CIT. Journal of Computing and Information Technology, Vol. 24, No. 3, September 2016, 237–252
doi: 10.20532/cit.2016.1002835

Mitigating Malicious Attacks Using Trust Based Secure-BEFORE Routing Strategy in Mobile Ad Hoc Networks

Rutuja Shah, Sumathy Subramaniam and Dhinesh Babu Lekala Dasarathan

School of Information Technology and Engineering, VIT University, Vellore, India

Mobile ad hoc Networks (MANET), being infrastructureless and dynamic in nature, are predominantly susceptible to attacks such as black hole, worm hole, cunning gray hole attack at source or destination. Various solutions have been put forth so far in literature in order to mitigate the effects of these attacks on the network performance and to improve the reliability of the network. However, these attacks are still prominently a serious threat in MANET. Hence, a trust based routing strategy termed Secure-BEFORE routing (BEst FOrwarding Route Estimation) is proposed to ensure optimal route estimation in computing the trust value and hop counts using the dummy packets inside the network at 1-hop level. It is observed that the overall performance of the network is improved in providing one-hop level security by maintaining the packet equivalence ratio. Malicious and suspicious nodes are isolated and eliminated from the network, based on their behavior.

ACM CCS (2012) Classification: Security and privacy → Network security → Mobile and wireless security

Keywords: black hole attack, gray hole attack, worm hole attack, secure-BEFORE routing, SRNT (MANET)

1. Introduction

Mobile ad-hoc networks are more susceptible to more security breaches than the wired networks. Self configuring infrastructure and dynamic nature without any centralized controller to co-ordinate packet transmission poses challenges in identifying and addressing the security issues. Mobility of the nodes in mobile ad hoc networks leads to frequent changes in the topology of the network. Nodes joining and leaving the network require monitoring and subsequently authenticating to ensure if they are genuine. Unauthentic participation of malicious or suspicious nodes attempts to reduce the performance of the network. Challenges faced due to packet drop attacks in mobile ad hoc networks are addressed to an extent by a fellowship model as discussed by Balakrishnan and Varadharajan [1]. A one hop restricted route reply is used as a status reply when a genuine node forwards a packet. However, MANETs have come across serious security threats which tend to affect the end-to-end delay, buffer mechanism, response time and in general overall throughput of the network leading to performance degradation. Hence, it is difficult to manage such networks economically.

Ad hoc networks face the security threats due to certain attacks experienced by the nodes which are categorized under packet drop attacks such as worm hole, gray hole and black hole attacks. These attacks usually vary from each other depending upon the strategy of the attack, frequency of the attack and losses caused to the network due to the attack.

Malicious nodes attempt to behave similarly to the genuine nodes in the network and resemble the same in terms of configuration, protocol, computational power, etc. They behave maliciously by dropping the packets in order to imbalance the network activities and thereby reduce the throughput. Worm hole attack usually follows the collaborative approach to perform the attack inside MANETs where a group of malicious nodes are involved in the attack. The malicious node which receives the packet relays

it through another route instead of forwarding it to the required destination. Such relayed packets are then diverted to a group of malicious nodes which never delivers the packet to the intended destination node. Gray hole attacks are hard to handle since the malicious nodes often change their behavior. Gray hole attack at source is a type of attack in which the malicious nodes drop all the packets originating from a particular source. Similarly, gray hole attack at destination is a type of attack in which the malicious nodes drop all the packets destined to a particular destination inside the network. Thus, in both cases the packet delivery ratio is affected, which leads to poor throughput of the network.

Various attacks (both external and internal) have been responsible for deterioration of the overall network performance of MANET. In order to mitigate their effects, there is a need for a strong optimum solution which could sentinel the mobile ad hoc network against such attacks periodically. This work attempts to address the node capturing attacks with secure before routing strategy in building trust among the nodes in mobile ad hoc networks.

Section 2 provides a brief review of the literature highlighting the background on the effects of various malicious attacks and different defense mechanisms. Section 3 elaborates the detailed system design proposed. Section 4 covers the implementation methodology and Section 5 highlights the simulation results with discussions. Section 6 gives the concluding remarks with Section 7 highlighting the future scope.

2. Background

Gupta and Pandey [2] have proposed a trust based routing algorithm considering the honest value of the participating nodes with Ad hoc On-Demand Distance Vector Routing (AODV) as the routing protocol. The honest value also known as trust value is used in addition to the hop count. Honest value is incremented during Route Request (RREQ) phase and decremented during Route Replay (RREP) phase, depending on the hop value and then the best path is arrived. As further enhancement, before forwarding the data the node evaluates the routing path according to trusted metrics using HAODV (hybrid-AODV).

Tamilselvan and Sankaranarayanan [3] have proposed a modified AODV routing approach incorporating Collect Route Reply Table (CRRT), where a timer is set to collect the replies of all the requests sent for routing path setup after receiving the first request. The threshold value and the arrival time of first request decides the validity of the route. Mechanism to choose a reliable forwarding node based on randomized route reply message mitigates the malicious nodes.

Tamilselvan and Sankaranarayanan [4], have also proposed an improvisation on their previous work by using fidelity level, considering the faithful performance of the node. The source sends route request (RREQ) to all the nodes in its neighborhood using Ad hoc On-Demand Distance Vector Routing (AODV) protocol. A timer t is set to collect the replies. Fidelity level of responding node and each of its next hop levels are verified. If the fidelity levels are the same, then the node with less hop count is selected for route establishment, thus minimizing the possibility of collective black hole attack and eventually the packet drop attack. Performance in terms of better packet delivery ratio is achieved.

Sujatha *et al.* [5], discuss using genetic algorithm with soft computing technique which implements the law of selection and evolution. This method is used in high traffic networks to distinguish genuine and malicious connections, thereby reducing black hole attack. Li *et al*. [6] have presented a concept where the nodes are categorized according to their behavior. They have proposed a trust based scheme, which uses behavior metrics like packet delivery rate (PDR), packet modification rate (PMR) and packet misrouted rate (PMIR) to establish trust among the participating nodes.

Wahane *et al*. [7], have introduced slightly modified AODV routing protocol using data routing information (DRI) table with cross-checking to mitigate the cooperative black hole attack. In order to identify multiple black hole nodes acting in co-operation, two bits of additional information are tracked from the nodes responding to RREQ of the source node. This approach has

attempted to reduce the end-to-end delay and improve network performance in terms of maximum throughput. Bradley *et al.* [8] have come up with "WATCHERS", a behavioral approach on the basis of principle of packet flow conservation which detects and reacts to routers that drop or misroute packets. Here the number of packets incoming to the node, except the ones destined to it, and the number of packets forwarded by the node, except the ones generated by it, are validated periodically by all the neighbors of the suspicious router. Similarly, a mechanism that detects bad routers which groups with its neighbors and those that alter packets are proposed to be addressed with suitable authentication mechanisms.

Balakrishnan and Varadharajan [1], combined the fellowship model with energy level model. Here the nodes have the obligation to follow the fellowship model in order to stay inside the network. The commitment to render network services inside the network is calculated using the energy levels of the participating nodes. It involves the parameters such as proportion of outgoing energy and the initial energy. Depending upon the activeness of the node, using the energy level which is directly proportional to the possibility of the node being honest with a threshold, the nodes are isolated from the network if behaved maliciously. However, large computation of energy levels using complex mathematical computation at every node inside network leads to huge overhead.

In order to curb the gray hole and black hole attacks in MANET, various strategies were used by Yang *et al.* [9], which include computing direct trust value (DTV) and indirect trust value (ITV) using some predefined threshold and related parameters. The Neighbor Recommendation Trust Model (NRTM) is used with indirect trust value to reduce co-operative black hole attacks. They have proposed a method to prevent gray hole and one kind of black hole attack based on watch dog mechanism using direct and indirect trust values.

The trust management scheme proposed by Venkanna and Velusamy [10] is a common way to detect and isolate the compromised nodes. The WATCHDOG strategy is used to observe the behavior of the suspected nodes. The information about the behavior of the nodes is fed to the reputation system (RS) updated by the reputation table (RT). Velloso *et al.* [11], proposed a recommendation Exchange protocol (REP), that exchanges trust information only about the neighbors based on relationship maturity to improve the efficiency by mitigating the colluding attacks in the network.

Unlike hard security solutions that require deploying cryptographic algorithms which require large computational power and bandwidth, soft security system basically determines the trust based on the nodes behavioral history without requiring more computational power. Such, trust based models are based on a particular node's behavior and the trust values keep changing periodically. Roy *et al.* [12] propose a dynamic trust management system (DTMS) that helps in distinguishing the authorized and malicious nodes in the network. Another approach proposed in Buchegger and Le Boudec [13], include the CONFIDANT (Cooperation Of Nodes Fairness In Dynamic Ad hoc Networks) protocol, which modifies the reputation system and maintains a path rater for secured communication.

Michiardi and Molva [14] used an alarm to signal the neighbors about the malicious nodes. COllaborative REputation (CORE) is used for collaborative monitoring. It divides the reputation of the node into 3 levels such as subjective reputation, (reputation which is calculated directly using the direct interaction between the subject and its neighbor), indirect reputation, (which is a positive report by other nodes), and finally the functional reputation, (which is based upon the behavior monitored during a specific task carried out).

El Defrawy and Tsudik [15], have used an ALARM which gives secure correspondence and protection in both suspicious and unfriendly systems with sensible proficiency. ALARM is a protected and secured connection state based directing convention. Node secrecy and assurance are targets of security. Security implies hubs confirmation and uprightness of areas secure information sending an ALARM on utilizing the node's current positions.

The real concern in mobile ad hoc network is to build the steering security in the vicinity of noxious nodes, where the element topology of

MANET permits nodes to join and leave the system any time. This elementary property has rendered it powerless against different security attacks. Bhalaji [16] discusses relationship enhanced DSR protocol that identifies the malicious nodes and isolates them from snooping and forwarding active data.

Methods to address link level security threats are proposed to lessen the threats while routing in mobile ad hoc networks, as put forth by Garg and Mahapatra [17]. A trust model that mitigates the selfish behaviour of the nodes in delay tolerant network is proposed by Chen *et al.* [18]. Their proposed approach achieves improved delivery ratio with lesser delay compared to Bayesian based trust model.

Various schemes are proposed in literature in order to identify and isolate the malicious nodes and various security threats with few theoretical proposals and few through simulations. However, perfect solutions which can curb various attacks in MANETs are still a deficit. Solutions proposed by the few are impractical, provide lesser throughput or do not have much impact on the overall network performance. Few have comparable and measurable impact on network performance, but at the cost of security risk in the network. Many of the earlier researchers have come up with theoretical solutions with no practical implementations or supplemented experiments to address this issue. Few solutions have either been expensive to deal with or involved large and complex computations pertaining to maintenance of resources of network setup. This has lead to the need for a solution to restrain the impact of more than one type of attacks by a single strategic framework with optimum or best possible results, which has eventually been the motivation behind this paper. Table 1 shows a comparative analysis emphasized with the perspective in which the proposed approach is better than existing approaches.

Table 1. Comparative analysis of approaches used in MANETs against malicious attack.

Existing Techniques	**Description**	**Base protocol**	**Types of attacks addressed**	**Gap identified**
Gupta and Pandey	Honest and Trust value mechanism	AODV with trust based	Black hole attack	Insecure
Tamilselvan and Sankaranarayanan	CRRT (collect route reply table)	AODV	Black hole & cooperative Black hole attack	May lead to stale entries
Li *et al.*	SVM (support vector machine) categorizes nodes based on behavior metrics like PMR,PDR,PMER	Any MANET routing protol	Black hole attack	Overhead to populate and maintain XML data
Wahane *et al.*	Modified AODV using DRI (data routing information) table	AODV	Black hole attack	Overhead to maintain large number of entries in table at every node
Balakrishnan and Varadharajan	Fellowship model using energy levels of nodes	Any MANET routing protocol	Packet drop attack	Involves complex mathematical computations
Buchegger and Le Boudec	CONFIDANT (Cooperation Of Nodes Fairness In Dynamic Ad hoc Networks) and maintains a path rater	AODV	Co-operative black hole attack	Insecure
Proposed Approach with 1-hop security	Secure-BEFORE strategy using AODV	AODV	Black hole, Worm hole and Gray hole attacks at source as well as at destination	Insecure against node capture attack

3. Proposed System Design

A secure-BEFORE (BEst FOrwarding Routing Estimation) methodology is proposed, that not only mitigates various malicious attacks in MANETs, but also improves the overall network performance utilizing the optimum resources. For establishing a communication between a source S and the destination D, a Secure Route Node table (SRN table) is maintained at the source node S with fields holding values of hop count, packet equivalence ratio, trust_value and Optimum Route flag (OR_flag). When RREQ message is sent, the intermediate nodes having route to that particular destination respond with a RREP message back to the source node.

At source node S, multiple RREP packets may be received. Since the proposed methodology follows 1-hop level, node S considers the RREP of only those nodes which are just one hop away from the destination for further processing. Further, a dummy packet (a packet with no data) is sent via intermediate nodes which are just 1 hop away towards the destination and wait until a confirmation signal (CNF) is received at the source via intermediate nodes. The dummy packet is received at the destination only via genuine nodes because malicious node either drops or diverts the packets without forwarding them towards the destination. Thus, the destination node sends CNF signal through the intermediate node whose dummy packet reaches the destination correctly.

On receiving the CNF signal, the table values for OR_flag and the trust values are modified. The OR_flag is set to 1 and the trust value of intermediate genuine node is increased by 1 in SRN table which is maintained at source node S. Subsequent packets are then sent from source node to the destination through genuine intermediate nodes as per the update in the table.

At the end of a complete data transmission, the OR_flag is reset back to 0. The node structure table is updated accordingly. It maintains the hop-count, packet equivalence ratio, trust values and optimum route flag. These values are updated accordingly during various phases of the proposed approach as discussed.

Nomenclature:

- to_node: next node towards destination;
- Hop_count: number of hops between the source and destination;
- Packet Equivalence Ratio (P.E.R): number of packets received by a particular node to the number of packets transmitted from the same node;
- Trust_value: based on node's behavior and previous history (integer values are assigned);
- Optimum Route flag (OR_flag): taking boolean values, i.e. 0 or 1;
- SRN (Secure Route Node) table: maintains hop-count, packet equivalence ratio, trust_value and Optimum Route flag (OR_flag).

3.1. Module Description

The module description of the proposed scheme is given in Figure 1, where d_packet is the dummy packet and CNF is confirmation signal. Various phases encountered by the nodes while establishing the path for data transmission in the network are as described below:

(i) Secure-BEFORE routing phase: A dummy packet is sent by source node towards the destination. The source waits until a CNF signal is received via intermediate nodes. Accordingly, the intermediate nodes and the source node modify the table values respectively once the CNF signal is received.

(ii) Transmission phase: Once the table modifications are carried out, actual data packet is sent to the destination through the intermediate nodes via which the CNF signal was received.

(iii) Updating phase: During the updating phase, after submission of consequent packets, Secure Route Node (SRN) table is updated.

(iv) Reset Phase: When successful transmission occurs through genuine nodes, the SNR table values are reset.

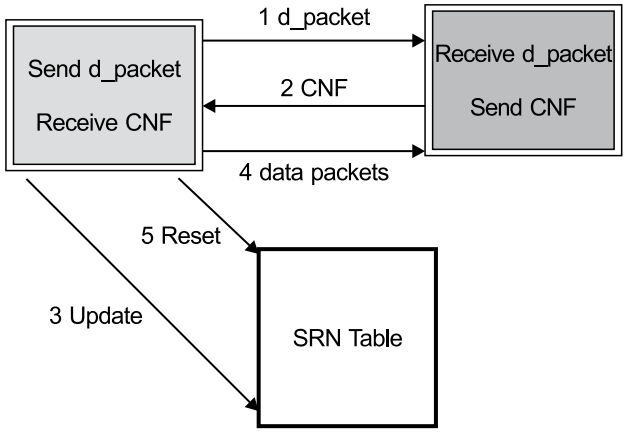

Figure 1. Scenario description.

3.2. Justification Behind Using Dummy Packets to Detect Malicious Nodes

Handshake signals used to confirm the availability of the intended nodes (control signals) at times do not help in obtaining a feasible secured route to forward data packets towards the destination. Moreover, they do not help in detecting the presence of malicious nodes in the network. Hence, the dummy packet is sent in as a preliminary handshaking signal which is treated as normal packet by all nodes in the network. Also, dummy packets do not carry any valid data while normal data packets carry valid data. Only the node that originates the dummy packet recognizes it. Dummy packet is disseminated in the network to observe the behavior of the nodes inside the network.

Trust_value component maintained in the SRN table is incremented only when the CNF signal is sent back to the source from destination via genuine intermediate nodes. Such recorded update values in the SRN table ensure the optimum combination of trust value and the packet equivalence ratio which is further used to determine the next best-fit forwarding node for packet transmission. The motive of proposing a 1-hop security scheme aiming at the destination node is that most attacks are targeted at the point just before the packet reaches the destination as the volume of valuable information that could be sneaked or affected would be high. Hence, this proposed approach incorporates the authentication scheme just before the destination, i.e. at the node closer to the destination just at 1-hop level only.

From the simulation results obtained with different scenarios, considering the presence of malicious node and absence of malicious node, different time intervals, and the number of retransmission attempts made, it is observed that the proposed 1-hop secure-BEFORE routing strategy outperforms the existing work in terms of better throughput and overall network performance.

It is observed that the nodes closer to the destination node or the destination node itself are targeted more by suspicious nodes aiming to deprive valuable content since the packets travel long distance consuming the network resources. When packets traverse from a source all the way and get dropped just nearer / closer to the destination before they reach the destination, they lead to loss in more information and cause more impact on the performance of the network in terms of retransmissions.

The threshold value for trust is decided mutually using agreement protocols among all the nodes in the network and the nodes with lesser trust value i.e. the value crossing minimum threshold, for a longer time is expelled out of the network. Results obtained after implementing the proposed 1-hop security against gray hole attack at source, destination and against packet drop attack, worm hole attack reveals a substantial improvement in throughput, packet delivery ratio and less end-to-end delay, thus improving the overall network performance. The trust values are updated periodically, thus improving the life of the network as a whole. Different scenarios with and without malicious nodes as described below are analyzed with the proposed approach.

Case i. Presence of one genuine node and one malicious node, both at one-hop level distance from destination is considered and secure-BEFORE routing strategy is applied.

Case ii. Presence of one or more malicious nodes at one-hop level distance from destination is considered. Packets will not be sent unless there is occurrence of a genuine node at one-hop distance and verification of the same is done using secure-BEFORE strategy.

Case iii. With presence of one or more genuine nodes at one-hop level distance from destination, the node with better trust value is used to forward the packets. Also, if both genuine

nodes have same trust value, then either of the nodes based on the distance metric is chosen for further packet transmissions.

3.3. Sample Scenario Illustration

In order to implement one-hop level security using secure-BEFORE routing strategy, a sample network scenario as shown in Figure 2 is considered to track the behavior of malicious nodes for illustration. It consists of source node S, destination node D, malicious node M and a normal node N. Source node S is 2 hops away from the destination node D and the intermediate nodes M and N are just 1 hop away from the destination node D. Sample node structure followed at source node S is given in Table 2.

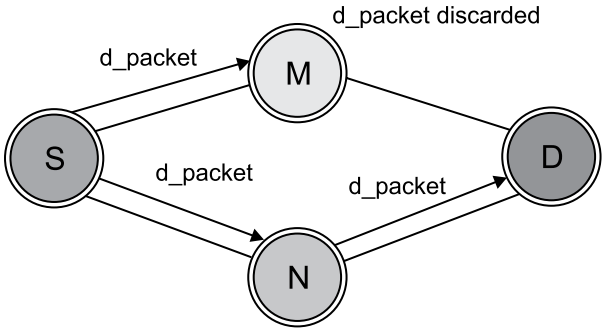

Figure 2. Basic network scenario.

Table 2. Node structure at source node (SRN table).

Node	Hop_count	P.E.R	Trust_value	OR_flag
M	1	1	0	0
N	1	1	0	0

Primarily, the network setup is done with few mobile nodes along with Application, Profile and Mobility Configuration set in the simulation environment. The settings are done with applications and profiles created to render FTP, Email and Database services inside the network. The initial trust_value for both nodes is assumed as 0 and P.E.R is set as 1. Normal nodes maintain good ratio of packet delivery. So, P.E.R values are mostly 1, since they forward all the packets towards destination, while the malicious nodes have poor packet delivery ratio since they tend to drop the packets to disrupt the network performance and hence P.E.R is modified accordingly.

The route discovery phase begins by sending Route Request (RREQ) message from source node to next hop node in search of optimum route to destination node D. In mobile ad hoc networks route establishment relies on the participation of the neighbor nodes which act as forwarders until a path is established for the packets to reach the destination. The intermediate nodes having a route to destination respond with Route Reply (RREP), towards source node and the rest simply forwards it to their next hop nodes. This process is repeated until a route to the destination node is established.

Upon the successful exchange of RREQ and RREP messages among the nodes forming the network, a dummy packet is sent by the source, to determine the genuine nodes with the one-hop level secure-BEFORE strategy using AODV as base routing protocol. Once the exchange of dummy packet and confirmation signal are performed, packet transmission is initiated successfully.

To achieve this, packet size is kept constant (0) in the node setting of source, intermediate and at the destination. Also, a packet discarder is used which drops every packet destined to it. This is done to ensure that the dummy packet reaches destination via the normal node and not through the packet discarder. The settings are as given: start time = 5.0 ms, end time = 300 ms, discard count = All. After CNF signal is received, node S updates the OR_flag by setting it to 1 and also increases the trust_value of node N by 1 as shown in Table 3.

Table 3. Modified node structure at source node (SRN table).

Node	Hop_count	P.E.R	Trust_value	OR_flag
M	1	1	0	0
N	1	1	1	1

It is observed that the d_packet is discarded or dropped by malicious node M while the genuine node N forwards it to the destination. Upon receiving the d_packet from source node S via intermediate normal node N, the destination node D sends a CNF signal through the same

route back on reverse path towards the source node S, as shown in Figure 3.

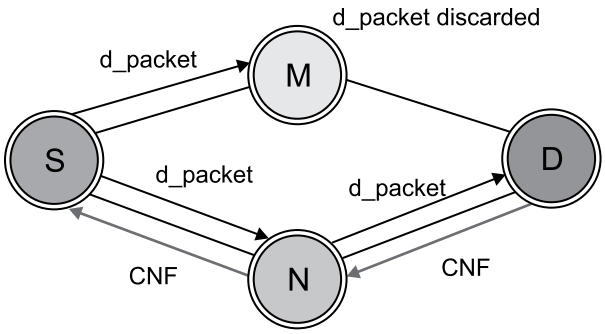

Figure 3. Network scenario with confirmation exchange.

Since the dummy packet forwarded via normal node reaches the destination, the destination node sends a CNF signal via same route towards the source node using reverse path. Thus, the source node confirms the best link to forward actual data packet and performs the data transmission subsequently via genuine nodes thus resetting the values in SRN table, as shown in Table 4.

Table 4. Updated node structure at source node (SRN table).

Node	Hop_count	P.E.R	Trust_value	OR_flag
M	1	1	0	0
N	1	1	1	0

Once the values are updated, the source node S sends actual data packets towards the destination node D through the optimum path identified as trusted path (node N in this case). Thus, subsequent data packet transmission is done and OR_flag is reset to 0 periodically. This is achieved in OPNET by setting packet inter-arrival time to exponential (0.03) and packet size as exponential (16 000) for the nodes inside MANET in order to proceed with packet transmission and reception.

The network scenario is simulated in OPNET considering both the cases, such as with the presence of the malicious nodes using a packet discarder inside the network as well as the case where the malicious node is removed from the network where its trust value and packet equivalence ratio are poor. The parameters used for the analysis are traffic sent, traffic received, number of retransmission attempts made, route discovery time, load and throughput.

Initial trust value of zero is assigned to all the nodes in the network. Trust values are updated based on the nodes experience during packet transmissions, as described. Based on the updated trust values, best 1-hop node is chosen for packet forwarding. The trust value of the node from which the confirmation is received is incremented. The trust value of the suspected node is checked to see if it is below the threshold. If so, the node is expelled from the network. Otherwise, packet transmission is set for the chosen route through the genuine nodes, as described in the flow diagram given in Figure 4.

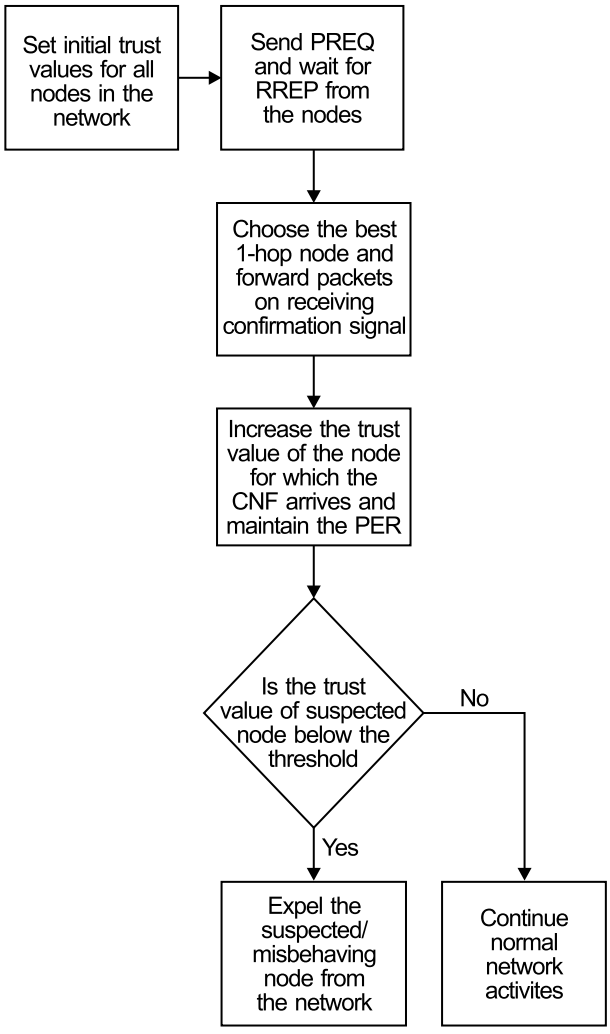

Figure 4. Flowchart of Secure BEFORE routing scheme.

For optimum selection of the node to send the data packets, the proposed scheme can be mathematically computed as given in (1),

$$SBSP_{via\ Node_j} = P.E.R_j * \sum_{i=1}^{n} \text{trust on } Node_j \quad (1)$$

where $SBSP_{via\ Node_j}$ is Secure-BEFORE Shortest Path via $Node_j$ and $P.E.R_j$ is the Packet Equivalence Ratio for $Node_j$ and $\sum$ (i = 1 to n) is the summation of the trust values for $Node_j$ for recent n different sessions and $Node_j$ is the node for which trust values are computed to obtain Secure-BEFORE Shortest Path.

4. Implementation Methodology

To simulate and demonstrate the effects of malicious attacks in MANET and to understand its consequences through simulation study, there is a need to use a discrete event simulator. A very wide variety of simulation tools are available like NS-2, OPNET [19], Glomosim, QualNet, OMNet++ etc. OPNET is used in this simulation study which provides better results with accuracy and supports with a user friendly GUI interface on Windows platform. OPNET 17.5 (formerly known as Riverbed 17.5 modeler) is used with Windows platform (32/64 bit OS) using Visual studio and C++ library.

4.1. Sample Scenario

A campus network scenario of 800 m × 800 m is created with 10 mobile nodes. IEEE 802.11 wireless network standard is used to deploy the application scenario. Application configuration is profoundly used to run the applications on mobile nodes in the network and configure the user profile. Profile configuration and mobility configuration settings such as start time, duration, number of repetitions and the application profile are set as specified in Table 5. Performance of the network in the presence and absence of malicious nodes is observed. Further, the behavior of the malicious nodes with and without the proposed defense mechanism is observed.

Table 5. Profile and mobility settings.

Profile Config. Settings	Value	Mobility Config. Settings	Value
Start time	Uniform (5,10)	Speed	Uniform int (0,10)
Duration	End of profile	Pause time	Constant (50)
No. of repetitions	Unlimited	Start time	Constant (10)
Appln. profiles	Serial (ordered)	Stop time	End of simulation

Parameters such as the channel settings, routing protocol, network layer protocol used, physical characteristics, data rate, buffer size, duration of simulation etc. are set for the simulations as shown in Table 6.

Table 6. Parameter settings.

Parameter	Value
Campus Network	800 m × 800 m
Simulation time	300 (s)
No. of nodes	10
Routing Protocol	AODV
Networking protocol	IP
Application	FTP, Database and Email
Seed value	128
Kernel mode	Optimized
Operation mode	Serial (ordered)
Start time	Uniform (100,110)
Duration	End of simulation
Data rate	11 Mbps
Buffer size (bits)	1 024 000

4.2. Network Model (With and Without Malicious Nodes)

In order to create a malicious network model, few nodes are intentionally made to behave

maliciously inside the network. To achieve this, the packet interval size is increased to exponential (0.005) and packet size is kept as uniform (190,220). Unlike the network with normal nodes, it is observed that the frequency of packet drops is high in the network with malicious nodes.

Figures 5 and 6 show the comparative results in terms of packets sent, packets received and packets dropped with respect to a network with all normal behaving nodes and the network with malicious nodes. It is observed that the packet delivery ratio is high in the network with normal nodes and comparatively less in the network with malicious nodes.

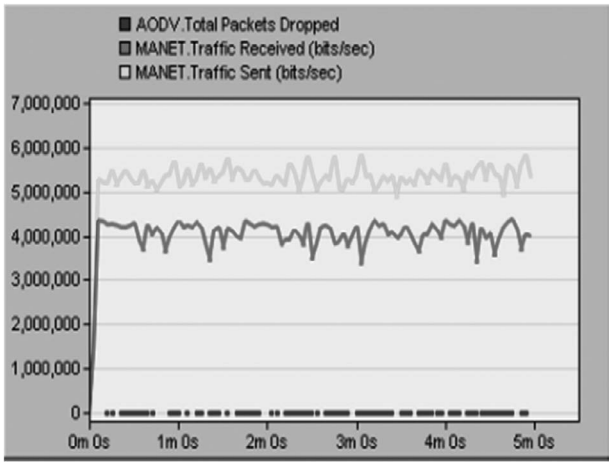

Figure 5. Normal network model: Time (s) vs. Number of packets (bits/sec).

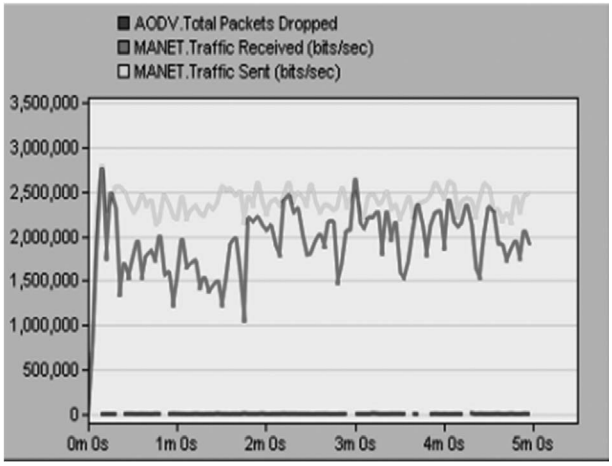

Figure 6. Malicious network model: Time (s) vs. Number of packets (bits/sec).

5. Simulation Results and Discussions

The proposed approach is simulated in different phases of network scenarios using OPNET. The network scenario which includes the presence of malicious nodes with no use of any defensive mechanism to curb it, is compared against the network scenario which involves malicious nodes which are curbed by making use of the proposed 1-hop security mechanism (Secure-BEFORE routing).

The parameters considered for evaluation are end-to-end delay, retransmission attempts, route discovery time, total number of packets dropped, network load and throughput generated. Table 7 provides the simulation results obtained for various parameters of a network incorporating normal nodes and malicious nodes.

Table 7. Simulation results.

Parameter	Values (network with normal nodes)	Values (network with malicious nodes)
Delay (s) range	1 – 1.5	2 – 10
Throughput (bits/sec)	4 000 000 – 4 500 000	3 000 000 – 3 500 000
Network load (bits/sec)	400 000	300 000
Traffic sent (bits/sec)	5 000 000	2 500 000
Traffic received (bits/sec)	4 000 000	1 500 000
Number of packets dropped	100	650–850
Route discovery time (s)	2 s	10 s
Retransmission attempts (s)	0.35–0.45	0.18–0.35

The simulation results obtained and the observations made are given in Table 8 upon comparing the traditional approach with the proposed 1-hop Secure-BEFORE Routing approach.

Table 8. Comparison of statistical values.

Parameter	Normal approach	Proposed approach	Observations
Delay (s)	3.5	1	Decreases
Route Discovery Time (s)	0.0125	0.0075	Decreases
Retransmission attempts (packets)	2.065	0.0275	Decreases
Network load (bits/s)	2 000 000	2 800 000	Increases
Throughput (bits/s)	2 250 000	2 750 000	Increases
Total no. of packets dropped	5000	50	Decreases

The normal approach has no defensive strategy to reduce the harm done by malicious nodes on network performance while the proposed approach makes use of 1-hop security level termed as secure-BEFORE strategy to mitigate the harm done by malicious nodes. From the results obtained, it is observed that the performance of network in the presence of malicious nodes, when addressed using secure-BEFORE strategy, is much better than the network scenario with presence of malicious nodes without use of any defensive mechanism against malicious attacks. The delay and retransmission attempts are reduced by 71% and 98% respectively, since the packets are sent without much delay and eventually leading to lesser frequency in retransmission attempts. Since lesser number of packets gets dropped, the time required to find new route to send packets i.e. the route discovery time and total number of packets dropped are also observed to have reduced considerably by 40% and 99% respectively.

The network is maintained to sustain the traffic flow and the packet delivery ratio. The throughput generated is more than normal network scenario and shows an increase of around 22% because the overall improvement of other network parameters also (in turn) helps to improve the network throughput. Thus, the 1-hop secure-BEFORE strategy on an overall perspective proves to improve the network performance and provides a reliable network avoiding malicious attacks during the packet transmission.

Figures 7, 8, 9, 10 and 11 represent the impact on the network parameters chosen for analysis such as throughput, network load, traffic sent, traffic received and packet drop rate respectively. As observed from Figure 7, the throughput of the network without malicious nodes is high compared to the network with malicious nodes. With respect to network load in Figure 8, network without malicious nodes is able to support more load as compared to the network with malicious nodes.

Figures 9 and 10 prove that the number of packets sent and received is (relatively) higher in the network without malicious nodes than in the network with malicious nodes. The packet drop rate is less in the network without malicious nodes than in the network with malicious nodes as malicious nodes tend to drop the packets as given in Figure 11.

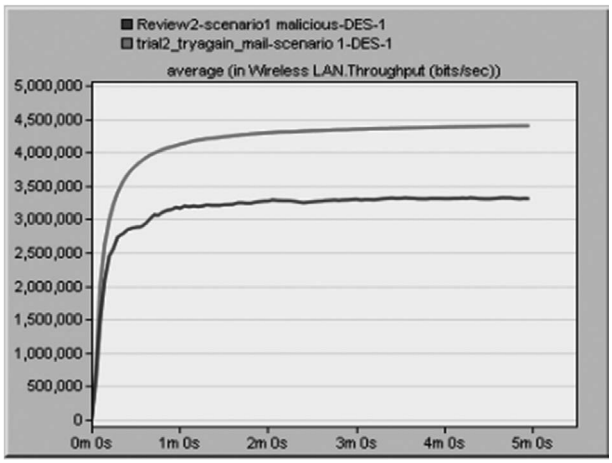

Figure 7. Time (s) vs Throughput (bits/sec).

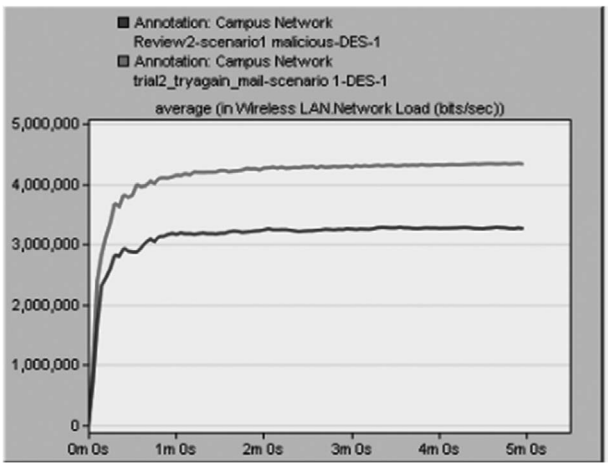

Figure 8. Time(s) vs Network load (bits/sec).

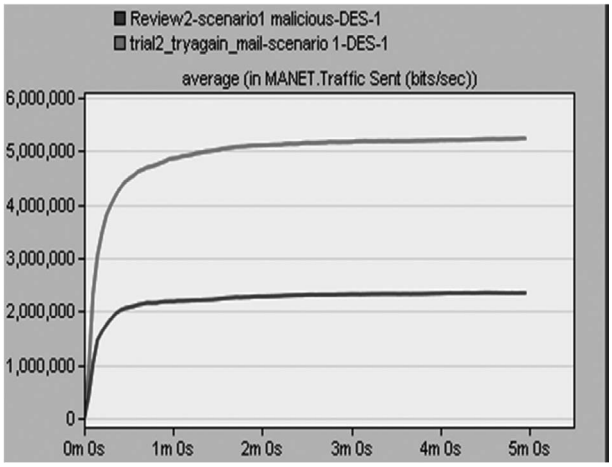

Figure 9. Time(s) vs. Traffic sent (bits/sec).

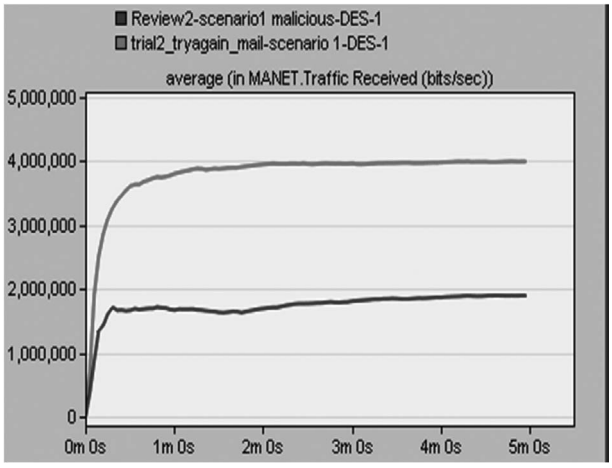

Figure 10. Time (s) vs.Traffic received (bits/sec).

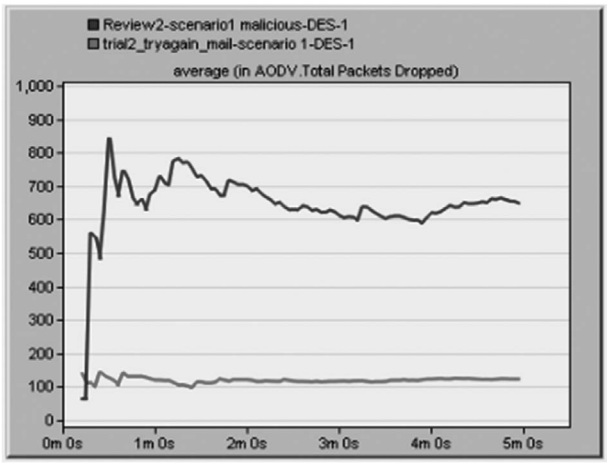

Figure 11. Time (s) vs. Number of packets dropped.

Similarly, Figures 12, and 13 represent the route discovery time and the number of retransmission attempts respectively where *trial2_tryagain_mail-scenario 1-DES-1* is the network scenario with normal nodes and *Review-2-scenario1 malicious-DES-1* is the network scenario with malicious nodes.

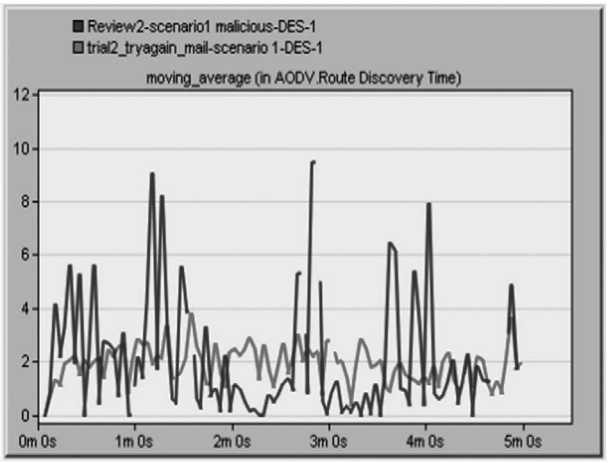

Figure 12. Time (s) vs. Route discovery time (s).

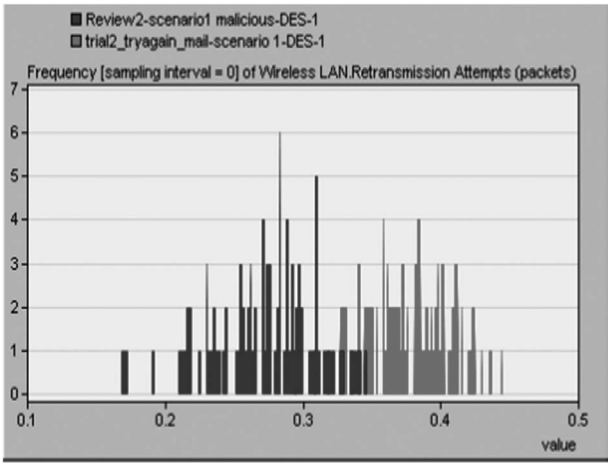

Figure 13. Time (s) vs. Number of retransmission attempts.

Review 3-scenario1 secure BEFORE-DES-1 is the network scenario with malicious nodes without any defense mechanism and *Review 4-scenario 2 secure BEFORE-DES-1* is the network scenario with malicious nodes using the proposed secure-BEFORE routing strategy used as a defensive mechanism in the proposed approach. Figures 14, 15, 16 and 17 represent the network parameters such as packet delivery ratio, network load, number of retransmission attempts and route discovery time respectively. From Figure 14, it is observed that the packet

delivery ratio in the network with the proposed defensive mechanism is high, with good support of network load as in Figure 15.

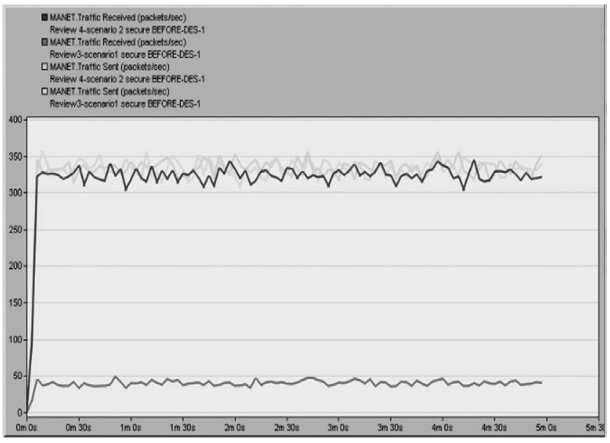

Figure 14. Traffic analysis time (s) vs. Traffic sent/received (bits/sec).

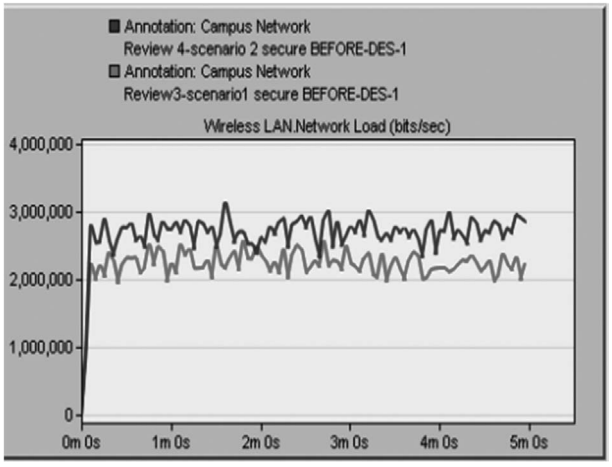

Figure 15. Time (s) vs. Network load (bits/sec).

Figure 16 shows that the number of retransmission attempt is less with the proposed defense mechanism and the route discovery time is minimal as given in Figure 17. Also, it is observed that the following parameters outperform the traditional approach in terms of throughput (Figure 18), which is high using the defensive mechanism with the proposed approach to alleviate the malicious nodes. In addition, the number of packets dropped and the delay incurred (as obtained and given in Figures 19 and 20) indicate that the drop rate is less and the delay incurred is minimal, too.

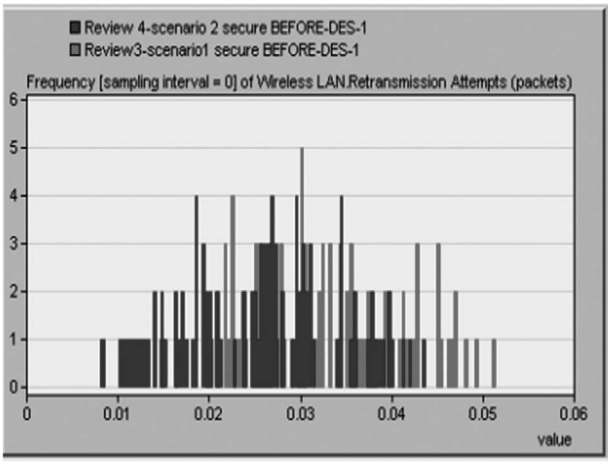

Figure 16. Time (s) vs. Number of retransmission attempts.

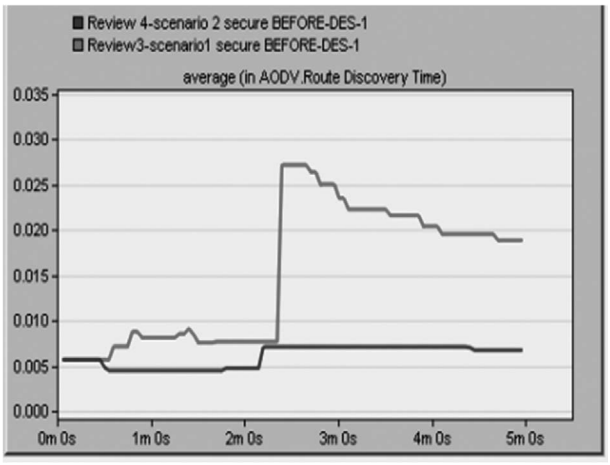

Figure 17. Time (s) vs. Route discovery time (s).

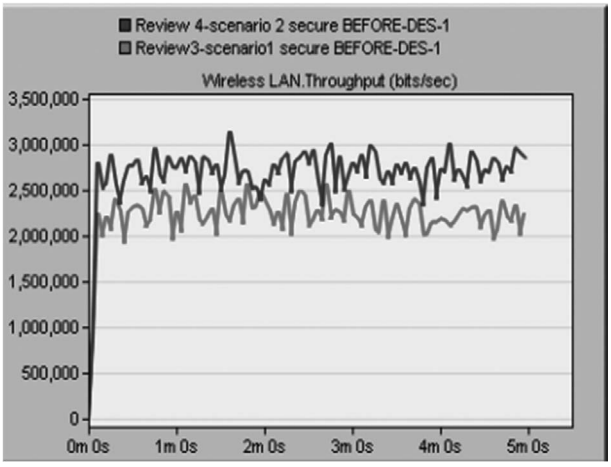

Figure 18. Time (s) vs. Throughput (bits/sec).

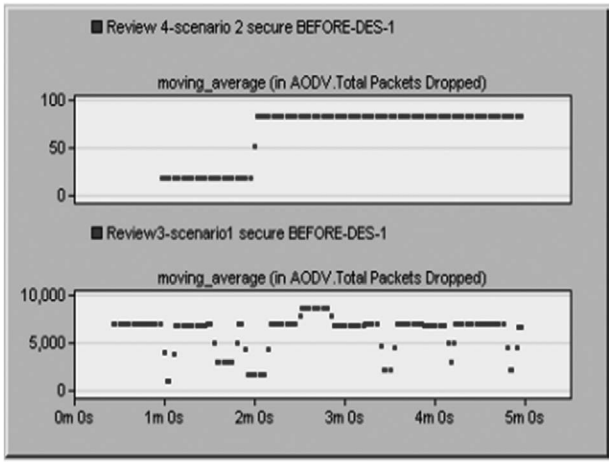

Figure 19. Time (s) vs. Total number of packets dropped.

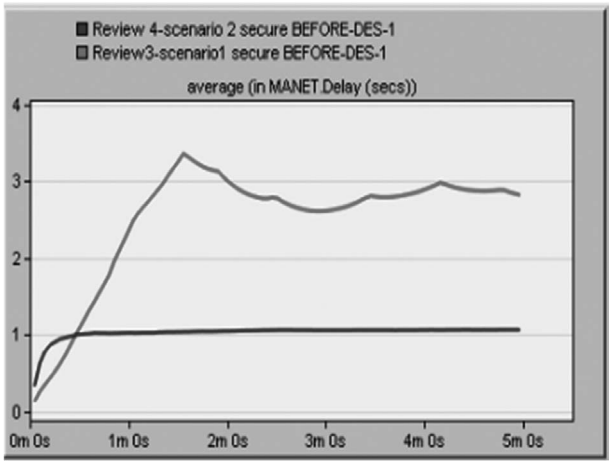

Figure 20. Time (s) vs. Delay (s).

6. Conclusion

From the simulation results obtained and the comparative analysis performed on various networking parameters involved in this simulation, it is evident that the presence of malicious nodes affects the overall network performance of mobile ad hoc network in general. Attacks such as black hole, worm hole, and gray hole, at source or destination and packet drop attacks which deteriorate the network performance causing harm to the regular network activities, are substantially mitigated using the proposed approach. The secure-BEFORE routing strategy ensures that the network performance is maintained considerably in order to achieve better transmission of packets across the networks with one-hop level security. AODV routing mechanism is used for packet routing. Periodical updates lead to attack-proof, secured packet transmission and reception across the nodes in mobile ad hoc network.

7. Further Enhancements

Efficient security mechanisms to mitigate the malicious attacks are highly essential to improve the performance of a network. They involve inclusion of more influential security techniques in order to prevent node capturing attacks. Timely implementation of optimum security strategies results in strongly resistant packet transmission methods in long distance communications over the large scale networks. A security mechanism with exchange of secret code using private key can be used between source and destination in order to check authenticity of the intermediate nodes i.e. the dummy packet could be sent in an encrypted format to the destination via various routes. The intermediate nodes cannot decipher it due to lack of knowledge of secret key among them. Thus, instead of making use of mere dummy packets, secure-BEFORE routing strategy can be used with enhanced security technique by taking care of the complexity level and making it more optimum and robust against different attacks in dense networks.

References

[1] V. Balakrishnan and V. Varadharajan, "Short Paper: Fellowship in Mobile Ad hoc Networks", *First IEEE International Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm 2005)*, pp. 225–227, 2005. http://dx.doi.org/10.1109/securecomm.2005.40

[2] N. K. Gupta and K. Pandey, "Trust Based Ad-hoc on Demand Routing Protocol for MANET", *Sixth International IEEE Conference on Contemporary Computing (IC3)*, pp. 225–231, 2013. http://dx.doi.org/10.1109/ic3.2013.6612195

[3] L. Tamilselvan and V. Sankaranarayanan, "Prevention of blackhole attack in MANET", *The 2nd IEEE International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007)*, pp. 21–27, 2007. http://dx.doi.org/10.1109/auswireless.2007.61

[4] L. Tamilselvan and V. Sankaranarayanan, "Prevention of Co-Operative Black Hole Attack in MANET", *Journal of Networks*, vol. 3, no. 5, pp. 13–20, 2008.
http://dx.doi.org/10.4304/jnw.3.5.13-20

[5] K. S. Sujatha *et al*., "Design of Genetic Algorithm Based IDS for MANET", *IEEE International Conference on Recent Trends in Information Technology (ICRTIT)*, pp. 28–33, 2012.
http://dx.doi.org/10.1109/icrtit.2012.6206796

[6] W. Li *et al*., "based automated trust management system for mobile ad-hoc networks", *IEEE Conference on Military Communications*, pp. 1102–1107, 2011.
http://dx.doi.org/10.1109/milcom.2011.6127446

[7] G. Wahane *et al*., "Technique for detection of cooperative black hole attack using true-link in Mobile Ad-hoc Networks", *37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO 2014)*, pp. 1428–1434, 2014.
http://dx.doi.org/10.1109/mipro.2014.6859791

[8] K. Bradley *et al*., "Detecting disruptive routers: a distributed network monitoring approach", *IEEE Symposium on Network*, vol. 12, no. 5, pp. 50–60, 1998.
http://dx.doi.org/10.1109/secpri.1998.674828
http://dx.doi.org/10.1109/65.730751

[9] B. Yang *et al*., "Historical evidence based trust management strategy against black hole attacks in MANET", *14th IEEE International Conference on Advanced Communication Technology (ICACT)*, pp. 394–399. 2012.

[10] U. Venkanna and R. L. Velusamy, "Black hole attack and their counter measure based on trust management in manet: A survey", *3rd International Conference on Advances in Recent Technologies in Communication and Computing*, pp. 232–236, 2011.
http://dx.doi.org/10.1049/ic.2011.0087

[11] P. Velloso *et al*., "Trust Management in Mobile Ad Hoc Networks Using a Scalable Maturity -Based Model", *IEEE transactions on network and service management*, vol. 7, no. 3, pp. 172–185, 2010.
http://dx.doi.org/10.1109/TNSM.2010.1009.I9P0339

[12] S. D. Roy *et al*., "Countering sinkhole and black hole attacks on sensor networks using Dynamic Trust Management", *IEEE Symposium on Computers and Communications*, pp. 537–542, July 2008.
http://dx.doi.org/10.1109/iscc.2008.4625768

[13] S. Buchegger and J. Y. Le Boudec, "Performance analysis of the CONFIDANT protocol in dynamic ad-hoc networks", *3rd ACM International Symposium on Mobile Ad-hoc Networking and Computing*, vol. 5, no. 1, pp. 226–236, June 2002.

[14] P. Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks", *6th IEEE Joint Working Conference on Communication and Multimedia Security*, vol. 7, no. 3, pp. 107–121, January 2002.
http://dx.doi.org/10.1007/978-0-387-35612-9_9

[15] K. El Defrawy and G. Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs", *IEEE Transactions on Mobile Computing*, vol. 10, no. 9, pp. 1345–1358, Sept. 2011.
http://dx.doi.org/10.1109/TMC.2010.256

[16] N. Bhalaji, "A Novel Routing Technique against Packet Dropping Attack in Ad-hoc Networks", *Journal of Computer Science*, vol. 4, no. 7, pp. 538–544, 2008.
http://dx.doi.org/10.3844/jcssp.2008.538.544

[17] N. Garg and R. P. Mahapatra, "MANET Security Issues", *International Journal of Computer Science and Network Security*, (August 2009), vol. 9, no.8, pp.241–246, August 2009.

[18] R. Chen *et al*., "Dynamic trust management for delay tolerant networks and its application to secure routing", *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 5, pp. 1200–1210, 2014.
http://dx.doi.org/10.1109/TPDS.2013.116

[19] A. S. Sethi and V. Y. Hnatyshin, "The Practical OPNET User Guide for Computer Network Simulation", New York: CRC Press, 2012.
http://dx.doi.org/10.1201/b12515

Received: October 2015
Revised: April 2016
Accepted: May 2016

Contact addresses:
Rutuja Shah
Vellore Institute of Technology
Near Katpadi Rd Vellore
Tamil Nadu – 632014
India
e-mail: shah.rutuja.89@gmail.com

Sumathy Subramaniam
Vellore Institute of Technology
Near Katpadi Rd Vellore
Tamil Nadu – 632014
India
e-mail: ssumathy@vit.ac.in

Dhinesh Babu Lekala Dasarathan
Vellore Institute of Technology
Near Katpadi Rd Vellore
Tamil Nadu – 632014
India
e-mail: lddhineshbabu@vit.ac.in

Rutuja Shah has pursued her M.Tech in Information Technology from VIT University, India. Her research interests include trust management in wireless ad hoc networks. She has published a paper in an international journal on node monitoring with fellowship model against black hole attack.

Sumathy Subramaniam received her B.E in Electronics and Communication Engineering from Vellore Engineering College affiliated to Madras University, M.Tech in Computer Science and Engineering and PhD from VIT University. She is currently a faculty in the School of Information Technology and Engineering, VIT University, India. Her research interests include trust and reliability in wireless networks and routing in hybrid wireless networks.

Dhinesh Babu Lekala Dasarathan received his B.E in Electrical and Electronics Engineering and M.E in Computer Science and Engineering from the University of Madras and PhD from VIT University. He is currently a faculty in the School of Information Technology and Engineering at VIT University, Vellore, India. His research interests include cloud computing, grid and distributed computing, big data analytics and social computing.