A Scheme for Finding and Blocking Black Hole Nodes in Mobile Ad Hoc Networks

Zulfiqar Ali Zardari[1], Jingsha He[1,2], Nafei Zhu[1], Muhammad Salman Pathan[1], Muhammad Qasim Memon[3], Muhammad Iftikhar Hussain[1], Peng He[1] and Chengyue Chang[4]

(Corresponding author: Nafei Zhu)

Faculty of Information Technology, Beijing Engineering Research Center for IoT Software and Systems[1]
Beijing University of Technology, Beijing 100124, China
College of Computer and Information Science, China Three Gorges University[2]
Advanced Innovation Center for Future Education, Beijing Normal University[3]
Machinery Industry Information Center, Beijing 100823, China[4]
(Email: znf@bjut.edu.cn)

(Received Dec. 8, 2018; Revised and Accepted May 18, 2019; First Online Spet. 8, 2019)

Abstract

Security of wireless nodes are a major concern in mobile ad hoc networks (MANETs). In this paper, we propose a scheme for detecting and blocking malicious nodes in MANETs. Our proposed scheme relies on specially deployed nodes called FBS nodes to continuously monitor the behaviour of the network nodes. When an FBS node detects a node that exhibits suspicious behaviour, it declares that node as a black hole node. Afterwards, all data and control messages from that node will be discarded. Experiment results show that the proposed scheme can reduce the number of packets dropped by malicious nodes with a low false positive rate.

Keywords: AODV; Blackhole Node; FBS Nodes; Mobile Ad Hoc Network; Throughput

1 Introduction

MANET is a class of wireless networks in which nodes don't rely on a centralised infrastructure to communicate with each other. When nodes lie within the transmission range of each other, they can communicate directly. Otherwise, nodes will rely on the help of other intermediate nodes to realise communication, thus forming a multi-hop communication paradigm. In MANET nodes are independent, can connect anytime and anywhere in the network. Meanwhile, nodes have limited memory, limited energy power, and limited bandwidth. There is no fixed architecture, so nodes act as host well as a router to transfer the data packets to the destination node. Due to the mobility of the nodes, continuous change occurs in the topology. Nodes communicate with each other with different routing protocols to perform the networking function to transmit the data packets from source to destination node [12, 21, 30]. MANET possess various characteristics such as dynamic topology, the absence of central control, shared media, *etc.* MANET can be used in special environments such as emergency operation, battlefields and rescue operations where the rapid deployment of a wired network is difficult.

MANET have various malicious threat such as denial-of-service (DoS) [6, 18, 22]. One type of DoS attacks can be realized in MANETS in which a malicious node provides false routing information during the route finding process to mislead the source node to select an active route to the destination that includes the malicious node so that packet drop behaviour would occur [2, 8, 23]. A DoS attack of this kind is called a black hole attack in which a malicious node drops all the data packets that pass through it. Before data transmission, when a source node wants to send data packets to a destination node, the source node would first check its routing table for any fresh routes heading to destinations node. If no such routes exist, the source node will broadcast an RREQ packet in the network to search for an optimal path. All intermediate nodes, upon receiving the RREQ packet, checks their routing tables for a fresh route to the destination. If no such routes exist, they would further send the RREQ packets to their neighbours that incorporate a hop count number and a destination sequence number in the RREQ packet. Eventually, after receiving the RREQ packet, the destination node sends an RREP packet back to the source node through intermediate nodes that have a fresh route to the destination node.

The choice of an RREP packet by the source node heavily depends on the destination sequence number contained in the packet. If the destination sequence number in an RREP packet is high, the RREP is considered to be optimal. A black hole node always replies to the source node with a very high fabricated destination se-

quence number to distract the source node by choosing the route that includes the black hole node as the fresh path to the destination. Then the black hole node drops all the packets that it gets [4, 10, 20]. Black hole attacks can be launched by a single node or through collaboration. In a single-node black hole attack, only one malicious node is involved, whereas, in a collaborative black hole attack, two or more black hole nodes work in collaboration to disrupt the normal operation of the network. In collaborative black hole attack, two malicious nodes collaborate to commit malicious activities [14, 27, 29].

Many approaches have been proposed in recent years for the detection of collaborative black hole attacks. But few have provided improved results [11, 28]. Although some proposed techniques, such as location-based, trust-based, acknowledgement-based, fuzzy logic and sequence number based, can detect black hole attacks [9, 13, 17, 24, 25], they exhibit the following drawbacks:

- Unable to detect multi-node black hole attacks;
- Unable to detect collaborative black hole attacks;
- High routing overhead and delay;
- Unable to handle the mobility of the nodes.

This paper proposes an improved solution called FBS that can find and isolate collaborative black hole nodes in MANETs. The proposed FBS scheme relies on monitoring nodes that are specially deployed in the network to detect malicious nodes. When a node exhibits any ambiguous behaviour, the monitoring nodes will suspect it to be a malicious node. The, an alert message is broadcast through the network notifying all other nodes about the identity of the malicious node. The proposed FBS scheme has the following advantages and characteristics:

- Monitoring nodes are deployed to cover the entire network and continuously exchange information with each other to cope with the issues of node mobility.
- FBS provides an efficient way of detecting and blocking single and collaborative black hole nodes by incorporating an investigation table.
- FBS improves network performance in the following aspects: Very low false positive rate, high throughput, packet delivery ratio, minimum routing overhead and lower average delay, as compared to existing schemes.
- FBS nodes don't take part in the normal routing process, resulting in higher computation and energy efficiency.

The rest of this paper is organized as follows. Section 2 explains the recent approaches related to the field of interest. Section 3 describes the proposed scheme and explains its functionalities and algorithms. Section 4 presents detailed experimental results. Finally, Sections 5 concludes the paper.

2 Related Works

Jhaveri *et al.* proposed an approach based on the highest threshold value of sequence number to isolate the malicious node [13]. The sequence number based detection scheme (SNBDS) includes three different modes of malicious attacks and have different false routing and selective packet drop attack methods. During routing, the threshold value for the sequence number is calculated at each node. If the difference between the destination sequence numbers in the RREP packet of a particular node is greater than the threshold value of the sequence number, the node is declared as suspicious. A bait request packet (RREQ) with a nonexistent destination address and the destination sequence number is then sent to the suspicious node to confirm its status. If it replies, it is declared as a malicious node. The detection mechanism in this scheme heavily depends upon the bait request. Thus, if the node doesn't respond to the bait request, this mechanism would fail. A lot of control packets are generated in this approach to detect malicious nodes.

Vishvas *et al.* proposed an algorithm to detect a malicious node based on its trust and energy status [16]. The trust value and energy status of a node are used to identify the behaviour of a node. Initially, all the nodes are assigned a trust value of 0.5. A node trust value increases gradually from 0.5 to 1 depending on its packet forwarding behaviour. Energy model calculates the energy of every node in the network as it is assumed that nodes that have high energy values don't participate in the network by not forwarding any kind of data packets further. So, whenever the source node wants to send data packets to the destination node, it only chooses the nodes that have a high value of trust and an energy level that is not greater than a set threshold. The nodes have low trust values, and high energy values are considered as malicious nodes. Due to the dynamic nature of MANETs, some nodes may drop a certain amount of packets because of frequent link breakages, so this mechanism has a high false positive aspect.

Abdelhaq *et al.* proposed the local intrusion detection (LID)-AODV mechanism to find the black hole attack in MANETs [1]. Whenever any node sends RREP packet back to the source node, an intermediate node along the path gets the RREP packet and sends further route request FREQ to the next hop node (NHN) of the sending node. After getting the further route reply FRREP from the NHN node, the intermediate node along the path checks to see whether the NHN node has a valid route to the destination. If it has a valid route, then a node sending the RREP is considered as a normal node. Otherwise, it is a black hole node. The scheme completely fails in the collaborative black hole scenario, where one black hole node behaves as genuine and forwards all the data packets to other collaborative nodes.

Dorri proposed a method to eliminate collaborative malicious nodes from the network by incorporating extended data routing information (EDRI) tables in the

AODV routing protocol [7]. Each EDRI table contains three fields, *i.e.*, FROM (the number of packets received form NHN node), THROUGH (the number of packets sent through the NHN node) and BHN (the black hole node status). Every node maintains the EDRI list to update the status of NHN node. Whenever the source node receives an RREP packet, it checks the EDRI table of each node. If the difference between FROM and THROUGH values exceeds a certain threshold, then the node is considered as a black hole node. A dummy data control packet is further sent to the suspected node to confirm its status. A black hole node will drop the packet, so its status will be confirmed as normal. To avoid false positive rates, every node maintains an extra table to identify the malicious node and sends extra control packet which increases the routing overhead and end to end delay factors.

Kollati *et al.* proposed an algorithm by integrating Integrated Bloom Filter into watchdog algorithm for the detection of the malicious node [15]. A certificate authority (CA) is used in this approach to identify the malicious behaviour of a node by key generation and verification with hashing techniques. During packet forwarding, when a node forwards a data packet, it also embeds a hash value into it. If the hash value between two nodes is not the same, a node is considered as a black hole node as it drops a certain amount of packets. The black hole list is then updated by the CA and the identity of the black hole node is shared in the network so that any kind of transaction is avoided in the future. Extra computation and end to end delay are involved during routing. The obvious mobility conditions can make a node drop some amount of packets, resulting in different hash values, causing a high false positive rate in his approach.

Nissar *et al.* proposed an authentication based scheme to secure MANET using AODV routing protocol against routing attacks [19]. This scheme works in two phases, *i.e.* secure route request phase and secure route reply phase. In the scheme, it is assumed that all the nodes share their public keys with other nodes so that digital certificates can update a repository of nodes. During the first phase, the source node sends the RREQ message in the network by embedding its digital signature. When an intermediate node receives the RREQ packet, it checks the signature in it and, only after verification is successful, does it send further the RREQ by embedding its signature. Otherwise, the RREQ is considered as malicious. During the second phase, when an intermediate node having a fresh route or destination itself sends back RREP, it embeds its private key into the RREP packet. All the intermediate nodes in the reverse path authenticate the key by the sender. If the pattern is correct, it is further sent back to reverse path, else dropped as considered by the malicious node. A high end to end delay is present in this approach

Saluvala *et al.* proposed a technique that provides an authentication mechanism for every node in the network participating during routing in MANETs [3]. Each node in the network, before broadcasting RREQ further, adds 1's complement of its IP address. The receiving node authenticates the RREQ packet of its source by adding the appended one's compliment and source IP address to it to get all ones. For any node not aware of ones compliment of its IP address, all the packets from the node are dropped.

Baqer *et al.* proposed a secure trust-based approach based on the safety status of an RREP packet during routing [5]. Each node in the network maintains two tables, *i.e.*, trust level and malicious node tables. Initially, every node is considered as a trusted node in the network. When an intermediate node in the network receives an RRRP packet, the malicious table is inquired to check if the identity of the RREP packet is already listed as a black hole node. If it is, the RREP packet is dropped. Otherwise, a security procedure is adopted based on the destination sequence number of the node. If the node provides a fabricated destination sequence number that exceeds the threshold value, the trust value of the node is decremented and updated in the list. All the nodes having trust values below one are considered as black hole nodes and included in the malicious node list table.

Thanuja *et al.* proposed a method to avoid collaborative black hole attack by using data routing information (DRI) table [26]. Each node maintains a DRI table to update the information of packet forwarding of its NHN node. When the source node gets an RREP packet from an intermediate node, it checks the DRI table of that node to judge the number of packets is received and then forwarded. If the difference between FROM and 'THROUGH' fields exceeds the set threshold, then the node is considered as a black hole node. Furthermore, a FREQ packet is sent to the malicious nodes NHN to identify the identity of any collaborative black hole node. If the NHN's difference also exceeds the threshold and it doesn't contain any valid route towards the destination, then the nodes are considered as being working in collaboration. An alert packet is then broadcast in the network by the source node with the identities of the malicious nodes.

The proposed FBS scheme is different from the above existing approaches. In this scheme, we don't use beacon messages, bait requests or extra packets to check whether a route is safe. Due to extra routing overhead and delays in the network, some of the existing solutions don't detect collaborative black hole nodes, whereas the FBS scheme can detect collaborative black hole nodes with a very low false positive rate. Moreover, the detection rate of black hole nodes of the proposed scheme is high as compared to the other approaches.

3 The Proposed Finding and Blocking Scheme

The proposed finding and blocking scheme (FBS) relies on the statistical investigation. When a source node wishes to communicate with a destination node, it broadcasts

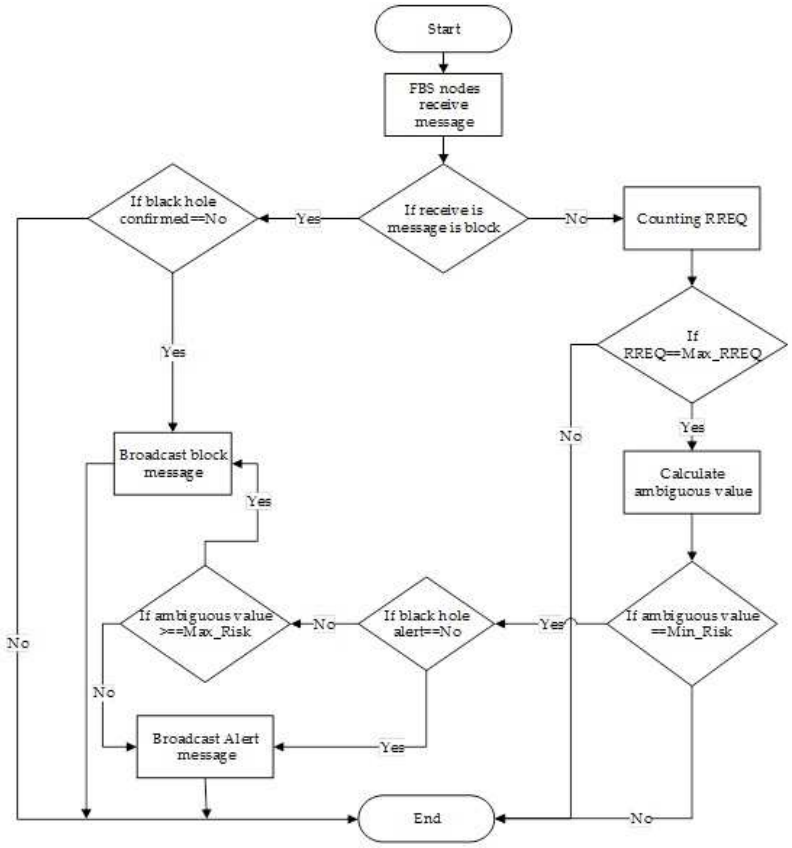

Figure 1: Flowchart of the proposed FBS scheme

RREQ packets in the network. After getting the RREQ packet, the RREP packet is sent back to the source node by an intermediate node having a fresh route to the destination or the destination node itself. In this process, whenever a black hole node gets the RREQ packet, it doesn't forward the RREQ further but sends back the RREP with the highest fake destination sequence number to distract the source node. Whereas in the collaborative attack, some of the RREQ packets are sent by a black hole node to its collaborator. The main intention of black hole nodes not forwarding RREQ is to drop all data packets during the communication process. To cope with this problem, special FBS nodes are employed in FBS which continuously monitors every node in the network in terms of the number of RREQ packets it forwards.

There are two types of nodes in the network. Regular nodes are the normal intermediate nodes which send data to other nodes to exchange the information between each other. Each node maintains a block table in which the identity of the malicious node is saved, broadcast by FBS node as shown in Table 1. All the packets coming from the malicious nodes are then blocked by regular nodes. FBS nodes are the nodes which detect the black hole nodes by some process running on them. Each FBS node maintains an investigation table according to which the decision is made about the status of the node as shown in Table 2.

The node position field describes whether the node is currently in the range of the FBS node. The nodes that move out of the range of the FBS node (i.e., whose RREQs cannot be detected by the FBS node) are set as inactive. According to Table 2, nodes 44 and 32 are active, whereas node 42 is inactive. The RREQ counting field shows that the neighbouring nodes 44, 32, and 42 have broadcast 5, 5 and 6 RREQs, respectively. The Ambiguous Value field in the investigation table represents the current ambiguous value of the respective node as calculated by the FBS node. The Blackhole Alert and Blackhole Confirmed fields show that this or any other FBS node has broadcast an Alert or Block message against the malicious node. The Alert and Block messages are shown in Table 3 and Table 4, respectively. According to the table, only node 42 is declared as a black hole alert, whereas no node is yet announced as a black hole. The primary objective of the FBS nodes is to detect the malicious behaviour of nodes in the network.

The proposed scheme performs the following four tasks:

Maximum request count. At any point when the RREQ count of an individual node reaches the maximum request count, FBS node starts calculating the ambiguous value in the investigation table for each node. Maximum request count is calculated to find any black hole node which is not forwarding the RREQ to neighbour nodes.

Minimum request count. During ambiguous value calculation, if an FBS node finds a node with RREQ

Table 1: FBS investigation table

Node Position	Node ID	RREQ Counting	Ambigious Value	Black Hole Alert	Black Hole Confirmed
Active	44	5	0	No	No
Active	32	5	0	No	No
Inactive	42	6	3	Yes	No

Table 2: Block message

Malevolent Node	FBS Broadcaster Node
51	54

Table 3: Alert message

Malevolent Node	FBS Broadcaster Node
52	53

Table 4: Block table

Malevolent Node ID	FBS Node
51 & 52	54

counts less than minimum request count but positions as active, the ambiguous value id is incremented for that node.

Minimum risk. At any point when the node's ambiguous value is equivalent to minimum risk, an FBS node broadcasts an alert message through the network to notify other FBS nodes. This value is set to half of the maximum risk.

Maximum risk. At any point when the node's ambiguous value is equivalent to maximum risk, an FBS node broadcasts a block message through the network to inform other FBS and regular nodes about the identity of the malicious node.

The following parameters of the FBS node are used for different purposes: Route request count, Ambiguous value, Alert message, and Block message.

Route request count. When an FBS node receives an RREQ packet, it starts counting the RREQs. Each FBS node maintains it's neighbours record in the investigation table. Firstly, it checks whether RREQ sent by a node is already present in the table. If not, it would insert the identity of the fresh entry into the table, and the node position is set as an active node, RREQ Counting to 1, ambiguous value to 0 and black hole alert and black hole confirmed value to NO. If the broadcasting node ID is already in the investigation table, the FBS node will check the black hole confirmed status of the node. If it is yes, then the node is already declared as a black hole, and there is no need to further do any processing. If the black hole confirmed field is NO, then it checks the node position filed in the investigation table and changes it to active if it is inactive. Also, the RREQ count is incremented by one. When the newly obtained value is less than the maximum request count, the process terminates. However, if the value is equal to the maximum request count, the FBS node will start calculating the ambiguous value process. Following is the algorithm for the route request count PROCESS.

Ambiguous value. Ambiguous value is very important in identifying black hole nodes. Ambiguous value process checks all the nodes in the investigation table whose status is active. If the RREQ value of a node is less than the minimum request count, the ambiguous value of that node is incremented. After the increment, if it is equal to minimum risk value and black hole field is NO, the FBS will broadcast an alert message through the network, which includes malicious node ID and its ID, and change the black hole confirmed field of that node to YES. This process continues until all the remaining nodes status is saved in the investigation table. If the new ambiguous value is equal to maximum risk value and black hole confirmation is NO, then a block message is forwarded by the FBS node, which will change the status of black hole confirmation to YES. To reduce the false positive rate (FPR), if a node that has ambiguous value more than zero and acts as a regular node, *i.e.* RREQ forwarded is more than minimum request count, its ambiguous value is decremented, which will decrease the chance of a regular node being declared as a black hole node.

Alert message. When the ambiguous value reaches the minimum risk value, FBS node will send an alert message if it is not previously sent. When this message is received by any regular node, it ignores the message. However, when the FBS node receives an alert message, it finds the malevolent node ID (contained in the alert message) into its investigation table. If the ID is not found, a new entry is created for it, and the ambiguous value is set to the minimum risk value, and the black hole alert is set to YES. The FBS node again broadcasts the alert message. If the investigation table already holds the malevolent node ID, then the black hole alert field is checked. If this field is YES, it indicates that FBS already broadcast the alert message and the process is terminated. If the alert field is NO, then the ambiguous value of the malevolent node is fixed to the minimum risk, and black hole alert is fixed as YES. The purpose of

the alert message is to inform other FBS nodes of the black hole node in the network. Due to the mobility of nodes in MANETs, nodes change their location from one position to another frequently. To cope with this mobility issue, each FBS node shares the information about that node with other FBS nodes, and they are deployed in such a way that they can reach each other. So, if a node changes its location, another FBS node has already had the information of that particular node. Therefore, it can be easily detected wherever it is in the network.

Block message. When the ambiguous value of a node reaches the maximum risk, the FBS node sends a block message (if not previously sent). When a block message is received from FBS node by a regular node, the malevolent ID and broadcaster FBS nodes ID is inserted in the block table by a regular node if they are not added yet.

Meanwhile, when an FBS node receives a block message, it will check the malevolent node ID in its investigation table. If ID doesn't exist in the investigation table, a new entry is inserted in the table and the ambiguous value set to the maximum risk value and black hole alert and confirmation fields set to YES. The FBS node then rebroadcasts the block message. If the malicious node ID is already present in the investigation table, its black hole confirmed field is checked. If the black hole confirmed field value is YES, then it means that the FBS node has already broadcast the block message for that malicious node and the process terminates. If black hole confirmed field is NO, then the malevolent nodes ambiguous value is set to the maximum risk value, black hole alert and confirmation are set to YES and block message is rebroadcast. The purpose of the block message is to inform the normal and FBS nodes in the network of the black hole attack and to spread the message throughout the network with the help of FBS nodes since normal nodes don't participate in broadcasting the block message. The FBS nodes ID is included in the alert message for authentication. Figure 1 is the flow chart of the proposed FBS scheme. When a FBS node receives any message, first it checks to see if the received message is a block message. If it is a block message, the FBS node will check its black hole confirmed value in the investigation table. If not, the FBS node will count RREQ packets of neighbour nodes. If the black hole confirmed value is YES, the FBS node then broadcasts the block message. Otherwise, the process terminates.

Meanwhile, if the RREQ is equal to Max_RREQ, then the FBS node calculates its ambiguous value. If the ambiguous value is equal to minimum risk, then the FBS node checks its black hole alert value. If black hole alert value is "YES", then it broadcasts the alert message if the value is "NO", then it checks its ambiguous value. If the ambiguous value is equal to or greater than the maximum risk, then it broadcasts a block message. Otherwise, it broadcasts an alert message and terminates the process.

Table 5: Simulation parameters

Parameter	**Value**
Network Simulator	NS-2(ver.2.34)
Dimension	1000?1000 m
Regular nodes	200
FBS nodes	9 (fixed)
Mobility model	The random walk mobility model
Simulation time	1000 s
Traffic type	CBR/UDP
Packet size	512 bytes
Mobility speed	0.5-01m/s
Pause time	5-20 s

4 Experiment and Analysis

NS-2 (ver.2.34) was utilized for network simulation to evaluate the performance of the proposed FBS scheme in which 200 regular nodes were deployed in a 1000×1000 m area with nine fixed FBS nodes located in such a way that they can cover all the network area. AODV routing protocol is used in this work. The traffic type constant bit rate (CBR) is used for non-connection oriented traffic model for sending the traffic. The total amount of time for the simulation is 1,000s, the mobility of the nodes varies from 5 to 35 m/s, and the size of the packets is 512 bytes. The transmission range is 250m for all the nodes in the network including the FBS nodes. The proposed FBS scheme is compared to three existing approaches, *i.e.*, the AODV routing protocol, Local Intrusion Detection AODV (LID-AODV) and Hybridization of particle swarm optimization with genetic algorithm (HPSO-GA), to demonstrate the performance of the proposed scheme under black hole attacks. The reason for selecting these approaches are these are similar to the proposed scheme. AODV routing protocol is appropriate for big networks, and it is widely used in literature in the last many years. HPSO-GA neighbor information is used for detection of black hole node, *i.e.* nodes data routing information (DRI). In LID-AODV approach it also takes the information from the previous node and after the next node to detect the malicious node. Whereas in our proposed scheme, special FBS monitoring nodes perform the detection of black hole node by route request RREQ packet from neighboring nodes. Table 5 lists the parameters involved in the simulation.

Detection rate. It is an important metric to show the efficiency of the proposed scheme in detecting malicious nodes. Figure 2 shows the detection rate of different techniques as compared to the proposed FBS scheme. The Figure 2 also shows the overall confidence interval 97% was calculated over ten replications. As can be seen from the Figure 2, the detection rate of the proposed FBS scheme is better than all the participating routing protocols, *i.e.*, 97.33%

at 200 nodes as compared to AODV, LID-AODV and HPSO-GA. In a comparative analysis, it was observed that there are 2.1%, 7.7% and 9.6% improvement in the detection rate of malicious nodes by FSB scheme than HPSO-GA, LID-AODV and AODV, respectively. The reason behind the improved detection rate lies in the efficient detection scheme by FBS nodes. The continuous information sharing among FBS nodes makes them aware of the nodes that frequently move from one position to another due to mobility in MANETs.

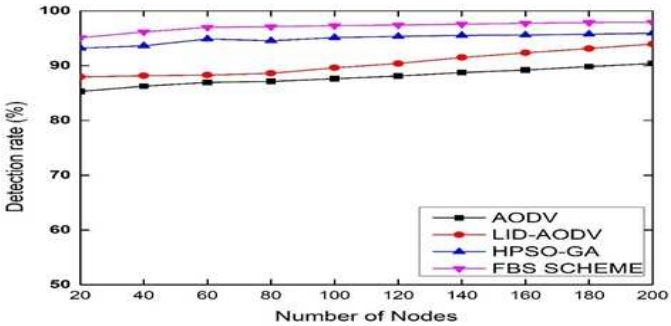

Figure 2: Detection rate (%)

Average delay. Figure 3 shows the average delay concerning time in seconds (sec). As the number of nodes increases in the network, there is an increase in the end to end delay in the network. Because of frequent malicious attacks and mobility conditions require protocols to perform various operations to detect malicious behaviour. A decrease of 0.19s, 0.11s and 0.5s in delay was achieved by the proposed FBS scheme as compared to HPSO-GA, LID AODV and AODV, respectively. Analysis indicates that the FBS scheme has lower end-to-end delay compared to other techniques due to efficient and early detection of black hole nodes in the network. Also, FBS nodes don't participate in normal routing, resulting in less computation in the network.

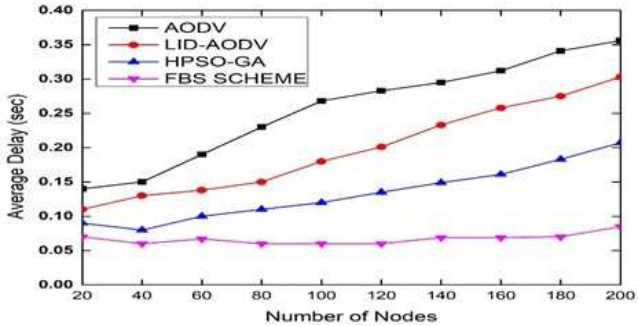

Figure 3: Average delay (%)

Packet delivery rate. Figure 4 shows the packet delivery rate (PDR) of all the participating routing protocols. As the number of nodes increases in the network, there is a drop in the packet delivery rate due to frequent packet drop attacks by malicious nodes. As can be seen from the figure, packet delivery rate of the proposed FBS scheme is higher than other techniques against black hole attacks due to early and efficient detection performed by the FBS nodes during the routing process. PDR of the proposed scheme is 97.45% per 200 nodes, an improvement of 2.49%, 6.93% and 9.21% compared to HPSO-GA, LID-AODV and AODV, respectively. The proposed FBS scheme provides a secure route to destinations with a very low number of malicious nodes during data transmission. Since FBS nodes are effective in the detection of black hole attack by removing malicious nodes from the network quickly, delivery of packets is increased.

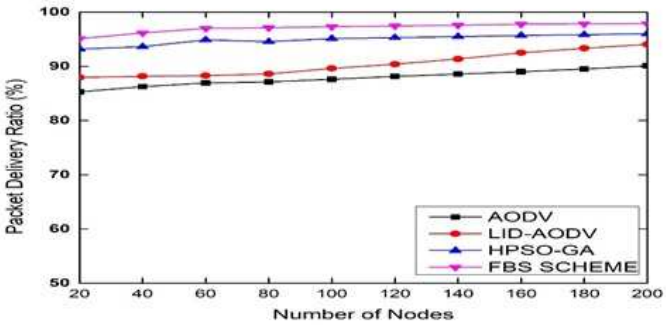

Figure 4: Packet delivery ratio (%)

Throughput. It can be seen from Figure 5 that the throughput of the proposed FBS scheme is much better than other techniques. The throughput of the proposed scheme is 78.9 kbps at 200 nodes, improving the throughput by 5.56%, 9.55%, and 14.92% over HPSO-GA, LID-AODV and AODV, respectively. The reason behind the improved results in the early detection of black hole nodes, which makes the routes to destinations better protected from black hole nodes in turn, increases the throughput by avoiding packet drops.

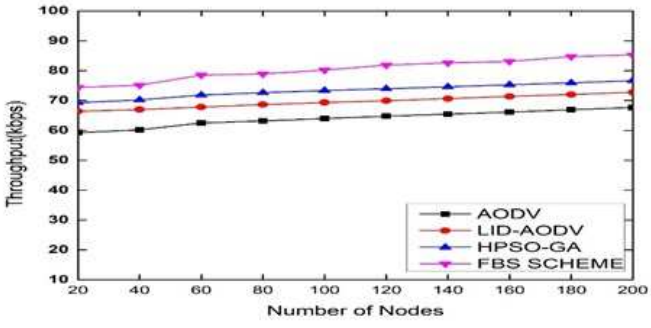

Figure 5: Throughput (%)

Routing overhead. Figure 6 shows the overhead routing comparison of the proposed FBS scheme to other techniques. According to the scenario, the proposed scheme has less routing overhead of 4687 bytes at 200

nodes. Compared to the routing overhead in HPSO-GA, LID-AODV and AODV, the difference is 1300, 1437, 1637 bytes, respectively. At some points, routing overhead is high because the mobility of nodes incurs more control packets to cope with the problem of frequent route hand-offs and new path discoveries.

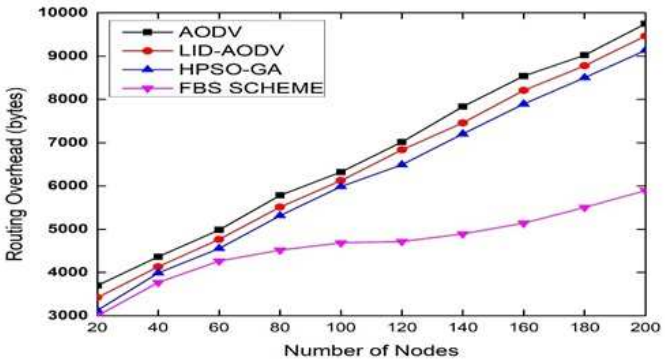

Figure 6: Routing Overhead (%)

5 Conclusion

In this paper, we proposed a solution to deal with black hole nodes in MANETs by using FBS nodes. The objective of the proposed study is to provide both detection and prevention of single and cooperative black hole nodes in the network. In the proposed scheme, FBS nodes continuously monitor the neighbouring nodes in terms of the number of RREQ packets forwarding. Because the black hole nodes don't forwards the RREQ packets to other normal nodes, except few to their collaborators. Whenever an FBS node detects any suspicious behaviour, it increments the ambiguous value for that node. Once the ambiguous value reaches the threshold value, it broadcasts an alert message, and if the ambiguous value exceeds the threshold, it declares the node as a malicious node and broadcast an alert in the network. Finally, all the nodes will add an entry of that node in their block table list and will ignore all the traffic from such node. To manage mobility, all the FBS nodes continuously share the information, to update the information of those nodes which leaves their region.

In addition, the proposed scheme does not require extra processing or any hardware for detection of black hole node. Also, it does not affect the intermediate nodes. The performance of the proposed scheme is compared with some existing techniques, and we found that the proposed scheme provides better outcomes in terms packet delivery ratio, throughput, detection rate, average delay, *i.e.* up to 97.45%, 78.9%, 97.33% and 0.7%, respectively, as compared to other techniques. The FBS nodes provide early and efficient detection of black hole nodes in the network so that the detection rate is high and the packet drop and false positive ratio is very low as compared to the other techniques.

Acknowledgments

The work in this paper has been supported by National Natural Science Foundation of China (61602456).

References

[1] M. Abdelhaq, S. Serhan, R. Alsaqour, and R. Hassan, "A local intrusion detection routing security over manet network," in *Proceedings of International Conference on Electrical Engineering and Informatics*, pp. 1–6, 2011.

[2] S. Aluvala, K. R. Sekhar, and D. Vodnala, "An empirical study of routing attacks in mobile ad-hoc networks," *Procedia Computer Science*, vol. 92, pp. 554–561, 2016.

[3] S. Aluvala, K. R. Sekhar, and D. Vodnala, "A novel technique for node authentication in mobile ad hoc networks," *Perspectives in Science*, vol. 8, pp. 680–682, 2016.

[4] S. K. Arora and H. Monga, "Performance evaluation of manet on the basis of knowledge base algorithm," *Optik*, vol. 127, no. 18, pp. 7283–7291, 2016.

[5] M. Baqer, M. Kamel, I. Alameri, and A. N. Onaizah, "Staodv: A secure and trust based approach to mitigate blackhole attack on aodv based manet," in *IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC'17)*, pp. 1278–1282,, 2017.

[6] S. Dhende, S. Musale, S. Shirbahadurkar, and A. Najan, "Saodv: Black hole and gray hole attack detection protocol in manets," in *International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET'17)*, pp. 2391–2394, 2017.

[7] A. Dorri, "An edri-based approach for detecting and eliminating cooperative black hole nodes in manet," *Wireless Networks*, vol. 23, no. 6, pp. 1767–1778, 2017.

[8] A. Dorri, S. Vaseghi, and O. Gharib, "Debh: Detecting and eliminating black holes in mobile ad hoc network," *Wireless Networks*, vol. 24, no. 8, pp. 2943–2955, 2018.

[9] A. M. Fahad and R. C. Muniyandi, "Harmony search algorithm to prevent malicious nodes in mobile ad hoc networks (manets)," *Information Technology Journal*, vol. 15, no. 3, pp. 84–90, 2016.

[10] S. Gurung and S. Chauhan, "A dynamic threshold based approach for mitigating black-hole attack in manet," *Wireless Networks*, vol. 24, no. 8, pp. 2957-2971, 2017.

[11] S. Gurung and S. Chauhan, "A review of black-hole attack mitigation techniques and its drawbacks in mobile ad-hoc network," in *International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET'17)*, pp. 2379–2385, 2017.

[12] M. Inam, Z. Li, A. Ali, and A. Zahoor, "A novel protocol for vehicle cluster formation and vehicle head selection in vehicular ad-hoc networks," *International Journal of Electronics and Information Engineering*, vol. 10, no. 2, pp. 103–119, 2019.

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

[14] D. Khan and M. Jamil, "Study of detecting and overcoming black hole attacks in manet: A review," in *International Symposium on Wireless Systems and Networks (ISWSN'17)*, pp. 1–4, 2017.

[15] V. K. Kollati, "Ibfwa: Integrated bloom filter in watchdog algorithm for hybrid black hole attack detection in manet," *Information Security Journal: A Global Perspective*, vol. 26, no. 1, pp. 49–60, 2017.

[16] V. H. Kshirsagar, A. M. Kanthe, and D. Simunic, "Trust based detection and elimination of packet drop attack in the mobile ad-hoc networks," *Wireless Personal Communications*, vol. 100, no. 2, pp. 311–320, 2018.

[17] R. Kumar and R. Chadha, "International journal of engineering sciences & research technology mitigation of black hole attack using generic algorithms and fuzzy logic,".

[18] G. Liu, Z. Yan, and W. Pedrycz, "Data collection for attack detection and security measurement in mobile ad hoc networks: A survey," *Journal of Network and Computer Applications*, vol. 105, pp. 105–122, 2018.

[19] N. Nissar, N. Naja, and A. Jamali, "Lightweight authentication-based scheme for aodv in ad-hoc networks," in *International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS)*, pp. 1–6, 2017.

[20] C. Panos, C. Ntantogian, S. Malliaros, and C. Xenakis, "Analyzing, quantifying, and detecting the blackhole attack in infrastructure-less networks," *Computer Networks*, vol. 113, pp. 94–110, 2017.

[21] M. Pathan, N. Zhu, J. He, Z. Zardari, M. Memon, and M. Hussain, "An efficient trust-based scheme for secure and quality of service routing in manets," *Future Internet*, vol. 10, no. 2, pp. 16, 2018.

[22] M. S. Pathan, J. He, N. Zhu, Z. A. Zardari, M. Q. Memon, and A. Azmat, "An efficient scheme for detection and prevention of black hole attacks in aodv-based manets," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 1, pp. 243–251, 2019.

[23] A. Rana, D. Sharma, "Mobile ad-hoc clustering using inclusive particle swarm optimization algorithm," *International Journal of Electronics and Information Engineering*, vol. 8, no. 1, pp. 1-8, 2018.

[24] S. Shahabi, M. Ghazvini, and M. Bakhtiarian, "A modified algorithm to improve security and performance of aodv protocol against black hole attack," *Wireless Networks*, vol. 22, no. 5, pp. 1505–1511, 2016.

[25] A. Siddiqua, K. Sridevi, and A. A. K. Mohammed, "Preventing black hole attacks in manets using secure knowledge algorithm," in *International Conference on Signal Processing and Communication Engineering Systems*, pp. 421–425, 2015.

[26] R. Thanuja and A. Umamakeswari, "Black hole detection using evolutionary algorithm for IDS/IPS in manets," *Cluster Computing*, pp. 1–13, 2018.

[27] F. H. Tseng, H. P. Chiang, and H. C. Chao, "Black hole along with other attacks in manets: A survey," *Journal of Information Processing Systems*, vol. 14, no. 1, 2018.

[28] T. Varshney, T. Sharma, and P. Sharma, "Implementation of watchdog protocol with aodv in mobile ad hoc network," in *The Fourth International Conference on Communication Systems and Network Technologies*, pp. 217–221, 2014.

[29] V. S. Venu and D. Avula, "Invincible AODV to detect black hole and gray hole attacks in mobile ad hoc networks," *International Journal of Communication Systems*, vol. 31, no. 6, pp. e3518, 2018.

[30] Z. A. Zardari, J. He, N. Zhu, K. H. Mohammadani, M. S. Pathan, M. I. Hussain, and M. Q. Memon, "A dual attack detection technique to identify black and gray hole attacks using an intrusion detection system and a connected dominating set in manets," *Future Internet*, vol. 11, no. 3, p. 61, 2019.

Biography

Zulfiqar Ali Zardari. Zulfiqar Ali Zardari received his B.E. and M.E degree from Mehran University of Engineering and Technology Jamshoro in Sindh, Pakistan 2011 and 2015 respectively. Currently, he is doing PhD in Faculty of Information Technology, Beijing University of Technology, China. He has published six research papers as a first and co-author in national and international journals. His research interest area is Mobile ad hoc networks, Wireless Communications, Information Security, sensor network security, Computer Networks and Network Security.

He Jingsha. He Jingsha received his B.S. degree from Xi'an Jiaotong University in Xi'an, China and his M.S. and PhD degrees from the University of Maryland at College Park in the USA. He is currently a professor in the School of Software Engineering at Beijing University of Technology in China. Professor He has published over 170 research papers in scholarly journals and international conferences and has received nearly 30 patents in the United States and China. His main research interests include information security, network measurement, and wireless ad hoc, mesh and sensor network security.

Nafei Zhu. Nafei Zhu received her B.S. and M.S. degrees from Central South University, China in 2003 and 2006, respectively, and her PhD degree in computer science and technology from Beijing University of Technology in Beijing, China in 2012. From 2015

to 2017, she was a postdoc and an assistant researcher in the Trusted Computing and Information Assurance Laboratory, State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences in China. She is now on the Faculty of Information Technology at Beijing University of Technology. Dr Zhu has published over 20 research papers in scholarly journals and international conferences (16 of which have been indexed by SCI/EI/ISTP). Her research interests include information security and privacy, wireless communications and network measurement.

Muhammad Salman Pathan. Muhammad Salman Pathan received his B.E. and M.E degree from Mehran University of Engineering and Technology, Pakistan in 2011 and 2014 respectively. Currently, he is doing PhD at the Faculty of Information Technology, Beijing University of Technology, China. His research interest is Wireless Communications, Information Security, sensor network security. He has published various research papers in his area.

Muhammad Qasim Memon. Muhammad Qasim Memon received his B.E. degree in Computer System Engineering and M.E. in Information Technology from Mehran University of Engineering & Technology Jamshoro (MUET) Pakistan in 2010 and 2014, respectively. He received his PhD degree in software Engineering from Beijing University of Technology in 2018. Currently, he is working as a Post-Doctoral fellow at advance innovation center for future education (AIFCE), Beijing Normal University, China. His research interests include Text mining, information extraction, text analytics, and wireless sensor networks.

Muhammad Iftikhar Hussain. Muhammad Iftikhar Hussain is currently doing PhD at Faculty of Information Technology, Beijing University of Technology, China. His Research interests include Information Security, Hybrid Cloud Computing Security and Hybrid Cloud Computing Infrastructure and Design. He did his MS Computer Science from Superior University Lahore with distinction. He served as Senior System Engineer in Television and Media Network (Express-News) for four years, one year as System Administrator in 92NEWSHD and two years as Lecturer / Advisor IEEE SUL in Superior University Lahore.

Peng He. Peng He is currently a professor in the College of Computer and Information Technology, China Three Gorges University. He graduated from Hefei University of Technology in 1986 with a bachelor's degree in computer application and from Xi'an Jiaotong University in 1989 with a Master's degree in computer software. He worked in National Time Service Center, Chinese Academy of Sciences (CAS) and participated in 30 research projects, including the seventh national 5-year-plan, the rehearsal of 'eight-five' project from the State Bureau of Surveying and Mapping, CAS youth fund project, Hubei technology research-program, *etc.* Prof. He won the western young scientist's achievement award and the third class award of technology advancement by CAS and the Hubei teaching research achievement award, *etc.* and has been an Education Information Expert of Ministry of Education and a Standing Director of Education Information Technology, Hubei. Prof. He has published over 50 journal papers, some of which have been indexed by EI and ISTP. His research focuses on transmission protocols and information security based on network time synchronization.

Chengyue Chang. Chengyue Chang graduated from Beijing University of Technology in Beijing, China with a Master's degree in software engineering. She is currently an engineer in the Machinery Industry Information Center engaging in the development of Internet software. Ms. Chang's research interests include network security and network forensics.