Wireless Netw
DOI 10.1007/s11276-016-1353-5

A novel approach for mitigating gray hole attack in MANET

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

Abstract Mobile ad hoc network (MANET) is defined as the category of wireless network that is capable of operating without any fixed infrastructure. The main assumption considered in this network is that all nodes are trusted nodes but in real scenario, some nodes can be malicious node and therefore can perform selective dropping of data packets instead of forwarding the data packets to the destination node. These malicious nodes behave normally during route discovery phase and afterwards drop fractions of the data packets routed through them. Such type of attack is known as smart gray hole attack which is variation of sequence number based gray hole attack. In this paper, we have launched smart gray hole attack and proposed a new mechanism for mitigating the impact of smart gray hole attack. Mitigating Gray hole Attack Mechanism (MGAM) uses several special nodes called as G-IDS (gray hole-intrusion detection system) nodes which are deployed in MANETs for detecting and preventing smart gray hole attack. G-IDS nodes overhear the transmission of its neighbouring nodes and when it detects that the node is dropping the data packets which are greater than threshold value then it broadcast the ALERT message in the network notifying about the identity of malicious node. The identified malicious is then blocked from further its participation by dropping the request and reply packet. In order to validate the effectiveness of our proposed mechanism, NS-2.35 simulator is used. The simulation results show that the proposed mechanism performs slightly well as compared with the existing scheme under smart gray hole attack.

Keywords MANET · Denial of service attack · Smart gray hole attack · Gray hole intrusion detection system

1 Introduction

Mobile ad hoc network (MANET) is a progressing and most pervasive technology in wireless network which is recognized as an infrastructure less network [1]. It is self-configurable, temporary and scalable type of networks [2]. These types of networks are suitable for critical operation such as battlefield, emergency rescue operation etc. where it is difficult to set up infrastructure based network [3]. In this type of network, each device not only acts as a host and but also as a router [4]. The routing protocol such as ad hoc on-demand distance vector (AODV) [5], Dynamic source routing (DSR) [6] etc. which are used for communication are based on assumption that all nodes are cooperative and trustworthy [7]. Therefore, the MANET routing protocols are highly vulnerable to various types of denial of service (DoS) attacks [8], particularly packet dropping attack. The packet dropping attack can be categorized as *Full packet drop* and *Partial packet drop* attack. The full packet drop attack is known as black hole attack and the partial packet drop attack is known as gray hole attack. In case of *Full packet drop* attack, the malicious node do not participate in route discovery process and try to attracts the data traffic by giving false routing information and drops all the data packet received by it whereas in case of *Partial packet drop* attack, the malicious node participates genuinely in the route

✉ Shashi Gurung
gurungshashi68@gmail.com

Siddhartha Chauhan
siddharthachauhan1@gmail.com

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

Published online: 26 August 2016

discovery process and also forwards the genuine reply packet received from the destination. When the source node sends the data packets through the path which contains gray hole node, it drops some of the data packets and the performance of the network slightly degrades. Therefore, there is need to provide security in ad-hoc network for dealing with the attacks. In this paper, the main contribution is that we have proposed a new mechanism called as Mitigating Gray hole Attack Mechanism (MGAM) for reducing the impact of smart gray hole attack in the network.

The remainder of the paper is structured as follows. Sect. 2 describes different types of gray hole attack and the procedures for launching smart gray hole attack. In Sect. 3, we explained about various existing schemes for dealing with gray hole attack in MANET. In Sect. 4, we describes in detail about the working mechanism of proposed methodology. Section 5 discusses about the experimental parameters and analysis in NS-2. In Sect. 6, we shows the performance comparison of our approach with ABM. The advantages and shortcomings of proposed approach and conclusions are discussed in Sects. 7 and 8 respectively.

2 Gray hole attack

Gray hole attack or selective forwarding attack is denial of service attack [8, 9] which is variation of black hole attack in which initially the node do not appear as a malicious but later on turns into malicious one and drops selective data packets. There can be two types of possible gray hole attacks in the MANET as depicted in Fig. 1. The first type of gray hole attack is *Sequence Number* based gray hole attack which is introduced in [10] in which the node gives false route reply by sending high destination sequence number with minimum hop count to the source node The source node on receiving the reply packets starts sending the data packets through the route which contains gray hole node and then selectively drops the data packets. The second type of gray hole attack is *Smart* gray hole attack which is variation of sequence number based gray hole attack in which the node behaves normally during the route discovery process and then drops some fractions of the data packets. The gray hole node behaves in an unpredictable manner in the network and therefore, it is difficult to detect these attack [11, 12] than the black hole node where the malicious node drops all the received data packets [13–16]. In order to launch the smart gray hole attack, we have presented the procedure as shown in 2.1 and 2.2 subsections. Initially the smart gray hole node is made to participates normally in route discovery process in order to find the route towards the destination but when it receives the data packets, it checks whether the trusted variable is *True* or *False*. If smart gray hole attack is to be launched between Time T1 and T2, the *Trusted* variable is set to the *False* and then it performs selective packet drop otherwise it forwards the data packets to the next node or to the destination node.

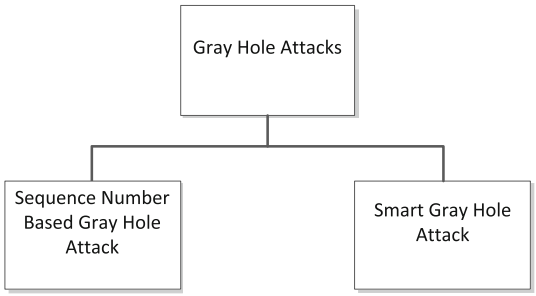

Fig. 1 Types of gray hole attacks

2.1 Action performed by malicious nodes on receiving request packet

```
If (Request is not for me) then
  Search for Destination in the Routing Table
    If Not in Routing Table
      Broadcast Route Request  // To find the destination node
  Else
    Send Reply
Else
  Update  Routing Table
  Send Reply
End if
```

2.2 Action performed by malicious nodes on receiving data packets

```
If (Data packet is not for me )
 If (Current_Time > Set_Time1 && Current_Time < Set_Time2)
  If (Trusted==False)
   Drop Fractions of Data packets
  Else
   Forward the Data packets to next hop or Destination node
  End If
 End If
Else
Accept the Data Packet
End if
```

3 Related work

There are many existing schemes which have been proposed by many researchers for dealing with selective packet dropping attack.

The author in [17] proposed a technique that can detects chain of collaborative malicious nodes which performs selective packet drop in the network. In this approach, the total data traffic is divided into some small sized blocks. The source node sends a prelude message to the destination node before sending a block of the data to notify it about the incoming data block and starts the timer. After sending prelude message, it broadcasts a monitor message to all its neighbour nodes to monitor the activities of the next node and begins with the transmission of data packets. On the other hand, the destination node sends a postlude message which contains the number of data packets received by destination node. If the source node receives the postlude message within the expiry of timer, it checks the number of received packet with the total number of sent packet by it and if the differences is within the tolerable range, it sends the next block of the data packet else it starts detection of malicious node and then remove malicious node from the network by collecting the responses from the monitoring nodes. The drawback of this approach is that it has high routing overhead due to various extra control packets and the author has not done performance evaluation of the proposed approach.

In [18], special nodes called as IDS nodes are deployed in the network which has the ability to overhear its nearby transmission. In this technique, only the destination nodes are allowed to send the reply packet on receiving the request packet and intermediate nodes are forbidden to send the reply packet. There are certain rules according to which if nodes does not works, it is declared as malicious node. The IDS node monitors and increases the suspicious value of its nearby node according to abnormal difference between requests (RREQs) and replies (RREPs) packets transmitted from the node. If any intermediate node is not the destination node and that has never broadcasted a request packet for a specific path, but forwarded a reply packet for the path, then nearby IDS node will increment its suspicious value by 1 in its suspicious node table. When the suspicious value of a node becomes greater than the threshold value, IDS nodes broadcast a block message to all nodes in the network for blocking suspicious node and thus isolating it from the network. Although this approach is able to detect the black hole attack and sequence number based gray hole attack in the network but it fails in case of smart gray hole attack. The smart gray hole node participates correctly in route discovery and also forwards the request packet due to which it is unable to detect it and hence is the limitation of this approach.

In [12], the author has proposed a new methodology for mitigating the effects of the gray hole node by employing special nodes i.e. intrusion detection system (IDS) in the network. The source node intimates to the destination node about the number of packets it will forward through alternative path. Whenever the destination node does not get the actual number of data packets, it transmits query request (QRREQ) packet to the node which is at a distance of 2- hop from it and waits for the query reply (QRREP) packet. The query reply (QRREP) packet contains data about the number of data packets forwarded by the node to its next hop neighbor in the source route. On receiving the query reply (QRREP) packet, the destination node verifies whether its previous hop node has relayed all the data packets that it received from its previous hop node. When the destination node found that its previous node has not forwarded all the packets received from its previous node, it makes its entry into suspected list and alert to the nearby IDS nodes about the suspected node. The IDS nodes listens to the malicious node's transmission and broadcast the block message in the network which contains the identity of malicious node whenever it detects any anomaly and then isolates the malicious node from the network. The limitation of this approach is that the malicious nodes can behave normally after receiving the query packet and can forward the data packets due to which the IDS node would not be in position to detect it.

An approach based on sequence number threshold is proposed in [10] that perform mitigation of gray hole attack in AODV based network. The authors proposed a SNBDS scheme that modifies the routing table by adding two new

fields which are node status and last reply time. The nodes status denotes whether the node is malicious or not and the last reply time denotes time of receipt of the last reply (RREP) for the destination node that updated its sequence number. In this approach, the authors have launched the three different types of gray hole by using false routing information which attracts the traffic towards it and performs selective packet drop in the network. A node receiving reply (RREP) packets detects the node sending reply (RREP) packet as a suspicious node if the difference between the destination sequence numbers in the reply packet and that of the routing table is greater than the calculated threshold value. A bait request (RREQ) packet is then sent to the suspicious node with nonexistent destination address and destination sequence number. If the suspicious node replies to the bait request (RREQ), it is declared as a malicious node and in the future the nodes discards all reply (RREP) packets. The limitation of this scheme is that it cannot mitigates the smart gray hole attack which participates genuinely in the network during route discovery process and sends correct information in the reply packet received either from the destination or any other intermediate node.

In [19], a new cooperative and distributed mechanism is proposed which consists of four security module for dealing with gray hole attack. The security modules are: (a) neighbourhood data collection, (b) local anomaly detection, (c) cooperative anomaly detection, and (d) global alarm raiser. In neighbourhood data collection modules, each node in the network gathers the data forwarding information in its neighbourhood and stores it in a Data Routing Information (DRI) table. The local anomaly detection module is invoked by a node whenever it identifies a suspicious node by checking its DRI table. The cooperative anomaly detection module is activated to increase the detection reliability by reducing the probability of false detection of local anomaly detection procedure. Finally global alarm raising module is invoked to broadcast alarm message to all the nodes in the network about the gray hole node that has been detected by the cooperative anomaly detection module. The identified malicious node is isolated from the network. The author has launched the simple gray hole by using false route reply but the smart gray hole node does not send false route reply and behaves normally during route discovery and drops selective data packets. Hence, the DRI based scheme also fails under the smart gray hole attack.

Most of the existing works deals with the mitigation of sequence number based gray hole attack in which the node gives false route reply in order to attract the traffic and drops selective data packet. There is also no evaluation of smart gray hole attack in different time periods with respect to node mobility in the available literature. The limitations of the existing schemes motivated us to propose a new mechanism which can deal with smart gray hole attack in the ad-hoc network. In this paper, we focus our attention on the second type of aforementioned gray hole attack i.e. smart gray hole attack in which the malicious node participates normally during route discovery, performs selective dropping of data packets for some duration and then changes its behaviour into normal one.

4 G-IDS -proposed grayhole intrusion detection system

In order to mitigate the impact of smart gray hole attack, we have proposed a new mechanism called as MGAM (Mitigating Gray hole Attack Mechanism), which is mainly used to compute the number of packets dropped by the particular node. All G-IDS nodes are in promiscuous mode in order to overhear the nearby transmission of neighbouring nodes. When any anomaly is detected by the G-IDS nodes, an ALERT message is broadcasted by it, alerting all nodes in the network for blocking the malicious node. The ALERT message contains the identity gray hole node, source address and destination address. All normal nodes upon receiving the ALERT message issued by G-IDS nodes will include the malicious node in their blacklist table, thus, the AODV routing protocol of the normal nodes is slightly modified. The various notations used in proposed approach have been described in Table 1 and the algorithm of proposed mechanism is given in Sect. 4.2. The following are the two assumptions which are considered while designing our proposed mechanism.

Table 1 Summary of notations

Notations	Meaning
N_{BLT}	Node's blacklist table
IDS_{BLT}	IDS's blacklist table
D_P	Data packet
DP_S	Number of data packets sent by node
DP_R	Number of data packets received by node
DP_F	Number of data packets forwarded by node
DP_D	Number of data packets dropped by node
R_Q	Request packet
R_P	Reply packet
A_P	ALERT packet
S_A	Source address
D_A	Destination address
T_H	Packet drop threshold
M_{ID}	Malicious ID

- Any G-IDS node will be within the transmission range of at least one G-IDS node in order to forward ALERT to each other i.e. a G-IDS node will always be neighbour to some other G-IDS node as shown in Fig. 2.
- Every G-IDS node is set in overhearing mode in order to overhear all transmission going on within its range.

In this paper, there are three different types of nodes in the network, which separately perform different function which is as follows.

- Smart Gray hole node: It selectively performing SGAODV (Smart Gray hole AODV) routing algorithm for smart gray hole attack in the network.
- Normal node: It executes a slightly revised AODV, called MAODV (Modified AODV), to conduct normal routing, and also blacklist the malicious nodes when it receives an ALERT packet broadcasted by G-IDS nodes.
- G-IDS node: It executes MGAM (Mitigating Gray hole Attack Mechanism) to mitigates and detects the gray hole nodes, and broadcasts an ALERT packets in the network when it detects any anomaly.

4.1 Proposed methodology description

According to AODV protocol, the source node broadcasts the request (RREQ) packet to find the path for communication with the destination node. On receiving the request (RREQ) packet, the destination or any intermediate node having the route towards the destination can send back the reply (RREP) packet to the source node. The malicious nodes which perform smart gray hole attack behave correctly during route discovery process and rebroadcast the request (RREQ) packet in the network if it do not have the path towards the destination. When the path is selected which contains the malicious node for sending data packets, it selectively drops the data packets as shown in Fig. 3. In order to mitigate gray hole attack, four fixed G-IDS nodes have been used which cover most of the simulation area and monitor the neighbouring node for checking whether the number of packets that it has received is being forwarded to its next hop or not. It computes the number of packets received by the node and the number of data packets forwarded by the node. If the difference between the number of received packets and number of forwarded packets are greater than the packet drop threshold (TH) value then G-IDS nodes broadcast an ALERT packet notifying to all the nodes in the network about the identity of gray hole nodes as shown in Fig. 4. On receiving an ALERT packet, the other nodes makes the entry of malicious node in their blacklist table and the source node deletes the destination entry from the routing table and starts new route discovery process by broadcasting new request packet in the network as depicted in

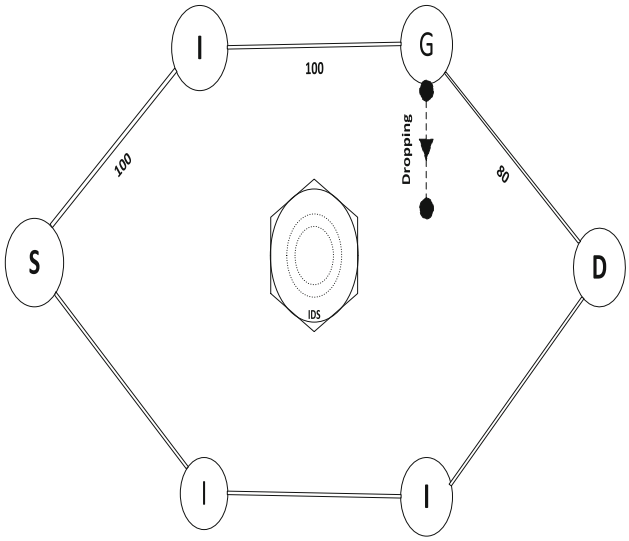

Fig. 3 G-IDS node overhearing packet transmission

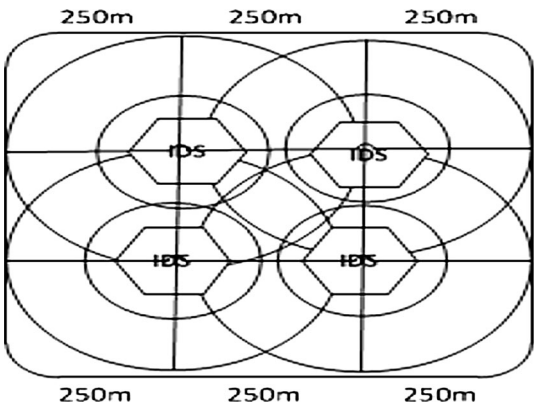

Fig. 2 Placement of G-IDS nodes

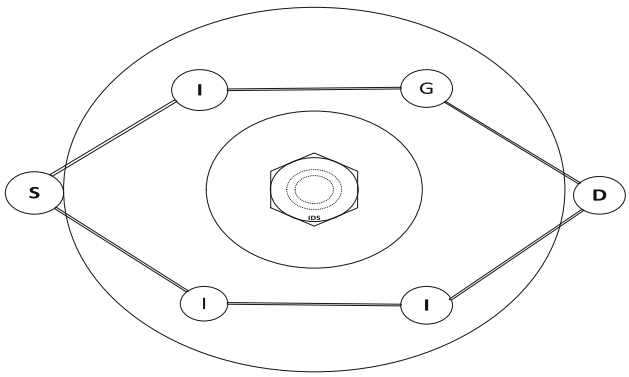

Fig. 4 Broadcasting ALERT packet

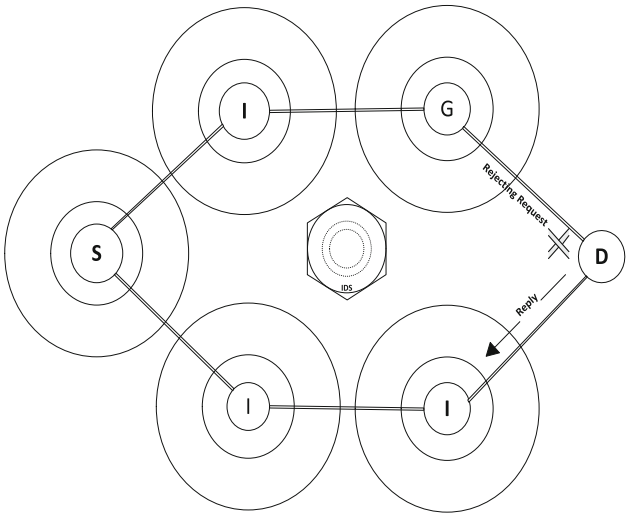

Fig. 5 New route discovery by source node S

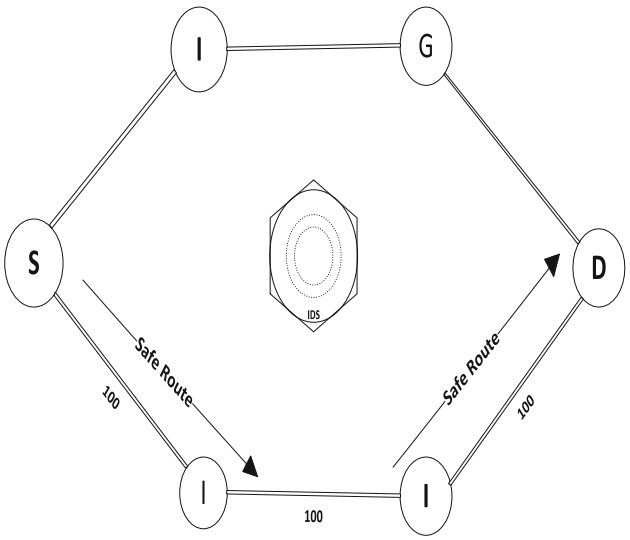

Fig. 6 Tranmission through safe route

Fig. 5. On receiving the request packet, each node checks whether the request is from malicious node or not. If it is from the malicious node then it is dropped by the node otherwise it broadcasts the route request packet to find the path towards the destination node. After receiving the reply from the destination node, the source node send data packets through safe route as depicted in Fig. 6. The

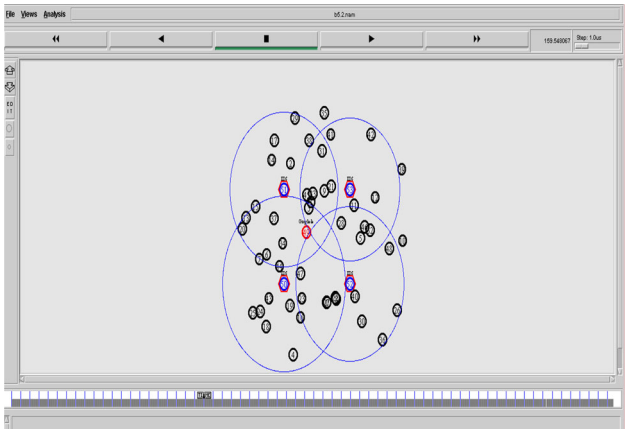

Fig. 7 G-IDS implementation in NS-2

implementation of proposed gray hole intrusion detection system (G-IDS) in NS-2 is shown in Fig. 7.

4.2 Algorithm

4.2.1 Action performed by G-IDS nodes in sniff mode

Calculates Number of Packets received (DP_R) by Node

Calculate Number of Packets sent (DP_S) by Node

Calculate Number of Packets Forwarded (DP_F) by Node

Calculate Number of Dropped Data Packets (DP_D) by following equation

$$DP_D = DP_R - DP_F$$

$$\text{Set } T_H = \frac{N}{100} \times \sum_{i=1}^{n} DPs$$

where N>0 and i is the number of source node sending data packets

If ($DP_D > T_H$)

Add Malicious Node ID (M_{ID}) in the IDS Black List Table (IDS_{BLT})

Broadcast ALERT packet containing Malicious ID (M_{ID}), Source Address (S_A) and Destination Address (D_A) in the network.

End if

4.2.2 Action performed by G-IDS nodes on receiving ALERT packet

If already received ALERT packets (A_P)

Drop ALERT packets (A_P)

Else

Add Malicious Node ID (M_{ID}) in the IDS Black List Table (IDS_{BLT})

Broadcast ALERT packet containing Malicious ID (M_{ID}), Source Address (S_A) and Destination Address (D_A) in the network

End if

4.2.3 Action performed by nodes on receiving ALERT packet

Check for Malicious entry in Node Blacklist table (N_{BLT})

If Malicious node ID (M_{ID}) is found

Drop ALERT packets (A_P)

Else

Creates entry for Malicious node ID (M_{ID}) in Node Black List Table (N_{BLT})

If Source node (S_A)

Delete entry of Destination Address (D_A) from routing table

Start new Route Discovery Process (RD_P)

End if

End if

4.2.4 Action performed by nodes on receiving request packet

Check for Malicious entry in Node Blacklist table (N_{BLT})

If Malicious node ID (M_{ID}) is found

Drop Request Packets (R_Q)

Else

If Destination node

Send Reply Packet (R_P)

Else

Forward Request Packet (R_Q)

End if

End if

4.2.5 Action performed by nodes on receiving reply packet

Check for Malicious entry in Node Blacklist table (N_{BLT})

If Malicious node ID (M_{ID}) is found

Drop Reply Packets (R_P)

Else

If Source node

Send Data Packet (D_P)

Else

Forward Reply Packet (R_P)

End if

End if

5 Experimental environmental setup and analysis

In this paper, NS-2.35 [20] simulator is used in order to validate the effectiveness of the proposed methodology against smart gray hole nodes. In an area of 750 × 750 m, 48 normal nodes executing AODV routing protocol were randomly distributed, and maximum of two malicious nodes, performing smart gray hole attack, are randomly located. Two pairs were randomly chosen for communication, each sending 10 KB of UDP–CBR packets per second. In each scenario, all nodes were located in different positions and moved with different mobility speed of 5, 15, 25 and 35 m/s. The important parameters used in the experiment are listed in

Table 2 Simulation parameters

Parameter	Value
Dimension	750 × 750 m
Total 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
MAC layer	IEEE 802.11
Malicious node (varying)	1–2
Mobility speed (varying)	5, 15, 25, 35 m/s
Protocol	AODV, SGAODV

Table 2, and all experimental value in this study refers to a mean value, which result from the 10 experiments.

In order to evaluate the performance of our proposed mechanism, we have used various performance metrics such as packet delivery rate, packet loss rate, average throughput, routing overhead and normalized routing overhead. Smart gray hole-AODV (SGAODV) protocol is used for launching the smart gray hole attack in the network. The smart gray hole attack is launched in such a way that it is behaving normal between 0 and 100 s of the simulation time and then performing selective packet dropping between 100 and 200 s. After this time period, it again behaves as a normal node for another 100 s and then changes its behaviour to perform selective packet drop attack between 300 and 400 s. Finally, after 400 s, it behaves as a normal node.

5.1 Performance metrics

The various performance metrics which have been used in order to evaluate the effectiveness of the proposed technique under smart gray hole attack are described in this section and meaning of notations used in the equations are given in Table 3.

5.1.1 Packet delivery rate

It is calculated by total number of packet received at the destination divided by total number of packets sent by the source $\times$ 100 %.

Table 3 Meaning of notations

Notations	Meaning
PDR	Packet delivery rate
PLR	Packet loss rate
AT	Average throughput
RO	Routing overhead
NRL	Normalized routing load
TPR	True positive rate
FPR	False positive rate
i	Number of source or destination node
j	Number of node generating control packets
X	Number of packet received
Y	Number of packet sent
P_S	Size of Packet
S_P	Stop Time of Simulation
S_T	Start Time of Simulation
R	Number of control packets
N_{DM}	Number of detected malicious node
T_{MN}	Total number of malicious node
N_{FDM}	Number of falsely detected malicious node
T_{NN}	Total number of normal nodes

$$\mathrm{PDR} = \frac{\sum_{i=1}^{n} X_i}{\sum_{i=1}^{n} Y_i} \times 100\,\%.$$

5.1.2 Packet loss rate

It is calculated by total number of packet dropped divided by total number of packets sent by the source $\times$ 100 %.

$$\mathrm{PLR} = \frac{\sum_{i=1}^{n} Y_i - \sum_{i=1}^{n} X_i}{\sum_{i=1}^{n} Y_i} \times 100\,\%.$$

5.1.3 Average throughput

It is calculated by total size of packets received at the destination in the network divided by difference of stop and start time of simulation time.

$$\mathrm{AT} = \frac{\sum_{i=1}^{n} X_i \times P_s}{S_P - S_T}.$$

5.1.4 Routing overhead

It denotes total number of control packets generated by the node in the network.

$$\mathrm{RO} = \sum_{j=1}^{n} R_j.$$

5.1.5 Normalized routing load

It is computed by total number of control packets generated by the node divided by total data packets received at the destination in the network.

$$\mathrm{NRL} = \frac{\sum_{j=1}^{n} R_j}{\sum_{i=1}^{n} X_i}.$$

5.1.6 True positive rate

The TP rate is calculated by number of detected malicious node divided by total number of malicious nodes in the network $\times$ 100 %.

$$\mathrm{TPR} = \frac{N_{DM}}{T_{MN}} \times 100\,\%.$$

5.1.7 False positive rate

The FP rate is calculated by number of nodes wrongly detected as malicious node divided by total number of normal nodes in the network $\times$ 100 %.

$$\text{FPR} = \frac{N_{FDM}}{T_{NN}} \times 100\,\%.$$

5.2 Packet delivery rate

It can be seen in Fig. 8, the average PDR for all mobility speed by AODV is about 96.99 % in the absence of a malicious node. When smart gray hole attack (SGAODV) is launched, the average PDR of SAODV is about 95.41 %. This is due to its normal behaviour in the route discovery but selective packet dropping of the data packets. When proposed approach is employed, the average PDR for all mobility speed is about 96.55, 96.56 and 95.68 % when packet drop threshold value is set to 1, 2 and 4 % of total data packets respectively. It can also be seen in Fig. 9, when there are two smart malicious nodes in the network, the PDR of SGAODV is about 93.69 %. When proposed approach is used by G-IDS, the average PDR for all mobility speed is about 95.31, 95.04 and 94.74 % when packet drop threshold value is set to 1, 2 and 4 % of total data packets respectively. It can be seen from the graph that our mechanism is able to improve the PDR of network under smart gray hole attack.

5.3 Packet loss rate

It can be seen in Fig. 10, the total average PLR for all mobility speed by AODV is about 2.99 % in the absence of a malicious node. When smart gray hole attack (SGAODV) is launched, the total average PLR of SAODV is about 4.59 %. This is due to its normal behaviour in the route discovery but selective packet dropping of the data packets. When proposed approach is employed, the total average PLR for all mobility speed is about 3.45, 3.44 and 4.31 % when packet drop threshold value is set to 1, 2 and 4 % of total data packets respectively. It can also be seen in Fig. 11, when there are two smart malicious nodes in the network, the total average PLR of SGAODV is about 6.31 %. When proposed approach is used by G-IDS, the total average PLR for all mobility speed is about 4.69, 4.96 and 5.26 % when packet drop threshold value is set to 1, 2 and 4 % of total data packets respectively. It can be seen from the graph that our mechanism has low PLR under smart gray hole attack in the network.

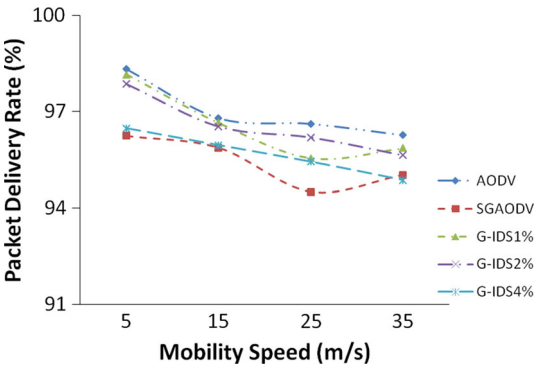

Fig. 8 PDR under one malicious node

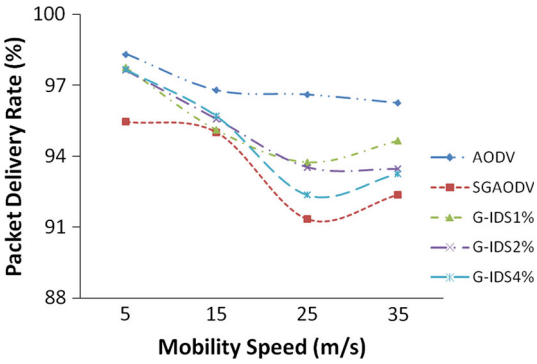

Fig. 9 PDR under two malicious nodes

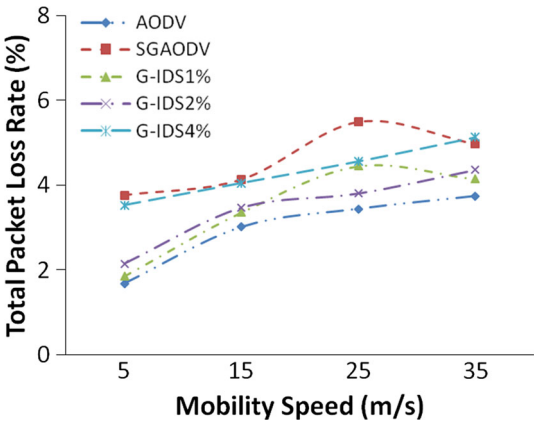

Fig. 10 Packet loss rate under one malicious node

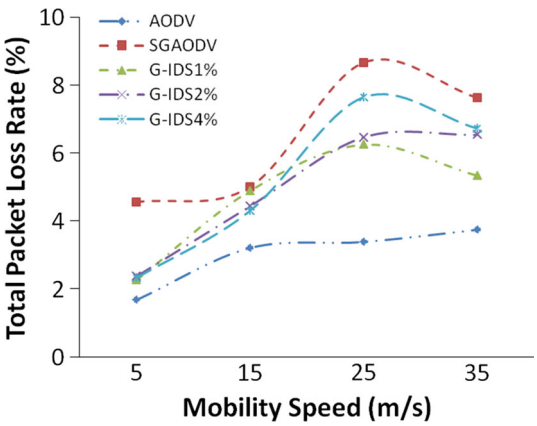

Fig. 11 Packet loss rate under two malicious nodes

5.4 Average throughput

From Fig. 12, it can be seen that the average throughput for all mobility speed by AODV is about 19.42 kbps in the absence of a malicious node. When smart gray hole attack (SGAODV) is launched, the average throughput of SAODV is about 19.09 kbps. This is due to its normal behaviour in the route discovery but selective packet dropping of the data packets. When proposed approach is employed in G-IDS, the average throughput for all mobility speed is about 19.30, 19.32 and 19.15 kbps when packet drop threshold value is set to 1, 2 and 4 % of total data packets respectively. It can also be seen in Fig. 13, when there are two smart malicious nodes in the network, average throughput of SGAODV is about 18.75 kbps. When proposed approach is used, the average throughput for all mobility speed is about 19.07, 19.02 and 18.93 kbps when packet drop threshold value is set to 1, 2 and 4 % of total data packets respectively. It can be seen from the graph that our mechanism is able to improve the average throughput of network under smart gray hole attack.

5.5 Routing overhead

Figure 14 shows that the routing overhead is increasing with the increase in mobility speed. The average routing overhead for all mobility speed by AODV is about 4600 control packets in the absence of a malicious node. When smart gray hole attack (SGAODV) is launched, the average routing overhead of SAODV is about 4664 control packets. When proposed approach is employed in G-IDS, the average routing overhead for all mobility speed is about 4694, 4753 and 4549 control packets when packet drop threshold value is set to 1, 2 and 4 % of total data packets respectively. It can also be seen in Fig. 15 that the routing overhead in case of two malicious nodes is increasing with the increase in the mobility speed. When there are two smart malicious nodes in the network, average routing overhead of SGAODV is about 4734. When proposed approach is used in G-IDS, the average routing overhead for all mobility speed is about 4837, 4766 and 4686 control packets when packet drop threshold value is set to 1, 2 and 4 % of total data packets respectively. It can be seen from the graph that with the increase in the mobility speed the

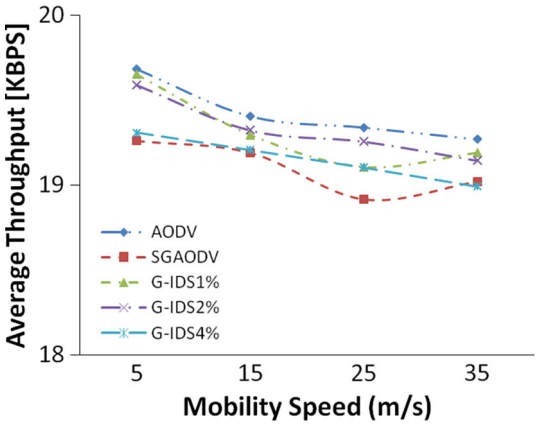

Fig. 12 Average throughput under one malicious node

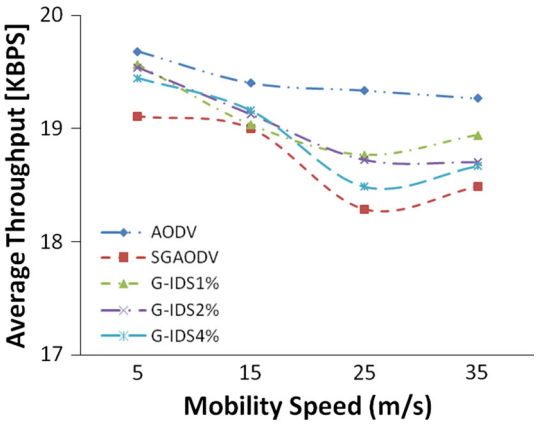

Fig. 13 Average throughput under two malicious node

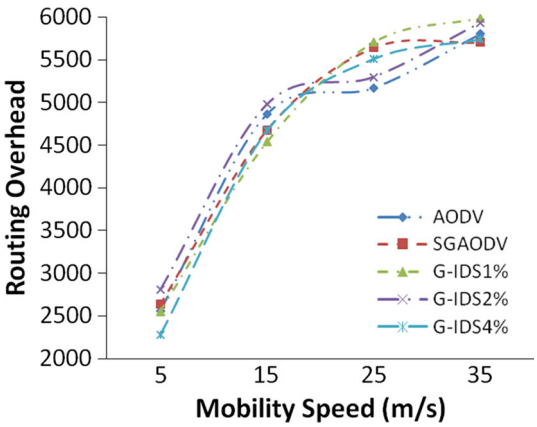

Fig. 14 Routing overhead under one malicious node

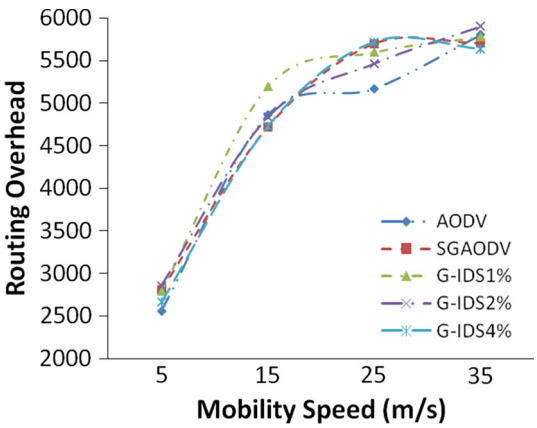

Fig. 15 Routing overhead under two malicious nodes

routing overhead of proposed approach is also increasing and moving parallely with that of standard AODV.

5.6 Normalized routing load

Figure 16 shows that the normalized routing overhead is increasing with the increase in mobility speed of the nodes. The average normalized routing load for all mobility speed by AODV is about 2.17 in the absence of a malicious node. When smart gray hole attack (SGAODV) is launched, the average normalized routing load of SAODV is about 2.24. When proposed approach is employed in G-IDS, the average normalized routing load for all mobility speed is about 2.23, 2.25 and 2.21 when packet drop threshold value is set to 1, 2 and 4 % of total data packets respectively. It can also be seen in Fig. 17 that the normalized routing load in case of two malicious nodes is increasing with the increase in the mobility speed. When there are two smart malicious nodes in the network, average normalized routing overhead of SGAODV is about 2.34. When proposed approach is used, the average routing normalized load for all mobility speed is about 2.33, 2.30 and 2.27 when packet drop threshold value is set to 1, 2 and 4 % of total data packets respectively. It can be seen from the graph that with the increase in the mobility speed the normalized routing load of proposed approach is also increasing and moving parallely with that of standard AODV.

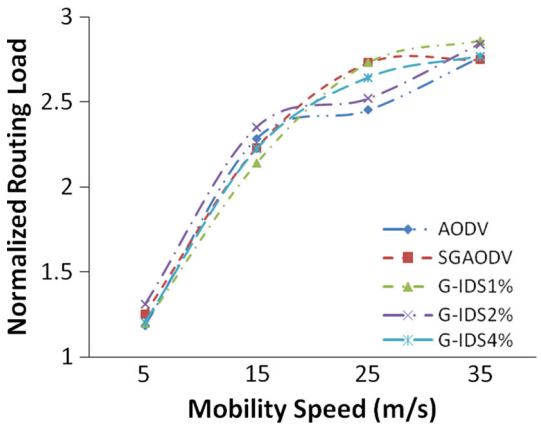

Fig. 16 Normalized routing overhead under one malicious nodes

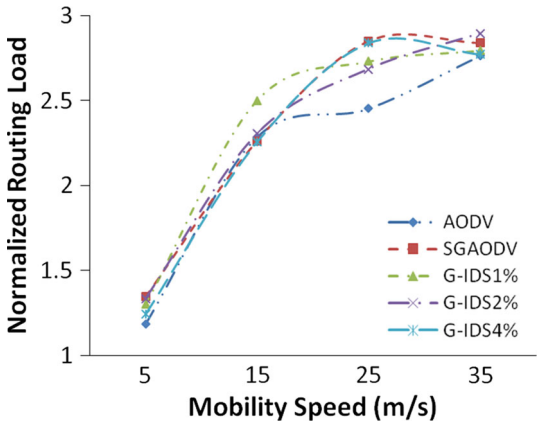

Fig. 17 Normalized routing overhead under two malicious nodes

Table 4 TP and FP rate for one malicious node

N	TP (%)	FP (%)
1	45	0.8
2	40	0.6
4	35	0

Table 5 TP and FP rate for two malicious nodes

N	TP (%)	FP (%)
1	40	1.2
2	35	0.8
4	30	0

5.7 True positive and false positive rate

In order to select optimal packet drop threshold value, we further calculated the average true positive and false positive rate for all mobility speed. When 1 % of total data packets is made as threshold value, it has been found that the true positive is about 45 % and false positive rate is about 0.8 %. When we set the threshold value to the 2 % of total data packets, it has been found that the true positive rate is about 40 % and false positive rate is about 0.6 %. When 4 % of total data packets is taken as threshold value, then it has been found that the true positive rate is about 35 % and false positive rate is about 0 % under one malicious node as shown in Table 4. In case of two malicious nodes, when 1 % of total data packets is made as threshold value, it has been found that the true positive is about 40 % and false positive rate is about 1.2 %. When we set the threshold value to 2 % of total data packets, the true positive rate is about 35 % and false positive rate is about 0.8 %. When 4 % of total data packets is taken as threshold value, then the true positive rate is about 30 % and false positive rate is about 0 % under two malicious node as shown in Table 5. From Tables 4 and 5, it can be seen that the optimal value for N is 4 i.e. the packet drop threshold value is 4 % of total data packets.

6 Performance comparison with existing scheme

In this section, the performance of our proposed approach has been compared with the existing ABM scheme [17]. The comparison with existing scheme has been done by taking optimal packet drop threshold value equal to 4 % of total data packets in our approach.

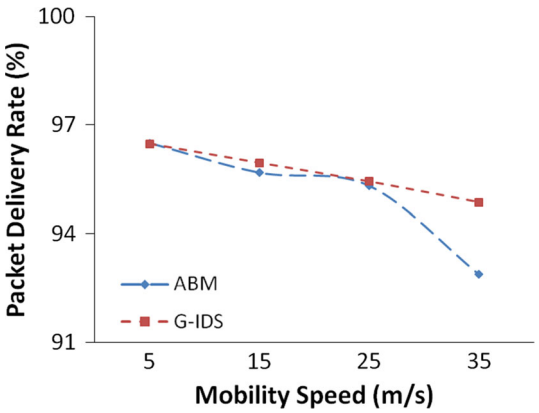

Fig. 18 PDR under one malicious node

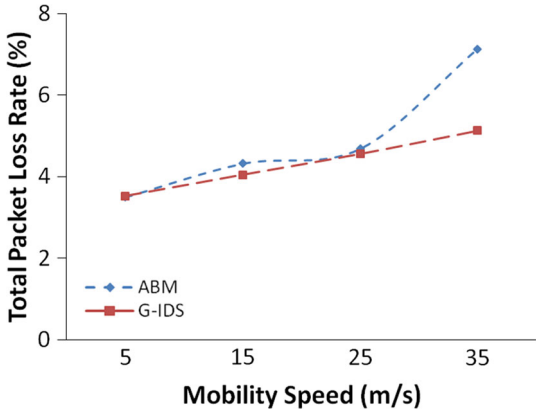

Fig. 20 Packet loss rate under one malicious node

6.1 Packet delivery rate

It can be seen in Fig. 18, the average PDR for all mobility speed in case of ABM is about 95.02 % in the presence of one smart gray hole node whereas in case of proposed approach, the average PDR for all mobility speed is about 95.68 %. It can also be seen in Fig. 19, when there are two smart gray hole nodes in the network, the PDR in case of ABM is about 93.45 % whereas in case of proposed approach, the average PDR for all mobility speed is about 94.74 %. It can be seen from the graph that our mechanism is having better performance as compared with ABM.

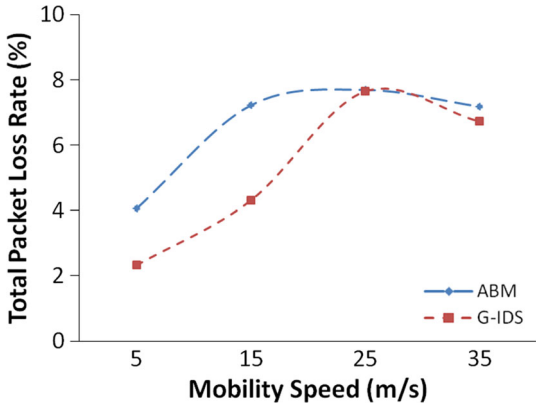

Fig. 21 Packet loss rate under two malicious nodes

6.2 Packet loss rate

It can be seen in Fig. 20, the average packet loss rate for all mobility speed in case of ABM is about 4.97 % in the presence of one smart gray hole node whereas in case of proposed approach, the average packet loss rate for all mobility speed is about 4.31 %. It can also be seen in Fig. 21, when there are two smart gray hole nodes in the network, the average packet loss rate in case of ABM is about 6.54 % whereas in case of proposed approach, the average packet loss rate for all mobility speed is about 5.26 %. It can be seen from the graph that our mechanism is having less packet loss as compared with ABM.

6.3 Average throughput

It can be seen in Fig. 22, the average throughput for all mobility speed in case of ABM is about 19.03 kbps in the

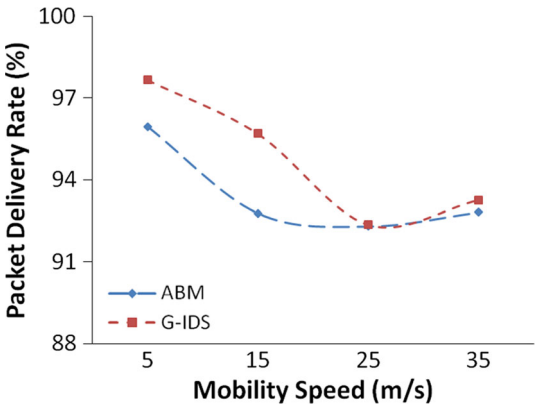

Fig. 19 PDR under two malicious nodes

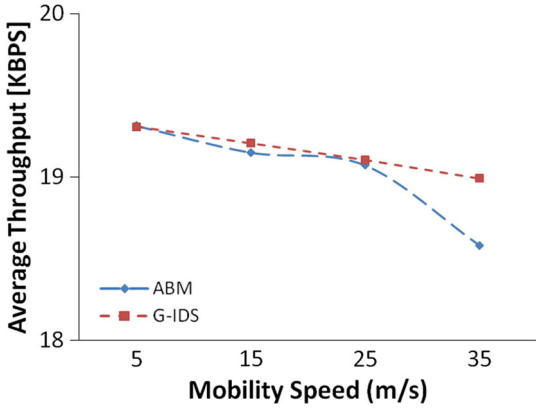

Fig. 22 Average throughput under one malicious node

presence of one smart gray hole node whereas in case of proposed approach, the average throughput for all mobility speed is about 19.15 kbps. It can also be seen in Fig. 23, when there are two smart gray hole nodes in the network, the average throughput in case of ABM is about 18.69 % whereas in case of proposed approach, the average throughput for all mobility speed is about 18.93 %. It can be seen from the graph that our mechanism is having better throughput as compared with ABM.

6.4 Routing overhead

Figure 24 shows that the routing overhead is increasing with the increase in mobility speed. The average routing overhead for all mobility speed in case of ABM is about 4482 control packets in the presence of a one smart gray hole node whereas in case of proposed approach, the average routing overhead for all mobility speed is about 4549 control packets. It can also be seen in Fig. 25 that the routing overhead in case of two malicious nodes is increasing with the increase in the mobility speed When there are two smart gray hole nodes in the network, average routing overhead in case of ABM is about 4416 control packets whereas in case of proposed approach, the average routing overhead for all mobility speed is about 4686 control packets. The slight increase in routing overhead in our approach is due to broadcasting of ALERT packets in the network.

6.5 Normalized routing load

Figure 26 shows that the normalized routing overhead is increasing with the increase in mobility speed. The average NRL for all mobility speed in case of ABM is about 2.18 in the presence of a one smart gray hole node whereas in case of proposed approach, the average NRL for all mobility speed is about 2.21. It can also be seen in Fig. 27 that the average NRL in case of two smart gray hole nodes is increasing with the increase in the mobility speed When there are two smart gray hole nodes in the network, the average NRL for all mobility speed in case of ABM is about 2.14 whereas in case of proposed approach, the average NRL for all mobility speed is about 2.27.

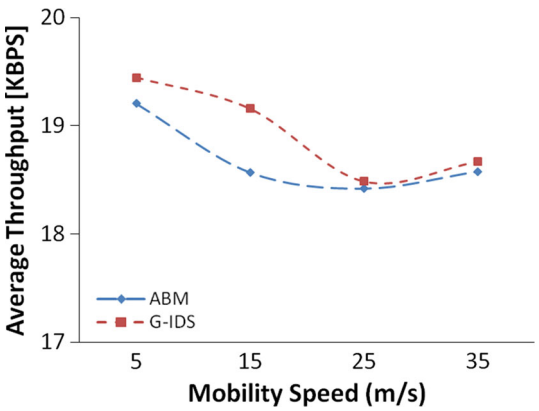

Fig. 23 Average throughput under two malicious node

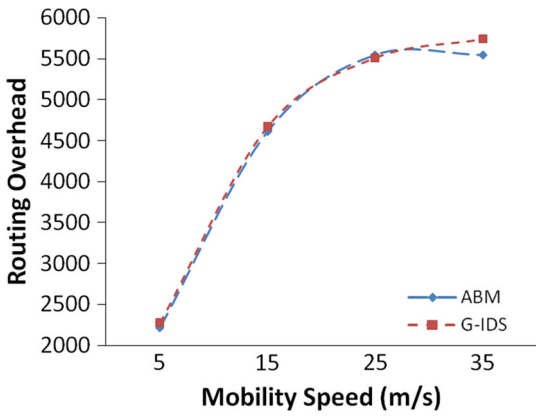

Fig. 24 Routing overhead under one malicious node

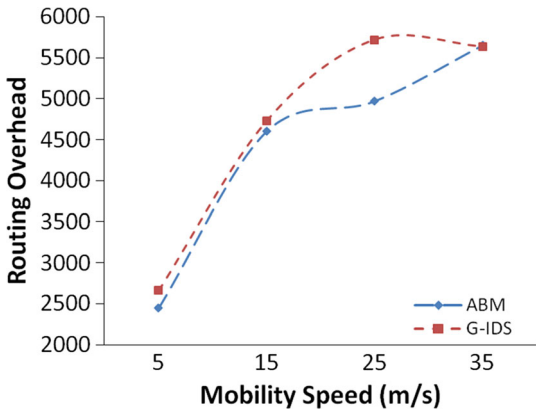

Fig. 25 Routing overhead under two malicious nodes

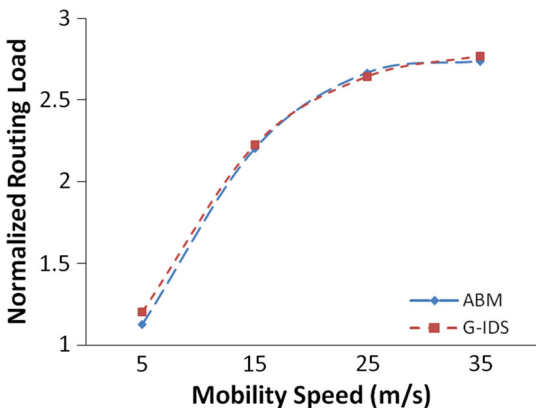

Fig. 26 Normalized routing overhead under one malicious nodes

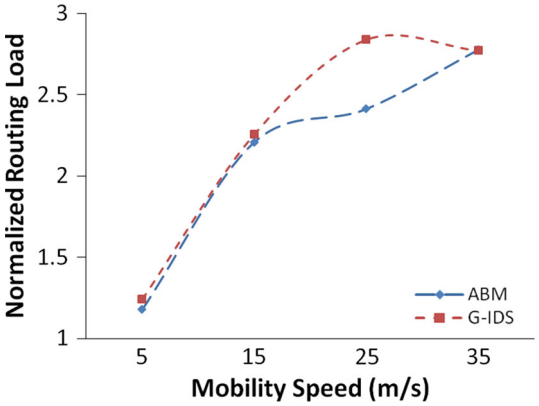

Fig. 27 Normalized routing overhead under two malicious nodes

6.6 True positive and false positive rate

In case of G-IDS, the TP is 35 % and FP is 0 % for one smart gray hole node in the network whereas in case of ABM, the TP is 0 % and the FP rate is 0 %. In case of two smart gray hole node, the TP of G-IDS is 30 % and the FP rate is 0 % whereas in case of ABM, the TP rate is 0 % and the FP rate is 0 % as depicted in Table 6.

7 Advantages and shortcomings of proposed approach

The proposed approach has following advantages: (1) It can deal with smart gray hole attack in which the malicious node participates correctly in route discovery and then drops selective data packets whereas the existing schemes in the available literature deal with sequence number based gray hole attack in which the gray hole node gives false route reply and drops selective data packets and hence cannot deal with smart gray hole attack. (2) Our proposed approach can deal with sequence number based attack because G-IDS nodes notify to the other nodes in the network about the identity of malicious node if the dropping of data packets are greater than threshold value. (3) The proposed approach not only detect the malicious nodes but also isolate the malicious nodes forever by notifying its identity to the nodes in the network. (4) Our approach doesn't use any additional control packet to detect the malicious node in the network. The proposed approach has the following shortcomings: (1) G-IDS nodes are the special nodes which have to be placed properly in the network in such a way that at least one G-IDS is within its transmission range in order to forward ALERT packet to each other in the network. The gray hole attacker will not be detected and blocked if it is outside the range of all G-IDS node due to improper placement of these special nodes. (2) These special nodes are fixed in the network and therefore cannot move. (3) G-IDS nodes have to placed in such a way to cover most of the simulation area. (4) With the increase in the size of the network area, more number of special nodes will be required in order to have maximum coverage of the network area.

Table 6 TP and FP rate for one and two malicious node

TP (G-IDS) (%)	TP (ABM) (%)	FP (GIDS) (%)	FP (ABM) (%)
35	0	0	0
30	0	0	0

8 Conclusion

In a MANET, each node cooperates with each other in order to provide multi-hop communication between source and destination. However there are some nodes who do not cooperate in forwarding the data packets and perform selective packet dropping which is known as gray hole attack. The gray hole attack can be sequence based or smart based. In sequence based, the gray hole node gives false route reply due to which it attracts the traffic towards itself and performs selective packet dropping but in case of smart gray hole attack, the attacker participates normally in route discovery and after getting data packets from the source nodes, it performs selective packet drop. In order to deal with the smart gray hole attack, we have proposed a new mechanism MGAM that mitigates the impact of the smart gray hole attack. The simulation results show that our proposed mechanism improves the network performance in terms of PDR, PLR and average throughput. We experimentally proved that the optimized packet drop threshold value at 4 % of total data packets is the best choice as the detection rate of malicious node is at least 30 % with 0 % false positive rate in the network. Moreover, we have also compared our scheme with the existing scheme which shows that our scheme is slightly better as compared with the existing one in terms of PDR, PLR and Average Throughput.

As a future work, we are planning to improve this approach by designing a new mechanism in which no special nodes will be deployed and normal mobile nodes will be chosen as a special nodes dynamically which will have the functionality of G-IDS nodes and will also cover most of the simulation area.

Acknowledgments The first author would like to thank Department of Electronics and Information Technology (DEITY), Government of India, for providing financial support to carry out the research work. The authors would also like to thank the anonymous reviewers and the editors for giving valuable suggestions in improving this paper.

References

1. Funde, R., & Chandre, P. (2015). Dynamic cluster head selection to detect gray hole attack using intrusion detection system in MANETs. In *Proceeding of ICCCT '15, ACM*, September 25–27, 2015. Allahabad, India. http://dx.doi.org/10.1145/2818567.2818581.
2. Murthy, C. S. R., & Manoj, B. S. (2004). *Ad hoc wireless networks: Architectures and protocols.* Prentice Hall PTR.
3. Sharma, B. (2015). A distributed cooperative approach to detect gray hole attack in MANET. In *Proceeding of WCI, ACM*, Kochi, India. http://dx.doi.org/10.1145/2791405.2791433.
4. Deng, H. M., Li, W., & Agrawal, D. P. (2002). Routing security in wireless ad hoc networks. *IEEE Communication Magazine, 40*(10), 70–75.
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. Heydari, V., & Yoo, S.-M. (2015). E2EACK: An end-to-end acknowledgment-based scheme against collusion black hole and slander attacks in MANETs. *Springer Wireless Network, New York*. doi:10.1007/s11276-015-1098-6.
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 & Communication Technologies.*
9. Shila, D. M., Cheng, Y., & Anjali, T. (2010). Mitigating selective forwarding attacks with a channel-aware approach in WMNs. *IEEE Transactions on Wireless Communications, 9*(5), 1661–1675.
10. Jhaveri, R. H., & Patel, N. M. (2015). A sequence number based bait detection scheme to thwart gray hole attack in mobile ad hoc networks. *Springer Wireless Network, 21*, 2781–2798. doi:10.1007/s11276-015-0945-9.
11. Vani, A., & Jadhao, M. M. (2013). Eliminating co-operative black hole and gray hole attacks using modified EDRI table in MANET. In *Proceeding of IEEE International Conference on Green Computing, Communication and Conservation of Energy (ICGCE)*, pp. 944–948.
12. Mohanapriya, M., & Krishnamurthi, I. (2014). Modified DSR protocol for detection and removal of selective black hole attack in MANET. *Elsevier Computers and Electrical Engineering, 40*, 530–538.
13. Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000) Mitigating routing misbehavior in mobile adhoc networks. In *Proceedings of MOBICOM'2000,* pp. 255–265.
14. Ramaswamy, S., Fu, Hu., Sreekantaradhya, M., Dixon, J., & Nygard, K. (2003). Prevention of cooperative black hole attack in wireless ad hoc networks. In *Proceedings of ICWN'03*, pp. 570–575.
15. Shahabi, S., Ghazvini, M., & Bakhtiarian, M. (2015). A modified algorithm to improve security and performance of AODV protocol against black hole attack. *Springer Wireless Network*. doi:10.1007/s11276-015-1032-y.
16. Gurung, S., & Saluja, K. K. (2014). Mitigating impact of blackhole attack in MANET. In *Proceedings 5th International Conference on Recent Trends in Information, Telecommunication and Computing*, pp. 229–237. doi: 02.ITC.2014.5.560.
17. Banerjee, S. (2008). Detection/removal of cooperative black and gray hole attack in mobile ad hoc networks. In *Proceedings of the World Congress on Engineering and Computer Science, WCECS*, October 22–24, SanFrancisco, USA.
18. Su, M. Y. (2011). Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. *Elsevier Computer Communication*.
19. Sen, J., Chandra, M. G., Reddy, H., & Balamuralidhar, P. (2007). A mechanism for detection of gray hole attack in mobile ad hoc network. In *Proceedings of the IEEE ICICS*.
20. The network simulator-ns-2. (2015). 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 Assitant Professor (Computer Engineering) in Jawaharlal Nehru Government Engineering College, Sundernagar, Himachal Pradesh 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 and network security.

Dr. 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 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.