Hindawi
Security and Communication Networks
Volume 2018, Article ID 3210207, 13 pages
https://doi.org/10.1155/2018/3210207

Research Article

A Sequence Number Prediction Based Bait Detection Scheme to Mitigate Sequence Number Attacks in MANETs

Rutvij H. Jhaveri,[1] **Aneri Desai**,[2] **Ankit Patel**,[2] **and Yubin Zhong**[3]

[1]*Delta-NTU Corporate Laboratory, Nanyang Technological University, Singapore 639798*
[2]*SVM Institute of Technology, Bharuch 392001, India*
[3]*Guangzhou University, Guangzhou 510006, China*

Correspondence should be addressed to Yubin Zhong; zhong_yb@163.com

Received 25 June 2018; Accepted 15 October 2018; Published 15 November 2018

Guest Editor: Lianyong Qi

Copyright © 2018 Rutvij H. Jhaveri et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The characteristics of MANET such as decentralized architecture, dynamic topologies make MANETs susceptible to various security attacks. Sequence number attacks are such type of security threats which tend to degrade the network functioning and performance by sending fabricated route reply packets (RREP) with the objective of getting involved in the route and drop some or all of the data packets during the data transmission phase. The sequence number adversary attempts to send a fabricated high destination number in the RREP packet which attracts the sender to establish a path through the adversary node. This paper proposes a proactive secure routing mechanism which is an improvement over the authors previously proposed scheme. It makes use of linear regression mechanism to predict the maximum destination sequence number that the neighboring node can insert in the RREP packet. As an additional security checkpoint, it uses a bait detection mechanism to establish confidence in marking a suspicious node as a malicious node. The proposed approach works in collaboration with the ad hoc on-demand distance vector routing (AODV) protocol. The simulation results depict that the approach improves the network performance in the presence of adversaries as compared to previously proposed scheme.

1. Introduction

The use of wireless network has increased tremendously due to the nonrestriction of the nodes to be stagnant physically [1]. MANETs are such infrastructure-less wireless networks where the communication between the nodes is performed through multihop paths [2]. MANETs have gained popularity in various domains such as military operations, natural calamities, maritime communications, vehicular computing, and remote weather forecasting due to the properties such as dynamic topology, easy configuration of nodes, and distributed administration [3, 4]. Despite the popularity of MANETs, its characteristics bring various vulnerabilities to its doorstep [5, 6].

In a MANET, each and every node has the responsibility to route the packets [7]. The routing protocols in MANET are divided into two major categories, namely, proactive routing protocols and reactive routing protocols [8]. The proactive protocols have per-defined routes between the nodes in the network whereas the reactive protocols establish on-demand routes; i.e., they are created when there is a need of communication between the nodes. The predefined routes may waste the network resources if no communication takes place through that route. As a result, the reactive routing protocols have gained more popularity for such networks [4]. However, the reactive routing protocols are prone to different types of attacks.

An adversary may take the benefit of the nodes being routers and perform many malicious activities to hinder the smooth communication between the nodes. This is due to the fact that the normal legitimate nodes may come under the influence of the adversaries and get compromised as there are no security mechanisms present in the traditional routing protocols [9, 10]. The issue of data privacy also exists in the infrastructure-less networks such as MANETs [11, 12]. Many researchers have done their research in finding

the solutions that addresses these various issues [13–15]. In order to facilitate smooth communication in the presence of such adversary nodes, various secure routing algorithms are proposed to overcome the negative effects of the adversaries. The cryptographic approaches are casually used to provide confidentiality in the network [13, 16]. The use of hashing mechanism is also used to resolve the privacy issues in the smooth communication of data between mobile nodes and vehicles [17]. In addition, cluster management and classification based techniques are also used to overcome the negative effects caused due to the dynamic topology of the nodes in a MANET [18, 19]. Moreover, many secure routing approaches have been proposed to achieve quality-of-services (QoS) by addressing the availability issue infringed by denial-of-service (DoS) attacks [8].

The sequence number attack (such as grayhole attack or blackhole attack) is a type of DoS attack where the attacker's intention is to prohibit the benign node from receiving the data packets [8]. The sequence number attacks cause packet forwarding misbehaviors during data transmission with the sole intention to degrade the network performance [3]. In the initial phase, the adversary node first attempts to become the part of the route. To accomplish this task, the adversary sends a fabricated route reply packet (RREP) claiming that it has fresher route towards the destination [20]. The adversary node does this by sending an RREP packet with a fabricated destination sequence number which indicates a high level of freshness of the route. As a result, the source node gets the impression that the node sending RREP (the adversary node) has a fresher route towards the destination [8]. Thus, the adversary node, after entering in the route between the source and the destination starts packet dropping behavior.

Many researchers have designed different schemes to overcome the performance losses caused by the sequence number attacks by targeting the common routines that the adversary follows [3]. The use of fuzzy systems also helps in overcoming the sequence number attackers [21, 22]. Recently machine learning approaches have achieved a great deal of attention from the researchers to overcome the negative effects of the adversary nodes [23, 24]. The detection of the adversaries can be either performed during the route discovery phase (i.e., proactive manner) or during the transmission of data (i.e., reactive manner). As the reactive approaches tend to detect the adversaries after some packet loss, they compromise QoS of the network. In this paper, we propose a reactive approach which detects adversary nodes during the route discovery phase as critical applications such as industry control systems or military operations may not afford to lose data packets. The proposed scheme, sequence number prediction based bait detection scheme (SNPBDS), is an enhancement to our previous scheme, sequence number based bait detection scheme (SNBDS) [3]. SNPBDS incorporates an additional mechanism based on linear regression [25] which predicts the threshold value of the destination sequence number of the RREP packet. When a node sends RREP with higher sequence number compared to the predicted threshold value, the node is marked as a suspicious node. To confirm the adversary node as a malicious node, a bait detection scheme is employed. If the suspicious node is marked as a malicious node, it is excluded from the route and control packets received from that node are ignored.

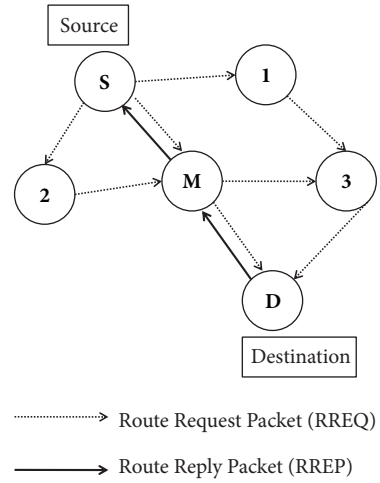


Figure 1: Operation of AODV protocol [2].

The paper is organized as follows. The working of the traditional sequence number based packet forwarding misbehavior attack is presented in Section 2. Section 3 presents the enhanced adversary model. Section 4 provides the related work and Section 5 presents the proposed approach followed by Simulation Results in Section 6. Finally Section 7 provides the conclusion to the paper.

2. Operation of the Sequence Number Attack

In MANETs adopting AODV routing protocol, the source node wishing to communicate to the destination first generates an RREQ packet and broadcasts the packet to its neighbors. The neighbors broadcast the request further until the packet reaches the destination or an intermediate node with a valid fresher path [2]. This node then replies with an RREP packet towards the reverse path to the source node. The RREP packet contains a destination sequence number which is used to denote the freshness of the route [4].

Figure 1 shows the route establishment in the AODV-based MANETs. The source node S generates an RREQ packet and broadcasts the packet to its neighboring nodes 1, 2, and M. These nodes pass the packets further and the RREQ packet reaches the destination D. The destination node selects the reverse path having the less hop count and, therefore, the RREQ from node 3 is discarded. Thus, the destination node D generates an RREP packet and forwards it to node E which then forwards the same to node S. In this way a path is formed as S-M-D for data communication.

As aforementioned, every RREP packet contains a destination sequence number to indicate freshness of the route. A sequence number adversary node in order to get involved in the route sends a fabricated RREP packet with a higher destination sequence number despite having a route towards the destination [2]. The operation of the AODV protocol in the presence of adversary node is shown in Figure 2. A legitimate internal node M turns into an adversary node which discards

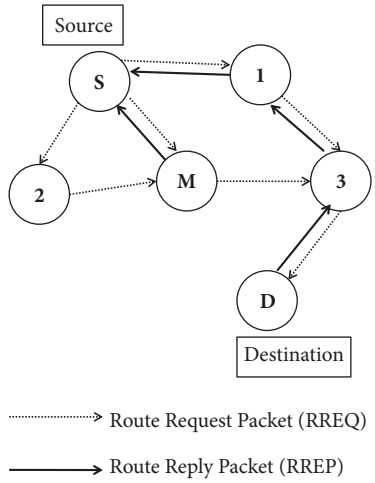


Figure 2: Operation of adversary during route discovery [3, 4].

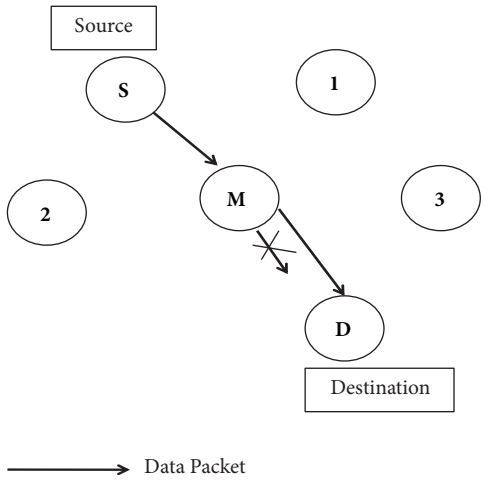


Figure 3: Operation of adversary during data transmission [3].

an RREQ packet which is supposed to be rebroadcasted to establish a path to the node D. Instead the adversary node M generates a forged reply packet with a higher destination sequence number and sends it on the reverse path towards the node S with a motive to deceive the source S that the node M is having a fresher valid route towards the destination D. As a result, the source node S gets the impression that node M has a fresher route to the destination D. On the other hand, the source node S ignores the benign RREP packet received from the node 1 which is generated by the destination node D as the RREP has a lower sequence number and higher hop count as compared to those received from the fabricated RREP generated by the adversary node M.

Once the route is formed through the adversary node M, the source node S starts sending the data packets. Node M after receiving the data packet may either forward or drop that packet. The same is illustrated in Figure 3. The adversary node may act as a genuine node for some time duration and as a malicious node for the remaining time [2, 20]. This unpredictive nature of the adversary makes its detection not so easy.

3. Related Work

Sequence number attacks degrade the network performance by taking the advantage of lack of security mechanism in the reactive routing protocols [3]. This has provided the motivation to researchers to incorporate distinct types of safety mechanisms in the routing protocols. In this section we discuss various security approaches which detect the adversary nodes either during the route discovery phase or during the data transmission phase.

3.1. Detection during Data Transmission Phase. An Extended Data Routing Information (EDRI) approach presented in [26] detects the adversaries by keeping the track of the data packets sent and received to and from the neighboring nodes in the EDRI table. This approach keeps the track of the neighboring nodes regarding the forwarding of the data packets with the help of promiscuous mode. If a neighboring node drops data packets more than predefined threshold, the neighboring node is considered as an adversary node. An enhancement to the EDRI approach is presented in [27] which includes a preventive mechanism along with the detection mechanism by using an alarm packet to alert all the nodes in the network about the detected malicious nodes with the help of data routing tables. A trust based approach is presented in [1, 28] where the nodes are assigned a trust value based on the past data communication. The trust value for the node is updated on the basis of the number of packets sent by the node. The node receiving the RREP accepts it if the forwarding node is marked as trusted node in the routing table; otherwise that RREP packet is discarded. A cooperation based defense mechanism (CBDM) scheme is presented in [29] where the cooperation value is calculated for every node using the probabilistic model. If the cooperation value of a node crosses the threshold value then that node is considered as suspicious node. As an additional check, a bait request is sent to the suspicious node and if the suspicious node replies to that request, then that node is considered to be malicious node. Another trust based approach is presented in [30] which makes the use of the contradiction mechanism where the data transmission is facilitated via the nodes having higher trust value. The trust value is calculated on the basis of the packets exchanged between the nodes.

3.2. Detection during the Route Discovery Time. The peak value calculation approach is presented in [31–33] where the node receiving the RREP packet calculates a threshold value of the destination sequence number. This threshold value is calculated with the help of the three parameters, namely, number of RREQs received and the number of RREPs received and the routing table sequence number. If the RREP received by the node contains a higher sequence number than the calculated threshold value, that RREP packet is discarded and the sender of that RREP packet is considered as a malicious node and that malicious node is excluded from the route. A cooperative bait detection scheme is presented in [34] where the source node selects the cooperating neighbor as the bait destination address. The source node then generates a bait request selecting the neighbor as the

Procedure 1: ***Actions by the malicious node after receiving an RREQ***

(1) Discard the received RREQ
(2) **If** (RREQ is NOT for me) **then**
(3) **If** (valid fresher route is available in the routing table) **then**
(4) Fill up RREP with Dest_Seqno=Routing_table_Dest_Seqno+*Random*(1,7) and Hop_Count=*Random*(1,3)
(5) Unicast the forged RREP on the reverse path to the source
(6) **End If**
(7) **Else**
(8) Fill up RREP with own Seqno and Hop_Count=1
(9) Unicast the genuine RREP on the reverse path to the source
(10) **End If**

Procedure 2: ***Actions by the malicious node after receiving a data packet from the source node***

(1) **If** (data packet is NOT for me) **then**
(2) **If** (Packet_ID mod *Random*(1,3) == 0) **then**
(3) Drop the data packet received from the source
(4) **Else**
(5) Forward the data packet
(6) **End If**
(7) **Else**
(8) Receive the data packet for me
(9) **End If**

Algorithm 1: Operation of adversary during Route discovery and data transmission [1, 3] (Algorithm 1 is reproduced from Rutvij et al. (2015), ([under the Creative Commons Attribution License/public domain)).

destination and then broadcasts the bait request for a route to that destination. If the node receiving the bait request sends the reply, that node is considered as a malicious node. A graph based approach is presented in [35] where the nodes with their neighbors for a graph like structure where every node monitors the control packets delivery of the neighboring nodes. Based upon the frequency of the communication, the nodes are assigned a fielder value which helps in deciding the next hop for the discovering the route.

4. Adversary Model

An enhanced and powerful adversary model is provided in [1, 3, 10]. In this model, the adversary node, as soon as it receives an RREQ packet, it generates a fabricated RREP packet which will have a marginally higher sequence number to attract the source node to form a path through it. The adversary node may generate this RREP packet even though it does not have a route towards the destination.

In this adversary model, the attacker node just increments the value of the destination sequence number by a random smaller value which keeps the fake destination number marginally higher. The adversary node then adds the fabricated and fraudulent destination sequence number and hop count values into the RREP packet. This mode of operation makes the detection of an attacker's presence in the network more difficult. Once one or more adversary nodes get into the route they may pretend to be as a benign node for some time period and carry out packet forwarding misbehaviors for other time periods [3].

The operations of the adversary during the route discovery phase and during the data transmission phase are shown in Algorithm 1 [1]. As shown in the algorithm, when the adversary node receives an RREQ packet, it fetches the destination sequence number form the routing table and adds a marginally incremented random value to that in order to forge the destination sequence number for the RREP packet. In addition, it enters a random hop count field in the fabricated RREP packet. The adversary node thus fools the source node about having the fresher and shorter route to the destination, and, as a result, it becomes part of this bogus route. The adversary now starts packet forwarding misbehavior by dropping the data packets in a random way. The nature of this capricious adversary makes its detection very difficult.

5. Proposed Work

The proposed approach, sequence number prediction based bait detection scheme (SNPBDS), attempts to detect the adversary nodes during the route discovery phase. This proactive detection during route discovery is imperative in several critical applications where we cannot afford to lose the data packets.

SNPBDS provides advancement to the SNBDS scheme presented in [3]. SNPBDS adds various fields in the routing table and in the neighbor table. A field for recording the past sequence numbers for a node is added in the routing table and the status field is added in the neighbor table to mark the status of the neighboring node as normal, suspicious, or malicious. Whenever any node receives an RREQ or RREP packet for a destination node, the past data field in the routing table is updated. Using the past sequence number history, we use linear regression technique to predict the highest destination sequence number possible for the RREP packet sent by the replying node.

5.1. Linear Regression Technique of Predicting Sequence Number [25]. The linear regression is defined with the help of a plot on the X- and Y-axis. There are two lines of regression that of Y on X and X on Y. The line of regression of Y on X is given by $Y = a_0 + a_1 X$ where a_0 and a_1 are unknown constants known as intercept and slope of the equation. This is used to predict the unknown value of the variable Y when value of the variable X is known. The equation for prediction is as follows:

$$Y = a_0 + a_1 X \tag{1}$$

The equations for calculating a_0 and a_1 are as follows:

$$a_1 = \frac{n\sum x_i y_i - \sum x_i \sum y_i}{n\sum x_i^2 - \left(\sum x_i\right)^2} \tag{2}$$

$$a_0 = \overline{y} - a_1 \overline{x} \tag{3}$$

Using (1), (2), and (3), we can predict the value Y which is based on X. In addition, to improve prediction we find error at every point and based on this error we improve our prediction. The equation for the calculating the error is as follows:

$$\min \sum_{i=1}^{n} e_i = \sum_{i=1}^{n} \left(y_i - a_0 - a_1 x_i\right) \tag{4}$$

Equation (4) defines the error at a particular point. Based on the last error, we can improve our prediction by performing addition and subtraction of the error value to the predicted value. The equation for the final predicted value is as follows:

$$P = Y + e \tag{5}$$

5.2. Application of Linear Regression in SNPBDS. Using linear regression technique discussed above, we now tend to predict the threshold value of the destination sequence number which is sent in the RREP packet by the neighboring node. We calculate the destination sequence number based on the time factor. We assume time (denoted as T) as the value of X and the sequence number (denoted as N) as the value of Y in (1). For predicting the new value of N, we need the past records of N and T. Table 1 shows the past history of the values of T and N.

As shown in Table 1, as we have 5 records till now, we take n=5. Now we wish to predict the threshold value of the destination sequence number for the received RREP packet.

According to (1) we have

$$N = a_0 + a_1 T \tag{6}$$

So now we first calculate the values of a_0 and a_1 using (2) and (3). According to (2) we have

$$\begin{aligned} a_1 &= \frac{n\sum T_i N_i - \sum T_i \sum N_i}{n\sum T_i^2 - \left(\sum T_i\right)^2} \\ a_1 &= \frac{5 \times 30147 - 432 \times 287}{5 \times 44202 - 287 * 287} \\ a_1 &= 0.19295 \end{aligned} \tag{7}$$

According to (3) we have

$$\begin{aligned} a_0 &= \overline{N} - a_1 \overline{T} \\ a_0 &= 57.4 - 0.19295 \times 86.4 \\ a_0 &= 40.72912 \end{aligned} \tag{8}$$

Replacing the values of (7) and (8) in (1) we have

$$N = 40.72912 + 0.19295 \times T \tag{9}$$

We want to predict the value of the destination sequence number at time of 160 seconds. Therefore, we take the value of T=160.

$$\begin{aligned} N &= 40.72912 + 0.19295 \times 160 \\ N &= 71.60112 \end{aligned} \tag{10}$$

Even though we calculated the value of N, it contains some error. To address it, we use (4). We calculate the error at time 138 and the sequence number at that time is 96. Therefore, we calculate

$$\begin{aligned} e &= 96 - 40.72912 - 0.19295 \times 138 \\ e &= 28.64378 \end{aligned} \tag{11}$$

Now accumulating the error in the predictive value according to (5) we get

$$\begin{aligned} P &= N + e \\ P &= 71.60112 + 28.64378 \\ P &= 100.2449 \end{aligned} \tag{12}$$

Thus by the use of linear regression technique, at time of 160 seconds, the predicted threshold of the destination sequence number is 100.

5.3. SNPBDS Methodology. This section describes the operations of the nodes adopting SNPDS while receiving RREQ and RREP packets.

5.3.1. Actions Performed by the Node Receiving the RREQ Packet. When a node receives an RREQ packet, it first checks the status of the node sending the RREQ packet in the neighbor table. If the status of the node in the neighbor table is marked as malicious, the node discards that RREQ packet. If the status of the node that has sent the RREQ packet has its status as normal, then the node receiving the RREQ packet will update the routing table entry for that particular destination.

(1) Algorithm. The steps followed by the node after receiving RREQ packet are shown in Algorithm 2.

5.3.2. Actions Performed by the Node Receiving the RREP Packet. The node receiving an RREP packet checks the status of the node forwarding the RREP packet in the neighbor table. If the status for that node is malicious,

```
Procedure 1: Actions by the node after receiving an RREQ
(1)  Retrieve the Status of the node forwarding RREQ packet
(2)  If (Status == malicious ) then
(3)       Discard the RREQ packet
(4)  End If
(5)  Else If (valid fresher route is available in the routing table) then
(6)       Generate the RREP packet and forward it towards the Source Node.
(7)  End If
(8)  Else
(9)       Update the Routing Information and forward the RREQ further.
(10) Exit
```

Algorithm 2: Operation of node after receiving RREQ packet.

```
Procedure 1: Actions by the node after receiving an RREQ
(1)  Retrieve the Status of the node forwarding RREP packet
(2)  If (Status == malicious) then
(3)       Discard the RREP packet
(4)  End If
(5)  Else If (Status==normal) then
(6)       Evaluate the predictive seq. number (PRED_SEQNO)
(7)  End If
(8)  If (DEST_SEQNO > PRED_SEQNO)
(9)       Status=suspicious
(10)      Update the Status of the node in the neighboring table.
(11) End If
(12) Else
(13)      Perform the normal routing operations.
(14) If (Status = suspicious)
(15)      Send BAIT_REQUEST to suspicious node
(16) End if
(17) If (BAIT_REPLY received)
(18)      Change the status of the node from suspicious to malicious
(19)      Delete the routing entry for the malicious node.
(20)      Initiate a local route discovery process to find an alternate route to the destination.
(21) End If
(22) Else
(23)      Change the Status from suspicious to normal and perform regular routing operations
(24) Exit
```

Algorithm 3: Operation of node after receiving RREP packet.

the received RREP packet is discarded. If the status value for the forwarding node is normal, the linear regression technique is employed to predict the threshold value of the destination sequence number based on the historical data. If the predicted destination sequence number is greater than the destination sequence number in the received RREP packet, the routing table is updated if necessary and the RREP is forwarded towards the source node. If the predicted sequence number is less than the destination sequence number received in the RREP packet, the receiving node marks the status of the node sending RREP packet as *suspicious*. The receiving node then sends a bait (forged) request packet to the suspicious node. If the suspicious node responds to the bait request, status of the suspicious node is changed from *suspicious* to *malicious* in the neighboring table and the RREP is discarded. The routing table entry having the malicious node as next hop node is then deleted and a local route discovery process is initiated to discover an alternate route. However, if the suspicious node does not reply to the bait request, the *suspicious* status of the node is changed back to *normal*. The steps followed by the node receiving RREP packet are depicted in Algorithm 3.

(1) Algorithm. See Algorithm 3.

5.4. Illustrative Example. As shown in Figure 4, the source node S wants to communicate to destination node D. The source node S generates the route request packet RQ1 and broadcasts it to its neighbor nodes 1 and 2. Nodes 1 and 2 then add the necessary information in RQ1 and generate the

Table 1: Historical data based on time.

T	N	T∗N	T∗T
30	17	510	900
67	49	3283	4489
85	58	4930	7225
112	73	8176	12544
138	96	13248	19044
Total = 432	**Total = 287**	**Total = 30147**	**Total = 44202**

Table 2: Parameters of request and reply packets.

	RQ1	RQ2	RQ3	RQ4	RP1	RP2	RP3	RP4
Source IP	S	1	2	3	D	3	1	M
Dest Seq, No.	15	15	15	15	17	17	17	17+5=22
Origin IP	S	S	S	S	S	S	S	S
Destination IP	D	D	D	D	D	D	D	D
Hop Count	1	2	2	3	1	2	3	2

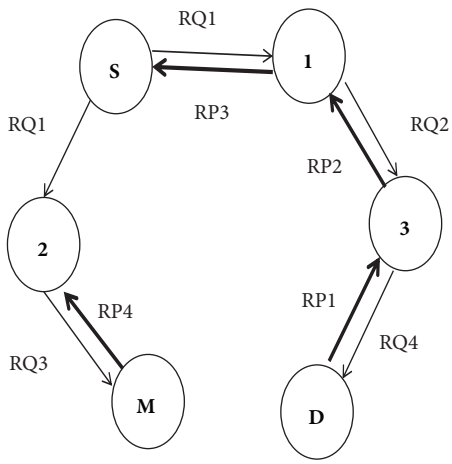


Figure 4: Route discovery process for a path from node S to node D.

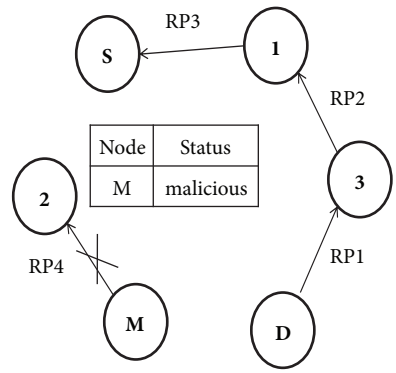


Figure 5: Avoiding the RREP from the malicious node.

packet RQ2 and RQ3, respectively, and forward it to their respective neighboring nodes 3 and M. Node 3 after adding the necessary information in RQ2 generates the packet RQ4 and forwards it to the destination node D. The destination node D generates the RREP packet and sends that packet through node 3 to the source node S as shown in Figure 4.

Node M behaving mischievously does not forward the RQ3 packet to node D. Rather it discards the request packet and generates a fabricated reply packet RP4 and sends it to node 2 as shown in Figure 7. The malicious node M randomly increments the destination sequence number by 3 and sets the hop count to 2 and inserts this fabricated information in the RREP packet RP4

The contents of the route request packets (RQ1, RQ2, RQ3, and RQ4) and route reply packets (RP1, RP2, RP3, and RP4) are shown in Table 2.

Node 2, after receiving the fabricated reply packet RP4, checks the status value for node M in the neighbor table. If the status value is equal to malicious, node 2 immediately discards the reply packet which is shown in Figure 5.

If the status value of node M in the neighbor table of node 2 is normal, node 2 applies the linear regression technique to predict the value of the destination sequence number. Node 2 now predicts the threshold value of the destination sequence number by considering the past history data of the sequence numbers. The collection of such data is shown in Table 3. The table shows that the predicted value of the destination sequence number is 10 which is less than the destination sequence number received in RP4 sent by M. Therefore, node 2 marks the status of node M as *suspicious* in the neighbor table.

As shown in Figure 6, when status of the node M changes from normal to suspicious, node 2 generates a bait request packet BRQ1. This is a dummy request packet to verify whether the suspicious node blindly replies to the request or not.

Node M, which is marked as suspicious, after receiving the bait request generates a reply BRP1 and sends it to node 2 as shown in Figure 7. Node 2 receives the packet BRP1 in reply

Table 3: Collection of past sequence numbers.

Node	Dest	Time	Seq No	Historical Data	
				Time	Seq No.
M	D	115	10	55	6
				...	...
				115	8
				115	10

Table 4: Parameters of bait request packet and its reply.

	BRQ1	BRP1
Source IP	4	4
DestSeq, No.	22	24
Origin IP	S	S
Destination IP	D	D
Hop Count	0	0

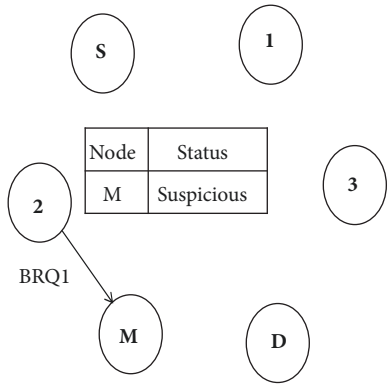


Figure 6: Node 2 sends bait request to node M.

to the bait request. Therefore, node 2 now marks the status of the node M as malicious and updates the value of status from suspicious to malicious.

The parameters of BRQ1 and BRP1 are shown in Table 4.

Node 2 after marking the status of node M as malicious discards the RREP packet and deletes the routing table entry having the node M as the next hop node. As a result, the node M is not allowed to enter the route. Node 2 now initiates a local route discovery process for the destination for which the routing table entry is discarded

6. Simulation Results and Analysis

6.1. Experimental Setup. In our experiments, we carry out simulations on the NS-2 simulator [36]. In order to prove that the SNPBDS approach provides better performance compared to the SNBDS approach, we compare the performance of both the approaches by varying various network parameters. For our experimental work, we select the maximum simulation time of 200 seconds with the terrain area of 1500 m x 1500 m. The performance of SNPBDS approach is compared with the simple AODV protocol, the AODV protocol with the adversary, and the SNBDS approach. The

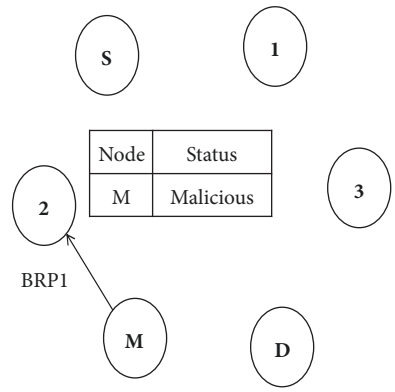


Figure 7: Node M replies to bait request.

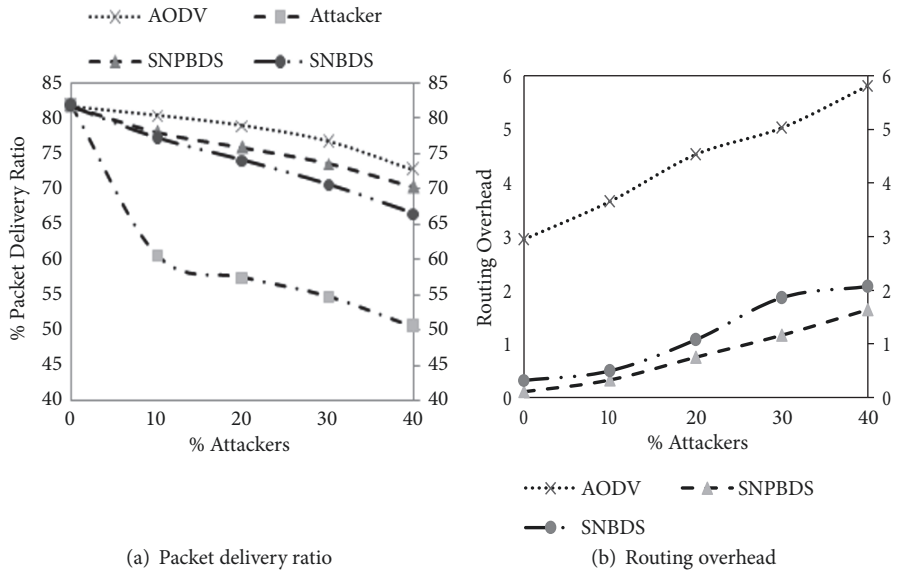
performance comparison of various approaches is based on the performance metrics such as packet delivery ratio and routing overhead. The detailed simulation parameters are shown in Table 5.

6.2. Result Analysis. We perform various tests to evaluate the performance AODV protocol, AODV protocol with adversary node, SNBDS approach, and the SNPBDS approach. The metrics selected for the evaluation of the approaches are the packet delivery ratio (PDR) and routing overhead. Packet delivery ratio (PDR) is defined as the ratio of the number of packets received by the destination to the number of packets sent by the source node [2]. Routing overhead refers to the ratio of the control packets transmitted to the ratio of the data packets transmitted [2]. The various test cases for the evaluation of the performance of different approaches are discussed below.

6.2.1. Test 1: Varying Number of Adversary Nodes. Figure 8(a) shows the graph of the packet delivery ratio of the various protocols. We have evaluated the PDR by varying the attacker count. The number of nodes in the network is 100. The range of the number of attacker nodes varies from 0% to 40% of the number of nodes in the network. Figure 8(a) shows the decrease of the PDR with the increase of the number of attacker nodes. The PDR of the AODV protocol in the presence of adversaries decreases from 80% to 50% with the increase in the number of adversaries. The SNPBDS approach provides the PDR in the range of 83% to 70%, The graph shows that the PDR of the SNPBDS approach is higher than the SNBDS approach. Figure 8(b) shows the graph of the routing overheard of the network operating

Table 5: Simulation parameters.

Parameters	Values
Simulator	NS 2.35
Routing Protocols	AODV, Attacker1, SNBDS, SNPBDS
Coverage Area	1500m x 1500 m
Mobility Model	Random Way Point
Simulation Time	200s
Number of nodes (varying)	50 – 100
Maximum Mobility (varying)	5 m to 25 m/s
Pause time (varying)	5 -25 s
No. of Connections (varying)	2 to 10
Transmission Rate (varying)	5 to 25 packets per second



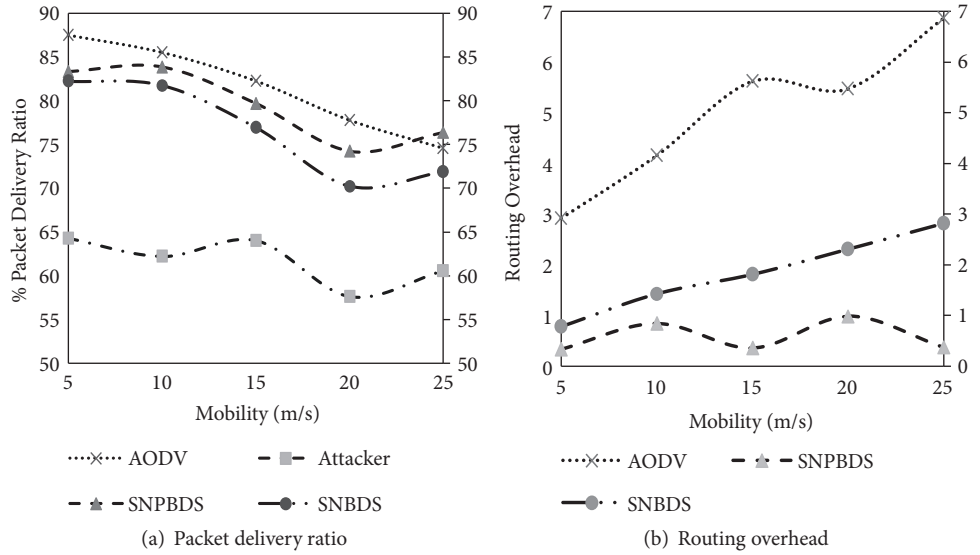
(a) Packet delivery ratio (b) Routing overhead

Figure 8: Performance comparison by varying number of adversary nodes.

with different protocols by varying the number of attacker nodes in the network. The routing overhead in the AODV protocol ranges from 3.0 to 6.0 with the increase in the number of adversaries. The routing overhead of the SNPBDS approach is in the range of 0 to 1.5 whereas the routing overhead of SNBDS approach falls in the range of 0.2 to 2.0. Thus SNPBDS protocol produces lower routing overhead compared to AODV protocol and SNBDS protocol. This is because the SNPBDS protocol eliminates the malicious node which results in the reduction of the frequency of route discovery which in turn leads to lower routing overhead.

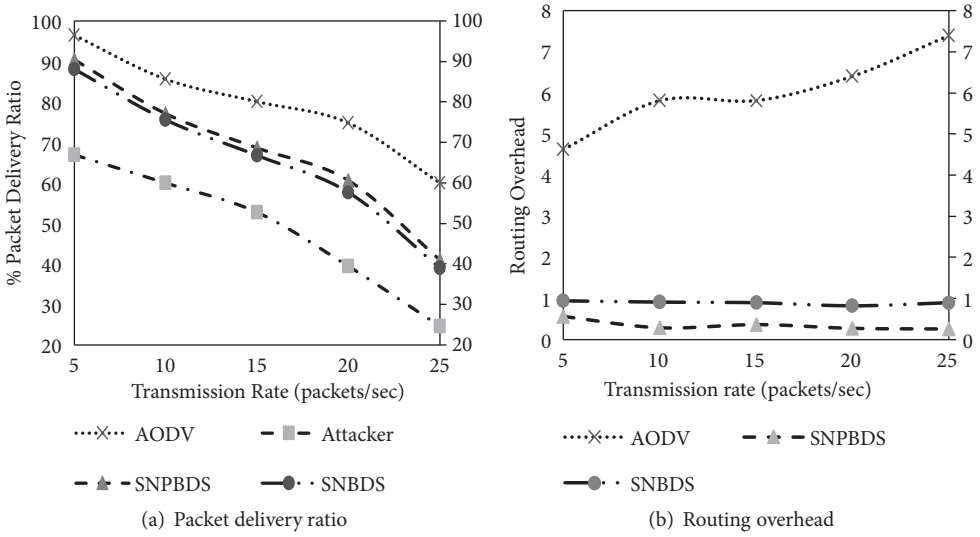
6.2.2. Test 2: Varying Mobility Speed. Figure 9(a) shows the PDR of the protocols by keeping the number of nodes and the number of attacker nodes fixed and varying the mobility speed. The number of nodes is 100 and the attacker nodes count is 10% of the total number of nodes. We vary the mobility speed of the nodes from 5m/s to 25m/s. We can see that, with the increase in the mobility speed, the PDR of AODV protocol gradually decreases from around 90% to 70%. With the attacker's interference, the PDR appears to be in the range of 60 to 65% with the varying speeds of the nodes. The SNBDS approach has PDR range of 70% to 82%. The SNPBDS approach provides the PDR of around 76% to 83%. Thus the performance of SNPBDS is better than the SNBDS approach. Figure 9(b) shows the routing overhead of the network by varying the mobility speed while keeping other parameters intact. The routing overhead of the SNPBDS approach is in the range of 0 to 1 which is better compared to SNBDS approach having routing overhead in the range of 1 to 3 and AODV protocol having the routing overhead in the range of 3 to 7 with the increase in the mobility speed. The results show that the effect of increase of mobility speed does not have a great impact on the value of routing overhead whereas, in AODV protocol and SNBDS approach, the routing overhead increases with the increase in the mobility speed which is due to the larger number of route discoveries.

6.2.3. Test 3: Varying Transmission Rate. Figure 10(a) shows the packet delivery ratios of various protocols under the effect of variable transmission speed. Varying the number of packets sent per unit time also impacts the performance of



(a) Packet delivery ratio (b) Routing overhead

Figure 9: Performance comparison by varying mobility speed.

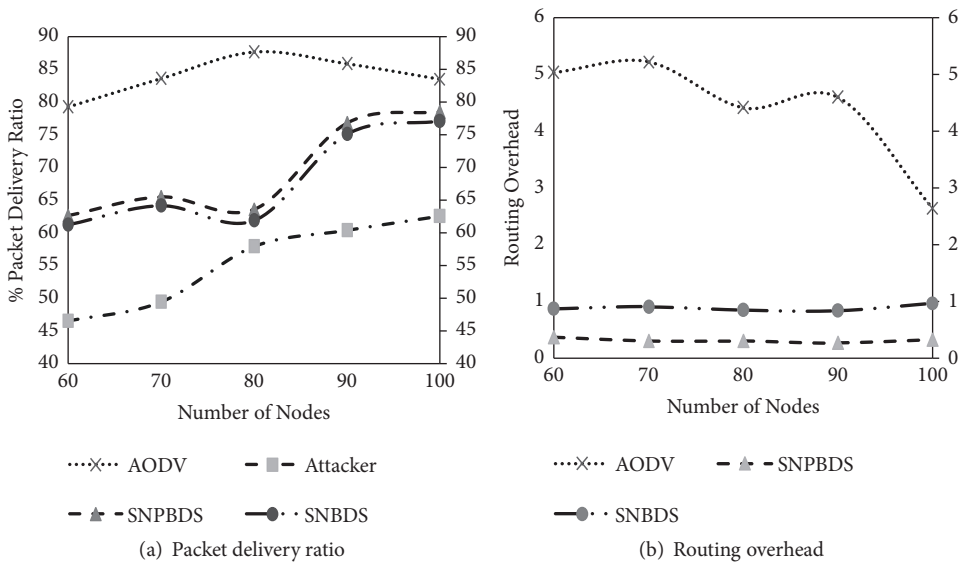


(a) Packet delivery ratio (b) Routing overhead

Figure 10: Performance comparison by varying transmission rate.

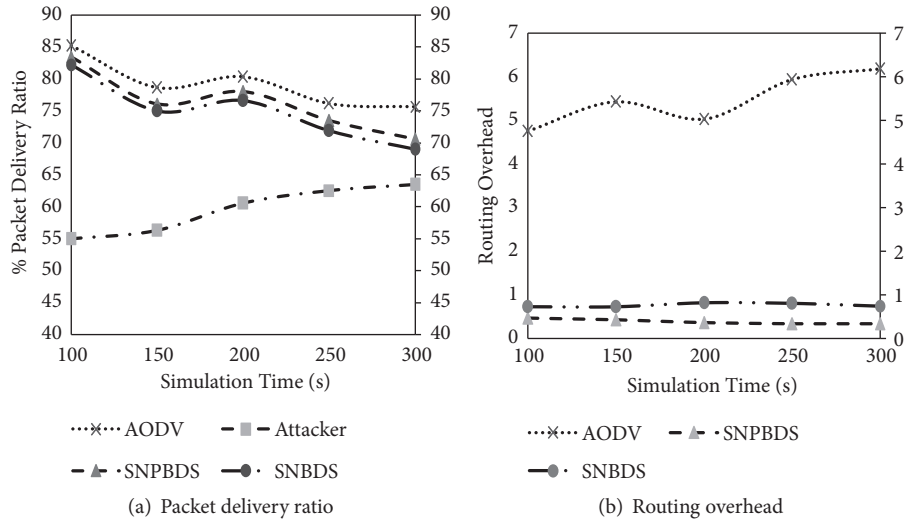
the network. We take the same number of nodes as 100 and 10% nodes as attacker nodes. Here we take a constant mobility speed for all the nodes and we vary the transmission speed from 5 packets per second to 25 packets per second. From the figure we observe that the PDR of all the protocols tend to decrease with the increase of the transmission speed. The AODV protocol provides the PDR in the range of 65 to 90%. In the presence of attacker nodes, the PDR declines from around 60% to 25% with the increase in the transmission speed. The SNBDS approach has the PDR in the range of 66% to 80%. The SNPBDS approach results in the PDR in the range of 70% to 81%. Thus in the presence of attacker nodes and by varying the transmission speeds, the SNPBDS approach provides better performance compared to SNBDS approach. Figure 10(b) shows the routing overhead incurred in the network while varying the transmission rate of packets and keeping other parameters intact. The routing overhead of the AODV protocol with the variation in the transmission time ranges from 4.5 to 7.5 which is very high compared to SNBDS approach having routing overhead of 1. The SNPBDS has the lowest routing overhead of 0.1 to 0.2. Figure 10 shows that the SNPBDS approach results in the steady routing overhead with the increase in the transmission rate of packets

6.2.4. Test 4: Varying Number of Nodes. Figure 11(a) shows the performance of the network by varying the number of nodes in the network. We take 10% of the nodes as the adversary nodes. The mobility speed and the transmission speed of the nodes are kept the same. The number of nodes varies from 60 to 100. We observe that the PDR of the network in the



(a) Packet delivery ratio (b) Routing overhead

Figure 11: Performance comparison by varying number of nodes.

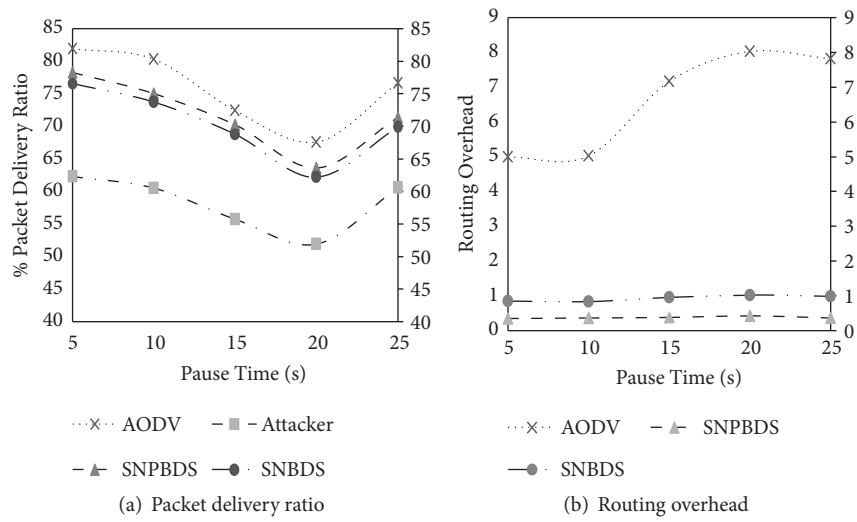


(a) Packet delivery ratio (b) Routing overhead

Figure 12: Performance comparison by varying simulation time.

attacker's presence is very low in the range of 40 to 60%. The SNBDS approach results in the PDR range of approximately 60 to 75% while the SNPBDS approach results in the PDR range of 70 to around 80%. Thus SNPBDS approach provides better results compared to SNBDS approach. Figure 11(b) depicts the routing overhead in the network obtained by varying the number of nodes in the network. The results show that the AODV protocol has lower routing protocol with the increase in the number of nodes. This is because as the number of nodes increases, the network becomes denser and nodes have path to majority of the destinations which results in sending of RREP packet from the intermediate nodes. As a result the RREP does not reach the destination which results in lower number of RREQ and RREP packets. This reduces the routing overhead in AODV protocol. The SNPBDS approach has better results compared to AODV and SNBDS approach. This is because the attacker is eliminated from the route during the route discovery which would result in increase of data packets without rediscovering the route.

6.2.5. Test 5: Varying Simulation Time. Figure 12(a) shows the performance of the network by varying the simulation time. We keep all the parameters as fixed and just vary the simulation time from 100 seconds to 300 seconds. The results show that the PDR reduces with the increase in the simulation time. The PDR in the presence of adversaries without any security mechanism falls in the range of 55% to 63%. The SNPBDS approach provides the PDR in the range of 70% to 84% compared to the SNBDS approach which provides the PDR in the range of 67% to 83%. Thus the



(a) Packet delivery ratio (b) Routing overhead

Figure 13: Performance comparison by varying pause time.

performance of SNPBDS is again better than the performance of the AODV protocol under the presence of adversaries and the SNBDS protocol. Figure 12(b) depicts the routing overhead of the network operating with the AODV, SNBDS, and SNPBDS approach by varying the simulation time and keeping other parameters intact. The routing overhead of the ADOV protocol goes from 4.7 to 6.0 with the increase of the simulation time. The routing overhead of the SNBDS approach is approximately around 0.8 to 0.9 which is higher compared to the SNPBDS approach which provides the routing overhead of 0.1 to 0.3. The results show that the SNPBDS approach has lower routing overhead due to the fact that the prediction algorithm will work for the entire simulation and the more the simulation time we have the more the past data we will have and the closer the value of predicted sequence number we will have. So this would result in lower routing overhead compared to other approaches.

6.2.6. Test 6: Varying Pause Time. Figure 13(a) shows the performance of the network by varying the pause time. The pause time is varied from 5 seconds to 25 seconds while keeping the other parameters intact. The PDR of the SNPBDS resides in the range of 72% to 78% which is better compared to SNBDS approach having the PDR range of 70% to 76% and AODV protocol with adversaries having PDR in the range of 60% to 62%. The results show that the PDR in SNPBDS approach is better than the SNBDS approach and the AODV protocol in the presence of attacker nodes. Figure 13(b) shows the routing overhead incurred in the network by varying the pause time while other parameters are kept intact. The SNPBDS approach produces the lower routing overhead of 0.2 compared to SNBDS approach having the routing overhead of 1. The AODV protocol provides very high routing overhead of 5 to 8 with the variation in the pause time. The SNPBDS approach provides the lowest routing overhead compared to the three approaches shown in Figure 13(b).

7. Conclusion

The nodes in MANET need to depend on other nodes to facilitate communication in the network. The characteristics of MANET provide great value to the adversaries which tend to degrade the network performance. Our proposed proactive scheme (SNPBDS) counters the threat of such adversaries by predicting adversaries in the route discovery phase. The proposed scheme attempts to prevent the adversaries form entering the route and, hence, increases the packet delivery rate and thereby the quality-of-services. The prediction of the destination sequence number and the bait request provide a double security check to confirm the status of the node as malicious. The scheme is evaluated under various network conditions against a strong adversary model. The performance evaluation of SNPBDS against SNBDS shows that SNPBDS provides considerable improvement packet delivery rate and normalized routing overhead.

The scheme can be enhanced by implementing hybrid approach (proactive and reactive) which would provide two-layer security during route discovery as well as data transmission.

Data Availability

Data used to support the findings of this study are available upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] R. H. Jhaveri and N. M. Patel, "Attack-pattern discovery based enhanced trust model for secure routing in mobile ad-hoc networks," *International Journal of Communication Systems*, vol. 30, no. 7, 2017.

[2] A. D. Patel and R. H. Jhaveri, "Addressing packet forwarding misbehavior with two phase security scheme for AODV-based MANETs," *International Journal of Computer Network and Information Security*, vol. 8, no. 5, pp. 55–62, 2016.

[3] R. H. Jhaveri and N. M. Patel, "A sequence number based bait detection scheme to thwart grayhole attack in mobile ad hoc networks," *Wireless Networks*, vol. 21, no. 8, pp. 2781–2798, 2015.

[4] A. D. Patel and K. Chawda, "Blackhole and grayhole attacks in MANET," in *Proceedings of the International Conference on Information Communication and Embedded Systems (ICICES '14)*, pp. 1–6, Chennai, India, February 2014.

[5] R. H. Jhaveri and N. M. Patel, "Mobile ad-hoc networking with AODV: A review," *Internation Journal of Next Generation Computing*, vol. 6, no. 3, pp. 165–191, 2015.

[6] M. S. Khan, D. Midi, M. I. Khan, and E. Bertino, "Fine-grained analysis of packet loss in MANETs," *IEEE Access*, vol. 5, pp. 7798–7807, 2017.

[7] Z. Zhao, H. Hu, G.-J. Ahn, and R. Wu, "Risk-aware mitigation for MANET routing attacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 2, pp. 250–260, 2012.

[8] R. H. Jhaveri, S. J. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in *Proceedings of the 2nd International Conference on Advanced Computing and Communication Technologies (ACCT '12)*, pp. 535–541, January 2012.

[9] R. H. Jhaveri, N. M. Patel, Y. Zhong, and A. K. Sangaiah, "Sensitivity Analysis of an Attack-Pattern Discovery Based Trusted Routing Scheme for Mobile Ad-Hoc Networks in Industrial IoT," *IEEE Access*, vol. 6, pp. 20085–20103, 2018.

[10] R. H. Jhaveri and N. M. Patel, "Evaluating energy efficiency of secure routing schemes for mobile ad-hoc networks," *International Journal of Next Generation Computing*, vol. 7, no. 2, pp. 130–143, 2016.

[11] B. Li, Y. Huang, Z. Liu, J. Li, Z. Tian, and S.-M. Yiu, "HybridORAM: Practical oblivious cloud storage with constant bandwidth," *Journal of Information Sciences*, 2018.

[12] Y. Li, G. Wang, L. Nie, Q. Wang, and W. Tan, "Distance metric optimization driven convolutional neural network for age invariant face recognition," *Pattern Recognition*, vol. 75, pp. 51–62, 2018.

[13] Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen, and Y. Tang, "An ID-based linearly homomorphic signature scheme and its application in blockchain," *IEEE Access*, vol. 6, pp. 20632–20640, 2018.

[14] J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, and Y. Tang, "Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks," *Journal of Network and Computer Applications*, vol. 106, pp. 117–123, 2018.

[15] C. Gao, Q. Cheng, P. He, W. Susilo, and J. Li, "Privacy-preserving Naive Bayes classifiers secure against the substitution-then-comparison attack," *Information Sciences*, vol. 444, pp. 72–88, 2018.

[16] Q. Lin, J. Li, Z. Huang, W. Chen, and J. Shen, "A short linearly homomorphic proxy signature scheme," *IEEE Access*, vol. 6, pp. 12966–12972, 2018.

[17] Y. Zhang, J. Li, D. Zheng, P. Li, and Y. Tian, "Privacy-preserving communication and power injection over vehicle networks and 5G smart grid slice," *Journal of Network and Computer Applications*, vol. 122, 2018.

[18] F. Aftab, Z. Zhang, and A. Ahmad, "Self-organization based clustering in MANETs using zone based group mobility," *IEEE Access*, vol. 5, pp. 27464–27476, 2017.

[19] T. Li, J. Li, Z. Liu, P. Li, and C. Jia, "Differentially private Naive Bayes learning over multiple data sources," *Information Sciences*, vol. 444, pp. 89–104, 2018.

[20] A. D. Patel and K. Chawda, "Dual Security Against Grayhole Attack in MANETs," *Advances in Intelligent Systems and Computing*, vol. 309, no. 2, pp. 33–37, 2015.

[21] H. Wang, W. Wang, Z. Cui, X. Zhou, J. Zhao, and Y. Li, "A new dynamic firefly algorithm for demand estimation of water resources," *Information Sciences*, vol. 438, pp. 95–106, 2018.

[22] M. N. Mejri and J. Ben-Othman, "GDVAN: a new greedy behavior attack detection algorithm for VANETs," *IEEE Transactions on Mobile Computing*, vol. 16, no. 3, pp. 759–771, 2017.

[23] Z. Liu, Z. Wu, T. Li, J. Li, and C. Shen, "GMM and CNN hybrid method for short utterance speaker recognition," *IEEE Transactions on Industrial Informatics*, 2018.

[24] J. Li, L. Sun, Q. Yan, Z. Li, W. Srisa-an, and H. Ye, "Significant Permission Identification for Machine Learning based android malware detection," *IEEE Transactions on Industrial Informatics*, 2018.

[25] Onlinestatbook.com, http://onlinestatbook.com/2/regression/intro.html.

[26] G. Singh Bindra, A. Kapoor, A. Narang, and A. Agrawal, "Detection and removal of co-operative blackhole and grayhole attacks in MANETs," in *Proceedings of the International Conference on System Engineering and Technology (ICSET '12)*, pp. 1–5, Bangdung, Indonesia, September 2012.

[27] A. D. Patel, R. H. Jhaveri, and S. N. Shah, "I-EDRI Scheme to Mitigate Grayhole Attack in MANETs," *Advances in Intelligent Systems and Computing*, vol. 309, no. 2, pp. 39–43, 2015.

[28] R. H. Jhaveri, N. M. Patel, and D. C. Jinwala, "A composite trust model for secure routing in mobile ad-hoc networks," in *Adhoc Networks*, J. H. Ortiz, Ed., chapter 2, pp. 19–45, Intech, 2017.

[29] J. P. Bhoiwala and R. H. Jhaveri, "Cooperation based defense mechanism against selfish nodes in DTNs," in *Proceedings of the 10th International Conference on Security of Information and Networks (SIN '17)*, pp. 268–273, October 2017.

[30] N. Schweitzer, A. Stulman, R. D. Margalit, and A. Shabtai, "Contradiction based gray-hole attack minimization for ad-hoc networks," *IEEE Transactions on Mobile Computing*, vol. 16, no. 8, pp. 2174–2183, 2017.

[31] W. Yang, G. Wang, M. Z. A. Bhuiyan, and K.-K. R. Choo, "Hypergraph partitioning for social networks based on information entropy modularity," *Journal of Network and Computer Applications*, vol. 86, pp. 59–71, 2017.

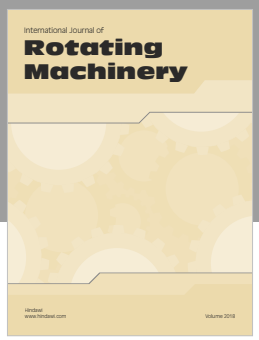
[32] Q. Liu, G. Wang, F. Li, S. Yang, and J. Wu, "Preserving privacy with probabilistic indistinguishability in weighted social networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 28, no. 5, pp. 1417–1429, 2017.

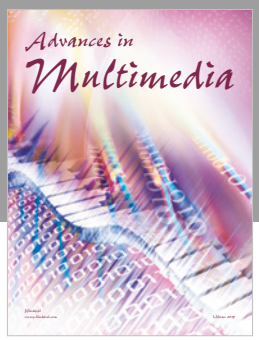
[33] H. Shen, C. Gao, D. He, and L. Wu, "New biometrics-based authentication scheme for multi-server environment in critical systems," *Journal of Ambient Intelligence and Humanized Computing*, vol. 6, no. 6, pp. 825–834, 2015.

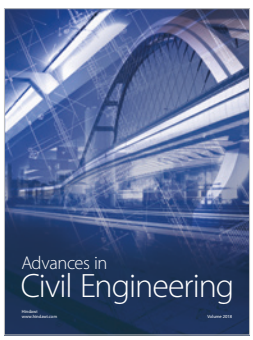
[34] J.-M. Chang, P.-C. Tsou, I. Woungang, H.-C. Chao, and C.-F. Lai, "Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach," *IEEE Systems Journal*, vol. 9, no. 1, pp. 65–75, 2015.

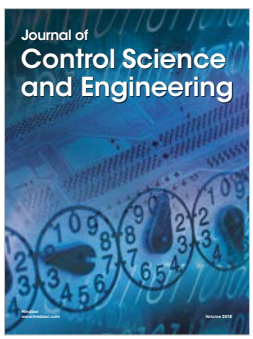
[35] Y. Liu and W. Trappe, "Topology adaptation for robust ad hoc cyberphysical networks under puncture-style attacks," *Tsinghua Science and Technology*, vol. 20, no. 4, pp. 364–375, 2015.

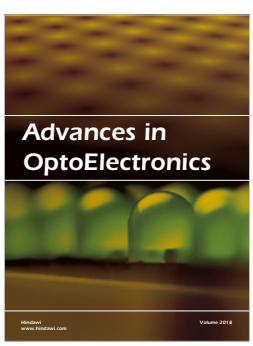
[36] Isi.edu, https://www.isi.edu/nsnam/ns/.

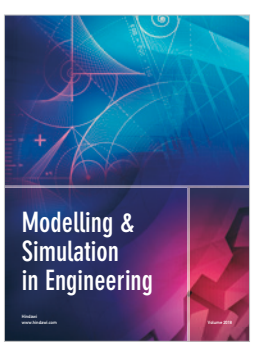


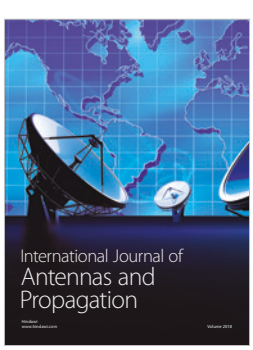


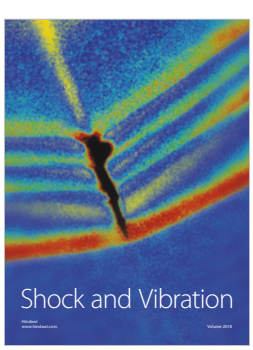


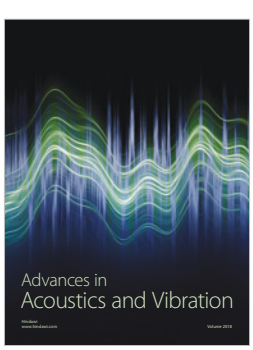












Hindawi

Submit your manuscripts at
www.hindawi.com