future internet

MDPI

Article

A Dual Attack Detection Technique to Identify Black and Gray Hole Attacks Using an Intrusion Detection System and a Connected Dominating Set in MANETs

Zulfiqar Ali Zardari [1], Jingsha He [1], Nafei Zhu [1,*], Khalid Hussain Mohammadani [2], Muhammad Salman Pathan [1], Muhammad Iftikhar Hussain [1] and Muhammad Qasim Memon [3]

1 Faculty of Information Technology & Beijing Engineering Research Center for IoT Software and Systems, Beijing University of Technology, Beijing 100124, China; zulfiqar@emails.bjut.edu.cn (Z.A.Z.); jhe@bjut.edu.cn (J.H.); salman@emails.bjut.edu.cn (M.S.P.); hussain@emails.bjut.edu.cn (M.I.H.)
2 School of Electronic Engineering, Beijing University of Posts and Telecommunications (BUPT), Beijing 100876, China; khalid.mohammadani@gmail.com
3 Advance Innovation Center for Future Education, Beijing Normal University, Beijing 100875, China; memon_kasim@yahoo.com
* Correspondence: znf@bjut.edu.cn; Tel.: +86-188-1059-9602

Received: 5 January 2019; Accepted: 22 February 2019; Published: 5 March 2019

Abstract: A mobile ad-hoc network (MANET) is a temporary network of wireless mobile nodes. In a MANET, it is assumed that all of the nodes cooperate with each other to transfer data packets in a multi-hop fashion. However, some malicious nodes don't cooperate with other nodes and disturb the network through false routing information. In this paper, we propose a prominent technique, called dual attack detection for black and gray hole attacks (DDBG), for MANETs. The proposed DDBG technique selects the intrusion detection system (IDS) node using the connected dominating set (CDS) technique with two additional features; the energy and its nonexistence in the blacklist are also checked before putting the nodes into the IDS set. The CDS is an effective, distinguished, and localized approach for detecting nearly-connected dominating sets of nodes in a small range in mobile ad hoc networks. The selected IDS nodes broadcast a kind of status packet within a size of the dominating set for retrieving the complete behavioral information from their nodes. Later, IDS nodes use our DDBG technique to analyze the collected behavioral information to detect the malicious nodes and add them to the blacklist if the behavior of the node is suspicious. Our experimental results show that the quality of the service parameters of the proposed technique outperforms the existing routing schemes.

Keywords: MANET; DoS attack; black hole; gray hole; IDS node; CDS; status packet; dual attack

1. Introduction

Mobile ad-hoc networks (MANETs) have gained a significant reputation in recent years due to the current proliferation of the latest technology (i.e., smartphones, tablets, personal digital assistants, etc.) [1]. Due to the dynamic environment, nodes are wirelessly connected with each other to transfer the data packets. The transportation of data packets between nodes occurs in an open medium without any central support, therefore, nodes exchange information at any time in the network. If the source and destination nodes are not in the same range, the reliability of the communication merely depends upon the intermediate nodes to forward the data packets in a trusted manner. An intermediate node acts as a host and communicates directly with the source node if it is near, while it works as a router if it is far away from the destination node [2]. Meanwhile, wireless

nodes have constrained resources, in terms of possessing less battery power, a low memory, and limited bandwidth. The MANET is specifically designed for fast and easy communication between nodes. It is applied in battlefields, disaster management, rescue operations, maritime communications, personal or commercial information sharing, and in those areas where wired infrastructure is not possible. The MANET does not require any special infrastructure for deployment and it is cheap to set up anywhere [3,4]. When the source node wants to transmit the data packets to a targeted node through an open medium, it utilizes multi-hop with the help of intermediate nodes. Due to the dynamic topology, the unstructured network, the open medium, and the high mobility of the nodes, some malicious nodes may enter easily into the network. Malicious nodes try to disturb the network resources, in terms of dropping the data packets, stealing important information, or manipulating data packets, which produces undesirable situations, a type of phenomena called a Denial of Service (DoS) attack [5].

1.1. Denial of Service (DoS) Attacks

A DoS attack is any event that diminishes or eliminates a network's capacity to perform its expected function. The aim is to deprive the nodes' communication of network resources, in terms of dropping data packets and reducing the network bandwidth by preventing authorized users from accessing resources [6].

Figure 1 shows the taxonomy of DoS attacks. In MANETs, DoS attacks are divided into two main attacks, called full packet drop attacks (black hole attacks) and partial drop packet attacks (gray hole attacks). Black hole attacks can be further expanded into three attacks, including single hole attacks, multiple attacks, and collaborative attacks. As their names imply, a single node or more than one node can partake in malicious activities. On the other hand, a gray hole attack is a partial packet drop attack. It can also be divided into two attacks, i.e., sequence-based gray hole attacks and smart gray hole attacks [7].

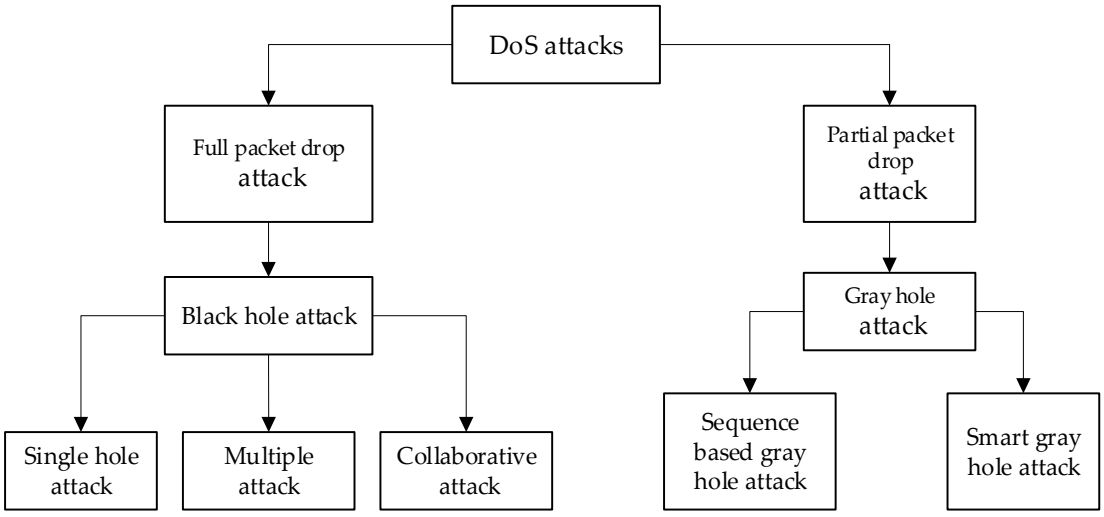

Figure 1. Classification of Denial of Service (DoS) attacks.

1.2. Black Hole Attacks

A black hole attack is a type of Denial of Service (DoS) attack which is one of the protuberant attacks. It is also called a full packet drop attack in MANETs. Due to the open medium and dynamic topology of MANETs, a black hole node can enter into the network easily in a stealthy manner. The appearance of black hole nodes occurs during the route discovery phase. Initially, the source node does not have any valid route to the destination node. The source node sends a route request (RREQ) packet to the intermediate nodes for route discovery. The legitimate node receives an RREQ packet from the source node and forwards it to the next node if it is not a destination node, however, when an

RREQ is received by a black hole node, it immediately sends a bogus route reply (RREP) with the high sequence number to win the route request. The sequence number is used to check the freshness of the route, in terms of how often that route is updated. The black hole node convinces the source node that it has a valid, short, and fresh route to the destination node, although it does not actually have any route to the destination node. In this way, the black hole node makes a feint to the source node and involves itself in the route between the initial node (source node) and the targeted node (destination node) in the network. Once the path is established, the source node starts sending data packets to the black hole node and eventually it drops all of the data packets without forwarding them to the destination node [8–10].

1.3. Gray Hole Attacks

A gray hole attack is a type of DoS attack which is an extension of a black hole attack. It drops the selective data packets during communication so it is called a partial packet drop attack. Initially, gray hole nodes do not appear as malicious nodes as they behave like normal nodes during the path discovery phase. To detect a gray hole node is a challenging task in MANETs because they send the correct sequence number during the path discovery phase. After some time, however, they turn into malicious nodes when the source node sends data packets to the destination node. As mentioned in Figure 1, gray hole attacks consist of two types of attacks, including sequence-based gray hole attacks and smart gray hole attacks. In sequence gray hole attacks, the malicious node sends the false routing information with a high sequence number and very few hop counts, to try to attract the traffic towards it. From time to time, it may or may not have any valid route to the destination node, whereas smart gray hole attacks are normally involved in the routing process to discover the destination node. They have a valid route to the destination node and drop the selective data packets at a particular time, hence they are called smart gray holes [11].

Many researchers have proposed different solutions to cope with the issue of black hole and gray hole attacks in MANETs. Most of the solutions, however, detect only one type of attack (either the black hole or gray hole attacks). Many solutions fail to detect gray hole attacks, especially the smart gray node when it behaves exactly as normal during the routing process. Moreover, numerous techniques use traditional security measures, which are not appropriate due to the special dynamic features of MANETs. Some of the methods broadcast extra beacon messages, bait requests, trap RREQs, neighborhood nodes, or additional packets for route checking and the detection of malicious nodes, which causes delays due to routing overhead or the cumbersome nature of the network.

The main focus of this paper is to detect the black and gray hole attacks in MANETs. In order to achieve this, a technique that achieves the dual detection of black hole and gray hole attacks (DDBG) is proposed. For the detection of malicious nodes, the proposed technique utilizes a connected dominating set (CDS) approach and selects the intrusion detection system (IDS) node as a query issuing node. In order to check the status of every query issuing node, the IDS node broadcasts a light-weight status packet periodically, which contains four questions to verify every node in the network. After receiving the status packet from the IDS node, legitimate nodes genuinely reply without any fabricated or forged information, whereas the malicious node sends fake information to the IDS nodes to prevent its identification by security mechanisms. The other reason for sending fake information is to drop the data packets from the source node. Due to the fabricated information of the malicious node, detection is easy because it does not satisfy the pre-defined questions of the status packets. Hence, the IDS node confirms that the node is a liar and is sending fake information, proving that the node is malicious. Once a node is identified as being malicious, the IDS node broadcasts a block message to apprise other nodes about this malicious node and to add this node to the blacklist.

1.4. Findings and Contribution

To the best of the author's knowledge, very little research literature is available to identify both the black and gray hole attacks in the dynamic environment of MANETs. Specifically, the utilization of CDS and IDS approaches are used for the detection of black hole and gray hole nodes.

The contributions are as follows:

- We have proposed a prominent technique for the detection of malicious attacks, such as black hole and gray hole attacks, through the intrusion detection system (IDS) nodes using the connected dominating set (CDS) technique. Our work is different from past research, wherein the approach used was only for black hole attacks [12–14] or the proposed scheme worked only for gray hole attacks [15–17].
- The proposed DDBG technique also detects the malicious nodes, particularly nodes with smart gray hole attacks, even in dense networks. Our approach is different from [18–20], where the proposed technique demonstrated an inadequate detection of the gray hole attacks in a dense network.
- Comprehensive experimental outcomes indicated that the proposed method is an effective and prominent approach for the detection of black and gray hole attacks.

The remaining work of the paper is arranged into the following sections: Section 2 describes the related work, Section 3 presents the proposed methodology and algorithm, Section 4 describes the simulation scenario and results, and Section 5 summarizes the paper.

2. Related Work

In recent years, DoS attacks have attracted the noteworthy consideration of researchers, as they can affect the routing performance of MANETs exceptionally. Most of the existing mechanisms focus only on the route discovery phase or the data transmission phase to mitigate malicious nodes. Moreover, many mechanisms have not used any attack models to judge the performance of the network. We have presented various mechanisms which are also used to isolate the malicious nodes from the MANETs. Some of the authors have proposed solutions, however, these solutions still have drawbacks. Table 1 lists some of the other existing techniques along with their drawbacks.

Table 1. Existing techniques along with their drawbacks.

S.No	Author & Year	Technique	Drawbacks
01	V.S. Venu (2018) [21]	Frame-checking sequence	The process is slow and has computational complexity
02	P. Tamilselvi (2017) [22]	Bait request	The delay is significant if the route is long
03	G. Arulkumaran (2017) [23]	Fuzzy logic	Fails to detect smart gray holes
04	S. Gopinath (2018) [24]	Location base	Required extra hardware, i.e., antenna, GPS, etc.
05	Mohanapriya (2014) [25]	Light-weight intrusion detection system (IDS)	The packet delivery ratio is affected due to gray holes being undetected
06	Arathy (2016) [26]	Destination Sequence Number (ADSN)	The method fails when smart gray holes send an average sequence number
07	Chang (2011) [27]	Cooperative bait detection scheme (CBDS)	The method is unclear and complex
08	Shashi Gurung (2017) [28]	AODV, MBDP-AODV	High routing overhead
09	Shashi Gurung (2018) [29]	AODV, BAODV, IDSAODV, MBDP-AODV	Fails to detect smart gray holes
10	K. Vijayakumar (2016) [30]	Crypto-key based on Diffie-Hellman	Fails to detect gray holes
11	Christoforos Panos (2017) [31]	Dynamic threshold cumulative sum	Only detects black hole attacks
12	Ali Dorri (2017) [32]	Extended Data Routing Information	Fails to detect smart gray holes

Table 1. *Cont.*

S.No	Author & Year	Technique	Drawbacks
13	Nachiket Kshatriya (2016) [33]	Detection engine on MAC layer	Huge routing overhead due to RTS and CTS
14	Sandeep Dhende (2017) [34]	Neighbor node opinion	Cannot handle mobility and routing overhead
15	Sina Shahabi (2016) [35]	Behavior of nodes (IDSNAODV)	Failed in collaborative gray hole attacks
16	M. B. M. Kamel (2017) [36]	Trust value	Fails to detect gray holes
17	Vijaya Kumar (2017) [37]	Integrated Bloom Filter in Watchdog Algorithm	Complex and unclear methodology
18	R. Kumar (2016) [38]	Fuzzy logic generic algorithm	The methodology is unclear
19	Arvind Dhakaa (2015) [39]	Control sequence packets	Fails to detect smart gray holes
20	Neha Sharma (2016) [40]	Route Discovery and Monitoring phase	Fails when gray hole nodes in cooperative
	Proposed solution	Technique	Different from existing solutions
	DDBG	Connected Dominating Set and Intrusion Detection System	• Proposed solutions detect both black and gray hole nodes by sending the status packet periodically, which checks every node from time to time. • Proposed solutions detect the malicious nodes in a dynamic environment and can handle the mobility of the nodes. • Provides better performance than the existing solutions and doesn't require any extra hardware.

3. Proposed Methodology

In MANETs, the nodes have limited energy to establish communicational links to broadcast the data packets. Malicious nodes send beacon messages periodically in MANETs, creating a huge amount of unnecessary traffic to increase the routing overhead. Malicious nodes should be prevented in order to reduce the extra routing overhead. To cope with this problem, the proposed technique combines two different algorithms (i.e., CDS and IDS) to detect the malicious nodes (i.e., black hole and gray hole) and to reduce the routing overhead in MANETs. A dominating set of nodes is a subset of the network. All of the nodes are not necessarily connected within that subset but at least one node should be a member of that subset of the network. The dominating set must be connected, called a connected dominating set (CDS). A CDS has a lower number of connected nodes to cover the maximum range of the network [41]. The intrusion detection system (IDS) set is also a concept of the subset of the network. It is used to make a set of nodes based on the nodes' sufficient energy within the entire network. The IDS set is also implemented to reduce the traffic load and the overhead routing of the network.

For the detection and isolation of the malicious nodes from MANETs, we have proposed a technique called the dual attack detection for black and gray hole attacks (DDBG). Initially, the DDBG technique makes small groups of nodes within the network, via the help of the CDS technique. Secondly, the DDBG selects the IDS set of nodes from small groups of the CDS nodes which have enough energy and do not belong to the blacklist. In the third step, an IDS node with the highest energy in the IDS set is selected. The IDS node must be a trusted node. Next, the IDS node sends status packets periodically to detect the malicious node within the IDS set. If any node's behavior is suspected to be malicious then the IDS node broadcasts a block message to inform all nodes. All of the nodes will then stop communication with that particular malicious node.

From the subset of the network, a small group of nodes runs the IDS to broadcast the status and monitor the energy level. In our proposed technique, we have used an intrusion detection system to design and implement in the network. The IDS node broadcast a status packet to check the status of every node in the CDS. If any node's behavior is suspected to be malicious then the IDS node

broadcasts a block message to inform all nodes. All of the nodes will then stop communication with that particular malicious node.

3.1. Key Features of the Proposed DDBG Technique

- The selection of the IDS node is dynamic, after considering that the highly mobile environment of MANETs as the deployment of IDS nodes on fixed locations is not a practical approach in MANETs. To enhance the network performance and minimize the routing overhead, the proposed technique provides an optimized IDS node-based solution in MANETs.
- In MANETs, the mobility of the nodes is obvious, therefore, the topology of the network changes from time to time. The proposed technique manages the position of all of the IDS nodes according to the current network topology to cope with the dynamic environment of MANETs.
- The proposed technique provides the quick detection of black hole and gray hole nodes because if any node in the IDS set range is not responding or is sending false information, it is declared to be a malicious node for a short time.

3.2. Connected Dominating Set (CDS) and IDS Node Selection

A group of nodes is said to be a CDS if they are selected in such a way that they belong to an IDS set covering the entire range of the network. A trusted node with sufficient energy is selected as the IDS node for query processing. All of the nodes under the IDS set are connected with each other. They are connected in such a way to ensure the full coverage of the network. We have extended the CDS approach by selecting the IDS query issuing node from the IDS set. Before selecting this node, the proposed DDBG technique checks two factors, i.e., the trust and energy of a node. For a node to become trusted, all of the nodes in the IDS set must observe their neighboring node in promiscuous mode. Every node in the IDS set monitors the behavior of the neighboring node regarding the packet dropped or put forward and then this information is stored in their own table of knowledge.

Equation number (1) calculates the energy of the IDS node for query processing (status packet). The node must have energy and should be labeled as a trusted node. If both of these conditions apply to a node, then that node is selected for query issuing to send the query (status packets) periodically.

Let N be any node:
TE (N) = The total energy of the node when it is fully charged
BE (N) = The beginning energy level of the node
CE (N) = The current energy of the node
Γ= The maximum % of the BE (N) for the IDS query node
Θ= The minimum % of the TE (N) must be conserved.

Therefore, node N cannot be selected as a query issue node if:

$$\left(1 - \frac{CE}{BE}\right) \times 100 > \Gamma \text{ OR } \left(\frac{CE}{TE}\right) \times 100 < \Theta \quad (1)$$

The values of Γ and Θ are based on the average energy of the nodes in the network.

Figure 2 shows the whole process of the IDS nodes. The purpose of the deployment of an IDS node is to provide a strong defense mechanism against the black hole and gray hole attacks in MANETs. IDS nodes continuously observe the behavior of nodes by sending status packets to check if a node is legitimate or is a malicious node. If any node is misbehaving (i.e., dropping full data packets it receives, dropping half of the data packets, or dropping selective data packets during data communication), the IDS node broadcasts a block message to notify the other nodes about the malicious node.

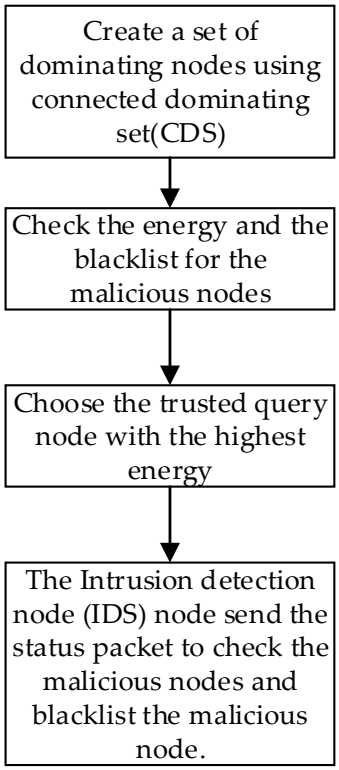

Figure 2. The selection of the query issuing node and the detection method.

There were two assumptions considered when designing the proposed DDBG technique, as follows:

- All of the nodes are connected within the IDS set and at least one IDS node must be in the range of the other IDS nodes, i.e., The IDS node can share the information about the malicious node to all of the remaining nodes in the entire range.
- All of the IDS nodes must have enough energy to broadcast the status packet to detect malicious behavior.

3.3. Applications

In MANETs, it is assumed that there are some malicious nodes present within the network. Attacker (malicious) nodes seek to steal information from nodes and disturb the network. In some hostile environments, like communication between military troops, the information is very confidential and important in estrangement situations. Stealing or fabricating this kind of information is very sensitive because it directly involves human life and safety. An attacker could hack the node that holds important information, aiming to sniff the communication of the opposite side and steal important information. An attacker node always takes advantage of this open medium communication to hear all of the information.

3.4. Status Packets

IDS nodes send status packets periodically to analyze the performance of every node in the network. Every node in the network receives this status packet and responds to the IDS node. In this way, the IDS node checks the packet forwarding behaviors of the nodes continuously, in order to distinguish between the normal and the malicious nodes. The status packet contains the following four questions from normal working nodes as shown in Table 2

Table 2. Intrusion detection system (IDS) analysis through questions in status packet.

Q.1 The Intrusion detection system (IDS) node asks the normal node: What is the sequence number?
Q.2 The Intrusion detection system (IDS) node asks the normal node How many packets have been received.
Q.3 The IDS node asks: How many packets have gone forward?
Q.4 The IDS node asks: How many packets have been dropped and why?

3.5. Adversary Attack Model

In this paper, we assume that various malicious (black and gray hole) nodes are present in the network. Malicious nodes attempt to find a way to disturb the network during communication without exposing their identities. During black hole attacks, a malicious node sends false information to the source node by deceiving it into believing that it has a valid and fresh route to the destination. In gray hole attacks, the attacker node drops selective packets during the data transmission phase. The detection of such malicious nodes is not an easy task because of their diverse behavior and the highly dynamic environment of MANETs. In this paper, we have included an adversary attack model to observe the diverse effect of different behaviors performed by the adversary on our proposed technique.

3.5.1. Sending Fake Information by the Black Hole Node

Initially, a black hole node enters in a sneaky manner, without participating in the routing process of the network. It carefully monitors the behavior of the normal nodes by listening to the incoming and outgoing traffic and keeping these packets in its memory for a short time. Whenever a source node doesn't have a valid router towards the destination, it sends RREQ packets in the network to find routes towards the destination. As soon as the black hole node receives the RREQ packet, it takes advantage of that time and shows itself off as a legitimate node, claiming that it has a valid and short route. It then sends the RREP with the highest sequence number and the lowest hop count. Based on the bogus reply of the black hole node, the source node establishes a route and it starts sending data packets to that node. After getting into that route, the black hole node drops all of the data packets instead of forwarding them to the destination node.

3.5.2. Selective Packet-Dropping by the Gray Hole Node

The behavior of the gray hole node is unpredictable because it changes rapidly from normal to malicious, so it is a challenging task to detect this behavior in MANETs. Gray hole nodes receive the RREQ packet from the source node and check-in the routing table for validity. If it has a valid route for the destination, the gray hole node sends a bogus RREP, with a high sequence number and a minimum hop count, towards the source node, or else sends the normal RREP. The gray hole node is smart enough to behave like a genuine node in order to hide from security mechanisms. During the route discovery process, it sends the correct sequence number but at the time of data transmission, its behavior becomes malicious and it starts dropping selective data packets, which is an undesirable situation. The main intention of the gray hole node is to degrade the network's performance.

3.6. Detection of Malicious Nodes

Initially, a network is set up by selecting the IDS set with enough energy to broadcast the status packets in the network. There are two types of nodes that are present in the network, legitimate nodes and malicious nodes. Initially, the blacklist (malicious node list) is empty, but after the first transmission, the IDS node predicts which nodes are malicious nodes and adds them to the blacklist. Before sending the data packets towards the destination node, it is essential to ensure the route from the source to the destination has no malicious nodes, in order to gain a high throughput. To find out which nodes are the malicious nodes in the network, the IDS nodes broadcast a status packet and wait for it to be acknowledged with a reply. All of the legitimate nodes receive the status packet and reply to all of the questions genuinely without any ambiguity. After some time, if there is no reply to the

status packet, then it is assumed that there must be some malicious activity found in the network. For malicious nodes, there will be two conditions; it either sends false information to the IDS node to hide its identity or it does not send any reply to the IDS node and simply drops the status packet. Because the malicious node is a fabricator node, it sends a fabricated reply and never shows its real identity to the IDS node. After receiving replies from all of the nodes, the IDS node checks which node is not responding properly and why. After some time, if any node is not responding, i.e., not answering the questions or sending bogus replies and failing to satisfy the pre-defined questions without any reason for the link failure, energy, or queue size, then the IDS node declares that node as a malicious node. The IDS node broadcasts the block message to notify all nodes in the network to block that malicious node. Immediately, all of the legitimate nodes will include the malicious node's ID in their blacklists.

3.7. Description of the Flow Chart

Figure 3 shows the flowchart of the proposed architecture system. During the proposed technique, the IDS starts broadcasting the status packet periodically to all nodes within its set range. All of the nodes in the IDS nodes' set range receive a status packet from the IDS node. When a legitimate node receives this status packet, it proceeds genuinely. Meanwhile, when a malicious node receives this packet, it reacts with abnormal behavior or provides false information to IDS nodes. According to the status packet, the first question is about whether any node is sending a high sequence number. Reaming nodes that send an average sequence number and drop all data packets are declared as black hole nodes. If any node is providing an average sequence number, not considered high, alongside the dropping of selective data packets, it is declared as a gray hole node. The second and third questions enquire about the data packets the malicious node has received and the data packets it has forwarded during communication. It is obvious that a malicious node provides bogus information to the IDS node to attract traffic and drop the data packets instead of forwarding them to the next node. The last question relates to the reason for dropping the data packets and, if any malicious node claims that it dropped data packets because of the queue size or traffic congestion, the proposed technique has a solution for this problem. Generally, in the network, each node has an equal traffic load when compared to other legitimate nodes. There is no reason why that particular node (malicious node) should be dropping the data packets if the traffic load is the same for every node, so it establishes that the node in question is a liar and its aim was to drop the data packets. Once it is confirmed that the node is a malicious node, the IDS node broadcasts a block message consisting of the malicious node's ID and rejects all types of information sent by that particular malicious node, adding it to the blacklist. If any node found to be malicious in the set range moves to another set, then the IDS node already has information about that malicious node (calculated in the previous IDS set). Therefore, the IDS node also broadcasts a block message to their own range to block that malicious node.

3.8. Experiment

Our proposed technique was simulated with an open source network simulator NS-2, to evaluate the performance of the network. In the simulation IEEE, 802.11b 100 nodes were deployed, which covered most of the area of the network. The network size was 800 $\times$ 800 m and the simulation time was 500 s. Random walk mobility was used as the mobility model. The (ad hoc on-demand distance vector) AODV protocol and the proposed DDBG protocol were implemented to check the performance of the network. The system did not require any special hardware to simulate the results, as the standard system had the capability to run and predict the results through simulation. Table 3 shows the parameters used for the simulation.

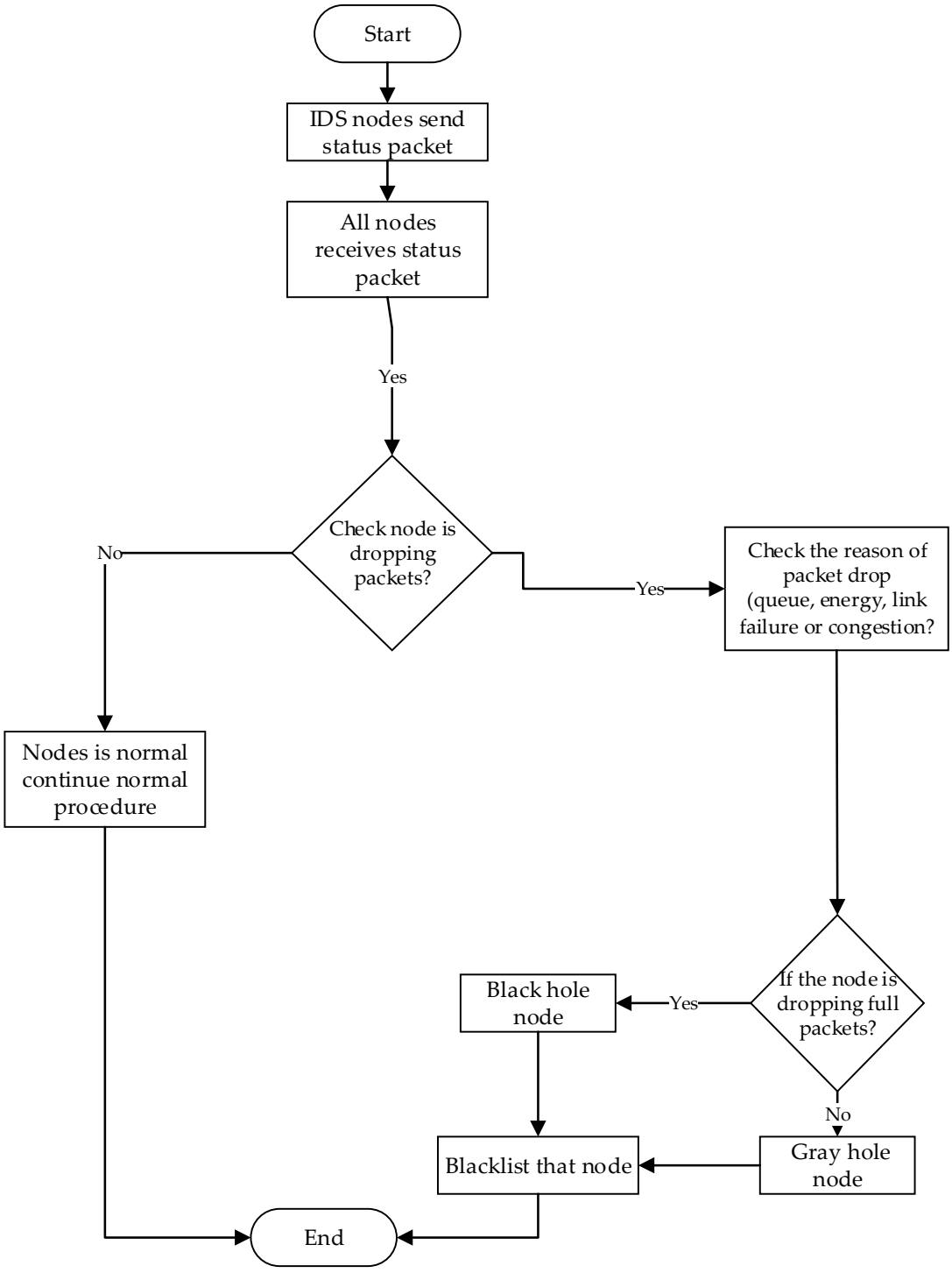

Figure 3. Flowchart of the proposed method.

Table 3. The simulation parameters.

Parameters	Value
Simulator	NS-2(ver.2.35)
Network area	800 × 800 m
Normal nodes	100
Mobility model	Random Walk mobility (Bonn Motion)
Routing Protocol	Ad hoc on-demand distance vector (AODV)
Simulation time	600 s
MAC type	IEEE 802.11
Traffic type	Constant bitrate (CBR)
Agent	UDP
Packet size	512 bytes
Mobility	0.5–1.0 m/s
Pause time	5–20 s

4. Results and Analysis

The performance of both the ad hoc on-demand distance vector (AODV) and the DDBG protocols was evaluated in the presence of malicious nodes. We have compared our simulation results with ADOV, local intrusion detection (LID-AODV), and hybridization of particle swarm optimization-genetic algorithm HPSO-GA [42–44]. The reason for choosing these techniques to compare with our protocol is that these are the latest approaches in research literature using IDS and that they are similar to our technique, i.e., of gathering information from nodes. Moreover, results are based on performances metrics such as detection rate, packet delivery ratio, throughput, routing overhead and average delay. Result analysis is further discussed for each of the performance metrics separately.

4.1. Detection Rate (%) of Malicious Nodes

Table 4 shows the results of detection rate based on our proposed method. The detection rate is an important metric in examining the accuracy of the status packet to detect malicious nodes. The reason for selecting this metric is to show the ability of DDBG to identify the malicious nodes in the network. In Figure 4, the x-axis shows the number of nodes and the y-axis shows the detection rate (the finding accuracy) of DDBG compared to native AODV, LID-AODV, and HPSO-GA. It shows that the detection rate of DDBG is the highest (98%). The reason for this is that our proposed technique received replies from every legitimate node, while the malicious nodes did not reply correctly or dropped the status packet. As soon as the number of malicious nodes increases in the network, the proposed DDBG technique gets more chances to detect the malicious nodes because it sends the false queries to IDS nodes. Therefore, the proposed technique detects the malicious nodes more rapidly than the others, hence the detection rate increases as the number of nodes increases, which is the highest detection rate recorded at 98.15%.

Table 4. The detection rate evaluation values.

Ad Hoc On-Demand Distance Vector (AODV)	Local Intrusion Detection (LID)-ADOV	Hybridization of Particle Swarm Optimization-Genetic Algorithm (HPSO-GA)	Proposed DDBG
85.32%	87.97%	93.21%	95.39%
86.28%	88.18%	93.65%	96.11%
86.94%	88.29%	93.91%	96.98%
87.15%	88.63%	94.58%	97.52%
87.63%	89.35%	95.13%	98.15%

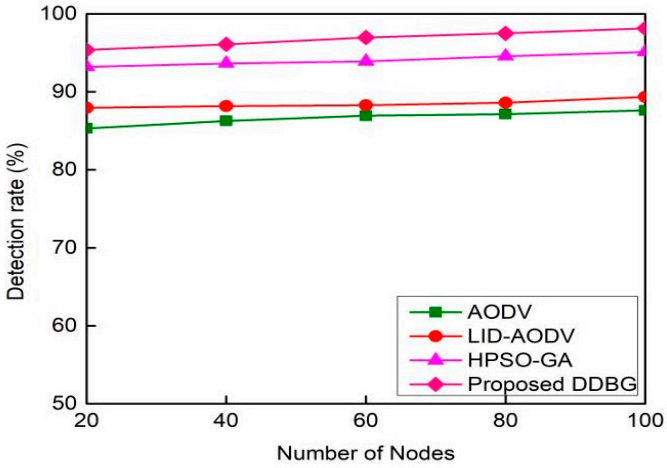

Figure 4. The detection rate (%).

4.2. Packet Delivery Ratio (PDR) (%)

Figure 5 shows the PDR of AODV, LID-AODV, HPSO-GA, and DDBG. The PDR of DDBG is the highest recorded (97%) because, after the detection of malicious nodes, packets are easily delivered more quickly to the destination node. As the malicious nodes increase, indeed they will cover most of the network and will disturb the communication by sending fake replies and not delivering data packets to the destination properly. However, after the deployment of our proposed technique, it was observed that the PDR is slightly increased, as it blacklists the malicious nodes with status packet queries in a short amount of time. Nevertheless, the PDR is much improved when compared to the other three protocols. Moreover, result analysis of packet delivery shown in Table 5 indicates that the proposed method outperforms AODV, LID-AODV and HPSO-GA.

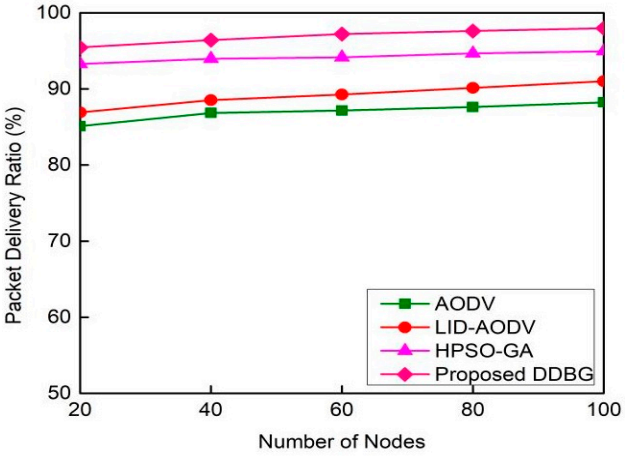

Figure 5. The packet delivery ratio (%).

Table 5. The packet delivery ratio evaluation values.

Ad Hoc On-Demand Distance Vector (AODV)	Local Intrusion Detection (LID)-ADOV	Hybridization of Particle Swarm Optimization-Genetic Algorithm (HPSO-GA)	Proposed
85.12%	86.93%	93.28%	95.46%
86.85%	88.53%	93.96%	96.42%
87.16%	89.28%	94.15%	97.22%
87.63%	90.15%	94.68%	97.62%
88.24%	91.028%	94.96%	97.98%

4.3. Throughput (kbps)

Figure 6 shows the throughput of the network when the nodes are transferring the data packets. As shown in the figure, the proposed technique and the native AODV are compared in the presence of malicious nodes in the network. When any two normal nodes are communicating and any malicious node sends the false routing information, claiming that it has a valid route when it actually wants to drop the data packets, it decreases the throughput. Another reason for this is the mobility of the nodes, which directly affects the performance of the network, as the movement of the nodes causes link breakage, leading to a decrease in the throughput of the network. Table 6 shows the improved results reported based on throughput (kbps) of the proposed technique. As in our proposed technique, all of the IDS nodes send status packets to which every node responds positively. If any node does not satisfy the pre-defined conditions then the IDS node marks it as a malicious node and the other nodes stop communication with that particular node.

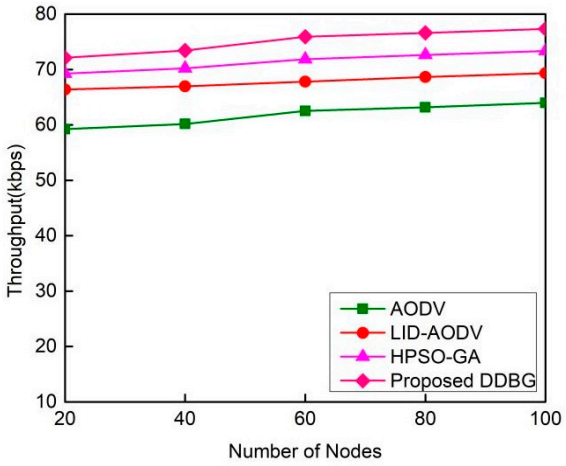

Figure 6. The throughput (kbps).

Table 6. The throughput evaluation values.

Ad Hoc On-Demand Distance Vector (AODV)	Local Intrusion Detection (LID)-ADOV	Hybridization of Particle Swarm Optimization-Genetic Algorithm (HPSO-GA)	Proposed
59.23	66.398	69.26	72.122
60.18	66.98	70.21	73.44
62.52	67.81	71.86	75.91
63.18	68.65	72.63	76.61
63.98	69.35	73.34	77.33

4.4. Routing Overhead (Bytes)

Figure 7 shows the results of routing overhead in the network, in which the native AODV and the proposed technique can be compared. It can be seen in the proposed DDBG technique that there is a slight lag at a point, as the number of nodes is increasing; the reason for this is that the IDS node sends packets periodically. When a packet is broadcasted by the IDS node, it takes less time to reach every node in the IDS set instead of the entire network. In spite of sending broadcast status packets periodically, the routing overhead of the proposed technique increases. The overall performance of the proposed method in terms of the overhead is improved more than other methods as shown in Table 7.

4.5. Average Delay (sec)

Figure 8 shows the delay in the results of the AODV and the proposed technique by means of the time taken by the nodes to deliver the packets to the targeted node on time. The Results shows that

the AODV delay of the network is high because the malicious node drops the data packets during the transmission. In our proposed technique, the delay is slightly higher at meager points, as the number of nodes is increasing because the IDS nodes are continuously sending packets to normal nodes for the status. Moreover, the link failure is obvious in MANETs, meaning that the nodes re-transmit the data packets to the destination node again, so the time taken for this may be the reason for the delay. After the deployment of the IDS nodes, however, there are few computations to predict the given answers from the query point. Table 8 shows the average delay with varying number of nodes. It can be seen that at meager points in particular, the proposed DDBG performs much better than other methods.

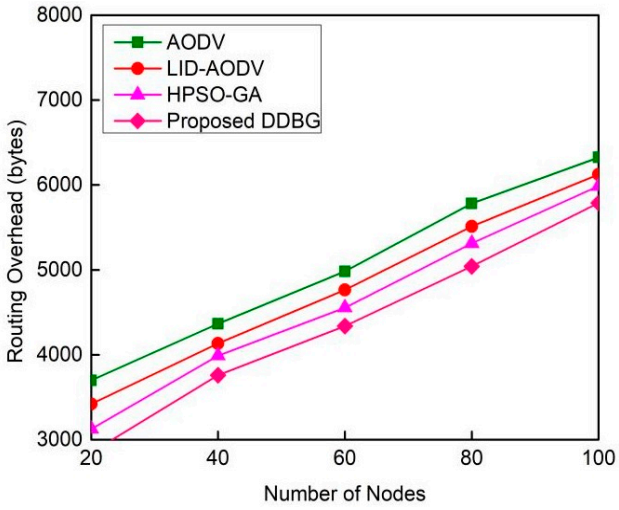

Figure 7. The routing overhead (bytes).

Table 7. The routing overhead evaluation values.

Ad Hoc On-Demand Distance Vector (AODV)	Local Intrusion Detection (LID)-ADOV	Hybridization of Particle Swarm Optimization-Genetic Algorithm (HPSO-GA)	Proposed
3698	3421	3126	2849
4365	4134	3989	3758
4982	4765	4554	4337
5782	5512	5312	5042
6324	6124	5987	5787

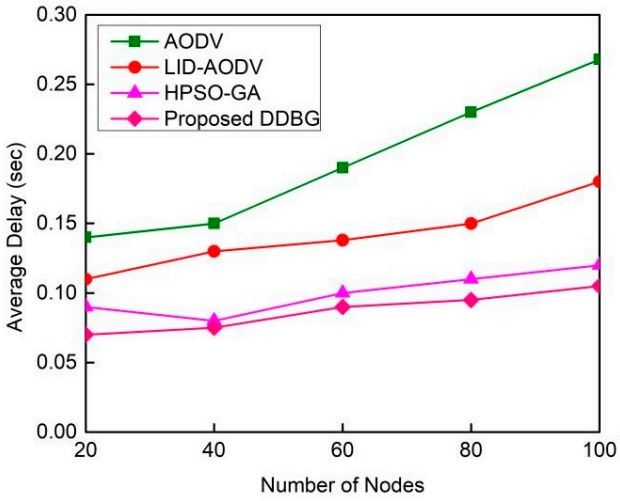

Figure 8. The average delay (s).

Table 8. The average delay(s).evaluation values.

Ad Hoc On-Demand Distance Vector (AODV)	Local Intrusion Detection (LID)-ADOV	Hybridization of Particle Swarm Optimization-Genetic Algorithm (HPSO-GA)	Proposed
0.14	0.11	0.09	0.07
0.15	0.13	0.08	0.075
0.19	0.138	0.1	0.09
0.23	0.15	0.11	0.095
0.268	0.18	0.12	0.105

5. Conclusions

In MANETs, various attacks disturb the network operation during communication, which is a major concern. The rapid detection of malicious attacks is an essential task to prolong the lifetime of the network. In order to maintain the accuracy of the detection rate of malicious nodes, in this research we have proposed a technique which provides a detection mechanism for black and gray hole nodes in MANETs. The CDS approach and IDS nodes are used to detect malicious nodes. Using the CDS approach, small-sized groups of nodes are created, which are called IDS sets. In the IDS set, a trusted node with the highest energy will be selected as the IDS node for broadcasting the status packet. After the selection of the broadcaster node, it sends the status packets periodically in the IDS set to check that every node is forwarding the data packets properly or to identify any malicious nodes that are present. All of the legitimate nodes provide the correct routing information to the IDS node. Malicious nodes send false information to drop the data packets. After receiving all of the replies from all of the nodes, the IDS node compares the answers, as the malicious node is a liar and can easily be detected. The simulation results prove that our proposed technique is successful in detecting the malicious nodes, as it receives many replies from the status packet. The proposed technique provides a high packet delivery ratio and less delay because only trusted nodes communicate in the network after the detection of malicious nodes. One drawback of the proposed GGBG is the limited battery power of the nodes, as it cannot continuously monitor the nodes for a long period of time. Additionally, the proposed work detects well-known attacks but not all attacks. Our experimental outcomes indicated that the proposed DDBG technique is an effective and prominent approach for the detection of black and gray hole attacks. In future work, this technique can be extended into wireless sensor networks for any environmental fix to sense the data for a particular application.

Author Contributions: Conceptualization, J.H. and N.Z.; software, M.I.H.; validation., M.S.P., K.H.M. and M.Q.M.; formal analysis, J.H.; writing—original draft preparation, methodology, Z.A.Z.; writing—review and editing, supervision, J.H.; funding acquisition, N.Z.

Funding: This research has been funded by National Natural Science Foundation of China, grant number 61602456.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Kumar, S.; Dutta, K. Intrusion detection in mobile ad hoc networks: Techniques, systems, and future challenges. *Secur. Commun. Netw.* **2016**, *9*, 2484–2556. [CrossRef]
2. Liu, G.; Yan, Z.; Pedrycz, W. Data collection for attack detection and security measurement in Mobile Ad Hoc Networks: A survey. *J. Netw. Comput. Appl.* **2018**, *105*, 105–122. [CrossRef]
3. Pathan, M.; Zhu, N.; He, J.; Zardari, Z.; Memon, M.; Hussain, M. An Efficient Trust-Based Scheme for Secure and Quality of Service Routing in MANETs. *Future Internet* **2018**, *10*, 16. [CrossRef]
4. Hiremath, P.S.; T, A.; Pattan, P. Adaptive fuzzy inference system for detection and prevention of cooperative black hole attack in MANETs. In Proceedings of the 2016 International Conference on Information Science (ICIS), Kochi, India, 12–13 August 2016; pp. 245–251.

5. Roshani, P.; Patel, A. Techniquesto mitigate grayhole attack in MANET: A survey. In Proceedings of the International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, India, 17–18 March 2017; pp. 1–4.
6. Alsumayt, A.; Haggerty, J.; Lotfi, A. Detect DoS Attack Using MrDR Method in Merging Two MANETs. In Proceedings of the 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA), Crans-Montana, Switzerland, 23–25 March 2016; pp. 889–895.
7. Gurung, S.; Chauhan, S. Performance analysis of black-hole attack mitigation protocols under gray-hole attacks in MANET. *Wirel. Netw.* **2017**, 1–14. [CrossRef]
8. Tiruvakadu, D.S.K.; Pallapa, V. Honeypot Based Black-Hole Attack Confirmation in a MANET. *Int. J. Wirel. Inf. Netw.* **2018**, *25*, 434–448. [CrossRef]
9. Singh, D.; Singh, A. Enhanced Secure Trusted AODV (ESTA) Protocol to Mitigate Blackhole Attack in Mobile Ad Hoc Networks. *Future Internet* **2015**, *7*, 342–362. [CrossRef]
10. Dumne, P.R.; Manjaramkar, A. Cooperative bait detection scheme to prevent collaborative blackhole or grayhole attacks by malicious nodes in MANETs. In Proceedings of the 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 7–9 September 2016; pp. 486–490.
11. Gurung, S.; Chauhan, S. A novel approach for mitigating gray hole attack in MANET. *Wirel. Netw.* **2018**, *24*, 565–579. [CrossRef]
12. Khamayseh, Y.M.; Aljawarneh, S.A.; Asaad, A.E. Ensuring survivability against Black Hole Attacks in MANETS for preserving energy efficiency. *Sustain. Comput. Inform. Syst.* **2018**, *18*, 90–100. [CrossRef]
13. Hammamouche, A.; Omar, M.; Djebari, N.; Tari, A. Lightweight reputation-based approach against simple and cooperative black-hole attacks for MANET. *J. Inf. Secur. Appl.* **2018**, *43*, 12–20. [CrossRef]
14. Nitnaware, D.; Thakur, A. Black hole attack detection and prevention strategy in DYMO for MANET. In Proceedings of the 2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 11–12 February 2016; pp. 279–284.
15. Schweitzer, N.; Stulman, A.; Margalit, R.D.; Shabtai, A. Contradiction Based Gray-Hole Attack Minimization for Ad-Hoc Networks. *IEEE Trans. Mob. Comput.* **2017**, *16*, 2174–2183. [CrossRef]
16. Sachan, K.; Lokhande, M. An approach to detect Gray-hole attacks on Mobile ad-hoc Networks. In Proceedings of the 2016 International Conference on ICT in Business Industry & Government (ICTBIG), Indore, India, 18–19 November 2016; pp. 1–5.
17. Kumar, S.; Doohan, N.V. A modified approach for recognition and eradication of extenuation of gray-hole attack in MANET using AODV routing protocol. In Proceedings of the 2016 Symposium on Colossal Data Analysis and Networking (CDAN), Indore, India, 18–19 March 2016; pp. 1–5.
18. Liu, Q.; Yin, J.; Leung, V.C.M.; Cai, Z. FADE: Forwarding Assessment Based Detection of Collaborative Grey Hole Attacks in WMNs. *IEEE Trans. Wirel. Commun.* **2013**, *12*, 5124–5137. [CrossRef]
19. Gupta, J. Improved approach of co-operative gray hole attack prevention monitored by meta heuristic on MANET. In Proceedings of the 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC), Solan, India, 21–23 September 2017; pp. 356–361.
20. Pal, S.; Sikdar, B.; Chow, J.H. An Online Mechanism for Detection of Gray-Hole Attacks on PMU Data. *IEEE Trans. Smart Grid* **2018**, *9*, 2498–2507. [CrossRef]
21. Venu, V.S.; Avula, D. Invincible AODV to detect black hole and gray hole attacks in mobile ad hoc networks. *Int. J. Commun. Syst.* **2018**, *31*, 1–19.
22. Tamilselvi, P.; Ganesh Babu, C. An efficient approach to circumvent black hole nodes in MANET. *Clust. Comput.* **2017**, 1–9. [CrossRef]
23. Arulkumaran, G.; Gnanamurthy, R.K. Fuzzy Trust Approach for Detecting Black Hole Attack in Mobile Ad hoc Network Mobile. *Netw. Appl.* **2017**, 1–8.
24. Gopinath, S.; Vinoth Kumar, K.; Jaya Sankar, T. Secure location aware routing protocol with authentication for data integrity. *Clust. Comput.* **2018**, 1–10. [CrossRef]
25. Mohanapriya, M.; Krishnamurthi, I. Modified DSR protocol for detection and removal of selective black hole attack in MANET. *Comput. Electr. Eng.* **2014**, *40*, 530–538. [CrossRef]
26. Arathy, K.S.; Sminesh, C.N. A Novel Approach for Detection of Single and Collaborative Black Hole Attacks in MANET. *Procedia Technol.* **2016**, *25*, 264–271. [CrossRef]

27. Chang, J.; Tsou, P.; Chao, H.; Chen, J. CBDS: A Cooperative Bait Detection Scheme to prevent malicious node for MANET based on hybrid defense architecture. In Proceedings of the 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology (Wireless VITAE), Chennai, India, 28 February–3 March 2011; pp. 1–5.
28. Gurung, S.; Chauhan, S. A dynamic threshold based algorithm for improving security and performance of AODV under black-hole attack in MANET. *Wirel. Netw.* **2017**, 1–11. [CrossRef]
29. Gurung, S.; Chauhan, S. A dynamic threshold based approach for mitigating black-hole attack in MANET. *Wirel. Netw.* **2018**, *24*, 2957–2971. [CrossRef]
30. Vijayakumar, K.; Somasundaram, K. An Effective CBHDAP Protocol for Black Hole Attack Detection in MANET. *Indian J. Sci. Technol.* **2016**, *9*, 1–11.
31. Panos, C.; Ntantogian, C.; Malliaros, S.; Xenakis, C. Analyzing, quantifying, and detecting the black hole attack in infrastructure-less networks. *Comput. Netw.* **2017**, *113*, 94–110. [CrossRef]
32. Dorri, A. An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET. *Wirel. Netw.* **2017**, *23*, 1767–1778. [CrossRef]
33. Kshatriya, N.; Mallawat, K.; Biswas, A.S. Security in MANET using Detection Engine. In Proceedings of the 2016 International Conference on Computing, Analytics and Security Trends (CAST), Pune, India, 19–21 December 2016; pp. 128–132.
34. Dhende, S.; Musale, S.; Shirbahadurkar, S.; Najan, A. SAODV: Black hole and gray hole attack detection protocol in MANETs. In Proceedings of the 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 22–24 March 2017; pp. 2391–2394.
35. Shahabi, S.; Ghazvini, M.; Bakhtiarian, M. A modified algorithm to improve security and performance of AODV protocol against black hole attack. *Wirel. Netw.* **2016**, *22*, 1505–1511. [CrossRef]
36. Kamel, M.B.M.; Alameri, I.; Onaizah, A.N. STAODV: A secure and trust based approach to mitigate black hole attack on AODV based MANET. In Proceedings of the IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, China, 25–26 March 2017; pp. 1278–1282.
37. Vijaya, K.K.; Somasundaram, K. IBFWA: Integrated Bloom Filter in Watchdog Algorithm for hybrid black hole attack detection in MANET. *Inf. Secur. J. Glob. Perspect.* **2017**, *26*, 49–60.
38. Kumar, R.; Chadha, R. Mitigation of black hole attack using generic algorithms and fuzzy logic. *Int. J. Eng. Sci. Res. Technol.* **2016**, *5*, 818–826.
39. Dhakaa, A.; Nandal, A.; Dhaka, R.S. Gray and Black Hole Attack Identification using Control Packets in MANETs. *Procedia Comput. Sci.* **2015**, *54*, 83–91. [CrossRef]
40. Sharma, N.; Bisen, A.S. Detection as well as removal of black hole and gray hole attack in MANET. In Proceedings of the 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, India, 3–5 March 2016; pp. 3736–3739.
41. Li, Y.; Peng, S.; Chu, W. An Efficient Algorithm for Finding an Almost Connected Dominating Set of Small Size on Wireless Ad Hoc Networks. In Proceedings of the 2006 IEEE International Conference on Mobile Ad Hoc and Sensor Systems, Vancouver, BC, Canada, 9–12 October 2006; pp. 199–205.
42. Kukreja, D.; Dhurandher, S.K.; Reddy, B.V.R. Power aware malicious nodes detection for securing MANETs against packet forwarding misbehavior attack. *J. Ambient Intell. Humaniz. Comput.* **2018**, *9*, 941–956. [CrossRef]
43. Abdelhaq, M.; Serhan, S.; Alsaqour, R.; Hassan, R. A local intrusion detection routing security over MANET network. In Proceedings of the 2011 International Conference on Electrical Engineering and Informatics, Bandung, Indonesia, 17–19 July 2011; pp. 1–6.
44. Thanuja, R.; Umamakeswari, A. Black hole detection using evolutionary algorithm for IDS/IPS in MANETs. *Clust. Comput.* **2018**, 1–13. [CrossRef]