ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2022.0408

STRENGTHENING THE MOBILE AD HOC NETWORKS USING ENHANCED SELF-DETECTION ROUTING SCHEME

Ankita A. Mahamune[1] and M. M. Chandane[2]
Department of Computer Engineering and Information Technology, Veermata Jijabai Technological Institute, India

Abstract

Reliable routing in Mobile Ad hoc NETwork (MANET) depends on individual node cooperation. The entire network performance may degrade because of even a single misbehaving node participating as an intermediate node. Thus, there is a need for incorporating secure routing with MANET to successfully operate in an adverse environment where routing security threats are employed. Looking at a few of the unsuccessful attempts by state-of-the-art routing schemes at certain applications, this paper proposes a trust-based secure routing termed as Enhanced Self-Detection Routing Scheme (ESDRS). This proposed scheme incorporates a self-detection procedure into a standard dynamic routing protocol Ad hoc On-Demand Distance Vector (AODV), finally resulting in detection and reaction to malicious nodes in MANET. The validation of the proposed approach is carried out through a comparative performance analysis with the recent Evolutionary Self-Cooperative Trust (ESCT) scheme and the standard AODV. The comparison is based on computations of Packet Delivery Ratio (PDR), delay, throughput, jitter, number of dropped data packets, Probability of Detection (PoD) of malicious and benevolent behavior, and normalized routing overhead while varying the number of nodes, the number of attackers, and node speed. Simulation results affirm that the proposed scheme improves the metric values as compared to the other routing schemes.

Keywords:

Mobile Adhoc Network, AODV, Routing Disruption, Trust-Based Routing Scheme, Trust Metric

1. INTRODUCTION

A distributed architecture-less network having mobile nodes dynamically building up routes among themselves for transmission of packets is referred to as MANET [1, 2]. The widespread growth of mobile devices and the recent advances in such networks have opened a ubiquitous computing world where users can benefit from anywhere and at any time for unprepared participation. These networks have many applications like vehicular communication [3, 4], industrial wireless sensor networks [5], military operations, home wireless networks, emergency operations, etc. However, they are especially vulnerable due to their shared wireless medium, dynamic topology, no centralized operation, restricted power supply resources, etc. [6, 7].

Since the functioning of MANET requires individual node cooperation, its security is a primary concern. Generally, secure routing in MANET is an essential problem to solve for achieving reliable communication [8]. Secure routing is also difficult here because of the absence of centralized administration in the network and each node has to trust other nodes for routing their packets. So, the presence of any misbehaving node in the network can easily disrupt the operation within that network. Thus, secure routing through malicious nodes detection and reduction is an important aspect that has to be incorporated with ad hoc networks for the successful commercialization of such networks and to support secure applications.

Various studies conducted earlier on secure routing in MANETs produced several routing protocols assuming that every node is fully trusted and will always behave cooperatively. Thus, they are susceptible to routing disruptions by misbehaving nodes which do not cooperate or violate the routing rules. Hence, trust-based routing schemes now become a new approach for reliable routing in MANETs. The formulation of trust information computation methods is the key to these countermeasures. To mitigate routing disruption attacks, this paper proposes the ESDRS trust scheme as a solution for the black hole problem in MANET.

The key contributions made in this paper are briefed as under:

- The robust self-detection procedure is designed and implemented using AODV with suitability to larger and high mobility networks.
- The developed scheme can be applied to any kind of MANET scenario. Thus, it provides a solution to the limited application scope of state-of-the-art schemes like ESCT [9] [10].
- The effectiveness of the developed scheme is validated in the varying scenarios of network density, network mobility, and network attackers. The superior performance of the proposed scheme is proved against state-of-the-art ESCT and standard AODV based on the computations of eight popular network security metrics. The experimentation is performed using the sophisticated EXata simulator environment.

The remainder of the paper is organized as follows: Section 2 briefs a survey of the related work. Section 3 discusses the proposed ESDRS scheme in detail. Section 4 describes the simulation setup along with network scenarios under consideration. It further discusses the performance analysis and underlies the effectiveness of the proposed scheme. At last, conclusions are drawn in Section 5 along with a note on the future work.

2. RELATED WORK

Due to the increasing use of mobile devices and MANET applications, this area of research has always attracted many researchers to produce their studies. The details of the research requirements, taxonomy, various secure transmission techniques, and the challenges faced by the research community are surveyed by S. N. Mahapatra et al. [11]. The various trust management routing schemes are also surveyed in the works of Avani Sharma et al. [12] and R. K. Chahal et al. [13]. The recent research attempts in this domain based on the experimentations concerning different applications are as follows:

M. A. Qurashi et al. [14] tried to identify a trade-off between the communication overhead, energy consumption, and system performance in identifying attacks for lightweight Intrusion Detection Systems (IDS). The proposed methodology does not rely on the size of the network but on the selected network properties. The experimental work is carried out by varying network density. Further, H. Riasudheen et al. [15] proposed a cloud-assisted MANET operation intending to save energy as expected for the fifth-generation (5G) networks. This work underlines the need for fast local route recovery among mobile nodes and peer nodes to mitigate the issues of routing overhead, mobility, link failure, and low battery power. For reducing the network overhead, Huaqiang Xu et al. [16] on the other hand proposed a trust-based probabilistic broadcast scheme. The methodology relies on the probability to reduce redundant retransmissions of Route REQuest (RREQ) packets. Another research again on statistical modeling can be cited in the work of P. Theerthagiri et al. [17], where a Markov random process is utilized for the evaluation of node reliability and link stability. Since the selection of such statistical models is mostly dependent on its suitability to an application at hand, the universal acceptance of these probabilistic methods is difficult. Next to this, J. Wilson et al. [1] extended the application of a conventional route selection algorithm for multi-objective data transmission. This work focuses on restricted energy levels of mobile nodes to bring stable communication by balancing the load. The work of N. Djedjig et al. [18] presented a trust aware and cooperative routing with the name 'Metric-based RPL Trustworthiness Scheme (MRTS)' to enhance the network security. Here, the experimentation does not consider the node-mobility. The literature cites the trust-based routing methodologies to be the most appealing. These can be further classified in reputation-based and credit-based schemes as follows:

2.1 REPUTATION-BASED APPROACH

The reputation or observed behavior of nodes can be obtained by direct observation or exchange of reputation messages among the nodes. In most of the reputation-based approaches, each node evaluates reputation levels of neighboring nodes according to its packet forwarding status [19]. These reputation levels are shared with neighbors to obtain undetermined trust information about the network [20], [21]. Further, these reputation levels are converted into usable trust metrics to differentiate malicious and benign nodes in a network.

2.2 CREDIT-BASED APPROACH

In this approach, the transfer of a packet across the network is treated as a deal. Service providing nodes are offered credits while service receiving nodes are charged. During the cooperation, nodes upload the receipt to the credit service center showing their actions of receiving or forwarding. After that, credits will be offered accordingly. However, these requirements limit the application area of the credit system in MANETs. Hence, trust-based security schemes have been proposed recently as reputation-based methods in MANETs. R. J. Cai et al. has presented a reputation-based ESCT scheme in [9] on the underlying dynamic routing protocol Dynamic Source Routing (DSR). But it is limited by the following aspect:

ESCT requires the dynamic exchange of information between a source node and its prior destination to identify malicious nodes in a route. Detection procedure is invoked only when a source node becomes a direct neighbor of its past destination node. But there may be situations where prior destination never becomes a direct neighbor of its source or intermediate node [25].

In cases of disasters like flood, fire or earthquake, the existing infrastructure is often damaged or destroyed. So, to overcome the problems incurred by missing infrastructure, using an ad hoc network, information is relayed from one rescue team member to another over a small mobile device. But it may happen that, a destination rescue team member (previous destination) will not directly meet its source rescue team member due to the unavailability of the route because of disaster or obstacles prevent direct communication [26].

Also, in case of military applications, where effective data collection is critical, obstacles may prevent direct communication among entities like soldiers, vehicles, and military information headquarters. Thus, in such applications where nodes cannot move within a range of each other, the routing scheme is not applicable. This will prevent the execution of detection procedure and hence, properties of intermediate nodes on the route to the destination will remain undetermined.

The proposed scheme ESDRS serves to promisingly handle this limitation which is discussed in the subsequent section.

3. PROPOSED SCHEME – ESDRS

The ESDRS scheme does not rely on the assumption that a source or an intermediate node can meet its prior destination. Instead, the proposed detection procedure is initiated by source or intermediate node when it becomes a direct neighbor of any node in a network. As AODV outperforms DSR in terms of storing capacity and memory overhead [22], it is more scalable and suitable for larger networks. So, the ESDRS is proposed on the top of dynamic routing protocol AODV.

3.1 TRUST INFORMATION COMPUTATION IN ESDRS

This section describes the mathematical steps that are used to compute the trust information about the nodes in MANET. The main notations used in this paper are described in Table 1. Here, $CC[i][j]$ denotes the co-operative count and $UC[i][j]$ denotes the uncooperative count of the intermediate nodes j calculated by a monitoring node i i.e., either a source or an intermediate node on the basis of number data packets correctly forwarded by those intermediate nodes j towards the destination. $TL[i][j]$ denotes the computed trust level of the intermediate node j by node i. The probabilities $PL_b[i][j]$ and $PL_m[i][j]$ are computed using Dempster-Shafer theory [23] which combines $CC[i][j]$ and $UC[i][j]$ values to a usable trust metric [9] as follows:

Table.1. Notations

Symbol	Description
m	Total number of data packets sent from a source node

k	Number of data packets lost during transmission from a source node to a destination node
$CC[i][j]$	Co-operative count node i calculates for node j
$UC[i][j]$	Uncooperative count node i calculates for node j
$PL_b[i][j]$	Probability that node i guesses node j will cooperatively forward packets furth
$PL_m[i][j]$	Probability that node i guesses node j will not cooperatively forward packets further
$T\,L[i][j]$	Trust level assigned by node i to node j
α	Self-detection threshold

$$PL_b[i][j] = CC[i][j]/(CC[i][j]+UC[i][j]+2)$$
$$PL_m[i][j] = UC[i][j]/(CC[i][j]+UC[i][j]+2) \quad (1)$$

The resulting trust metrics $PL_b[i][j]$ and $PL_m[i][j]$ signify the packet forwarding ratio which means the actual number of data packets forwarded by a node to the expected number of data packets to be forwarded by that node. For the normal node, its value should be greater than 50 percent i.e., $\alpha > 0.5$. Hence, the value for the self-detection threshold α is set to 0.7 [9]. If $PL_b[i][j]$ is greater than the self-detection threshold α, node i will indicate node j as a benign (i.e., sets $TL[i][j] = 1$) or if $PL_m\,[i][j]$ is greater than the self-detection threshold α, node i will indicate node j as a malicious node (i.e., sets $TL[i][j] = -1$). Otherwise, trust level of node j remains undetermined (i.e., $TL[i][j] = 0$). Algorithm - 1 shows the working of the proposed scheme ESDRS to identify benign and malicious nodes in a network.

To demonstrate the procedure of trust information computation in Algorithm 1, an example of a MANET scenario is shown in Fig.1.

Algorithm 1: Working of the Proposed Scheme - ESDRS

1: Node X receives Hello message from any other node in a network i.e., node X becomes a direct neighbor of any node in a network.
2: **if** node X is a source node or an intermediary node on an active route (i.e., X has sent/forwarded any data packet to destination before **then**
3: X computes CC and UC for all intermediary nodes between itself and its destination.
4: X combines CC and UC values to usable trust metrics PL_b and PL_m using Eq.(1).
5: Based on PL_b and PL_m values, X computes trust levels (TL) of intermediary nodes between itself and its destination.
6: X modifies its TL to store the trust levels of recognized nodes.
7: **else**
8: Skip the further detection process.
9: **end if**

The scenario shows the MANET with thirty arbitrarily placed nodes with random mobility. Node 1 is a source node sending data packets to a destination node 5. Packets are being transferred using a constant bit rate (CBR). For instance, assuming that source node 1 wants to send a total of 30 packets to its destination node 5. From figure 1, route discovery finds a route from source 1 to its destination 5 as: node 1 → node 9 → node 2 → node 7 → node 5. Once, a route from source to its destination is found, data transmission begins during which procedure to discover malicious nodes is invoked. During transmission each node periodically broadcasts a Hello message to its neighboring nodes as shown in figure 2 and proposed scheme invokes detection procedure when a source or any participating/intermediate node receives a Hello message from any node in the network i.e., they are becoming direct neighbors. Working of the ESDRS for the MANET scenario as shown in figure 1 is demonstrated below.

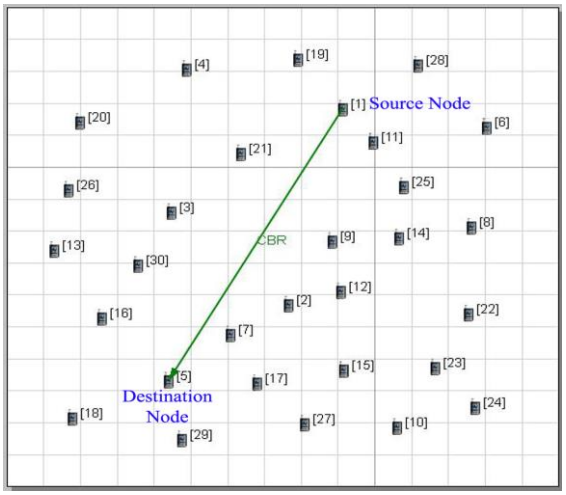

Fig.1. An example of a MANET scenario with 30 mobile nodes.

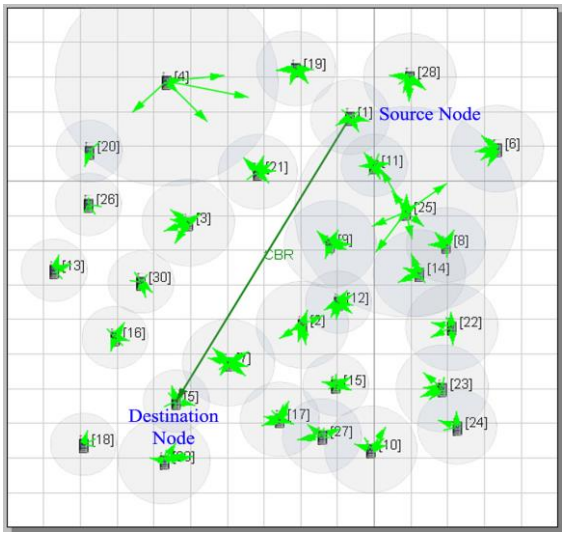

Fig.2. Periodic broadcast of Hello message

Let, during data transmission, node 1 received hello from another node in a network and till now node 1 has sent 30 packets to node 5. Assume that, intermediate node 7 is acting as a black hole i.e., node 7 will drop all of the data packets that are to be forwarded further. If the number of received packets by destination is 20 then $k = 10$ (i.e., 10 data packets are lost during transmission). Then the trust levels of participating nodes (here, nodes 9, 2, and 7) can be obtained as follows:

$CC[1][7] = 20$

$UC[1][7] = \lceil k/ \text{ no. of intermediate nodes} \rceil = \lceil 10/3 \rceil = 4$

From Eq.(1),

PL_b [1][7] = CC[1][7]/(CC[1][7]+UC[1][7]+2) = 20/(20+4+2) = 0.7692 and

PL_m [1][7] = UC[1][7]/(CC[1][7]+UC[1][7]+2) = 4/(20+4+2) = 0.1538

As PL_b [1][7] > self-detection threshold (α = 0.7) and PL_m [1][7] < self-detection threshold, node 1 sets trust level of node 7 as 1 (i.e. benign node). Hence, TL[1][7] = 1.

Similarly, trust levels are calculated by node 1 for next intermediate node 9 as:

CC[1][9] = 20

UC[1][9] = ⌈k/ no. of intermediate nodes⌉ = ⌈10/3⌉ = 4

From Eq.(1),

PL_b [1][9] = CC[1][9]/(CC[1][9]+UC[1][9]+2) = 20/(20+4+2) = 0.7692 and

PL_m [1][9] = UC[1][9]/(CC[1][9]+UC[1][9]+2) = 4/(20+4+2) = 0.1538

As PL_b [1][9] > self-detection threshold (α = 0.7) and PL_m [*1*][*9*] < self-detection threshold, node 1 sets trust level of node 9 as 1 (i.e. benign node). Hence, *TL*[*1*][*9*] = 1. Similarly, *TL*[*1*][*2*] = 1 is obtained for next intermediate node 2.

The obtained trust levels (benign (1) or malicious (-1)) are further used by observing nodes to exclude malicious nodes in the network. For example, when any malicious node (i.e., with trust level equal to -1) is encountered by a sending node in the next packet transmission process, it invokes a route maintenance procedure to avoid that malicious node to be a part of a next active route.

The proposed method increases the number of initiations of the self-detection procedure and thus decreases the possibility of undetermined malicious nodes. This may cause increased overhead due to greater Hello message exchange. But, without a satisfied PDR it would be trivial to care about overhead.

4. SIMULATION RESULTS AND DISCUSSION

This section details the simulation setup utilized for the experimentation, an overview of an attacker model, and the various evaluation metrics for performance measurement. These are followed by the experimental results and the performance analysis.

4.1 SIMULATION SETUP

Mobile networks usually have to face tougher challenges than those to all other networks. These include dealing with atmospheric conditions, bandwidth management, mobility effects, limited battery power, security threats, session management, scalability, traffic congestion, and quality of service trade-offs. EXata [24] is a sophisticated simulator cum emulator software that permits to digitally represent entire network devices and related effects. It also facilitates to analyze each and every situation where the performance of a real network is affected. Hence, the proposed routing scheme is tested using simulations conducted in EXata environment. The details of experimental setup are as shown in Table.2.

Table.2. Details of experimental setup.

Specifications	Details
Software	EXata Network Simulator/Emulator
Processor	Common 32-bit KVM processor 2.90 GHz (2 processors)
RAM	4 GB
System	Windows-7 32-bit Operating System

In this work, a MANET with randomly placed nodes having random waypoint mobility is used and nodes are chosen as misbehaving nodes that drop all the data packets that do not belong to them. The inter-channel interference model is disabled and only co-channel interference is considered.

The simulation parameters used in configuring this MANET are as shown in Table.3.

Table.3. Simulation Parameters

Parameter	Value
Simulation area (*m*×*m*)	1500 × 1500
Mobility Pattern	Random Waypoint
Number of nodes	10, 15, 20, 25, 30
Node max speed (mps)	5, 10, 15, 20, 25
Number of attackers	1, 2, 3, 4, 5
Number of data packets sent from source	40
CBR transmission time	1 s to 45 s
CBR transmission interval	1 s
Packet size	512 bytes
Data rate	2 Mbps
Simulation time (s)	45 s
Node pause time (s)	0 s
Transmission range	250 m
Physical protocol	IEEE 802.11b
MAC protocol	IEEE 802.11
Network protocol	IPv4
Routing protocol	AODV
Transport protocol	UDP
Application protocol	CBR
Self-detection threshold (α)	0.7

4.2 ATTACKER MODEL

Selfish and malicious nodes are the causes of misbehavior in the network making AODV susceptible to various kinds of routing disruption attacks [2, 25]. The experimentation is conducted by assuming selfish node as attacker that can drop all the data packets that do not belong to them i.e., black holes. To avoid detection during the route discovery process, a selfish node shows normal behavior. On the other hand, once it is selected as a part of an active route towards destination it shows abnormal behavior by dropping all the data packets that are to be forwarded further [26].

1.1 EVALUATION METRICS

The following evaluation metrics are computed for the performance evaluation of the proposed scheme ESDRS. Variation in the resultant values of these metrics is tested considering the impact of node density (number of nodes in a network), attack scenario (number of attackers in a network), and node mobility (node speed).

- **PDR:** It is the ratio of the number of data packets correctly received by a destination node to the total number of data packets sent by a source node.
- **End-to-end Delay:** It is the average amount of time a data packet takes to travel across the network from a source node to its destination node.
- **Throughput:** It is the average number of bits received by a destination node per unit time.
- **Jitter:** It is the variance in the time delay between data packets over a network. It is a disturbance in the normal flow of sending data packets. It is also known by packet delay variance or network jitter.
- **Number of data packets dropped:** It is the fraction of data packets that are dropped by malicious nodes without any notification. The loss percentage should be minimum.
- **PoD of malicious behavior:** It is the ratio of the number of nodes whose malicious behavior is identified correctly to the actual number of such nodes present in the network. The expected value of this PoD is 1.
- **PoD of benevolent behavior:** It is the ratio of the number of nodes whose benevolent behavior is identified correctly to the actual number of such nodes present in the network. The expected value of this PoD is 1.
- **Normalized Routing Overhead/Control Overhead:** It is the ratio of the total number of generated control packets (including Hello message, RREQ and Route REPly (RREP)) to the total number of received data packets. The overhead should be minimum.

4.3 EXPERIMENTAL RESULTS

Since the efficiency of a routing protocol in MANET can be tested based on the guarantee of correct route discovery, correct delivery of data packets towards a destination, detection of malicious attackers, and stability against attacks, the performance of the proposed scheme ESDRS is measured based on the metrics discussed above. Its potential is validated against standard AODV and ESCT (implemented with AODV). The results corresponding to the experimentation of variations in number of nodes, number of attackers and node speed are respectively shown in Table.4-Table.6.

Table.4. Experimentation with variation in Number of Nodes.

Performance Metrics	No. of Nodes	Standard AODV	ESCT	Proposed Scheme - ESDRS
PDR	10	24/40	24/40	27/40
	15	38/40	38/40	38/40
	20	25/40	25/40	29/40
	25	25/40	25/40	26/40
	30	28/40	28/40	28/40
End-to-End Delay (s)	10	0.01525	0.01525	0.01511
	15	0.01288	0.01288	0.01288
	20	0.01562	0.01562	0.01442
	25	0.01542	0.01542	0.01509
	30	0.02447	0.02447	0.02447
Throughput (bits/s)	10	2239.95	2239.95	2519.94
	15	3546.67	3546.67	3546.67
	20	2334.03	2334.03	3055.18
	25	2333.71	2333.71	2427.05
	30	2940.40	2940.40	2940.40
Jitter (s)	10	0.00526	0.00526	0.00480
	15	0.00388	0.00388	0.00388
	20	0.00552	0.00552	0.00497
	25	0.00529	0.00529	0.00557
	30	0.02110	0.02110	0.02110
No. of data packets dropped	10	14	14	9
	15	0	0	0
	20	13	10	9
	25	12	12	9
	30	8	8	8
PoD of malicious behavior	10	0.00	1.00	1.00
	15	0.00	0.00	0.00
	20	0.00	1.00	1.00
	25	0.00	1.00	1.00
	30	0.00	0.00	0.00
PoD of benevolent behavior	10	0.00	0.00	1.00
	15	0.00	0.00	1.00
	20	0.00	0.00	1.00
	25	0.00	0.00	1.00
	30	0.00	0.00	1.00
No. of hello packets	10	414	414	399
	15	621	621	621
	20	814	805	814
	25	1027	1027	1003
	30	1222	1222	1222
No. of RREQ packets	10	4	4	3
	15	3	3	3
	20	6	6	3
	25	5	5	5
	30	7	7	7
No. of RREP packets	10	3	3	4
	15	2	2	2
	20	4	6	3
	25	3	3	5

	30	5	5	5

4.4 PERFORMANCE ANALYSIS

Considering the measurement of PDR, the comparative performance analysis of the routing schemes is made through the plots shown in (a), (c), and (e) of Figure 3. The desired value of PDR is always 1. To see this overall comparison for PDR, it is found that ESDRS outperforms the other two in all the cases of variations. An increase in the number of attackers has resulted in the corresponding decrease in PDR but, still, the ESDRS is successful to achieve the highest possible PDR as compared to the other two schemes.

Table.5. Experimentation with variation in Number of Attackers

Performance Metrics	No. of Attackers	Standard AODV	ESCT	Proposed Scheme - ESDRS
PDR	1	25/40	25/40	29/40
	2	25/40	25/40	29/40
	3	9/40	9/40	2/40
	4	0/40	0/40	14/40
	5	0/40	0/40	10/40
End-to-End Delay (s)	1	0.01562	0.01562	0.01442
	2	0.01562	0.01562	0.01442
	3	0.00874	0.00874	0.02720
	4	0.00000	0.00000	0.00863
	5	0.00000	0.00000	0.00726
Throughput (bits/s)	1	2334.03	2334.03	3055.18
	2	2334.03	2334.03	3055.18
	3	1942.37	1942.37	221.448
	4	0.00000	0.00000	3022.39
	5	0.00000	0.00000	1107.25
Jitter (s)	1	0.00552	0.00552	0.00497
	2	0.00552	0.00552	0.00497
	3	0.00191	0.00191	0.04013
	4	0.00000	0.00000	0.00188
	5	0.00000	0.00000	0.00032
No. of data packets dropped	1	13	10	9
	2	13	10	9
	3	26	26	30
	4	39	39	20
	5	39	39	22
PoD of malicious behavior	1	0.00	1.00	1.00
	2	0.00	0.50	0.50
	3	0.00	0.33	0.66
	4	0.00	0.50	0.75
	5	0.00	0.40	0.60
	1	0.00	0.00	1.00
	2	0.00	0.00	1.00
PoD of benevolent behavior	3	0.00	0.00	0.00
	4	0.00	0.00	0.00
	5	0.00	0.00	0.00
No. of hello packets	1	814	805	814
	2	814	805	814
	3	809	809	780
	4	832	832	763
	5	832	832	784
No. of RREQ packets	1	6	6	3
	2	6	6	3
	3	7	7	7
	4	4	4	4
	5	4	4	6
No. of RREP packets	1	4	6	3
	2	4	6	3
	3	12	12	8
	4	2	2	7
	5	2	2	7

The routing schemes are further compared based on end-to-end delay and the corresponding results are plotted in (b), (d), and (f) of Figure 3. In all the three schemes, it is noticed that for an increase in the number of nodes, the end-to-end delay also increases.

Table.6. Experimentation with variation in Node Speed.

Performance Metrics	Node Speed	Standard AODV	ESCT	Proposed Scheme - ESDRS
PDR	5	40/40	40/40	40/40
	10	13/40	12/40	29/40
	15	19/40	19/40	37/40
	20	23/40	23/40	37/40
	25	30/40	30/40	39/40
End-to-End Delay (s)	5	0.01340	0.01340	0.01340
	10	0.07314	0.06971	0.01442
	15	0.00692	0.00692	0.00894
	20	0.00560	0.00560	0.01088
	25	0.00524	0.00524	0.00943
Throughput (bits/s)	5	4212.19	4212.19	4212.19
	10	3778.28	2589.83	3050.18
	15	3389.03	3389.03	3968.39
	20	3772.63	3772.63	3897.05
	25	4241.52	4241.52	4107.72
Jitter (s)	5	0.00303	0.00303	0.00303
	10	0.13300	0.13540	0.00497
	15	0.00263	0.00263	0.00466
	20	0.00159	0.00159	0.00596
	25	0.00122	0.00122	0.00475

No. of data packets dropped	5	0	0	0
	10	24	24	9
	15	16	16	0
	20	13	13	0
	25	9	9	0
PoD of malicious behavior	5	0.00	0.00	0.00
	10	0.00	0.00	1.00
	15	0.00	0.00	1.00
	20	0.00	0.00	1.00
	25	0.00	0.00	1.00
PoD of benevolent behavior	5	0.00	0.00	1.00
	10	0.00	0.00	1.00
	15	0.00	0.00	1.00
	20	0.00	0.00	1.00
	25	0.00	0.00	1.00
No. of hello packets	5	846	846	846
	10	794	794	814
	15	830	830	833
	20	833	833	834
	25	834	834	834
No. of RREQ packets	5	2	2	2
	10	9	9	3
	15	7	7	3
	20	3	3	3
	25	3	3	3
No. of RREP packets	5	1	1	1
	10	14	15	3
	15	6	6	2
	20	2	2	2
	25	2	2	2

But with increasing node speed, ESDRS shows more delay as compared to the other two schemes. This is due to the greater number of node interactions taken place during node misbehavior detection. When ESDRS is executed, nodes try to avoid attackers although they will have to opt longer paths, rather than using the shortest path. Therefore, with the rise in the number of attackers within the network, the end-to-end delay of ESDRS increases as compared to the other two schemes. On the other hand, the end-to-end delay of standard AODV and ESCT reduces with the rise in the number of attackers. The reason is most of the data packets are not received by the destination but being dropped by the attackers in the presence of an increased number of attackers. The packet delay measurement does not include all such lost data packets.

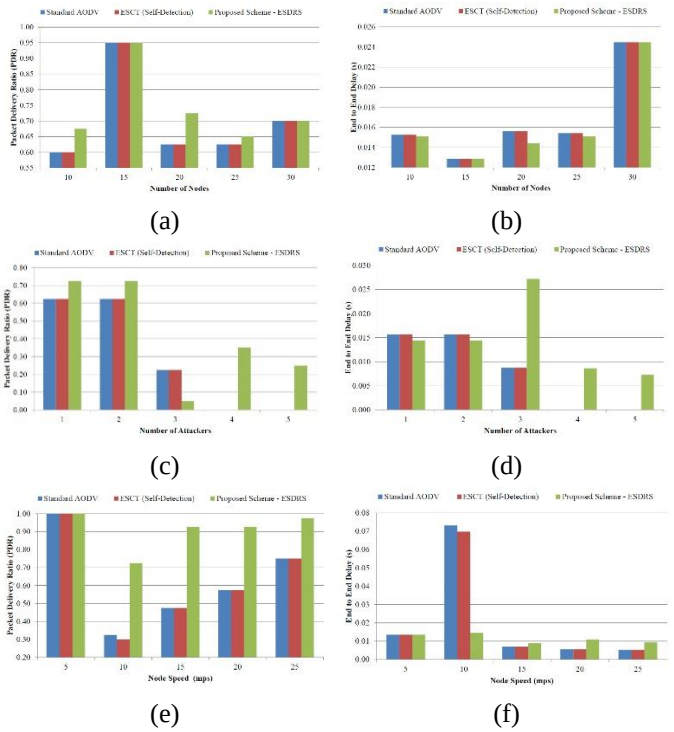

Fig.3. Comparison of routing schemes considering measurement of PDR and end-to-end delay w.r.t. variation in number of nodes, number of attackers, and node speed.

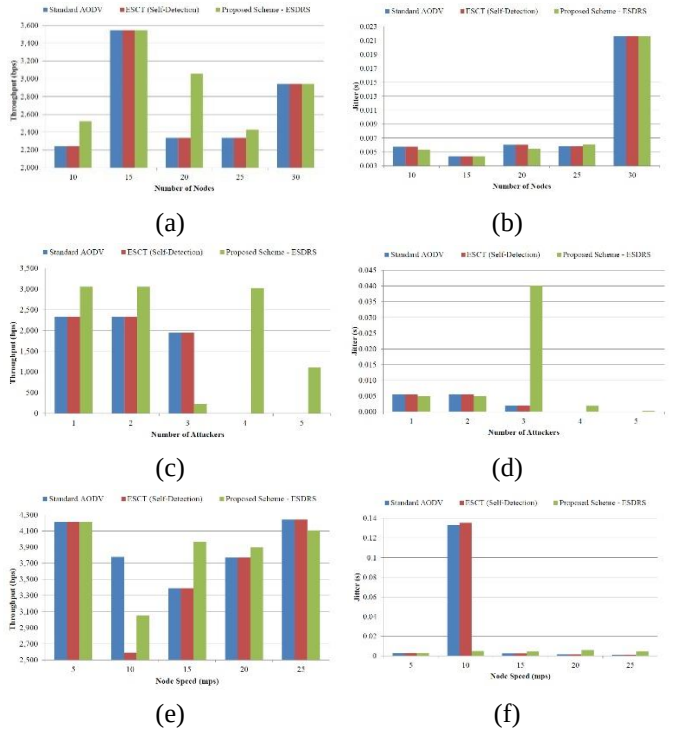

Fig.4. Comparison of routing schemes considering measurement of throughput and jitter w. r. t. variation in number of nodes, number of attackers, and node speed.

7///

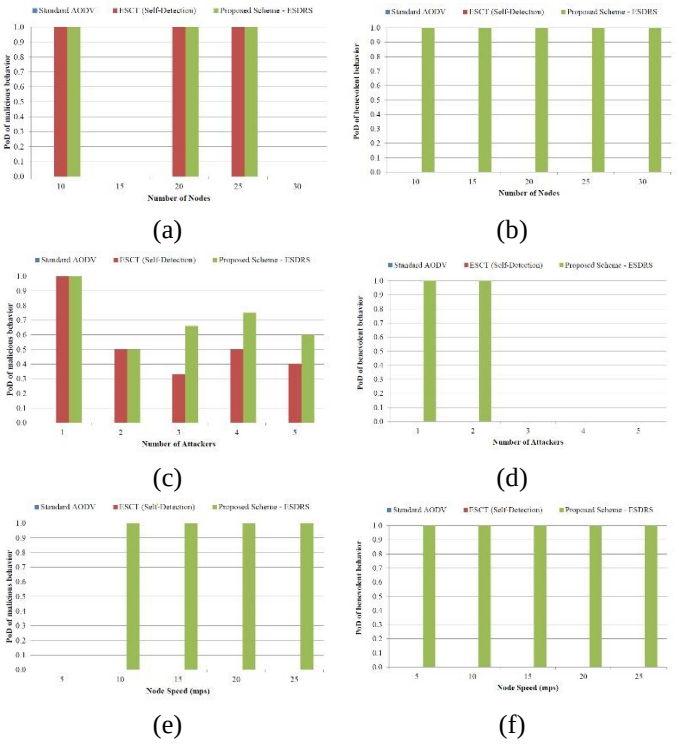

Fig.5. Comparison of routing schemes considering measurement of PoD of malicious behavior and PoD of benevolent behavior w.r.t. variation in number of nodes, number of attackers, and node speed

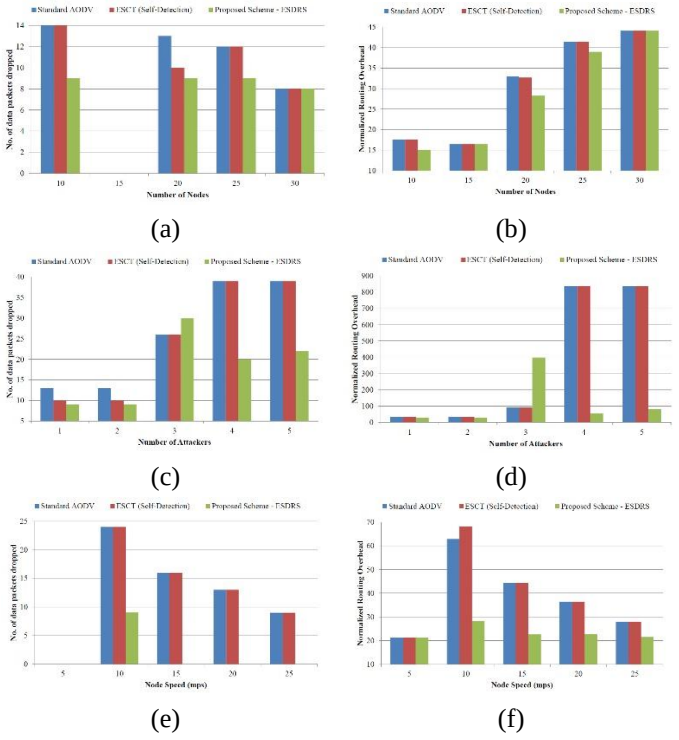

Fig.6. Comparison of routing schemes considering measurement of number of data packets dropped and normalized routing overhead w.r.t. variation in number of nodes, number of attackers, and node speed

Three routing schemes are also compared based on achieved throughput and comparisons are plotted in (a), (c), and (e) of Figure 4. For efficient routing, it is always desired to obtain maximum throughput. Since ESDRS can ensure more data packets being received by destination nodes under the same adversarial environment, the throughput also improves. The average performance of the proposed ESDRS routing scheme shows comparatively more throughput achieved than the other two.

Further, the variation in packet arrival delay i.e., jitter is used for comparison of routing schemes. The (b), (d), and (f) of Figure 4 show computed jitter for respective variations in the number of nodes, the number of attackers, and node speed. Ideally, jitter should be maintained at a minimum. The computational complexity increased to identify trust levels of participating nodes partially limit the routing efficiency of the proposed scheme to achieve the desired level of jitter.

The comparative performance analysis is extended based on measuring the PoD of malicious behavior and that of benevolent behavior. The respective performances of routing schemes for the variations in the number of nodes, the number of attackers, and the node speed are plotted in Figure 5. Since, there is no detection methodology in the standard AODV routing, the PoD for both malicious and benevolent behavior is computed to zero. Also, the failure of ESCT is observed to detect the benevolent nodes in the network for all kinds of network variations. Whereas, the proposed scheme ESDRS successfully detects such nodes. The superior performance of ESDRS over the ESCT in all kinds of network variations is also evident for the detection of malicious nodes.

The three routing schemes are further compared based on the number of data packets dropped by malicious nodes and the comparative performances are shown in (a), (c), and (e) of Figure 6. In all the three scenarios, the proposed scheme ESDRS has the least or zero drop of data packets than that by ESCT and standard AODV. The efficiency of the proposed scheme ESDRS can be very clearly validated when ESCT and standard AODV drops all the data packets for the rise in number of attackers, but ESDRS still manages the routing with the least possible drop of data packets.

Finally, the routing schemes are also tested based on the scheme overhead in terms of the number of control packets i.e., Hello packets, RREQ packets, and RREP packets. The normalized routing overhead is computed as the ratio of total number of generated control packets to the total number of received data packets. It is plotted in (b), (d), and (f) of Figure 6 showing respective plot against variations in the number of nodes, the number of attackers, and node speed. For an ideal routing scheme, the routing overhead should always be a minimum. Practically, it is obvious that the routing overhead increases with an increase in the number of nodes. Here, the proposed scheme ESDRS successfully carries out the routing procedure with a minimal routing overhead as compared to other two. The superiority of the ESDRS over others is also clear for the normalized routing overhead plotted against the varying number of attackers and the node speed.

Lastly, the computational complexity is also analyzed. It is observed that, for the proposed routing scheme the comparative average amount of time required for a data packet to travel from

a source node to its destination node slightly increases with an increase in node's maximum speed. This is due to the greater number of node interactions taken place during node misbehavior detection. Also, ESDRS may have an increased overhead due to greater exchange of Hello messages but without a satisfied PDR it would be trivial to care about overhead. Comparatively, the existing schemes have significantly reduced PDR than the proposed scheme with an increase in the speed of nodes. Hence, the end-to-end delay for the existing schemes is computed to zero for the data packets that are not sent to the destination node.

5. CONCLUSION

In this paper, an enhanced trust-based routing scheme ESDRS is proposed as a solution to the limited application scope of state-of-the-art routing schemes like ESCT. The flexible applicability of the proposed scheme to any MANET scenario is due to a robust self-detection procedure designed using AODV. The experimentation in the EXata environment followed by a comparative performance analysis based on the computations of eight popular metrics measured for three types of network variations finds the proposed scheme ESDRS superior than ESCT and standard AODV. This proves ESDRS a promising option for secure routing in MANETs. Currently, the proposed scheme is experimentally validated considering the black hole attackers. In future work, we plan to improve the routing scheme for effective handling of the other attack scenarios like misrouting, modification, fabrication, and spoofing.

REFERENCES

[1] J. Wilson and K. Subramaniam, "Improved Multi Objective Data Transmission using Conventional Route Selection Algorithm in Mobile Ad Hoc Network", *Peer-to-Peer Networking and Applications*, Vol. 13, pp. 1091-1101, 2020.

[2] T. Li, J. Ma, Q. Pei, H. Song, Y. Shen and C. Sun, "DAPV: Diagnosing Anomalies in MANETs Routing with Provenance and Verification", *IEEE Access*, Vol. 7, pp. 35302-35316, 2019

[3] S. Du, J. Hou, S. Song, Y. Song and Y. Zhu, "A Geographical Hierarchy Greedy Routing Strategy for Vehicular Big Data Communications over Millimeter wave", *Physical Communication*, Vol. 40, pp. 1-9, 2020.

[4] D. Manivannan, S.S. Moni and S. Zeadally, "Secure Authentication and Privacy Preserving Techniques in Vehicular Ad-Hoc Networks", *Vehicular Communications*, Vol. 25, pp. 1-18, 2020.

[5] W. Fang, W. Zhang, W. Chen, Y. Liu and C. Tang, "TMSRS: Trust Management-based Secure Routing Scheme in Industrial Wireless Sensor Network with Fog Computing", *Wireless Networks*, Vol. 26, pp. 3169-3182, 2020.

[6] H.A. Ali, M.F. Areed and D.I. Elewely, "An On-Demand Power and Load-Aware Multi-Path Node-Disjoint Source Routing Scheme Implementation using NS2 for Mobile Ad-Hoc Networks", *Simulation Modelling Practice and Theory*, Vol. 80, pp. 50-65, 2018.

[7] D. Gan Zhang, J. Xin Gao, X. Huan Liu, T. Zhang and D. Xin Zhao, "Novel Approach of Distributed and Adaptive Trust Metrics for MANET", *Wireless Networks*, Vol. 25, pp. 3587-3603, 2019.

[8] H. Kojima, N. Yanai and J.P. Cruz, "ISDSRC: Improving the Security and Availability of Secure Routing Protocol", *IEEE Access*, Vol. 7, pp. 74849-74868, 2019.

[9] R.J. Cai, X.J. Li and P.H.J. Chong, "An Evolutionary Self-Cooperative Trust Scheme Against Routing Disruptions in MANETs", *IEEE Transactions on Mobile Computing*, Vol. 18, No. 1, pp. 42-55, 2019.

[10] M. Ponguwala and S. Rao, "E2-SR: A Novel Energy-Efficient Secure Routing Scheme to Protect MANET-IoT", *IET Communications*, Vol. 13, pp. 3207-3216, 2019.

[11] S.N. Mahapatra, B.K. Singh and V. Kumar, "A Survey on Secure Transmission in Internet of Things: Taxonomy, Recent Techniques, Research Requirements, and Challenges", *Arabian Journal for Science and Engineering*, Vol. 45, pp. 6211-6240, 2020.

[12] A. Sharma, E.S.Pilli, A.P. Mazumdar and P. Gera, "Towards Trustworthy Internet of Things: A Survey on Trust Management Applications and Schemes", *Computer Communications*, Vol. 160, pp. 475-493, 2020.

[13] R.K. Chahal, N. Kumar and S. Batra, "Trust Management in Social Internet of Things: A Taxonomy, Open Issues, and Challenges", *Computer Communications*, Vol. 150, pp. 13-46, 2020.

[14] M.A. Qurashi, C.M. Angelopoulos and V. Katos, "An Architecture for Resilient Intrusion Detection in Ad-Hoc Networks", *Journal of Information Security and Applications*, Vol. 53, pp. 1-12, 2020.\

[15] H. Riasudheen, K. Selvamani, S. Mukherjee and I. Divyasree, "An Efficient Energy-Aware Routing Scheme for Cloud-Assisted Manets in 5G", *Ad Hoc Networks*, Vol. 97, pp. 1-22, 2020.

[16] H. Xu, "Trust-Based Probabilistic Broadcast Scheme for Mobile Ad Hoc Networks", *IEEE Access*, Vol. 8, pp. 21380-21392, 2020.

[17] P. Theerthagiri, "FUCEM: Futuristic Cooperation Evaluation Model using Markov Process for Evaluating Node Reliability and Link Stability in Mobile Ad Hoc Network", *Wireless Networks*, Vol. 26, pp. 4173-4188, 2020.

[18] N. Djedjig, D. Tandjaoui, F. Medjek and I. Romdhani, "Trust-Aware and Cooperative Routing Protocol for IoT Security", *Journal of Information Security and Applications*, Vol. 52, pp. 1-17, 2020.

[19] X. Huang, R. Yu, J. Kang and Y. Zhang, "Distributed Reputation Management for Secure and Efficient Vehicular Edge Computing and Networks", *IEEE Access*, Vol. 5, pp. 25408-25420, 2017.

[20] A. Anand, H. Aggarwal and R. Rani, "Partially Distributed Dynamic Model for Secure and Reliable Routing in Mobile Ad hoc Networks", *Journal of Communications and Networks*, Vol.18, pp. 938-947, 2016.

[21] W. Gong, Z. You, D. Chen, X. Zhao, M. Gu and K. Lam, "Trust based Routing for Misbehavior Detection in Ad Hoc Networks", *Journal of Networks*, Vol. 5, pp. 551-558, 2010.

[22] E. Ochola, L. Mejaele, M. Eloff and J. Van Der Poll, "MANET Reactive Routing Protocols Node Mobility Variation Effect in Analysing the Impact of Black Hole

Attack", *SAIEE Africa Research Journal*, Vol. 108, pp. 80-92, 2017.

[23] Z. Wei, H. Tang, F. R. Yu, M. Wang and P. Mason, "Security Enhancements for Mobile Ad Hoc Networks with Trust Management using Uncertain Reasoning", *IEEE Transactions on Vehicular Technology*, Vol. 63, pp. 4647-4658, 2014.

[24] Exata Network Emulator Software, Available at https://www.scalable-networks.com/exata-network-emulator-software, Accessed at 2021.

[25] D.J. Persis and T.P. Robert, "Review of Ad-Hoc on-Demand Distance Vector Protocol and its Swarm Intelligent Variants for Mobile Ad-hoc Network", *IET Networks*, Vol. 6, pp. 87-93, 2017.

[26] A.M. El-Semary and H. Diab, "BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs based on Chaotic Map", *IEEE Access*, Vol. 7, pp. 95197-95211, 2019.