–15 November 2002; pp. 78–87.
13. Deng, H.; Li, W.; Agrawal, D.P. Routing security in wireless ad hoc networks. *IEEE Commun. Mag.* **2002**, *40*, 70–75.
14. Pirzada, A.A.; McDonald, C. Secure routing with the AODV protocol. In Proceedings of the Asia-Pacific Conference on Communications, Perth, Australia, 3–5 October 2005; pp. 57–61.
15. Eichler, S.; Roman, C. Challenges of secure routing in MANETs: A simulative approach using AODV-SEC. In Proceedings of the 2006 IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS), Vancouver, BC, Canada, 9–12 October 2006; pp. 481–484.
16. Yi, S.; Naldurg, P.; Kravets, R. Security-aware ad hoc routing for wireless networks. In Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking & Computing, New York, NY, USA, 4–5 October 2001; pp. 299–302.
17. Kurkowski, S.; Camp, T.; Colagrosso, M.; MANET simulation studies: The incredibles. *ACM SIGMOBILE Mob. Comput. Commun. Rev.* **2005**, *9*, 50–61.
18. Andel, T.R. Yasinsac, A. On the Credibility of MANET Simulations. *IEEE Comput.* **2006**, *39*, 48–54.
19. Royer, E.M.; Perkins, C.E. An implementation study of the AODV routing protocol. In Proceedings of the IEEE Wireless Communications and Networking Conference, 2000, WCNC, Chicago, IL, USA, 23–28 September 2000; pp. 1003–1008.