Wireless Netw (2018) 24:2957–2971
https://doi.org/10.1007/s11276-017-1514-1

A dynamic threshold based approach for mitigating black-hole attack in MANET

Shashi Gurung[1,2] · **Siddhartha Chauhan**[1]

Published online: 26 April 2017

Abstract Mobile ad-hoc network is an infrastructure less type of network which does not require any kind of fixed infrastructure. It provides multi-hop communication between the source and destination nodes which are not within the direct range of each other through the intermediate nodes. These intermediate nodes cooperate with other nodes in finding an optimum and shortest route toward the destination. However, in holistic environments, some nodes do not cooperate with other nodes in finding the optimal route towards the destination and intentionally give the false route information of having the shortest path toward the destination with a high destination sequence number in order to attract the traffic toward itself and start dropping of the data packets instead of forwarding it. This type of routing misbehaviour is generally called as black hole attack or full packet dropping attack which is one of the most severe destructive attacks that lead to the network degradation. In this paper, we have proposed a protocol called as Mitigating Black Hole effects through Detection and Prevention (MBDP-AODV) based on a dynamic threshold value of the destination sequence number. In order to validate the efficiency of proposed protocol, the NS-2.35 simulator is used. The simulation results show that proposed protocol performs better as compared with existing one under black hole attack.

✉ Shashi Gurung
shashigurung49@yahoo.co.in

Siddhartha Chauhan
sid@nith.ac.in

[1] Department of Computer Science and Engineering, National Institute of Technology, Hamirpur, HP, India

[2] Computer Centre, Jawaharlal Nehru Government Engineering College, Sundernagar, HP, India

Keywords Black hole attack · MBDP-AODV · Behaviour of the node · Sequence number · Denial of service · Smart gray hole

1 Introduction

Mobile ad hoc network (MANET) is defined as the category of a wireless network that can be generally formed or set up spontaneously without the support of any fixed infrastructure or central coordinator. It is a temporary, self-configurable and infrastructure-less networks [1, 2] of mobile devices which communicate with each other directly if within the radio transmission range of each other or through intermediates nodes which provide multi-hop communication. In this type of network, each mobile node operates as a router [3] as well as a host [4]. In order to provide communication between the source and destination nodes, the routing protocol such as ad-hoc on-demand distance vector (AODV) [5], dynamic source routing (DSR) [6] etc. are used for finding the optimal path. As each node in MANET is free to move independently of each other in any direction, therefore, it dynamically changes its links with other nodes frequently. Due to dynamic topology and mobility characteristics, the links are frequently broken up and the source node is not able to communicate with the destination. If any node detects link breakage, it sends route error message to the source node. In the highly mobile environment, frequently route breakage leads to high routing overhead due to frequent route discovery and error message. There are different applications of mobile ad-hoc network which includes emergency rescue operation, military battlefield, disaster management [7] etc. but one of the basic assumptions that are considered for the design of routing protocols in MANETs is that every node is honest and trusted due to which it is vulnerable to several types of denial of service (DoS) attacks [8–11], particularly packet dropping attack. In order to launch such types of attack, a malicious node misbehaves during route discovery process and can drop some or all data packets passing through it. Due to openness characteristics, packet dropping attack poses a great threat to the routing function in MANETs. The malicious node can easily join the network and drops the data packets in order to disrupt the regular communications between source node and destination. All the routes which pass through the malicious node fail to establish a correct path between the source and destination nodes. Although upper layer acknowledgments such as transmission control protocol acknowledgment can detect end-to-end communication break but it is not able to find out accurately the node which leads to that breakage [12].

1.1 Motivation and contributions

There are many existing security mechanisms in the literature, but still, security issues in MANET are not fully addressed. Some schemes use extra special nodes that are deployed statically in the network in overhearing mode and have fixed threshold value which is not suitable for MANET due to its dynamic nature and some schemes mitigate the black hole attack by ignoring the first or subsequent reply packet from the other nodes rather than considering these multiple reply packets which could be used to derive the dynamic threshold value for destination sequence number. The limitation of existing security mechanism motivated us to propose a new protocol called as MBDP-AODV which is based on a dynamic threshold value of destination sequence number and mitigates the impact of black hole attack in MANET. In this paper, we made following contributions:

- Discussed taxonomy of packet dropping attacks and different possible behaviour of the node in the network.
- Proposed MBDP-AODV protocol which is based on a dynamic threshold value of destination sequence number for mitigating the effects of black hole attack in the network.
- Performance evaluation of proposed protocol and its comparison with an existing scheme in NS-2.

1.2 Organization of paper

The remaining part of this paper is organized as follows. Section 2 describes the black hole attack in MANET. In Sect. 3, we describe the launching of blackhole attack and the possible behaviour of a node in the network. In Sect. 4, we explain about various existing techniques for detection and prevention of black hole attack. Section 5 explains about the implementation of MBDP-AODV. Section 6 describes the experimental setting. Section 7 discusses the simulation results and performance analysis in ns2. In Sect. 8, we discuss advantages and shortcoming of our approach and finally, a conclusion with future work is described in Sect. 9.

2 Black hole attack

In an on-demand based routing protocol i.e. AODV, the normal node broadcast the route request packet whenever there is no path in the routing table for the destination. On receiving route request packet, the intermediate genuine node checks whether it is the destination or not. It will check whether it has a valid route to the destination not. If there is a valid path, it will send back genuine reply packet otherwise, it will broadcast the route request packet but malicious node exploits the weakness of the underlying routing protocols which are generally designed with the assumption of mutual cooperation among the nodes and gives false routing information in order to launch the black hole attack. The black hole attack can cause *denial of service attack (DoS) attack* [13] and comes under the category of *full packet dropping attack* [14] which disrupts the communication between the source node and destination node after acquiring the route by giving frequently false information in route reply packet to the source node and thereafter starts dropping the packets. In case of *full packet dropping attack,* the malicious node drops all the data packets and do not participate genuinely during route discovery process and sends false routing information in the reply packet to the source node in order to attract the traffic towards itself and whereas in case of *partial packet dropping attack*, the malicious node drops some fractions of data packets. It can participate genuinely in the route discovery process and drops selective data packets which are referred as *smart gray hole attack* [14]. It is also possible that the malicious node may give false routing information and then performs selective dropping of the data packets in spite of having a valid path towards the destination which is called as *sequence number based gray hole attack* [15] as depicted in Fig. 1.

Sometimes black hole node can also give correct information of having shortest path to the destination in the reply packet but even then it will drop the packet once it gains the traffic towards itself by sending high destination sequence number [16].There can be single, multiple or cooperative black-hole or gray-hole attack in the network. Single or multiple attack is launched via one of the existent or many independent malicious nodes in the network whereas collaborative attack is launched through the

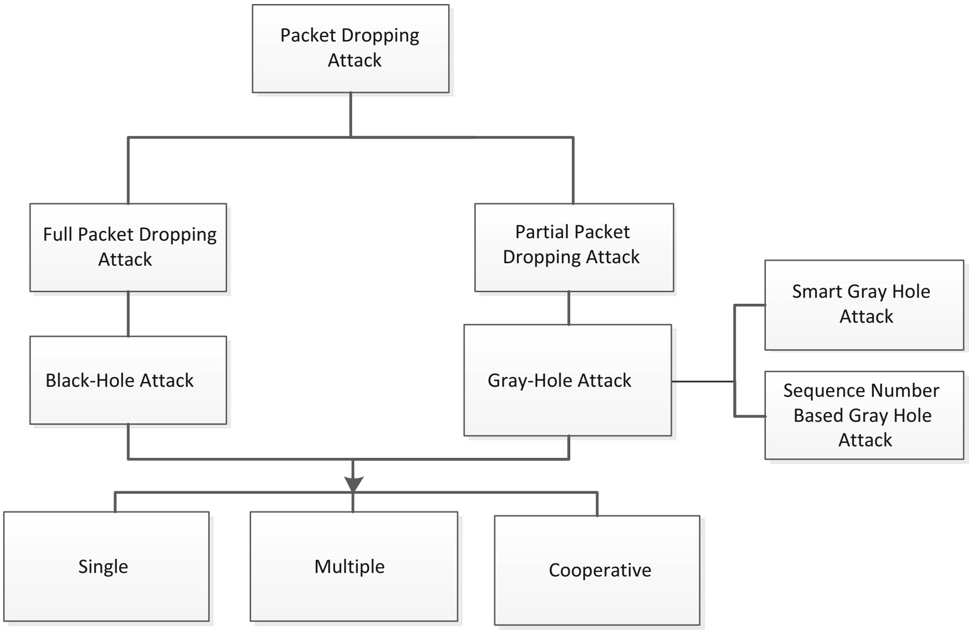

Fig. 1 Taxonomy of Packet Dropping Attack

cooperation between two or more malicious node [17]. Both black hole and gray hole attack can be easily performed on reactive routing protocols like AODV and DSR.

3 Launching black hole attack

For launching a black hole attack in MANET, the first and foremost step for a malicious node is that it should know how to acquire path or route immediately without any delay during route discovery. In any routing protocol, the source node always tries to communicate through the shortest path with the destination and that path should be valid. In AODV two main parameters play a very important role in deciding the final established route which is the shortest path and high destination sequence. The high destination sequence number represents about the freshness of the route. By considering these two parameters, the malicious nodes always tries to give false information of having the shortest path with a very high destination sequence number due to which the source node selects the path containing the malicious node thereby leading to the black hole attack as shown in Figs. 2 and 3. Thus, any node can misbehaves and creates a severe harm to the network by targeting at both data and control packets due to which the performance of network degrades.

3.1 Possible behaviour of node

There can be any possible behaviour of the node in the network which is represented in Table 1 in form of False ‘F’ and True ‘T’ status. If a node is not malicious (F); it will send true

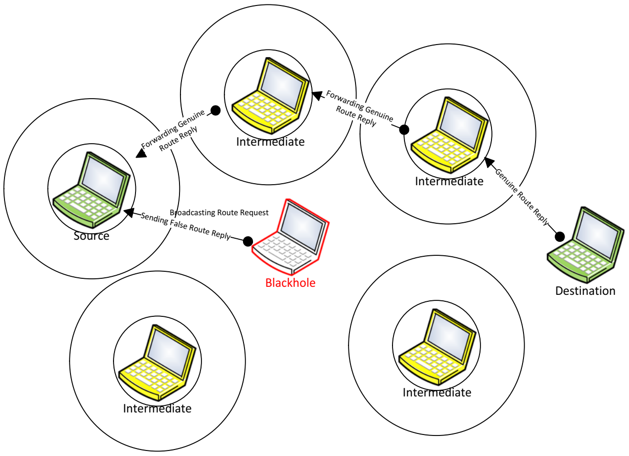
Intermediate
Forwarding Genuine Route Reply
Forwarding Genuine Route Reply
Intermediate
Genuine Route Reply
Source
Broadcasting Route Request
Sending False Route Reply
Blackhole
Destination
Intermediate
Intermediate

Fig. 2 False Route Reply by Black hole

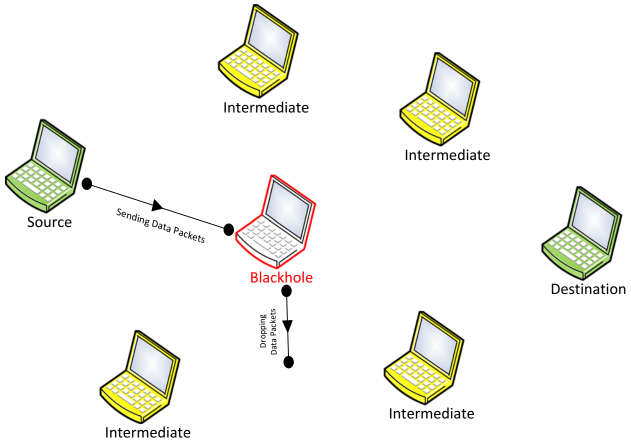

Fig. 3 Full Packet Dropping by Black hole

Table 1 Possible behaviour of node

S. no.	Malicious	Destination sequence number	Hop count	Packet drop	Attack	Description
1	F	T	T	F	F	No attack
2	T	F	F	T	T	Black hole/sequence no. based gray hole
3	T	F	T	T	T	Black hole/sequence no. based gray hole
4	T	T	F	T	T	Black hole/sequence no. based gray hole
5	T	T	T	T	T	Smart gray hole

information about destination sequence number (T) as well as (T) hop count in the reply packet. If the node is malicious (T), it can send false information about destination sequence number (F) as well as hop count (F) leading to a black hole or sequence number based gray hole attack in the network and starts dropping the data packets when it receives the data packets. If the node is malicious (T), it can send false information about destination sequence number (F) and true information about hop count in reply packet (T) which can also result in packet dropping attack in the network. If the node is malicious (T), it can send true information about destination sequence number (T) but with false information about hop count (F) leading to black hole or sequence number based gray hole attack in the network. If the node is malicious (T), it can also send true information about hop count (T) and true information about destination sequence number (T) but even then it will lead to smart gray hole attack in the network as depicted in Figs. 4 and 5.

4 Related work

There are various existing techniques which have been proposed by many researchers for dealing with packet dropping attack with its drawbacks in [18].

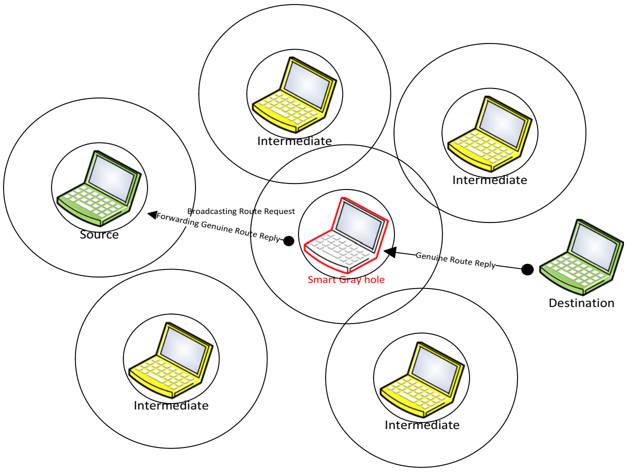

Fig. 4 Smart Gray Hole Participating genuinely in Route Discovery Process

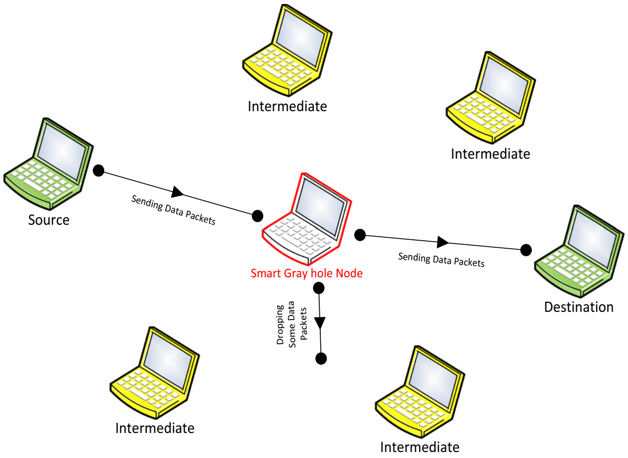

Fig. 5 Partial Packet Dropping by Smart Gray Hole

Clustering based approach [19] has been proposed to detect the black hole attack locally. By using a clustering algorithm, the network is divided into clusters and elects cluster head (CH) for the detection of black hole attacks in each cluster locally. The limitation of this approach is that overhead increases due to frequent cluster formation and maintenance in high mobility case.

In [20], the authors have proposed Cooperative bait detection scheme to detect the malicious node in the network. According to this scheme, the source node stochastically selects a next hop node with which it can cooperate by taking the address of this next hop node as bait destination address to make malicious nodes to send a reply message. The limitation of this approach is that it can select adjacent hop as bait addressing which can be malicious node and hence network performance will degrade.

In [21], the author proposed cluster-based datagram chunk dropping detection and prevention technique in which data to be transmitted is divided into chunks of size p. These chunks which are sent from source make their entry in a buffer at the source node and compares with the values of buffer maintained at each intermediate node. The drawback of this approach is that it introduces a high end to end delay.

In [22], anti-black hole mechanism is proposed in which special extra IDS nodes are deployed in the network which has the capability to overhear its nearby transmission. The IDS nodes increase the suspicious value of node according to the amount of abnormal difference between a request and reply packet transmitted from the node. The drawback of this approach is that extra special nodes called as IDS node are required and the network performance can also degrade if the malicious node is not detected due to improper deployment of IDS nodes in the network.

An approach based on IDS is proposed in [23] that overcome the limitation of the mechanism proposed in [22]. In this technique, the extra special IDS nodes are set in promiscuous mode only when destination node starts malicious node discovery process. The malicious node discovery process is started by the destination node when it discovers that the actual number of data packets that it is receiving from its previous hop node is significantly less than the number of data packets the source node sends. This approach has used fixed threshold value of 20% for data packet loss and has high routing overhead. It also takes more time in detecting the malicious due to verification process by destination node and then by nearby IDS node.

Reputation-based RIPsec framework is proposed in [24] that deal with the external and internal threats. In order to provide protection from external threats, encrypted links and encryption-wrapped nodes are used. But this framework is designed to operate in closed MANET which means only nodes that have been predetermined to be trusted and properly configured can access the network's resources.

In [25], IDSAODV protocol is proposed based on reply caching mechanism in which black hole attack is prevented by ignoring the first or two replies under one and two black hole nodes respectively and responding to the subsequent reply. The limitation of this protocol is that it cannot detect malicious node in the network. However, in our approach, multiple reply packets are gathered by the source node in order to calculate the dynamic threshold value based on destination sequence number for detection and prevention purpose.

In [16], the author proposed ANB-AODV protocol for dealing with black hole attack in which not only source node but intermediate node also updates its routing table whenever it receives next reply packet and ignores previous replies by assuming to be coming from malicious nodes. This approach also has some drawbacks which lead to degradation of the network performance by accepting the last reply which can come from black hole node if it is far away from the source node. Therefore, this approach is not able to detect the malicious node however in our approach; multiple replies packets are gathered in order to compute the dynamic threshold value based on destination sequence number for detection and prevention purpose.

Table 2 Summary of notations

Notations	Meaning
RT.SeqNo	Routing table sequence number
R.Table	Routing table
S.SeqNo	Suspected sequence number
D.SeqNo	Destination sequence number
Seq.No	Sequence number
RREP	Reply
K	Number of reply packets

5 MBDP-AODV: proposed protocol

In this section, we described the working mechanism of MBDP-AODV protocol for mitigating the black hole attack and presented the algorithm in Sect. 5.2. In MBDP-AODV, we have used two statistical features i.e. mean and standard deviation because during normal conditions and in the absence of attacker, the mean and standard deviation almost constantly increase but during the attack, the standard deviation grows quickly. We make following assumptions: (1) All the nodes are identical in terms of their physical characteristics. (2) The source and the destination nodes are trusted but intermediates are not. (3) The black-hole node sends false routing information with minimum hop count i.e. 1 and high destination sequence number in the reply packet. We have used various notations in our algorithms as described in Table 2.

The MBDP-AODV is designed with following features: (1) it uses dynamic threshold value for destination sequence number by considering multiple reply packets. (2) It does not require any special extra node which has to be placed statically in the network in order to cover most of the area. (3) The nodes need not be in overhearing mode. (4) It uses two statistical features i.e. mean and standard deviation for detection purpose. The proposed protocol consists of following three phases:

1. *Dynamic threshold calculation and suspicion* In this phase, the dynamic threshold value for the destination sequence number is computed by the source node.
2. *Detection* In this phase, the SUSPECT packet is sent by the source node to find the lair node (malicious) and then ALERT packet which contains the malicious id and suspected sequence number is broadcasted in the network.
3. *Prevention* In this phase, the malicious node is prevented from its participation in the route discovery

process and its reply is also ignored once it is detected by other nodes.

$$A = \sum_{i=1}^{K} \frac{D.SeqNo^{i}}{K} \qquad (1)$$

$$T = \sqrt{\sum_{i=1}^{K} \frac{(D.SeqNo^{i} - A)^{2}}{K}}. \qquad (2)$$

where $D.SeqNo^{i}$ is destination sequence number of ith reply packet and K is number of reply packet.

5.1 Protocol phases description

5.1.1 Dynamic threshold calculation and suspicion

Whenever source node wants to do communication with the destination node, it broadcasts the route request packet if it has no path towards the destination. In AODV routing protocol whenever destination node receives duplicate route request, it discards but in our approach the destination node after receiving duplicates route request from multiple nodes sends a reply to each node from which it has received route request. The source node receives multiple K replies from the various nodes as shown in Fig. 6 and calculates mean for destination sequence number by using K number of replies packets by using the formula as shown in Eq. (1). It then computes the standard deviation of destination sequence number by using the formula as shown in Eq. (2). The standard deviation value is taken as the final threshold value which is calculated by using the destination sequence number of K number of replies packet coming from various nodes. After calculation of threshold value, if it is greater than the average value, then the source node looks up for the destination node in the routing table to find whether the destination sequence number is greater than the threshold value or not. Each time new route request for the destination is broadcasted; new threshold value will be calculated. If the attacker is the next hop of the source node and there is any destination sequence number in routing table which is having the value greater than threshold and hop count equal to 1 then the source node suspects about the presence of malicious node in the network and makes alert to the other nodes in the network and deletes the suspected destination sequence number from the routing table. The SUSPECT message containing suspected sequence number is sent to the next hop by the source node if the next hop is not an attacker which would be further sent to its next hop until the malicious node is detected as shown in Fig. 7. The algorithm for calculating the dynamic threshold value is presented in procedure 1 of Sect. 5.2. The flowchart for action of source node when receiving request packets is presented in Fig. 8.

5.1.2 Detection

When any node receives the SUSPECT packet, it matches the destination sequence number in the routing table with the suspected sequence number included in the SUSPECT packet and also checks for the hop count in the routing table. If any node finds the destination sequence number in routing table matching with the suspected sequence number and hop count value equal to 1 then current node adds its next hop i.e. liar node as a malicous node in their blacklist table and broadcasts the ALERT packet in the whole network which contains the identity of malicious node and suspected destination sequence number as shown in Fig. 9. The algorithm for detecting the malicious node through a SUSPECT packet in the network is presented in

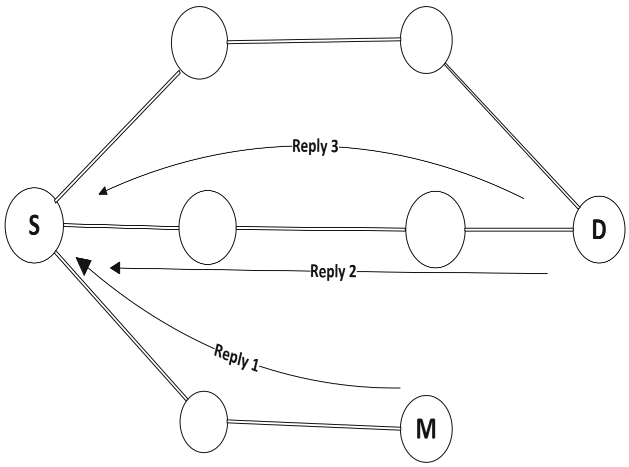

Fig. 6 Calculation of Dynamic Threshold Value

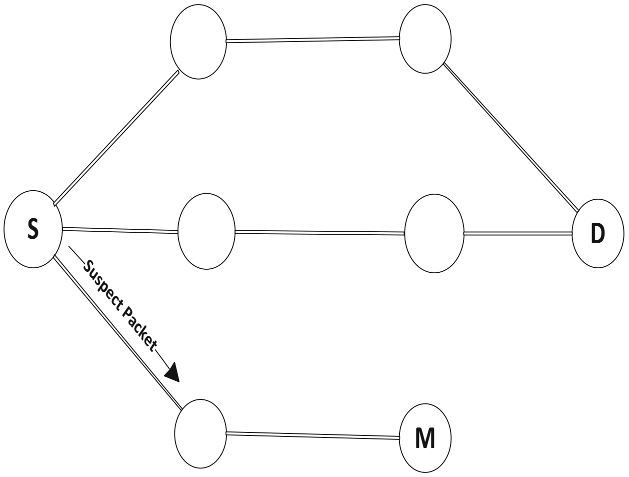

Fig. 7 Sending SUSPECT packet to Next Hop

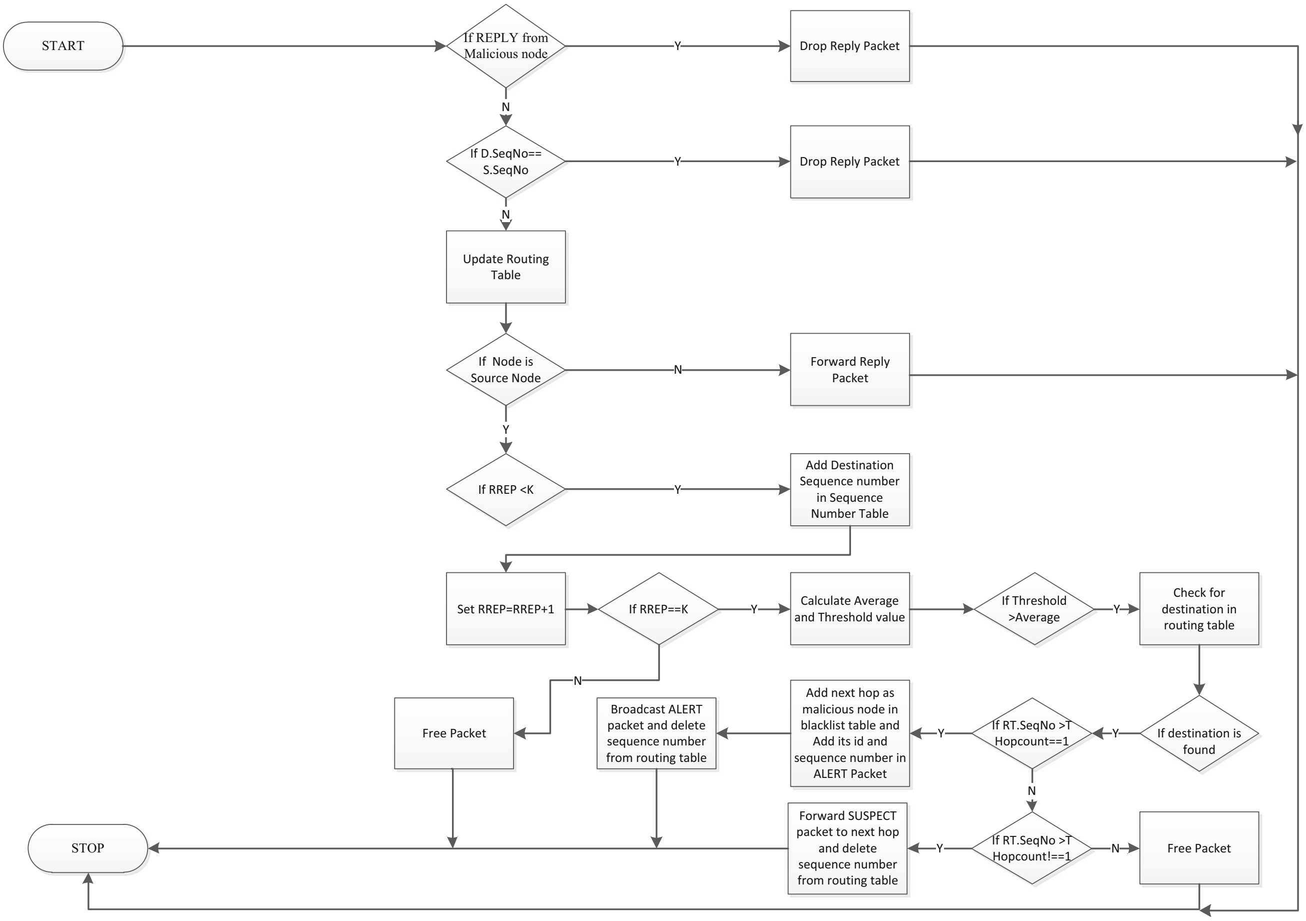
START
If REPLY from Malicious node
Y
Drop Reply Packet
N
If D.SeqNo== S.SeqNo
Y
Drop Reply Packet
N
Update Routing Table
If Node is Source Node
N
Forward Reply Packet
Y
If RREP <K
Y
Add Destination Sequence number in Sequence Number Table
Set RREP=RREP+1
If RREP==K
Y
Calculate Average and Threshold value
If Threshold >Average
Y
Check for destination in routing table
N
Free Packet
Broadcast ALERT packet and delete sequence number from routing table
Add next hop as malicious node in blacklist table and Add its id and sequence number in ALERT Packet
Y
If RT.SeqNo >T Hopcount==1
Y
If destination is found
N
STOP
Forward SUSPECT packet to next hop and delete sequence number from routing table
Y
If RT.SeqNo >T Hopcount!==1
N
Free Packet

Fig. 8 Flowchart for action of source node when receiving request packet

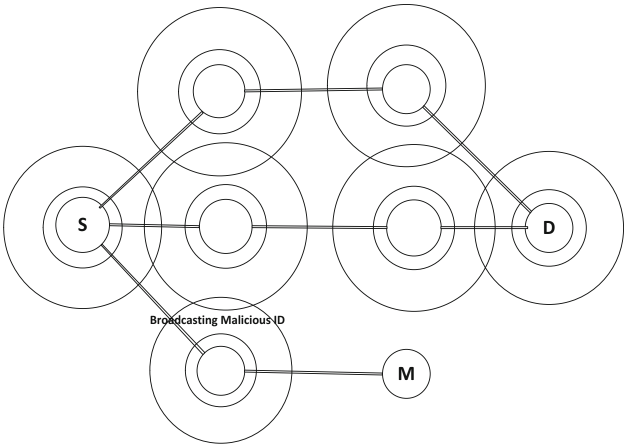

Fig. 9 Broadcasting ALERT packet

procedure 2 of Sect. 5.2. The flowchart for action of node when receiving SUSPECT packet is presented in Fig. 10.

5.1.3 *Prevention*

Once detection phase is over, the prevention phase comes into the play. The nodes in the network make an entry in their blacklist table on receiving the ALERT packet. If nodes already had made an entry for malicious nodes then it drops the ALERT packet otherwise malicious entry is done in the blacklist table and its entry is deleted from routing table as described in procedure 3 of Sect. 5.2. In this phase, the nodes in the network also check against its blacklist table before processing the request or reply packet to confirm whether the node is malicious or not. If the node id is found in the blacklist table then the current node simply drops a request or reply packet coming from the malicious node as shown in Fig. 11.

5.2 MBDP-AODV protocol-algorithm

Procedure 1 Action of source node when receiving multiple reply packets for calculating dynamic threshold.

```
Algorithm 1: Dynamic Threshold Calculation
if Reply from Malicious then
    Drop RREP packet ;
else if D.SeqNo==S.SeqNo then
    Drop RREP packet
else
    Update R.Table ;
    if Source node then
        if RREP < K then
            Add D.SeqNo. in Seq.No Table ;
        end if
        Set RREP: =RREP+1 ;
        if RREP==K then
            Set Average = $\sum_{i=1}^{K} \frac{D.SeqNo._i}{K}$ ;
            Set Threshold = $\sqrt{\sum_{i=1}^{K} \frac{(D.SeqNo._i - A)^2}{K}}$ ;
            if Threshold > Average then
                for Each entry in R.table do
                    if Destination is Found in R.Table then
                        if RT.SeqNo >Threshold and HopCount==1 then
                            Add Next Hop as Malicious in Blacklist Table ;
                            Add Next Hop and S.SeqNo in ALERT packet;
                            Broadcast ALERT packet ;
                            Delete S.SeqNo Entry from R.Table;
                        else if RT.SeqNo >Threshold and HopCount! =1
                        then
                            Forward SUSPECT Packet to Next Hop;
                            Delete S.SeqNo. Entry from R.Table;
                        else
                            Free Packet ;
                        end if
                    end if
                done
            end if
        else
            Free Packet ;
        end if
    else
        Forward RREP packet ;
    end if
end if
```

Procedure 2 Action of Next Hop when receiving SUSPECT packet in order to detect malicious node.

```
Algorithm 2: Detection Through SUSPECT Packet
if RT.Seqno==S.SeqNo and HopCount==1 then
    Add Next Hop and S.SeqNo into Blacklist Table ;
    Add Next Hop and S.SeqNo in ALERT packet;
    Broadcast ALERT packet;
    Delete S.SeqNo Entry from R.Table ;
else
    Forward SUSPECT packet to Next Hop ;
end if
```

Procedure 3 Action of node when receiving ALERT packet, Request or Reply packet in order to prevent malicious node.

```
Algorithm 3: Prevention
if ALERT Packet then
    if Malicious ID already present in BlackList Table then
        Drop ALERT packet ;
    else
        Add Malicious Id and S.SeqNo in BlackList Table ;
        Add Next Hop and S.SeqNo in ALERT packet;
        Broadcast ALERT packet ;
        Delete malicious entry from R.Table ;
    end if
end if
if REQUEST Packet then
    if Malicious ID already present in BlackList Table then
        Drop REQUEST packet ;
    else
        Process REQUEST packet;
    end if
end if
if RREP Packet then
    if Malicious ID already present in BlackList Table then
        Drop RREP packet ;
    else
        Process RREP packet;
    end if
end if
```

6 Experimental environment setup

In this paper, we have used NS-2.35 [26] simulator to validate the efficiency of the proposed methodology against black hole nodes. In an area of 750 m × 750 m, 50 normal nodes executing AODV routing protocol were randomly distributed, and a maximum of two malicious nodes, performing black hole attack, are randomly located. Two pairs were randomly chosen for data communication, each sending 10 KB UDP–CBR packets per second. The performance of the protocols in the network is tested at different mobility speed of 5, 15, 25 and 35 m/s. The main parameters of all NS-2 experiments are listed in Table 3, and all experimental value in this section refers to an average value of experiments.

In order to evaluate the performance of our protocol, we have used three metrics i.e. packet delivery rate, average throughput and routing overhead which has been compared with the existing IDSAODV [25] protocol. For launching black hole attack in the network, BAODV protocol is used by black-hole node as shown in Figs. 12 and 13. In this paper, BAODV means that AODV based network is under black-hole attack. In the simulation, IDSAODV protocol is also evaluated under one and two malicious nodes respectively.

Similarly, MBDP-AODV is evaluated under one and two malicious nodes respectively. The false positive rate and true positive rate for randomly moved black hole(s) is calculated. A true positive (TP) is a malicious node being correctly detected as a black hole whereas, a false positive (FP) is a normal node being wrongly detected as a black hole. The TP

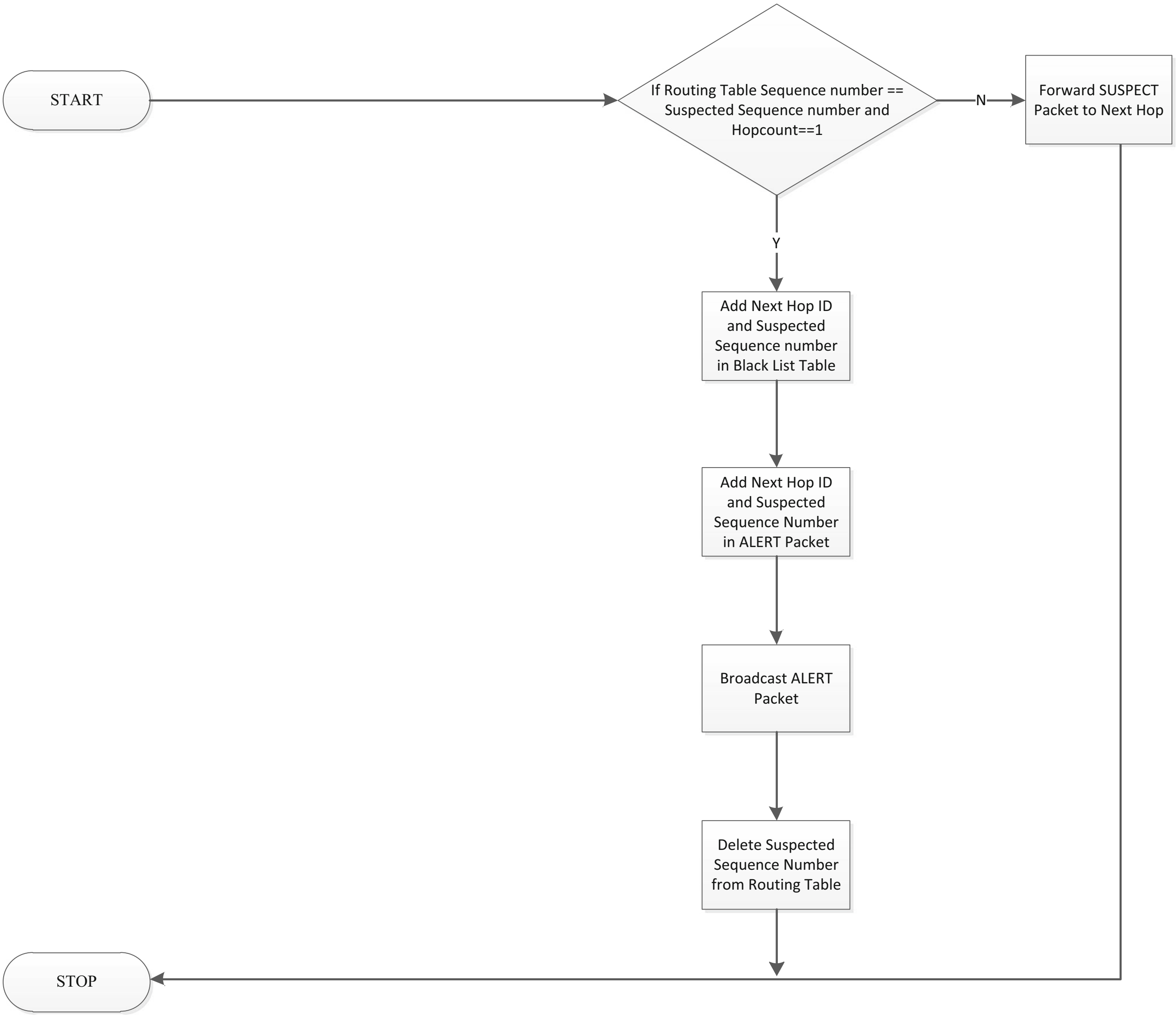
START
If Routing Table Sequence number == Suspected Sequence number and Hopcount==1
N
Forward SUSPECT Packet to Next Hop
Y
Add Next Hop ID and Suspected Sequence number in Black List Table
Add Next Hop ID and Suspected Sequence Number in ALERT Packet
Broadcast ALERT Packet
Delete Suspected Sequence Number from Routing Table
STOP

Fig. 10 Flowchart for action of node when receiving SUSPECT packet

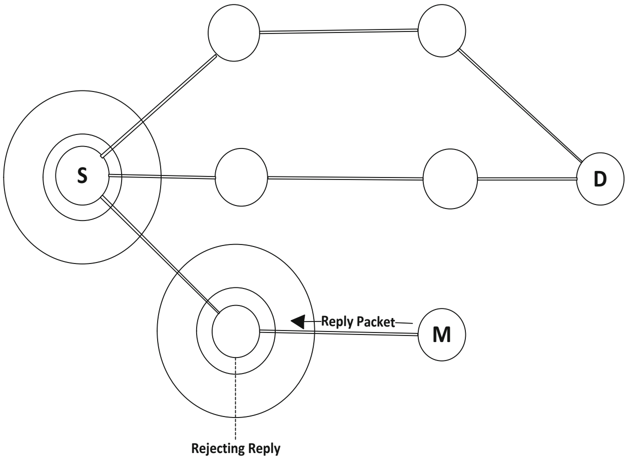

Fig. 11 Rejecting Reply From Malicious Node. S- Source Node, D-Destination Node, M- Malicious Node

rate is calculated by a total number of detected black hole node/total number of black hole node × 100%, which is the percentage of black hole nodes being correctly detected. Similarly, the FP rate is calculated by a total number of node wrongly detected as black hole/total number of a normal node × 100%, which is the percentage of the normal node being wrongly detected.

7 Simulation result and analysis

In this section, we have evaluated the performance of the network under black hole attack. We have also evaluated our proposed protocol and compared it with the existing scheme. The average values of metrics for all mobility speed have been presented in Table 4.

Table 3 Simulation parameters

Parameter	Value
Dimension	750 m × 750 m
Number of nodes	50
Simulation time	500 s
Propagation radio model	Two ray ground
Traffic type	CBR
Number of connections	2
Packet size	512 bytes
Connection	UDP
Mobility model	Random waypoint mobility model
MAC layer	IEEE 802.11
Malicious node (varying)	0–30%
Mobility speed (varying)	5, 15, 25, 35 m/s
Protocol	AODV, BAODV, IDSAODV, MBDP-AODV

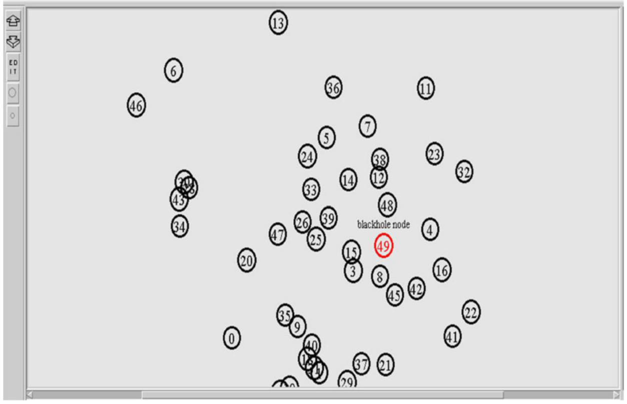

Fig. 12 Simulation under one black hole node

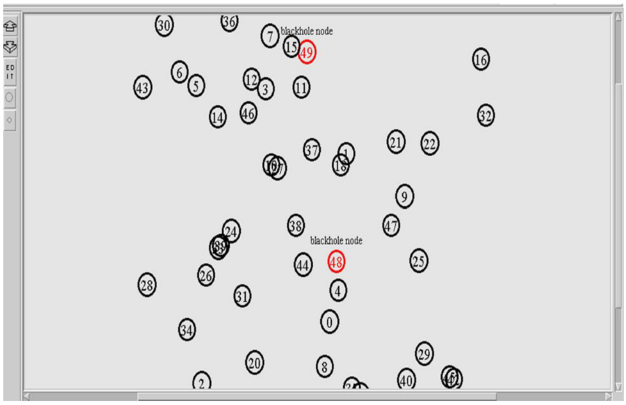

Fig. 13 Simulation under two black hole nodes

7.1 Packet delivery rate

Figures 14 and 15 show that when there was no attack in the AODV based network, the average packet delivery rate for all mobility speed was approximately about 96.99% but when there was a single moveable black hole node, the average packet delivery rate for all mobility in case of BAODV was approximately about 5.53%. The average packet delivery rate in case of IDSAODV under one black hole node was approximately about 19.79% but in proposed protocol, it was approximately about 92.54% or 91.22% when K = 3 or K = 4, respectively as shown in Fig. 14 which was increased by 72.57 or 71.43%, respectively. When there were two black hole nodes in the network, the average packet delivery rate for all mobility speed was 1.6%. In the case of IDSAODV, it was approximately about 7.72% but in our protocol, it was approximately about 89.27% or 87.26% when K = 3 or K = 4, respectively as shown in Fig. 15 which was increased by 81.55% or 79.54%, respectively. The PDR with K = 3 is slightly high as compared with the PDR with K = 4 due to the fast calculation of dynamic sequence number based threshold value in case of K = 3. Therefore increasing the value of K leads to low PDR of the network due to delay in calculation of sequence number based threshold value as the source node would have to wait for more number of reply packets coming from various nodes. It was also observed that the packet delivery rate of the normal network was slightly decreasing with the increase in mobility speed of the node. This was due to the path breakage between source and destination which occurred with the increase in mobility speed of the node. The packet delivery rate in case of one black hole attack was also decreasing due to packing dropping by itself and packet loss due to path breakage. When there were two black hole nodes in the network; the packet delivery rate was low as compared to one black hole node. In the case of IDSAODV, although there was an improvement in the network but it was also decreasing with the increase in the mobility speed of the node. When proposed protocol was used, it was observed that the packet delivery rate was slightly increasing with

Table 4 Average values for all mobility speeds under attack

S. no.	Metric	AODV (without attack)	No. of malicious node	BAODV (AODV under attack)	MBDP-AODV_3 (under attack)	MBDP-AODV_4 (under attack)	IDSAODV (under attack)
1	PDR (%)	96.99	1	5.53	92.54	91.22	19.79
2	PDR (%)	96.99	2	1.6	89.27	87.26	7.72
3	Throughput (kbps)	19.42	1	1.38	18.52	18.28	4.20
4	Throughput (kbps)	19.42	2	0.41	17.71	17.46	1.73
5	Routing overhead	4600	1	3725	8016	7807	3173
6	Routing overhead	4600	2	3099	7691	7682	3019

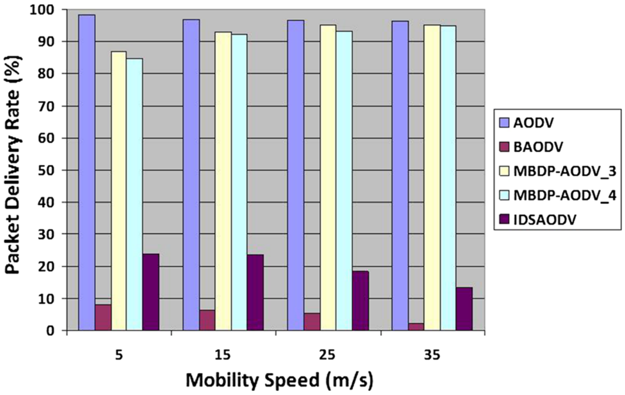

Fig. 14 PDR under one black-hole node

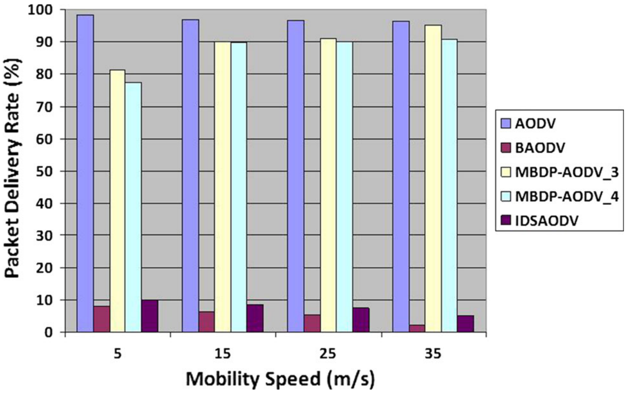

Fig. 15 PDR under two black-hole node

the increase in the mobility speed. This was due to the reason that in some experiments the attackers were near to the source node and the destination node was far away from it due to which the source node received the first reply from the malicious node and started data transmission towards it. When it received the other two replies from its neighbour nodes, it calculated the threshold value and then deleted the entry of malicious node from the routing table. As the mobility speed was increased, the attacker went out of the transmission range of source node due to which there was slight increase in packet delivery rate.

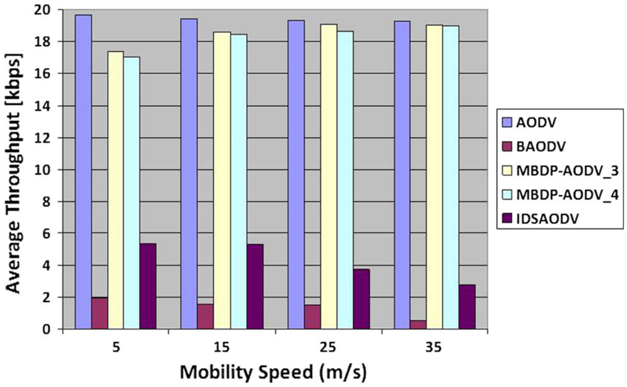

Fig. 16 Average Throughput under one black-hole node

7.2 Average throughput

From Figs. 16 and 17, it can be seen when there was no attack in the AODV based network the average throughput for all mobility was about 19.42 kbps but when there was a single moveable black hole node, the average throughput for all mobility in case of BAODV was about 1.38 kbps. The average throughput of IDSAODV protocol was about 4.2 kbps but in our protocol, it was 18.52 kbps or 18.28 kbps when K = 3 or K = 4 respectively as shown in Fig. 16 which was increased by 73.73% or 72.49% respectively. When there were two moveable black hole nodes in the network, the average throughput for all mobility was about 0.41 kbps. In IDSAODV protocol, the average throughput was about 1.73 kbps but in MBDP-AODV protocol it was about 17.71 kbps or 17.46 kbps when K = 3 or K = 4 respectively as shown in Fig. 17 which was increased by 82.29% or 80.99%. The average throughput with K = 3 is slightly high as compared with average throughput with K = 4 due to the fast calculation of dynamic sequence number based threshold value in case of K = 3. Therefore increasing the value of K leads to the low average throughput of the network due to delay in calculation of sequence number based threshold value as the source node would have to wait for more number of reply packets coming from various nodes. It was also

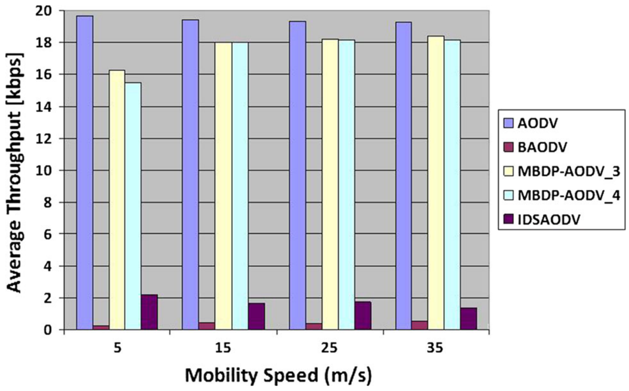

Fig. 17 Average Throughput under two black-hole nodes

observed that the average throughput rate of the normal network was slightly decreasing with the increase in mobility speed of the node. This was due to the path breakage between source and destination which occurred with the increase in mobility speed of the node. The average throughput in case of one black hole attack was also decreasing due to packing dropping by itself and packet loss due to path breaks. When there were two black hole nodes in the network; the average throughput rate was low as compared to one black hole node.

When IDSAODV was used, it was decreasing with the increase in the mobility speed of the node but when MBDP-AODV protocol was used, it was observed that the average throughput was slightly increasing with the increase in the mobility speed.

7.3 Routing overhead

As it can be seen in Figs. 18 and 19, when there was no attack in the AODV based network, the average routing overhead for all mobility speed was approximately about 4600 but when there was a single moveable black hole node, the average routing overhead was approximately about 3725. The average routing overhead for all mobility speed in case of IDSAODV under one black hole node was approximately about 3173 but in our protocol, it was approximately about 8016 or 7807 when K = 3 or K = 4, respectively as shown in Fig. 18. When there were two black hole nodes in the network, the average routing overhead for all mobility speed was 3099. In the case of IDSAODV, it was approximately about 3019 but in proposed protocol, it was approximately about 7691 or 7682 when K = 3 or K = 4, respectively as shown in Fig. 19. The high routing overhead in proposed protocol is due to the transmission of multiple reply packets by the destination node upon receiving the route request packet from various nodes.

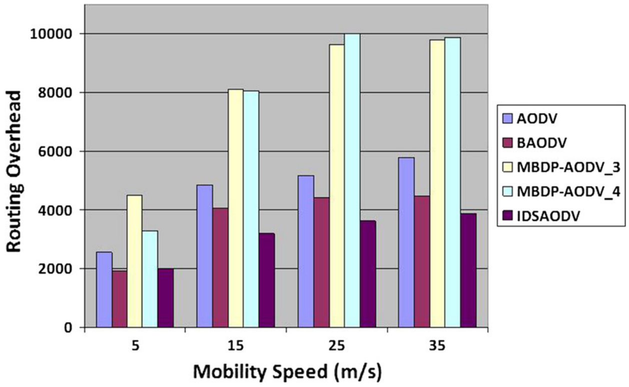

Fig. 18 Routing Overhead under one black-hole nodes

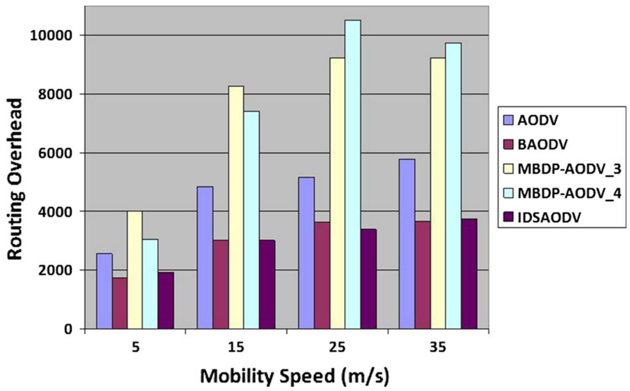

Fig. 19 Routing Overhead under two black-hole nodes

7.4 True positive and false positive rate

The TP rate and FP rate for any value of threshold K are listed in Table 5. Table 5(a) shows that for one black hole node in the network, it was detected successfully by using any threshold K with zero false positives. Since there was only one black hole node in the network, the TP rate reached 100%. Table 5(b) shows that when two black hole were present in the network, it was observed that the detection rate in case of K = 3 under two black hole nodes was high as compared with detection rate when K = 4.

7.5 Performance evaluation of MBDP-AODV at varying percentage of malicious nodes (MN)

In this section, we have evaluated our proposed protocol i.e. MBDP-AODV under the varying percentage of malicious nodes (MN) in the network at different mobility speeds which have been presented in Table 6.

7.5.1 Packet delivery rate

In the simulation, the mobility speed of nodes changes from 5 to 35 m/s. Meanwhile, the number of malicious

Table 5 TP rate and FP rate for randomly moved black hole(s)

K	Mobility speed (m/s)	TP rate (%)	FP rate (%)
(a) One black hole			
K = 3	5	100	0
	15	100	0
	25	100	0
	35	100	0
K = 4	5	100	0
	15	100	0
	25	100	0
	35	100	0
(b) Two black holes			
K = 3	5	80	0
	15	80	0
	25	90	0
	35	70	0
K = 4	5	60	0
	15	60	0
	25	70	0
	35	70	0

nodes (MN) increases from 0 to 30%. From the graph as depicted in Fig. 20, it can be seen that with the increase in the malicious node percentage, the packet delivery rate decreases. This is due to more number of false routing information in reply packet by the malicious node. When there are 0% malicious nodes in the network, the average packet delivery rate for all mobility speed is 96%.

When 2% or 4% of the nodes are malicious nodes in the network, the average packet delivery rate for all mobility speed is 92.54% or 89.27% respectively. In case, 10, 20 or 30% of the nodes are malicious nodes, the packet delivery rate for all mobility speed is 78.67, 47.39 or 32.54% respectively.

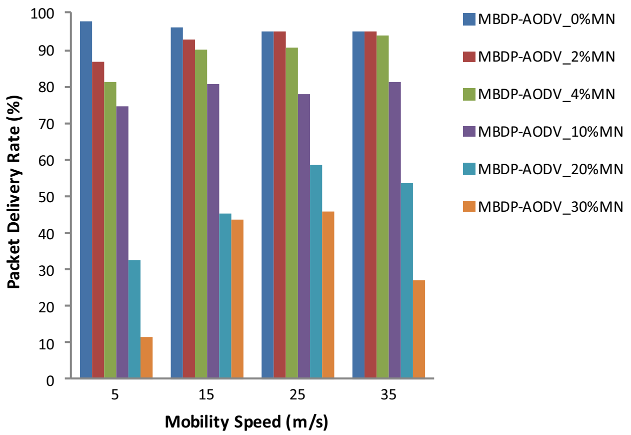

Fig. 20 PDR under different % of malicious node

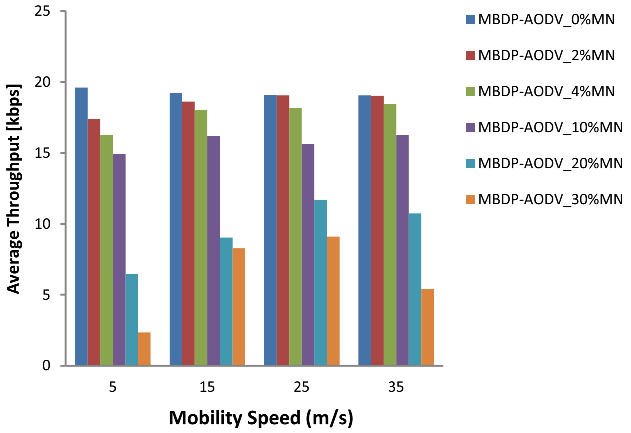

Fig. 21 Average Throughput under different % of malicious node

7.5.2 Average throughput

From the graph as depicted in Fig. 21, it can be seen that with the increase in the malicious node percentage, average throughput decreases. This is due to more number of false routing information in reply packet by the malicious node. When there are 0% malicious nodes in the network, the average throughput for all mobility speed is 19.23 kbps. When 2% or 4% of the nodes are malicious nodes in the network, the average throughput for all mobility speed is 18.52 or 17.71 kbps. In case, 10, 20 or 30% of the nodes are malicious nodes, the average throughput for all mobility speed is 15.74, 9.48 or 6.53 kbps, respectively.

Table 6 Performance of MBDP-AODV under varying % of malicious nodes

S. no.	Malicious node (%)	PDR (%)	Throughput (kbps)	Routing overhead
1	0	96	19.23	8341
2	2	92.54	18.52	8016
3	4	89.27	17.71	7691
4	10	78.67	15.74	7230
5	20	47.39	9.48	4894
6	30	32.54	6.53	4699

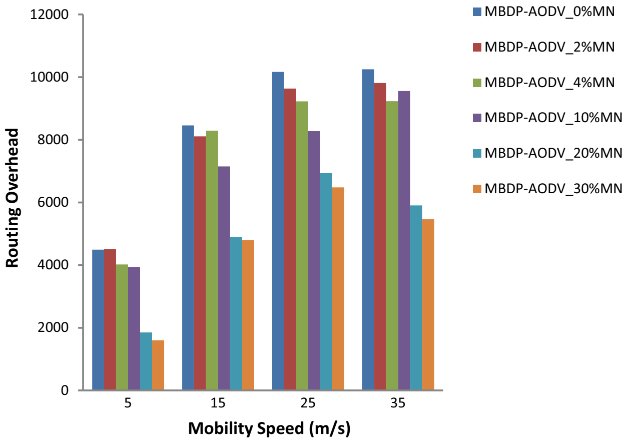

Fig. 22 Routing overhead under different % of malicious node

7.5.3 Routing overhead

From the graph as depicted in Fig. 22, it can be seen that when there are 0% malicious nodes in the network, the average routing overhead for all mobility speed is 8341. When 2% or 4% of the nodes are malicious nodes in the network, the average routing overhead for all mobility speed is 8016 or 7691, respectively. In case, 10, 20 or 30% of the nodes are malicious nodes, the average routing overhead for all mobility speed is 7230, 4894 or 4699, respectively. From the graph as depicted in Fig. 22, it can be seen that with the increase in the malicious strength, the routing overhead decreases because black hole nodes do not participate in route discovery process and do not broadcast the route request packet in the network due to which the neighbouring nodes do not get the route request packet which ultimately lead to generation of lesser control packets in the network.

8 Advantages and drawbacks of proposed protocol

There are various advantages of the proposed protocol which are as follows:

1. It can detect the black-hole node during route discovery phase rather than during data transmission phase.
2. The proposed protocol is based on sequence number dynamic threshold value.
3. It does not need to be in overhearing mode due to which energy is not wasted.
4. There is no need of any special extra IDS nodes in the network.
5. It can also mitigates the impact of cooperating malicious node's attack in which the first malicious node sends the data packet to the other node which drops the packets.

The proposed protocol has following drawback and limitation which are as follows:

1. It has high routing overhead as compared with other protocol because multiple reply packets are sent by the destination node.
2. It cannot deal with smart gray-hole attack.

9 Conclusion and future work

In this paper, we have presented about the different possible behaviour of the node that can lead to packet dropping attack in the network. It has been observed that the packet delivery rate is low when there are more number of black hole nodes in the ad-hoc network. In order to secure the network from this attack, we have proposed a new scheme based on dynamic destination sequence number threshold value. We have implemented our proposed methodology in NS-2.35 simulator which not only detects the malicious node but also prevents it from further participation during the route discovery. From the simulation results, it has been found that our proposed protocol performs well as compared with the existing one in term of packet delivery rate and average throughput under black hole attack. It has also been found that the when the value of K = 3, it performs slightly better as compared when the value of K = 4 under black hole attack due to the fast calculation of dynamic destination sequence number based threshold value. Moreover, with the increase in malicious node percentage, the performance of MBDP-AODV decreases. The limitation of this protocol is that it cannot detect smart gray hole attack due to its participation in route discovery process. As a future work, we are planning to extend this approach for dealing with smart gray hole attack.

Acknowledgements The first author would like to thank Department of Electronics and Information Technology (DEITY), Government of India, for supporting Ph.D. research scholar under Visvesvaraya Scheme. The authors would also like to thank the editor and anonymous reviewers for providing helpful comments in improving this manuscript.

References

1. Balaji, S., & Rajaram, M. (2016). SIPTAN: Securing inimitable and plundering track for ad hoc network. *Wireless Personal Communications*. doi:10.1007/s11277-016-3187-y.
2. Hwang, R. J., & Hsiao, Y. K. (2013). An anonymous distributed routing protocol in mobile ad-hoc networks. *Journal Supercomputing, 66,* 888–906. doi:10.1007/s11227-013-0920-0.
3. Singh, T., Singh, J., & Sharma, S. (2016). Energy efficient secured routing protocol for MANETs. *Wireless Networks*. doi:10.1007/s11276-015-1176-9.
4. Poongodi, T., & Karthikeyan, M. (2016). Localized secure routing architecture against cooperative black hole attack in mobile

ad hoc networks. *Wireless Personal Communications*. doi:10.1007/s11277-016-3318-5.

5. Perkins, C. E., Beliding-Royer, E., & Das, S. (2004). Ad hoc on-demand distance vector (AODV) routing. *IETF Internet Draft, MANET working group*.
6. Johnson, D. B., Maltz, D. A., & Hu, Y.-C. (2004). The dynamic source routing protocol for mobile ad-hoc network (DSR). *IETF Internet Draft*.
7. Dorri, A. (2016). An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET. *Wireless Networks*. doi:10.1007/s11276-016-1251-x.
8. Jhaveri, R. H., Patel, S. J., & Jinwala, D. C. (2012). DoS attacks in mobile ad hoc networks: A survey. In *IEEE 2nd international conference on advanced computing and communication technologies*.
9. Verma, K., Hasbullah, H., & Kumar, A. (2013). Prevention of DoS attacks in VANET. *Wireless Personal Communications, 73,* 95–126. doi:10.1007/s11277-013-1161-5.
10. Laxmi, V., Lal, C., Gaur, M. S., & Mehta, D. (2015). JellyFish attack: Analysis, detection and countermeasure in TCP-based MANET. *Journal of Information Security and Applications, 22,* 99–112.
11. Faghihniya, M. J., Hosseini, S. M., & Tahmasebi, M. (2016). Security upgrade against RREQ flooding attack by using balance index on vehicular adhoc network. *Wireless Networks*. doi:10.1007/s11276-016-1259-2.
12. Djahel, S., Abdesselam, F. N., & Zhang, Z. (2011). Mitigating packet dropping problem in mobile ad hoc networks: Proposals and challenges. In *IEEE communications survey and tutorial* (pp. 658–672).
13. Dabideen, S., & Aceves, J. J. G. L. (2012). Secure routing in MANETs using local times. *Wireless Networks, 18,* 811–826. doi:10.1007/s11276-012-0435-2.
14. Gurung, S., & Chauhan, S. (2016). A novel approach for mitigating grayhole attack in MANET. *Wireless Networks*. doi:10.1007/s11276-016-1353-5.
15. Jhaveri, R. H., & Patel, N. M. (2015). A sequence number based bait detection scheme to thwart grayhole attack in mobile ad hoc networks. *Wireless Networks, 21,* 2781–2798. doi:10.1007/s11276-015-0945-9.
16. Gurung, S., & Saluja, K. K. (2014). Mitigating impact of black hole attack in MANET. In *Proceedings of the 5th international conference on recent trends in information, telecommunication and computing*.
17. Shahabi, S., Ghazvini, M., & Bakhtiarian, M. (2015). A modified algorithm to improve security and performance of AODV protocol against black hole attack. *Wireless Networks*. doi:10.1007/s11276-015-1032-y.
18. Gurung, S., & Siddhartha, S. (2017). A review of black-hole attack mitigation techniques and its drawbacks in mobile ad-hoc network. In *Proceedings of the 2nd IEEE international conference on WiSPNET,* (pp. 2409–2415).
19. Shi, F., Liu, W., Jin, D., & Song, J. (2014). A cluster-based countermeasure against blackhole attacks in MANETs. *Telecommunication Systems, 57*(2), 119–136.
20. Chang, J. M., Tsou, P. C., Woungang, I., Chao, H. C., & Lai, C. F. (2015). Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach. *IEEE System Journal, 9*(1), 65–75. doi:10.1109/JSYST.2013.2296197.
21. Katal, A., Wazid, M., Goudar, R. H., & Singh, D. P. (2013). A cluster based detection and prevention mechanism against novel datagram chunk dropping attack in MANET multimedia transmission. In *Proceedings of IEEE conference on information and communication technologies* (pp. 479–484).
22. Su, M. Y. (2011). Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. *Computer Communications, 34*(1), 107–117. doi:10.1016/j.comcom.2010.08.007.
23. Mohanapriya, M., & Krishnamurthi, I. (2014). Modified DSR protocol for detection and removal of selective black hole attack in MANET. *Computers and Electrical Engineering, 40,* 530–538.
24. Lacey, T. H., Mills, R. F., Mullins, B. E., Raines, R. A., Oxley, M. E., & Rogers, S. K. (2012). RIPsec: Using reputation-based multilayer security to protect MANETs. *Computer and Security, 31,* 122–136.
25. Dokurer, S., Erten, Y. M., & Acar, C. E. (2007). Performance analysis of ad-hoc networks under black hole attacks. In *Proceedings of the IEEE SoutheastCon*.
26. The network simulator-ns-2. (2016). http://www.isi.edu/nsnam/ns/.

Shashi Gurung received the M.Tech. degree in computer science and engineering in 2014 and the B.Tech. degree in computer science and engineering in 2011 from Punjab Technical University, Jalandhar, Punjab, India. He is an Assistant Professor (Computer Engineering) in Jawaharlal Nehru Government Engineering College, Sundernagar and currently pursuing the Ph.D. degree in computer science and engineering at National Institute of Technology Hamirpur, Himachal Pradesh, India. His research interests include mobile ad hoc network (MANET) and network security. He has publications in reputed journal.

Siddhartha Chauhan received the Ph.D. degree in computer science and engineering from National Institute of Technology Hamirpur, Himachal Pradesh, India, in 2013 and the M.Tech. degree in computer science and engineering from Indian Institute of Technology Roorkee, Uttrakhand, India, in 2003. He has published many research papers in international conferences and reputed journal. He is currently with Department of Computer Science and Engineering, National Institute of Technology Hamirpur, Himachal Pradesh, India. His research interests include mobile ad hoc network and wireless sensor network. He has published many papers in reputed journal.