Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 9812135, 10 pages
https://doi.org/10.1155/2018/9812135

Research Article

Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique

Adwan Yasin and Mahmoud Abu Zant

Computer Science Department, Arab American University, Jenin, State of Palestine

Correspondence should be addressed to Adwan Yasin; adwan.yasin@aauj.edu

Received 13 April 2018; Revised 29 July 2018; Accepted 19 August 2018; Published 6 September 2018

Academic Editor: Luca Reggiani

Mobile Ad hoc Network (MANET) is a type of wireless networks that provides numerous applications in different areas. Security of MANET had become one of the hottest topics in networks fields. MANET is vulnerable to different types of attacks that affect its functionality and connectivity. The black-hole attack is considered one of the most widespread active attacks that degrade the performance and reliability of the network as a result of dropping all incoming packets by the malicious node. Black-hole node aims to fool every node in the network that wants to communicate with another node by pretending that it always has the best path to the destination node. AODV is a reactive routing protocol that has no techniques to detect and neutralize the black-hole node in the network. In this research, we enhanced AODV by integrating a new lightweight technique that uses timers and baiting in order to detect and isolate single and cooperative black-hole attacks. During the dynamic topology changing the suggested technique enables the MANET nodes to detect and isolate the black-hole nodes in the network. The implementation of the proposed technique is performed by using NS-2.35 simulation tools. The results of the suggested technique in terms of Throughput, End-to-End Delay, and Packet Delivery Ratio are very close to the native AODV without black holes.

1. Introduction

Wireless communication network could be controlled by a central infrastructure that controls communication between nodes in the network, or it could be an infrastructure-less which is called Ad hoc Networks. Mobile Ad hoc Network (MANET) is an application of the Wireless Ad hoc Network (WANET) that connects mobile nodes to each other. In MANET, nodes do not rely on a central node to coordinate the communication or to carry data between them; instead of that, they work together to carry data between nodes that cannot reach each other directly. In other words, nodes may work as a bridge between the sender and the receiver node when sender and receiver are not in the same coverage. The mobility of the nodes leads to a dynamic changing in the network topology. MANET routing protocols are designed to be adaptive to any dynamic topology changes [1]. MANET energy is one of the most important connectivity factors, as each node in the network has a limited amount of energy; consequently, we should work with an efficient mechanisms and protocols that avoid any unnecessary energy consumption. MANET connects nodes to each other using a wireless link, where bandwidth is considered an important network property. The bandwidth of the wireless links is much lower than the wired links. Wireless links signal can be affected by a noise, interference from another signal, or fading [2]. MANET is vulnerable to different types of attacks and threats. Since MANET uses wireless links to connect nodes together, data may be viewed or modified by an unauthorized user and that is called eavesdropping threat. MANET has no central infrastructure that controls the communication between nodes, so nodes rely on themselves to deliver data to the destination node. Thus, a malicious attacker node may alter the connection link or drop the forwarded data. Denial of Service (DoS) attack is considered one of the most serious threats to MANET, in which a malicious attacker node drains the battery of other nodes by requesting them to forward a huge amount of data. Attacks in MANET are divided into active and passive attacks. In active attacks, the attacker nodes work to affect the MANET operation, by

dropping the forwarded data, altering the connection links, or draining the nodes batteries. In passive attacks, the attacker nodes only eavesdrop on the communication between nodes without affecting the communication operation between them [3]. The rest of the paper is organized as follows: Section 2 presents a background about the black-hole attack in MANET and AODV routing protocol, Section 3 discusses the related work, Section 4 presents the proposed model, and Section 5 describes the methodology that is used to test the proposed model. Section 6 shows the results of the proposed model and comparison with other proposed models, and finally, the conclusion is shown in Section 7.

2. Background

2.1. Black-Hole Attack. It is an active attack type where the attacker node claims that it has the shortest route to any desired node in the network even if it does not have any route to it; consequently all the packets will pass through it and this enables the black-hole node to forward or discard packets during the data transmission. Normal nodes trust any reply for the requests that they broadcast and black-hole node takes the advantage of this and keeps replying to any request claiming that it has the shortest path to the desired node. Normally nodes start discovery phase in order to find a path to the destination node. The source node broadcasts a request to the destination node, any node receiving this request checks if it has a fresh path to the destination node. When black-hole node receives this request it immediately sends a reply to the broadcaster claiming that it has the freshest and the shortest path to the destination node. Source node believes that reply because there is no mechanism to verify that the request is from a normal node or from a black-hole node. Source node starts forwarding packets to black-hole node hoping to deliver these packets to the destination node, then black-hole node starts to drop these forwarded packets. Figure 1 shows an example of MANET black-hole attack. The black-hole attacks can be classified into two types: single and cooperative black-hole attacks where the classification is based on the number of attacker nodes. In a single black-hole attack, only one attacker node is active while in a cooperative black-hole attack, there is a group of attacker nodes that work together [4] in order to degrade the network reliability.

As shown in Figure 1 when source node requests a route to the destination node, black-hole node claims it has the shortest path to that desired node. Source node starts to forward packets to the black-hole node hoping to deliver these packets to the destination node; black-hole node drops all the forwarded packets to prevent the communication between the source and the destination node.

2.2. AODV. In this research, we have chosen Ad hoc On-Demand Distance Vector (AODV) routing protocol because it has a better performance characteristics than other reactive routing protocols under different performance metrics according to [5]; the reason that AODV is better than other reactive routing protocols is that it combines the techniques of both DSR routing protocol and DSDV and gets the advantages of both of them. The link creation between two

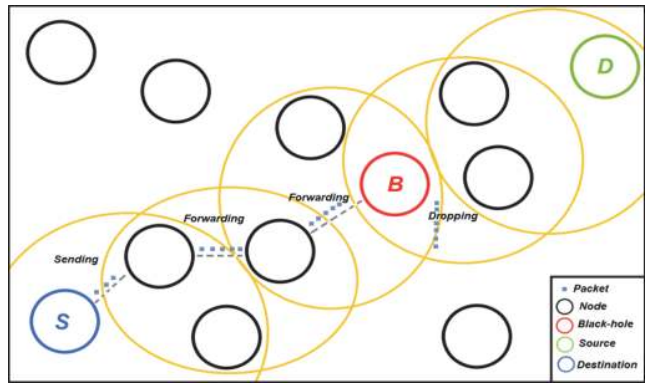

Figure 1: Illustration of black-hole attack in MANET.

nodes using AODV needs two types of control packets called route request (RREQ) and Route Reply (RREP). RREQ is broadcasted to adjacent nodes to ask them for a route to the desired node, nodes keep forwarding RREQ until it reaches the destination node, or a node that has a path to it. RREP is sent to the source node from the destination node or from an intermediate node that has a path to the destination node. After receiving a RREP source node starts to send packets to the destination node. In [6], the performance of the reactive routing protocol under different types of attacks has been studied. They found that the performance decreases upon attacks especially the black-hole attack in terms of Packet Delivery Ratio (PDR) and Throughput. In [7], they studied the performance of AODV under black-hole attack. They found that the black-hole attack has a huge impact on Throughput, End-to-End Delay, and Packet Delivery Ratio.

2.3. Problem Statement. Security of MANET is essential to prevent the harm that could be caused by different types of attacks. The black-hole attack is considered to be one of the popular attacks that harm the network and aim to prevent any connection in the network. AODV routing protocol works to find the shortest path between any two nodes that want to communicate in the network when the path is needed. AODV protocol is not provided with an algorithm that helps in detecting and preventing the black-hole attack. In this paper, we aim to enhance the AODV routing protocol with a lightweight technique to detect the black-hole attack and prevent its harm in the network.

3. Related Work

In this section, we are going to describe the developed techniques especially baiting techniques against black-hole attacks in reactive routing protocol and the limitations of each technique and how smart black-hole attack may overcome the developed technique. In terms of smart black-hole attack, we mean that the attacker node knows the used technique and it can use all of its features against the other MANET nodes.

In [8], the developed baiting technique depends on the own node id. The detection of black-hole node starts by broadcasting a bait request to all adjacent nodes. The bait request contains source sequence number (SSN) and source

id; when source node receives replies it checks if there is a reply that has a higher DSN than its own SSN; this indicates that the reply came from a black-hole since there is no node in the network should have a higher DSN than SSN of the source node. After the detection of the black-hole node in the network, source node broadcasts a black-hole alarm to all adjacent nodes to notify them. The limitations of this technique are that a smart black-hole node can check if the received RREQ asks for a route to the same source of the RREQ, then it simply does not reply to that request. Also, smart black-hole node can use the black-hole alarm and starts broadcasting false black-hole alarms to isolate selective nodes in the network.

In [9, 10], they developed a technique which depends on using Cooperative Bait Detection method Scheme (CBDS). In CBDS the detection of a black-hole is divided into three phases Bait, Reverse Trace, and Reactive Defense. In Bait phase source node selects one of its neighbors randomly and sends a bait request using its id. In Reverse Trace phase a list of the suspicious nodes is created from the RREP of the bait RREQ, then the neighbor nodes enter in promiscuous mode to detect if there is an attacker node in the path. For each black-hole node detected in the network, a black-hole alarm is broadcasted to neighbor nodes. In Reactive Defense phase source node checks if the PDR is lower than a determined threshold, then it runs Bait phase again. The limitation of this technique is that the nodes enter a promiscuous mode which is not acceptable to all nodes. Since some nodes do not want any unauthorized user to listen to their own transmissions, also being in promiscuous mode will facilitate passive attacks. A smart black-hole node can use the black-hole alarm feature and start broadcasting false black-hole alarms to isolate network nodes.

In [11], the developed scheme depends on using a fake id to bait a black-hole node. Source node starts by broadcasting a bait request that contains an id that does not exist in the network. The black-hole node will reply to that bait RREQ due to its normal behavior which replies to any RREQ in the network calming that it has the best path. The developed scheme is implemented in DSR so they modified the RREQ and RREP header in order to determine the black-hole node within the path. An alert is broadcasted to neighbor nodes when a black-hole node is detected. Source node keeps checking if there is a decrease below the determined threshold; it then starts the baiting again. The limitations of this scheme are that it increases the size of the control packets (RREQ and RREP) which leads to increase in the overhead in addition to the black-hole alerts that can be used by a smart black-hole to isolate nodes in the network.

In [12], the proposed model starts by flooding a fake request in the network. Any node reply is considered as a suspicious node; with the help of the neighbor nodes a black-hole node can be detected by checking if the suspicious node is forwarding packets to the destination node. The proposed model has a localization system that gives the position of the black-hole node since the model is developed to be used in the military. The limitation of this model is that it floods the network with a fake request, which may lead to congestion in the network.

In [13], the proposed system depends on a special type of nodes that is called guard nodes, which help in detecting black-hole nodes in the network. Guard nodes are nodes that are in the promiscuous mode that check the behavior of other nodes in the network. Guard nodes contain tables that record the behavior of the nodes in the network. Each node has a trust value that is determined according to its behavior in the network, and it decreases when the node only sends RREP and does not send RREQ. If the trust value of a node decreases below the determined threshold, then it is blocked or isolated. Guard nodes broadcast an alarm to all adjacent nodes when a black-hole node is detected. The limitations of this system are that it needs a special type of nodes (guard nodes) and a huge number of guard nodes to cover all the network; also this system has a high overhead because of having many tables.

In [14], the proposed model depends only on a validity bit that is set in RREP; in this model it is assumed that the attacker node is unaware of validity bit that should be sent upon sending the RREP. When the source node receives RREP it checks the validity bit if it is set to one, then it uses that path and if not then it considers the RREP from a black-hole node and discards it. The limitation of this model is the unrealistic assumption since attacker node who wants to attack network will use the same protocol and it will analyze it before the attacking, so any smart black-hole node will notice this validity bit and send an RREP to any request with a set validity bit.

In [15], the proposed model called SAODV detects black-hole and gray-hole nodes depending on neighbor nodes opinion. All nodes in SAODV contain two tables neighbor list (NL) which contains ids of neighbor nodes and opinion list (OL) which is used to classify nodes depending on their activities in the network. When the source node receives a reply to a route request it broadcasts an opinion message to neighbors requesting their opinions about the node that claims that it has the shortest path. If all nodes responded with NO message, then this node is a black-hole node; if some nodes responded with YES message and the rest with NO message then this node is a gray-hole node; otherwise, it is a normal node. If a black node is detected a notification alarm is broadcasted to the network. The limitations of this model are high overhead in the allocated space for OL tables and overhead in the opinion exchanged messages; in addition to that smart black-hole nodes can send a false opinion when they are requested for that which enables them to isolate normal nodes.

In [16], the proposed model uses fabricated requests to detect black-hole nodes in the network. Source starts by broadcasting a fabricated request in the network, any node reply to the fabricated request is considered as a black-hole node. Source node stores the average DSN received replies of the fabricated request. In this model, the source node broadcasts a request to the desired node; if it receives a reply it checks the reply DSN if it is close to the DSN stored average, then destination node considered e as a black-hole node; otherwise, the node is normal. The proposed model is provided with a prevention technique that uses digital signatures and trust value to reduce the effect of black-hole node in the network. We will compare our proposed model

with this model as we consider it the best-suggested model. We will also compare our model with the suggested model in [8].

There are several techniques and mechanisms that are implemented in AODV and DSR that are used to detect and isolate the black-hole node in MANET [4, 17, 18]. Some of these techniques depend on the value of the destination sequence number (DSN) that is used in AODV to determine the freshness of the route, because black-hole node always replies to any request and it always sets a high DSN value as in [19]. Some of the implemented techniques depend on neighbor nodes to determine the behavior of other nodes which is called Watchdog techniques where nodes are in promiscuous mode in which they start to listen and ensure that the other nodes are forwarding packets; in this way nodes can determine if there is a black-hole node that does not forward packets to other neighbors as in [20]. Some of the developed techniques use a trust-based algorithm, where each node in the network has a trust value that is determined by the behavior of the node in the network. If the value of the node is too low, then it is considered as a black-hole node as in [21]. And some of the used techniques use a fake packet as bait to detect black-hole nodes in the network. In batting techniques, nodes send a request for a nonexisting node in the network and wait for a reply for it since black-hole node always replies for any request, then black-hole node replies for the request of the fake node as in [11]. After reading and observing the baiting techniques that are used in MANET to detect black-hole node in the network we concluded three different baiting techniques.

(A) Baiting using own node id where any node wants to bait a black-hole node: it broadcasts a request contains its own id. When it receives a reply it checks if any of these replies has a higher DSN than its own source sequence number (SSN), then it is considered as a black-hole node, since it always replies to any request with a high DSN as in [8].

(B) Baiting using one of the neighbors ids where any node wants to bait a black-hole node: it selects one of the neighbor node ids and broadcasts a bait request which contains that neighbor id. Any node which sends a reply for that bait request may indicate that there is a black-hole node in the network, then the source node keeps track of the suspicious node and it identifies as a normal node or a black-hole node as in [9].

(C) Baiting using fake id where any node wants to bait a black-hole node: it broadcasts a request that contains a fake id that does not exist in the network. Any node which replies to that bait request is immediately considered as a black-hole as in [11].

The proposed technique uses fake id baiting technique in order to detect black-hole nodes in the network because of the following:

(i) Using own node id technique can be countered by black-hole node by checking that the requester node is the same as the destination node so the black-hole node will not respond to that request.

(ii) Using the neighbor id technique requires a lot of exchanged messages between neighbors which increases the network overhead.

(iii) Fake node id technique is hard to counter by the black-hole node as black-hole node does not know the ids of all nodes in the network.

4. Proposed Technique

The proposed technique is developed to resist smart black-hole attacks by employing timers and baiting messages (see Figure 2). The proposed technique consists of two phases: Baiting and Nonneighbor Reply. In Baiting phase each node has a bait-timer, the value of the timer is set randomly to B seconds, and each time the timer reaches B it creates and broadcasts a bait request with a randomly generated fake id. Depending on the natural behavior of a black-hole node when it receives any route request it responds with a reply claiming that it has the best path even if it does not exist. When the black-hole receives the baited request it sends a reply to the source node claiming that it has a route; when the source node receives the reply it immediately considers the node which responded as a black-hole and adds it to the black-hole list because it claimed to have a route to a fake node. In the bait request, the value of TTL (Time-To-live) is set to one in order to avoid congesting the network with fake requests. As in a native AODV when any node wants to communicate with another in the network it broadcasts RREQ to the destination node. In Nonneighbor Reply phase each node knows its adjacent nodes because of the hello message broadcasting process. When the source node receives a reply it checks the id of the Node With the Shortest Path (NWSP) if it is in the black-hole list; then it discards the reply; otherwise it checks if the id exists in the neighbor list by comparing the ID with ones in the neighbor list; if NWSP is not a neighbor node then the source node discards that reply to avoid any communication with unknown nodes. The proposed technique provides a self-detection and isolation for any black-hole node which enables the connectivity between MANET nodes. The suggested technique does not use the black-hole alarm in order to prevent any smart black-hole node from using this feature by broadcasting false alarms. We set the TTL of the bait request to one to avoid congesting the network by bait requests and responses. The randomness in both fake id and bait-timer will prevent the black-hole node from identifying any pattern to counter this technique. No overhead and special packets are used which make it a lightweight technique.

As shown in Figure 3 each node broadcasts hello message to identify its adjacent nodes. In Baiting phase each node creates a bait request with a random fake id and with a TTL equal to 1 and then broadcasts the bait requests to all its adjacent nodes; both black-hole nodes B1 and B2 will reply to the bait request. Nodes 2, 7, and 8 will add node B1 to their black-hole list because node B1 replied for each bait came from 2, 7, and 8 based on the natural behavior of the black-hole node that it replies to each request even if it does not have an existing route for the desired node. Nodes 6, 7, 9,

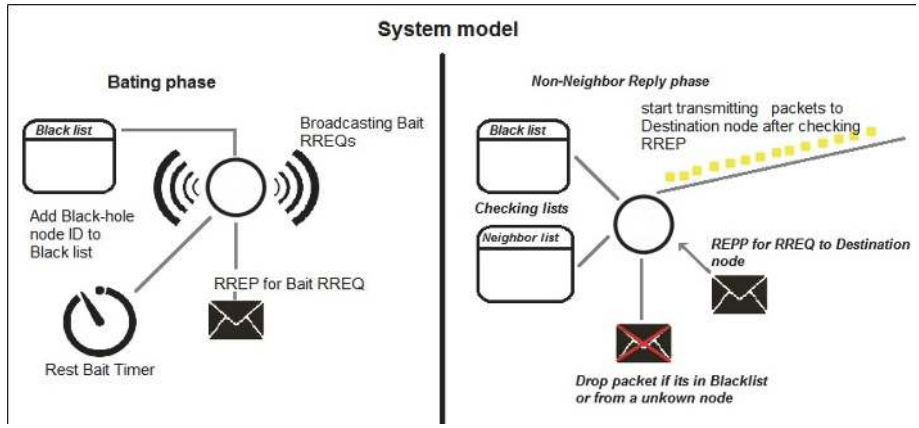

Figure 2: The proposed system model.

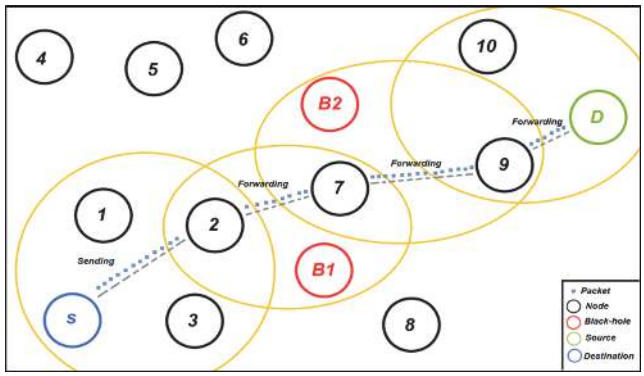

Figure 3: Sketch of black holes and baiting request.

and 10 will add B2 in their black-hole list because node B2 also replied for each bait request which came from 6, 7, 9, and 10. Each node resets bait-timer with a randomly B sec, when S wants to communicate with node D it broadcasts RREQ. Node 2 sends RREP claiming that it has the best path; node S checks if node 2 exits in its neighbor list or not; since node 2 in node S coverage then node 2 is in the neighbor list and node S starts to transmit data through 2 to D. Algorithms of the suggested technique are described in Algorithms 1 and 2.

Table 1: Environment parameters.

Simulation Environment Parameters
Speed
Maximum 15 mps
Pause Time
Pasue:5s
Time
Simulation Time 200s
Terrain
Coordination 1000∗1000 m
Connection
CBR (Constant Bit Rate)
Item size 512(byte)
Radio/physical layer parameters:
Radio type: 802.11b Radio
Data rate: 0.5 Mbps
MAC Protocol: 802.11
Routing Protocol: AODV & TBBT_AODV
Transport Protocol: UDP
Node: 25,50,100, and 150
Node Placement: Random
Transmission range: 150 m

5. Methodology

In order to verify the correctness of the suggested technique TBBT, the simulation was performed using NS-2.35 simulator. The creation of the scenarios is done by using the CMU tool which is an NS-2.35 tool that can be invoked by using "*setdest*" command. CMU tool is used to create the random movement and placement of nodes. In our experiment, we set the initial position of both source node and the destination node at the opposite edges of the network. The black-hole node initial position was in the middle of the network. We set the coordination of the network 1000x1000 meter, packet size to 512 bytes, node transmission range to 150, simulation time to 200 seconds, nodes max speed to 15 meter per second, which means that nodes can move in average speed between zero and 15, and pause time to 5s, which means that when any node in the network changes its position it will sit still in its new position for 5 seconds before it moves to another position in the network, and finally we used UDP as a transport protocol. We avoid using TCP as a transport protocol because TCP is provided with algorithms that try to avoid the network congestion like TCP Reno and TCP New Reno, which may affect the performance metrics results, because we are testing our protocol performance, not the packet flows in the network. Table 1 contains all the information about the environment parameters.

We compared the performance of both native AODV and TBBT_AODV under black-hole attack in three performance

```
Source Node
1 if CurrentTime ==Bait_Time then
2    Create Bait request;
3    Generate a random ID and Set it in Bait request;
4    Set TTL of Bait request to 1;// TTL (Time-To-Live)
5    Broadcast Bait request;
6    Reset Bait-time to a random time;
7 end if
8 for each received Reply to the Bait request do
9    Store NWSP ID in the Black-hole list;// NWSP (Node With the Shortest Path)
10 end for
```

Algorithm 1: Baiting phase.

```
Source Node
1 Broadcast request to the Destination node as native AODV;
2 for each received Reply to the Destination node request do
3    if NWSP in the Black-hole list then
4     Discard reply;
5    end if
6    if NWSP not in neighbor list && Not from Destination node then
7     Discard reply;
8    else
9     Continue as native AODV and start transmitting packets to the Destination node;
10 end if
11 end for
```

Algorithm 2: Nonneighbor Reply phase.

metrics End-to-End Delay, Throughput, and Packet Delivery Ratio which are considered the most affected parameters under black-hole attack in AODV according to [7]. We used AWK script to analyze the trace file that is generated from running NS-2.35. Throughput indicates the amount of data received at destination node from the source node during the full transmission time. The unit which is used to measure the Throughput is kilobits per second (kbps). It can be computed using formula (1):

$$T = \frac{P_r}{C_t} * \frac{8}{1024} \tag{1}$$

where T is Throughput, P_r is the amount of received packets at the destination node, and C_t is the connection time between the source node and the destination node. Average End-to-End Delay indicates the amount of time that the source node needs to transfer packets to the destination node. The unit which is used to measure the End-to-End Delay is millisecond (ms). It can be computed using formula (2):

$$A_{EtE} = \sum_{i-1}^{n} Rt_i - \frac{St_i}{n} \tag{2}$$

where A_{EtE} is average of End-to-End Delay, Rt_i is receive time of the packets at node i, St_i is send time of the packets at node i, and n is the total number of nodes in the network. Packet Delivery Ratio indicates the ratio of packets successfully received at the destination node to packets sent from the source node. It can be computed using formula (3):

$$PDR = \frac{P_r}{P_s} \tag{3}$$

where PDR is Packet Delivery Ratio, P_r is the amount of received packets at the destination node, and P_s is the amount of sent packets from the source node.

6. Results

(A) Single Black-Hole Node. As shown in Figure 4 the result of Throughput in native AODV when there is a black-hole node in the network was the lowest because of the packet dropping caused by the black-hole node. The result of Throughput in native AODV when there is no black-hole node in the network was the highest. Looking at the results of TBBT showed a higher throughput than native AODV when there is a black-hole node, but lower than native AODV when there is no black-hole node in the network. The throughput enhancement of suggested TBBT is due to dropping any reply from unknown nodes that claims that they have a shorter path than any other node to the destination node which leads to decreasing the throughput. In addition, the position of the black-hole node plays an important rule, as it may be located in the shortest path between the source and destination.

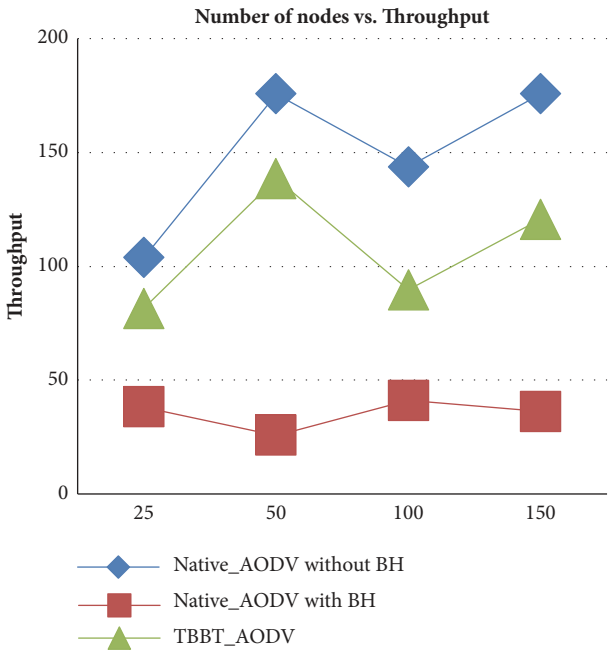

Figure 4: Results of Throughput versus the number of nodes.

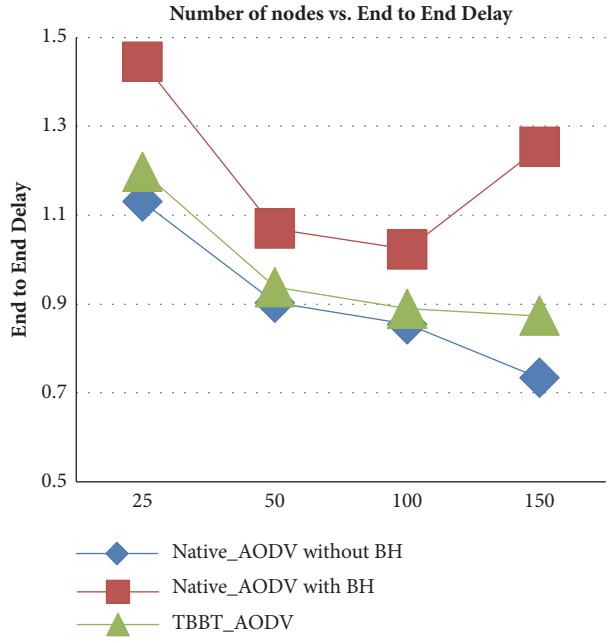

Figure 5: Results of average End-to-End Delay versus the number of nodes.

As shown in Figure 5 the result of End-to-End Delay in native AODV when there is a black-hole node in the network was the highest. The result of End-to-End Delay in native AODV when there is no black-hole node in the network was the lowest because of the AODV mechanism in selecting the shortest path. The results of TBBT showed a slight difference in End-to-End Delay results compared with native AODV when there is no black-hole node and this is because of the path selection mechanism in TBBT which remains the same as in native AODV.

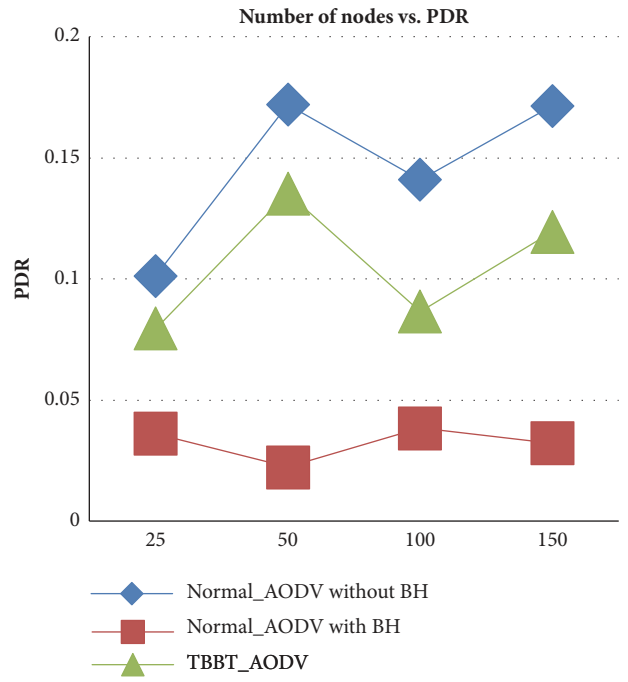

Figure 6: Results of PDR versus the number of nodes.

As shown in Figure 6 the result of PDR in native AODV when there is a black-hole node in the network was very low near zero because black-hole node always aims to the cut connection between any two nodes that try to communicate in the network and try to absorb all packets between them. The result of PDR in native AODV when there is no black-hole node in the network was the highest. Looking at the results of TBBT showed a higher PDR than native AODV when there is a black-hole node, but lower than native AODV when there is no black-hole node in the network. The PDR enhancement of suggested TBBT is because of the dropping of any reply that is from unknown node, which decreases PDR. In addition, the position of the black-hole node plays an important rule, as it may be located in the shortest path between the source and destination.

Table 2 shows the numeric results of Throughput, the average of End-to-End Delay, and Packet Delivery Ratio while the number of nodes increases.

(B) Cooperative Black-Hole Nodes. As shown in Figure 7 the result of native AODV against cooperative black-hole nodes showed a zero Throughput due to fact that increasing number of black-hole nodes in the network will indeed prevent the connection between the source node and the destination node. The result of Throughput in TBBT_AODV is decreased while increasing the number of black-hole nodes in the network. The drop in Throughput is because of the position of the black-hole that may be located in the path between the source node and the destination node, in addition to the fact that TBBT drops any reply from unknown nodes.

Table 2: Simulation results of dingle black hole.

Number of nodes	TBBT	Native_AODV Without BH	Native_AODV With BH
	Throughput (kpbs)		
25	81.388	103.835	38.162
50	138.527	175.736	25.644
100	89.642	143.648	41.051
150	120.600	175.689	36.148
	Avg of End-to-End Delay (ms)		
25	1.197	1.130	1.444
50	0.938	0.902	1.069
100	0.889	0.854	1.023
150	0.873	0.733	1.253
	Packet Delivery Ratio (%)		
25	0.07967	0.10135	0.03615
50	0.13542	0.17204	0.02245
100	0.08663	0.14097	0.03848
150	0.11960	0.17163	0.03219

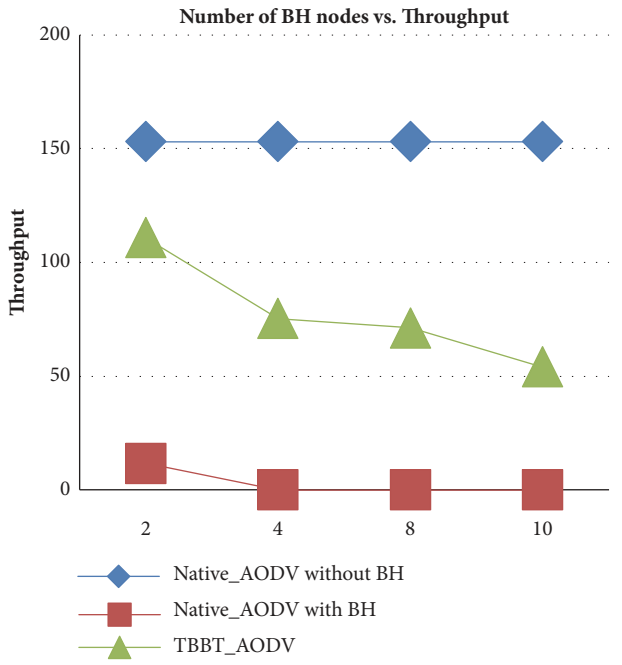

Figure 7: Results of Throughput versus the number of the black-hole nodes.

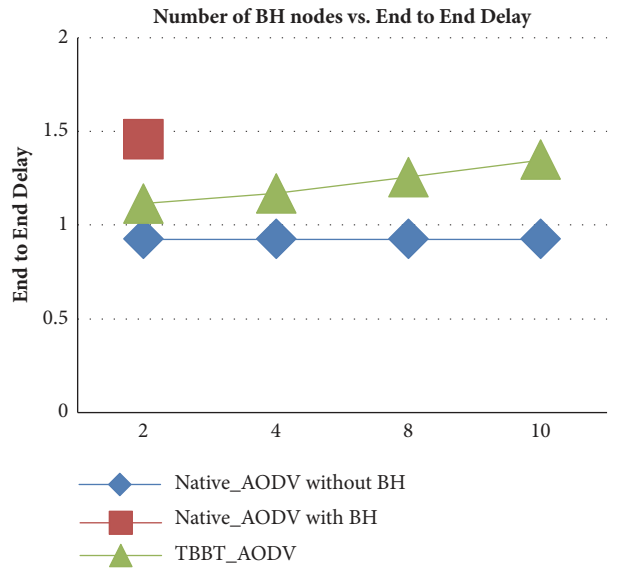

Figure 8: Results of average End-to-End Delay versus the number of black-hole nodes.

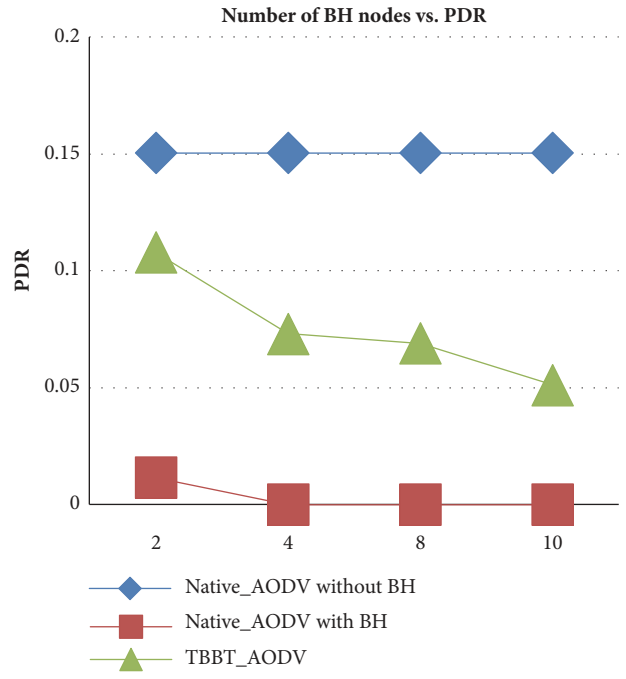

Figure 9: Results of PDR versus the number of the black-hole nodes.

As shown in Figure 8 the result of End-to-End Delay in native AODV when there were only two black-hole nodes in the network was the highest. Also when the number of black-hole nodes increased the connection between the source node and the destination node was prevented so the End-to-End Delay reached infinite. TBBT_AODV showed a slight difference End-to-End Delay results with native AODV while increasing number of black-hole nodes because the mechanism in selecting the path stays the same as in native AODV.

As shown in Figure 9 the result of native AODV against cooperative black-hole nodes showed a zero PDR because when the number of black-hole increases they will cover the whole network, which will indeed cut any communication between any two nodes in the network. The result of PDR in TBBT_AODV is decreased while increasing the number of black-hole nodes in the network. The decrease in PDR is because of the position of the black-hole nodes that may be located in the path between the source node and the

Table 3: Simulation results of cooperative black holes.

Number of BH	TBBT	Native_AODV Without BH	Native_AODV With BH
Throughput (kpbs)			
2	110.794	153.044	11.651
4	75.368	153.044	0
8	71.167	153.044	0
10	53.987	153.044	0
Avg of End-to-End Delay (ms)			
2	1.113	0.925	1.444
4	1.168	0.925	∞
8	1.254	0.925	∞
10	1.348	0.925	∞
Packet Delivery Ratio (%)			
2	0.10795	0.15045	0.01157
4	0.07318	0.15045	0
8	0.06901	0.15045	0
10	0.05128	0.15045	0

Table 4: Comparison results between TBBT and PAODV.

Metric	TBBT	PAODV
End-to-End Delay	22.31%(decrease)	70%(decrease)
Throughput	373.0% (increase)	12%(increase)

Table 5: Comparison results between TBBT and DAODV.

Metric	TBBT	DAODV
End-to-End Delay (Native AODV without Black-hole attack)	3.78% (increase)	1.69% (decrease)
Throughput (Native AODV without Black-hole attack)	15.60% (decrease)	29.69% (decrease)
End-to-End Delay (Native AODV with Black-hole attack)	9.04% (decrease)	33.48% (decrease)
Throughput (Native AODV with Black-hole attack)	542.85% (increase)	108.45% (increase)

destination node, in addition to the fact that TBBT drops any reply from unknown nodes.

Table 3 shows the numeric results of Throughput, the average of End-to-End Delay, and Packet Delivery Ratio while the number of black-hole nodes increases.

(C) Comparison with Other Proposed Models. We implemented our proposed model in two different scenarios in order to compare it with other models [8, 16] described in Section 4. We called the proposed model in [16] PAODV. PAODV cannot be countered by a smart black-hole node, unlike other proposed techniques which are previously discussed in Section 4. We simulated TBBT in the same metric as in PAODV where the number of nodes is varying from 15 to 50. TBBT obtained 22.31% decrease in End-to-End Delay and 373.0% increase in Throughput. The results of the simulation are shown in Table 4. By comparing the two results it is clear that TBBT is better than PAODV in terms of Throughput but not in terms of End-to-End Delay.

The second comparison is done with the proposed model in [8] which we called DAODV. We simulated TBBT using the same metrics as in DAODV where the mobility of nodes is varying from 0 to10. TBBT obtained a 3.78% increases in End-to-End Delay and 15.60% decreases in Throughput comparing to the native AODV without black-hole attack, a 9.04% decrease in End-to-End Delay and 542.85% increase in Throughput comparing to the native AODV with a black-hole attack. The results of the suggested model DAODV are shown in Table 5. It is clear that our proposed model is the best in terms of Throughput but not in terms of End-to-End Delay.

We should mention that when there is no nodes mobility, native AODV throughput is 151.529 in case if there is no black-hole node in the network otherwise the throughput is 14.346. TBBT throughput is 143.476 in case of black-hole existence which is very close to the native AODV and this is because the changing in the topology is very low and TBBT will not drop any packet from a known node within its range so there are no replies from unknown nodes.

7. Conclusions

The black-hole attack is considered to be one of the most serious attacks that affect the operation of MANET. The detection and isolation of any black-hole nodes in the network are considered an essential task to prevent network collapse. In this research, we introduced a smart black-hole detection and isolation technique that should be considered in constructing and developing any black-hole fighting protocols or techniques. The proposed TBBT integrates both timers and baiting techniques in order to enhance black-hole detection capability while preserving Throughput, End-to-End Delay, and Packet Delivery Ratio. The simulation results of the proposed technique showed that the End-to-End Delay, Throughput, and Packet Delivery Ratio are very close to the native AODV. As a future work, we aim to enhance the proposed model in order to increase the Throughput and Packet Delivery Ratio also to decrease the End-to-End Delay.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] S. Mirza and S. Z. Bakshi, "Introduction to MANET," *International Research Journal of Engineering and Technology*, vol. 5, no. 1, pp. 17–20, 2018.

[2] V. Goyal and G. Arora, "Review paper on security issues in mobile adhoc networks," *International Research Journal of Advanced Engineering and Science*, vol. 2, no. 1, pp. 203–207, 2017.

[3] M. M. Alani, "MANET security: A survey," in *Proceedings of the 2014 IEEE International Conference on Control System, Computing and Engineering (ICCSCE)*, pp. 559–564, Penang, Malaysia, November 2014.

[4] A. Joshi, "A review paper on black hole attack in MANET," *International Journal of Advance Research in Computer Science and Management Studies*, vol. 4, no. 5, pp. 16–21, 2016.

[5] A. K. S. Ali and U. V. Kulkarni, "Comparing and analyzing reactive routing protocols (aodv, dsr and tora) in QoS of manet," in *Proceedings of the 7th IEEE International Advanced Computing Conference, IACC 2017*, pp. 345–348, Hyderabad, India, January 2017.

[6] L. Prashar and R. K. Kapur, "Performance analysis of routing protocols under different types of attacks in MANETs," in *Proceedings of the 5th International Conference on Reliability, Infocom Technologies and Optimization, ICRITO 2016*, pp. 405–408, Noida, India, September 2016.

[7] H. Moudni, M. Er-Rouidi, H. Mouncif, and B. El Hadadi, "Performance analysis of AODV routing protocol in MANET under the influence of routing attacks," in *Proceedings of the 2nd International Conference on Electrical and Information Technologies, ICEIT 2016*, pp. 536–542, Tangiers, Morocco, May 2016.

[8] N. Kalia and H. Sharma, "Detection of Multiple Black hole nodes attack in MANET by modifying AODV protocol," *International Journal on Computer Science and Engineering*, vol. 8, no. 5, pp. 160–174, 2016.

[9] P. L. Chelani and S. T. Bagde, "Detecting collaborative attacks by malicious nodes in MANET: An improved bait detection scheme," in *Proceedings of the 2016 International Conference on Communication and Electronics Systems, ICCES 2016*, Coimbatore, India, October 2016.

[10] M. Sathya and M. Priyadharshini, "Detection and removal of black hole attack in mobile ad-hoc networks using cooperative bait detection method scheme," *International Journal of Scientific & Engineering Research*, vol. 7, no. 3, pp. 81–85, 2016.

[11] P.-C. Tsou, J.-M. Chang, Y.-H. Lin, H.-C. Chao, and J.-L. Chen, "Developing a BDSR scheme to avoid black hole attack based on proactive and reactive architecture in MANETs," in *Proceedings of the 13th International Conference on Advanced Communication Technology: Smart Service Innovation through Mobile Interactivity, ICACT 2011*, pp. 755–760, Seoul, Republic of Korea, February 2011.

[12] B. Singh, D. Srikanth, and C. R. S. Kumar, "Mitigating effects of black hole attack in mobile Ad-Hoc NETworks: Military perspective," in *Proceedings of the 2nd IEEE International Conference on Engineering and Technology, ICETECH 2016*, pp. 810–814, Coimbatore, India, March 2016.

[13] A. R. Rajeswari, K. Kulothungan, and A. Kannan, "GNB-AODV: guard node based –aodv to mitigate black hole attack in MANET," *International Journal of Scientific Research in Science, Engineering and Technology*, vol. 2, no. 6, pp. 671–677, 2016.

[14] S. R. Deshmukh, P. N. Chatur, and N. B. Bhople, "AODV-Based secure routing against blackhole attack in MANET," in *Proceedings of the 1st IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology, RTEICT 2016*, pp. 1960–1964, Bangalore, India, May 2016.

[15] S. Dhende, S. Musale, S. Shirbahadurkar, and A. Najan, "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)*, pp. 2391–2394, Chennai, India, March 2017.

[16] M. Sathish, K. Arumugam, S. N. Pari, and V. S. Harikrishnan, "Detection of single and collaborative black hole attack in MANET," in *Proceedings of the 2016 IEEE International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2016*, pp. 2040–2044, Chennai, India, March 2016.

[17] H. Kaur and K. Mangat, "Black hole attack in mobile ad hoc networks: a review," *International Journal of Advance Research, Ideas and Innovations in Technology*, vol. 3, no. 2, pp. 189–191, 2017.

[18] K. Kumar and T. S. Aulakh, "Black hole attack in MANETs preventions and advancements: a review," *International Journal of Computer Applications International Conference on Advances in Emerging Technology*, vol. 12, pp. 4–9, 2016.

[19] S. K. Arora, S. Vijan, and G. S. Gaba, "Detection and analysis of black hole attack using IDS," *Indian Journal of Science and Technology*, vol. 9, no. 20, pp. 1–5, 2016.

[20] T. Varshney, T. Sharma, and P. Sharma, "Implementation of Watchdog Protocol with AODV in Mobile Ad Hoc Network," in *Proceedings of the 2014 International Conference on Communication Systems and Network Technologies (CSNT)*, pp. 217–221, Bhopal, India, April 2014.

[21] A. Jain, U. Prajapati, and P. Chouhan, "Trust based mechanism with AODV protocol for prevention of black-hole attack in MANET scenario," in *Proceedings of the 2016 Symposium on Colossal Data Analysis and Networking, CDAN 2016*, Indore, India, March 2016.