An Efficient Scheme for Detection and Prevention of Black Hole Attacks in AODV-Based MANETs

Muhammad Salman Pathan[1], Jingsha He[2], Nafei Zhu[3], Zulfiqar Ali Zardari[4], Muhammad Qasim Memon[5], Aneeka Azmat[6]

Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China[1, 2, 3, 4]
Advanced Innovation Centre for Future Education, Beijing Normal University, Beijing, China[5]
School of Information, Computer, and Communication Technology[6]
Sirindhorn International Institute of Technology (SIIT)[6]
Thammasat University Pathum-Thani, Thailand[6]

***Abstract*—Mobile ad hoc network (MANET) is a set of independent mobile nodes, which connect to each other over a wireless channel without any centralized infrastructure, nor integrated security. MANET is a weak target to many Denial of Service (DOS) attacks, which seriously harms its functionality and connectivity. A black hole attack is a type of DOS attack, where the malevolent node tries to get all the data packets from a source node by sending fabricated fake route reply (RREP) packet, falsely pretending that it possesses the shortest path towards the destination node, and then drops all the packets it receives. In this paper, the AODV (Ad-hoc on-demand distance vector) routing protocol is improved by incorporating an efficient and simple mechanism to mitigate black hole attacks. Mechanism to detect black hole attacks from MANET (MDBM) uses fake route request (RREQ) packets with an unreal destination address in order to detect black hole nodes prior to the actual routing process. Simulation experiment conducted has verified the performance of the proposed detection and prevention scheme. The results demonstrated that the proposed mechanism performed well in terms of Packet Delivery Ratio, End-to-End Delay and Throughput under black hole attack.**

***Keywords*—Mobile ad hoc network; denial of service; black hole; fake route request packet; AD-hoc on-demand distance vector**

I. INTRODUCTION

As the advancements in pervasive wireless networks are at verge, MANETs has attracted the attention of the researchers around the globe recently [1]. MANET comprises of a set of nodes which are randomly distributed across network [2] and they can comminute with each other without any help of a centralized management or a fixed infrastructure [3]. In a MANET, nodes do not rely on a central node to coordinate with each other; instead, they work in a co-operative manner in order to carry the data between nodes [4], which are far from each other's. Therefore, all the nodes in the network must discover and maintain routes to other nodes. In MANETs, the nodes have constrained resources such as limited battery, bandwidth and a high mobility factor [5], which distinguish MANETs from other wireless networks [6]. Despite the mentioned issues of nodes, MANETs are extensively used in some scenarios where the speed of network implementation is highly required without any pre-constructed structure in advance, for example, military communication, emergency communication and mobile conferencing [7-9]. In order to set up a network of mobile nodes, some famous routing protocols like Ad-hoc on-demand distance vector (AODV) [10], dynamic source routing (DSR) [11], etc. are designed for locating the trusted and optimal path between nodes.

In spite of having some useful attributes, MANETs also comes up with some challenges. One of which is the security of routing protocols [12], which is always been overlooked during the design of default routing protocols. The foundation of traditional ad hoc routing protocols is laid on the assumption that they are already trusted and works in a cooperative manner which makes MANET a powerless target to many types of Denial of Service (DoS) attacks [13]. DOS attack primarily targets the service availability of routing protocols [14] in order to diminish the network capacity. One type of DoS attack which is very fatal for the network is the Packet Dropping Attack, such as Black-hole attack (Full Packet Drop Attack) [15]. During the route discovery process, a black hole node falsely claims that it owns the fresh and the shortest path towards the destination by replying with a fake RREP packet towards a source node [16]. Hence the source node selects the malicious node as the highly suitable node, having the shortest route for sending the data packets towards the destination and therefore all the packets are transmitted towards it. As a result, a black hole is created by the malicious node where all the data packets are thrown away [17] instead of sending them towards the desired destination. Black hole is the most serious attack against AODV routing protocol, as AODV doesn't incorporate any mechanism to detect a maliciously fabricated RREP packet by a malicious node [18].

Many security mechanisms are proposed for the security of MANETs, but still, there are some research gaps in MANETs that are not fully addressed. Most of the work published detects and eliminates the black-hole attack without considering the efficiency of the network, such as Packet Delivery Ratio, End-to-End Delay and Throughput, etc. [19]. Therefore, designing a protocol considering all the mentioned issues is of high importance. Accordingly, in this paper, the authors aim to enhance the AODV routing protocol with a simple and efficient mechanism to detect the black-hole nodes and prevent its harm in the network. The proposed scheme was designed at discovering black hole nodes by applying a fake messaging technique. In MDBM, the source node lures the black hole nodes to reply fake RREP packets, by appending a nonexistent

destination address in a bait RREQ packet. Finally, the ID's of black hole nodes are traced from fake RREP packets and appended in a blacklist in order to isolate them from the network. No, any extra ALERT packets were used in this approach in order to prevent a black hole node from falsely modifying the alert packets and to avoid the network congestion also. Thus, the proposed scheme can provide optimization and leads to improvement in terms of security and quality of service during routing.

A. Organization of the Paper

The remainder of this paper is organized as follows. Section 2 describes some more detail about black-hole attacks in AODV-based MANETs. Section 3 reviews some related work. Section 4 describes the proposed MDBM protocol for detection and prevention of black-hole nodes from network. Section 5 describes the simulation results and some discussions. Finally, Section 6 concludes this paper.

II. Black-Hole Attacks

This section describes the routing principles of the AODV routing protocol and then discuss the black-hole attacks in AODV-based MANETs. AODV comes into the category of reactive routing protocols [20], where the routes between nodes are created on an on demand. In AODV, when the source node wants to send data packets to the destination node, it looks up its routing table for an available and optimal route. If no such route exists in the routing table, the source node will broadcast a RREQ packet to start the route discovery process [21]. After receiving the RREQ packet, an intermediate node would update its routing table to record a route to get back to the source node and checks for the routes towards the destination node in its routing table. If the intermediate node doesn't have any fresh route to the destination node, it will also broadcast the RREQ packet to the nodes the next hop. All the intermediate nodes will also increment the hop count and sequence numbers before forwarding the RREQ packet. Finally, a RREP packet is sent back to the source node by the destination node after the RREQ packet reaches the destination or by an intermediate node that has a nearest route towards the destination node [22] [23]. In some situations, when a source node receives multiple RREP packets, only the RREP having highest sequence number among all get selected [24]. But, if the sequence numbers are same, the RREP with the lowest hop count will be selected. The sequence number of a node indicates the freshness of a route and a hop count determines the distance from source to destination node [25].

Black hole attack can seriously damage the performance of MANET, and this kind of attack is launched either by a single independent node or a group of malevolent nodes [26]. AODV protocol works on the sequence number of nodes for estimating the freshness of route. Accordingly, in a network that implements the AODV protocol, the black-hole node always claims to possess a fresh route towards all the requested destinations, by providing fabricated fake highest sequence number [27]. Whenever the source node broadcasts the RREQ packets in order to initiate the route discovery in the network, the black hole node quickly replies with a malicious reply packet including highest sequence number for specified destination [28], which is considered as a genuine reply from an intermediate node having an optimal route or by a destination node itself. As the normal nodes in MANET are designed based on the assumption that they work in a mutual cooperation system, source node believes that fake reply originated by malevolent node and rejects all other genuine RREP packets. After selecting the RREP by a malicious node, the source sends all the data traffic through black hole node [29], assuming that the destination will receive all the data packets optimally. Eventually, all the data packets are dropped that are passed through black hole node. The black hole attack causes DOS in network, which can cut the communication between source and destination nodes [30]. There can be different types of black hole attacks in the network i.e. single node, multiple nodes, collaborative and smart black hole attack. Single or multiple node attack is launched by one of the network nodes or multiple nodes working independently in the network, where the collaborative attack is done by the co-operation between few nodes [31]. A smart black hole attack is a type of malicious node which is intelligent enough to judge the security patterns of a routing protocol. A smart black hole node can surpass the security mechanism of a protocol by analyzing its working principles [32] and uses its entire malicious feature against other normal nodes.

Fig. 1 shows a scenario of a network having a black hole node. The source node SN starts the route discovery process by broadcasting RREQ packet in the network in order to find the routes for destination node DN. The RREQ packets broadcasted by SN are then received by the near neighbor nodes 1, 2 and 3. When the black hole node i.e. node 3, gets the RREQ packet, it quickly responds with a fake RREP packet without considering its own routing table for any routes towards DN. As the reply packet from node 3 contains the highest sequence number for DN, the source node immediately considers it and updates its routing table for the route towards malicious node and discards all the other RREP packets, even the reply packet from DN also. Once SN selects the path through node 3, it forwards the data packets towards black hole node for the intended destination node. As per the nature of black hole node, it throws all the data packets away, rather than sending it towards next hop nodes. The most critical influence of the black hole is that the PDR is diminished severely.

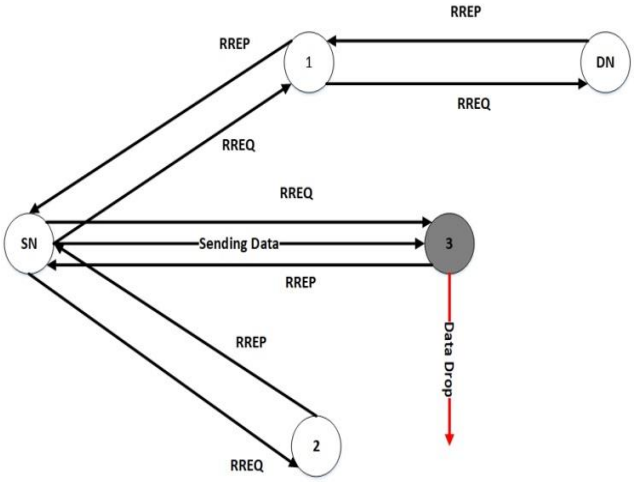

Fig. 1. Black Hole Attack.

III. Related Works

Black-hole attacks have attracted a great deal of attention in recent years since they can seriously impact the performance of reactive routing protocols. Many research proposals are published about detecting and isolating the black-hole attack, but most of the methods incorporate a lot of calculations and the use of extra control packets, nodes and tables for the detection purposes, which can produce higher end to end delay and a lot of overhead in the network. In this paper we collect and introduce the mechanisms that are proposed in recent years. In the rest of this section, we will survey some of the proposed schemes for isolating black-hole nodes to identify the various research gaps in order to defend the development of this proposed scheme.

Jhaveri et al. proposed an approach which is based on the fabricated highest sequence number by a malicious node in order to detect the attacker node [33]. The sequence number based bait detection scheme (SNBDS) includes two slight modification in the routing table of all nodes, i.e., 'Node Status' which is used to record the behavior of the node and 'Last Reply time' that is the updated sequence number for the desired destination node in the last RREP of any node. Three different attack models with various false routing behaviors are considered in this approach. A pre-specified value is calculated at each node during the routing process. Whenever the destination sequence number value in the RREP packet of a particular node exceeds the calculated threshold, the node is then declared as suspicious. In order to confirm the status of the suspicious node, a bait request packet with non-existent destination address is forwarded to the target node to confirm its status. If the node replies the bait request packet, its status is changed from suspicious to malicious node, and no any packets are then received or forwarded to that node, in order to completely isolate it. Calculation of threshold value at each node can increase delay and computational overhead.

Kumar et al. proposed a technique to detect the malicious nodes by using IDS nodes in [34]. The main objective of this work was to design a technique to detect the detect black-hole attack and also lessen the effect of malicious node on genuine nodes. In this approach, the detection of black-hole attack is based on the abnormal value of sequence number in the RREP packet by a node. The special IDS nodes monitor and overhear all the communication of nodes in the network. During monitoring, when IDS detects a node replying sequence number greater than a set threshold, it is listed in blacklist table of IDS and an Alert packet is broadcasted in the network containing I.D of malicious node in order to avoid any future transactions from it. The limitations of this approach are the use of extra IDS nodes which can increase the extra computational overhead and a fixed value of threshold which is not suitable in dynamic nature of MANETs. The improper deployment of IDS node can fail the system, causing poor detection of malicious nodes and an increase in routing overhead.

Dhende et al. proposed a secure AODV protocol (SAODV) for the detection and removal of DOS attacks [35]. In the scheme, neighbor's opinions based on the behavior of a node are considered in order to consider a node to participate in routing process. In this approach, every node maintains two tables, i.e., neighbors list (NL) and opinion table (OT) to detect the malicious nodes. When a node replies to a RREQ packet of the source node, the source node would send another request (FRREQ) to the neighbors of the intermediate node to get opinions. Two types of acknowledgment packets are then sent to the source node i.e. NO packet (NP) or YES packet (YP) by the intermediate nodes. If all the replies are YP for a node, then the node is considered as a black hole node. If some replies are YP and others are NP, the node is declared as a gray-hole node. An alarm is then broadcast by the source node in order to alert the other genuine nodes in the network about the identity of the malicious node. As each node needs to maintain two extra tables in order to detect a malicious node, there should be an excess of computational overhead in this mechanism.

Tamilselvi et al. proposed an efficient route discovery process which can bypass the black hole nodes during route discovery and uses only the reliable route for data transmission [36]. In this approach, source node selects an adjacent node, i.e. its one-hop neighbor node and takes its address as the destination address for RREQ packet in order to bait the malicious nodes. Firstly the source node sends the RREQ packet having bait destination address of neighbor node and an encrypted message encrypted by a public key. If a node has a route towards specified destination, it will reply the packet with encrypted message else forward the request packet. A black hole node will simply reply the RREQ packet having fabricated routing information and it cannot send the encrypted message. As the destination node will receive the false reply without encrypted message, it will simply drop the reply packet and alerts the source node about malicious node. A black hole node having information about the participating nodes in the network can surpass the security mechanism by not replying the bait RREQ and can impact the packet delivery ratio.

Dorri et al. proposed a novel approach called detecting and eliminating black holes (DEBH) for isolating the black hole nodes [37]. This approach uses a data control packet and an additional black hole check (BCh) table for malicious node detection. Each node keeps a BCh table for its neighbor which is maintained based on the past behavior of neighbor nodes. BCh table includes two fields i.e. nodes ID and a Boolean "Trustable". A '0' value in trustable column indicates that a node is malicious and '1' means trusted. Whenever an intermediate node sends the RREP packet back towards source node, it should also append its BCh table with it. After getting all the replies from intermediate nodes, a secure route is selected based on the BCh table of each node. Before sending the data on the selected path, a data control packet is sent to the path, in order to check the path validity. If a black hole node manages to enter the path, it will surely drop the data control packet and in this way the malicious node is detected, else the path is chosen. A lot of control packets are used in this approach which can increase overhead. Each node maintains BCh table for other nodes which can increase the delay during the routing process.

Noguchi et al. proposed a threshold-based method for prevention of black hole attacks using multiple RREPs [38]. In this approach, a threshold value for sequence number is updated by every intermediate node dynamically, based on the

average of sequence numbers of each RREP generating node. Whenever an intermediate node broadcast the RREQ packet, it gets multiple RREP's for the same destination from different nodes. In this approach, the nodes make the copies of every RREP packet it gets for corresponding RREQ packet. Every intermediate node maintains an average sequence number table in which the sequence numbers and I. D's of RREP generator are noted. After a time stamp the intermediate node calculates the average of all the sequence numbers from a particular node. If the average is higher than the sequence number of destination node listed in a RREQ packet, then the node is considered as black hole. An alert is broadcasted in the network containing the ID of node in order to isolate it. A black hole node can also fabricate the broadcasted ALERT packet by inserting the ID of any legitimate neighbor, making other nodes to list a normal node as a malicious node. Extra calculations performed by each node can increase overhead and delay.

Deshmukh et al. propose a secure DSR-based routing technique to detect black hole attack in [39]. This mechanism attaches an additional validity bit value with RREP in order to check the validity of a RREP packet. The "Validity Bit" field is a single bit value which is implemented at the destination node embedded in reply packet. If the validity field value is set to 1, it is considered that the originator of the RREP packet is the real destination node. The validity of reply is checked by the source node i.e. a RREP is genuine or not. If the source nodes gets a RREP packet having validity bit not set, then it is considered that the reply packet is sent by a malicious node, as the malicious node is not aware of any validity bit mechanism. Hence RREP packet will be dropped by source node. Hence, a black hole node is isolated from network. A destination node far away from the source node can increase the delay, as the destination node only has the functionality of setting the value of validity bit. A black hole node using the same protocol can notice the mechanism of validity bit and can send a reply with setting validity bit value.

Kamel et al. proposed a secure and trust based approach based on ad hoc on demand distance vector (STAODV) to improve the security of AODV routing protocol [40]. A trust level is used for each node in order to detect the malicious nodes from the network. Each node maintains two table i.e. 'malicious node table' and 'trust levels'. Initially all the participating nodes are considered as trusted, and trust values are updated upon the incoming RREP packet from a node. A threshold value is set in this approach, which is derived by the 'number of nodes in the network', 'RREP packet's destination sequence number' and 'routing table sequence number'. If the sequence number of any RREP packet exceeds the threshold, the trust value of that node is decremented by one. A node having negative trust value is considered as black hole node, and is listed in blacklist. No RREP packets are accepted by a node having negative trust value. The maintenance of an extra trust table by every node can increase the overhead.

Dumne et al. proposed a Cooperative Bait Detection method Scheme (CBDS) scheme for the detection of black hole attack [40]. The process for the detection of malicious node is divided into three phases in CBDS i.e. Initial Bait, Reverse tracing and Reactive Defense. During initial bait, the source node choses one of the near neighboring nodes and puts its address in bait RREQ packet. In Reverse Trace phase, the I.D'S of the malicious nodes are extracted from the fake RREP packets. An alarm then is broadcasted in the network notifying other nodes about the presence of malicious nodes so that any communication is denied for the malicious node by other normal nodes. During Reactive Defense phase, when the data packets are sent by the source node on the selected path, the PDR is calculated. If the PDR is less than the threshold, the data transmission is stopped and again the initial bait detection process is started for the nodes which surpass the security mechanism. The limitation of this technique is that promiscuous mode activation by all nodes is a resource consuming task. A black-hole node can falsely use the alarm packet and broadcasts fake alarms in the network in order to increase the false positive ratio and network congestion.

IV. MDBM: The Proposed Scheme

The proposed scheme works with an objective to detect the black hole attacks and prevent the network from their harm. This scheme is the modification of AODV routing protocol where the concept of fake RREQ packets [41] is included. The fake RREQ packets are broadcasted in the network before the actual route discovery. The reason behind doing so is to trace most of the malicious nodes in the network before the transmission of data, to prevent the data loss. In the proposed approach, an empirical format was designed for the fake request packet as presented in Fig. 2. This packet contains fields like Type, Reserved, Request ID and the Target Address which is completely fake and doesn't exist in the network. The fake RREQ packets last for a certain time period, similar to the real RREQ packets of AODV. Fig. 3 shows the real RREQ packet format used in the proposed scheme. The only difference as compared to the main format of RREQ packet is the addition of the Alert field which includes the list of malicious nodes. The authors have also modified the format of RREP packet of AODV to find the addresses of the nodes that generates RREP packet. In order to implement this mechanism, the structure of RREP packet is modified and an extra field is added into it called as RREP Generator Address. This field holds the address of a particular node which will generate the reply packet. When a node will reply to the RREQ packet, its address will be copied into this field, so that the source node can trace the address of the RREP generator node. Fig. 4 shows the structure of the modified RREP packet.

Option Type	Reserved	Request ID
Target Address(Fake not Existed Address)		
Source Address		
Path		

Fig. 2. Format of Fake RREQ Packet.

Request ID	Destination IP	Destination Seq_Num	Source Seq_Num
Alert (Addresses of Malicious Nodes)			
Path			

Fig. 3. Format of RREQ Packet.

Option Type	Opt Data Len	Length	RREP Generator Address
Source Address			
Path			

Fig. 4. Format of RREP Packet.

Before starting the actual AODV route discovery process, the source node broadcasts fake RREQ packets in the network. The source node is embedded with a bait timer ($Bait_{Time}$), and that timer value is set randomly to A seconds. Whenever the timer reaches to A seconds, the source node creates a Fake RREQ packet and broadcast it into the network with a randomly generated fake destination address. In order to avoid the network with full of fake RREQ packets, MDBM employs the same working mechanism of RREQ packet of AODV. The Fake request packet can only last for a period of time. As the black hole node replies to every request packet without looking at its routing table for proper routes, it will immediately respond to all the fake RREQ packets that it will receive, pretending that it has the shortest path towards destination node. As the source node receives the replies for the fake RREQ packets, all the RREP's are considered to be sent by malicious nodes. The I.D's of black hole nodes are then traced from RREP generator address field of the RREP packet in order to identify which node generated the reply packet for the fake request. All the traced I.D's of black hole nodes are then listed in a malicious nodes list ($Malicious_{list}$). Up to this stage, the proposed scheme succeeded in detecting several black hole nodes in the network.

The next stage is starting the route discovery process as native AODV and alarming other nodes about the occurrence of black hole node (s) in the network. Though, the alarm is not broadcasted in the network as a separate packet, in order to prevent a black hole node from falsely modifying the alert packet and to reduce network congestion also. The alarm is included in the Alert field (Alert) of real Request packet. Whenever a node gets the RREQ packet, it searches for the malicious node entries in it, and mark the malicious nodes in the routing table as black hole, rather than removing it from the table. In this way, none of the RREP packets will be accepted by a node that is already listed in the Malicious List. The main concept behind MDBM scheme is to use the fake information in RREQ packets to bait the black hole nodes to expose their identity so that they can be detected at early stages. The randomness in both Fake RREQ broadcast timer and virtual destination address will prevent the black-hole node from guessing any patterns of the proposed scheme. In following algorithms, the detailed mechanism of the proposed scheme for the detection and prevention of black hole attack in the network.

Algorithm 1. Detection Phase

Start
If $Current_{Time}$==$Bait_{Time}$ then
Create Fake RREQ;
Initiate TTL;
SN broadcasts Fake RREQ (Not existed destination address);
Reset $Bait_{Time}$;
End if
For each received RREP for Fake request do
Trace the black hole node using the RREP Generator Address field of RREP;
Construct and add the traced black hole nodes into $Malicious_{list}$;
End for
Append malicious list to RREQ (Alert Field);
Broadcast RREQ as native AODV;
END

Algorithm 2. Prevention Phase

Start
If RREQ Packet Then
Check for black-hole node entries in $Malicious_{List}$;
Mark the specified nodes as Black Hole in the routing table;
Process the RREQ Packet Further;
End If
If RREP Packet Then
If the node sending RREP already marked as Black Hole in routing table then
Discard the RREP packet;
Else
Process the RREP packet Further;
End If
End If
End

V. Results

NS-2 (ver. 2.35) simulator was used to evaluate the effectiveness of MDBM under the black hole attack. Simulations were performed varying the number of nodes and the number of malicious nodes. Packet drop ratio (PDR), average end-to-end delay (ED) and Network throughput (NP) metrics were used to assess the performance of the proposed scheme. The performance of MIGM was also compared to AODV under black hole attack to demonstrate the superiority of MDBM. The simulations were carried out in a 1000x1000 m2 area employing the IEEE 802.11 MAC protocol. During the simulations, both source and destination nodes were deployed at the opposite ends of the network initially. The benign nodes were distributed randomly throughout the area, equipped to run the AODV and MDBM. Table 1 lists the simulation parameters.

TABLE I. SIMULATION PARAMETERS

Parameters	Values
Coverage area	1000×1000m^2
MAC layer protocol	IEEE 802.11
Communication range of the node	250m
Type of traffic	CBR-UDP
Mobility model	Random
Nodes total number	100
Mobility	15 m/sec
Number of malicious nodes (varying)	0–10
Participating Protocols	AODV, MDBM

A. Test 1: Varying the Number of Nodes

In this test, simulations were performed by varying the number of nodes in the network from 25 to 100 nodes. The number of black hole nodes in the network was 1. All the other parameters were kept fixed.

1) Packet delivery ratio: As shown in Fig. 5, the packet delivery ratio decreases as the number of nodes increases. As we can see from Fig. 5, the PDR of AODV is highest i.e. 0.113% to 0.181% during the absence of black hole node. But in the presence of a black hole node, the PDR of AODV drops from 0.065 % to 0.139 %. The reason behind this fall in PDR is the absence of any security mechanism in AODV routing protocol for countering malicious activities during routing.

When MIGM is employed, there is an improvement in PDR from 0.043 % to 0.087 % as compared to AODV under black hole attack. The reason behind the improved results of MDBM is the early detection of black hole nodes by using fake RREQ packets so that most of the black hole nodes are detected and isolated before data transmission.

2) End to end delay: An increase in the number of nodes would tend to increase the delay of the routing protocols as shown in Fig. 6. The ED of AODV without any black hole node is lowest i.e. 1.13ms to 0.73ms, because of its shortest path selection strategy for destination node. When a black hole node was deployed in the network, the delay increases rapidly i.e. from 0.314 ms to 0.520 ms. The reason behind this increase is the continuous packet drop activities by black hole node and frequent new route discoveries by the source node in order to find other secure routes. MDBM mechanism showed better results in terms of delay as compared to AODV under black hole attack i.e. a decrease in delay from 0.247 ms to 0.830 ms. MDBM showed similar performance as AODV without black hole node, because of the same procedure of route selection as native AODV. And also, no extra control packets or calculation are involved in order to detect malicious node.

3) Network throughput: There is a decrease in NP of the participating protocols as the number of nodes increases as shown in Fig. 7. As we can see in Fig. 7, the results of native AODV in terms of NTP were highest in the absence of black hole node i.e. 104.74 kbps to 177.79 kbps. But when a black hole node involved in the routing process, the NTP of AODV decreases from 65.67 kbps to 139.54 kbps. As compared to AODV under a black hole attack, the results of the proposed approach are better in terms of throughput i.e. an improvement from 22.457 kbps to 55.089 kbps. The improved results imply that the destination node will receive a higher ratio of data packets in a time unit. That is, MDBM is a more effective mechanism for detecting the most number of black nodes before data transmission.

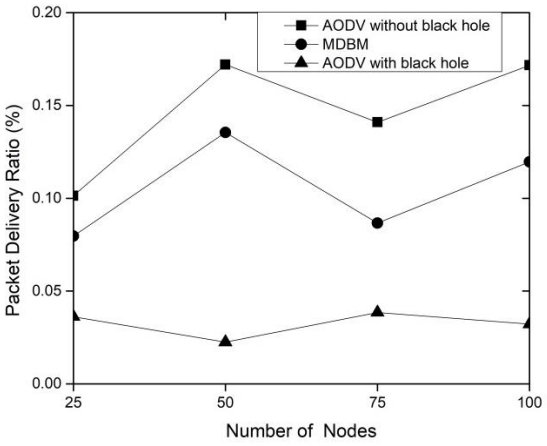

Fig. 5. Packet Delivery Ratio versus Number of Nodes.

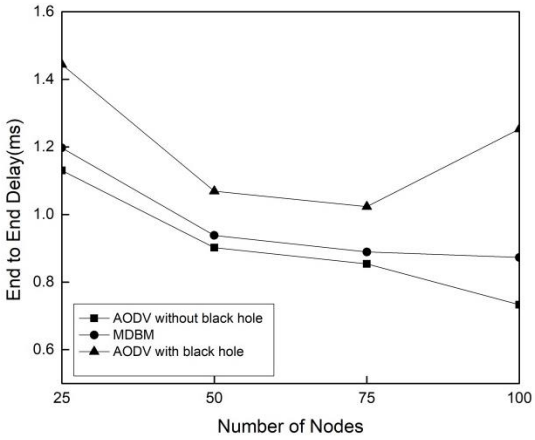

Fig. 6. End-to-End Delay Versus. Number of Nodes.

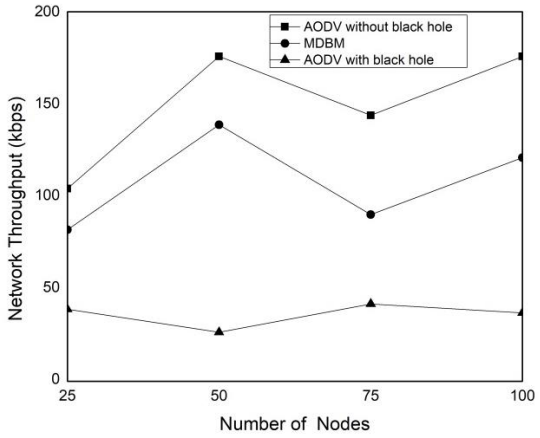

Fig. 7. Network Throughput versus Number of Nodes.

B. Test 2: Varying the Number of Malicious Nodes

In this test, the simulations were performed by changing the number of malicious nodes from 2 to 10 nodes in the network and keeping the number of normal nodes 50. All the other parameters were kept fixed.

1) Packets delivery ratio: As shown in Fig. 8, as the percentage of malicious nodes increases, there is a significant drop in packet delivery ratio. The reason behind this drop is the increased packet dropping activities by black hole nodes. As we can see from Fig. 8, AODV showed a PDR nearly zero when multiple black hole nodes are present in the network. The reason behind the poor results is the coverage of network with black hole nodes which will indeed cut any communication between source and destination nodes. The PDR of MDBM is also decreased i.e. 0.04% to 0.09% as compared to native AODV, but much better results under black hole attack.

2) End to end delay: As shown in Fig. 9, with the increase in the number of black hole nodes, the end to end delay in the network is increasing. The reason behind this increase is the increased malicious activities of black hole nodes making source node initiating route hand-off mechanisms frequently. As we can see from the Fig. 9, the ED of AODV was the highest as the number of black hole nodes increased from 2. MDBM showed better results in terms of ED delay under multiple black hole nodes. The reason behind the better results is the efficient and early detection of black hole nodes before data transmission and no use of any extra packets and calculations.

3) Network throughput: As shown in Fig. 10, the NP of AODV against multiple black-hole nodes is nearly zero. The reason is the increasing number of malicious nodes will cause a lot of packet drops, so that none of the packets would be received by the destination node in a unit time. The results of the proposed scheme are better than the native AODV under multiple black hole nodes, as the proposed technique incorporates an efficient security mechanism which can reduce a huge amount of black hole nodes before data transmission.

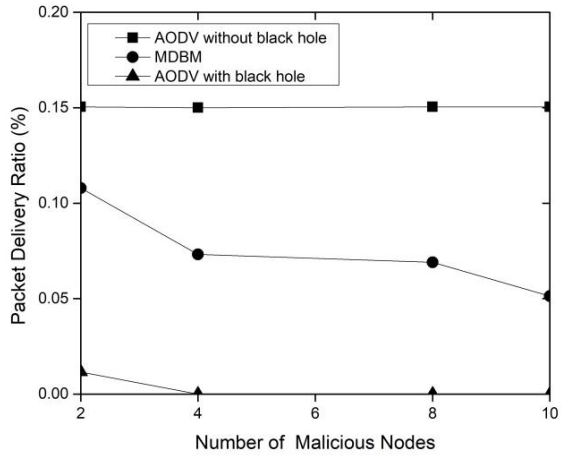

Fig. 8. Packet Delivery Ratio versus Number of Malicious Nodes.

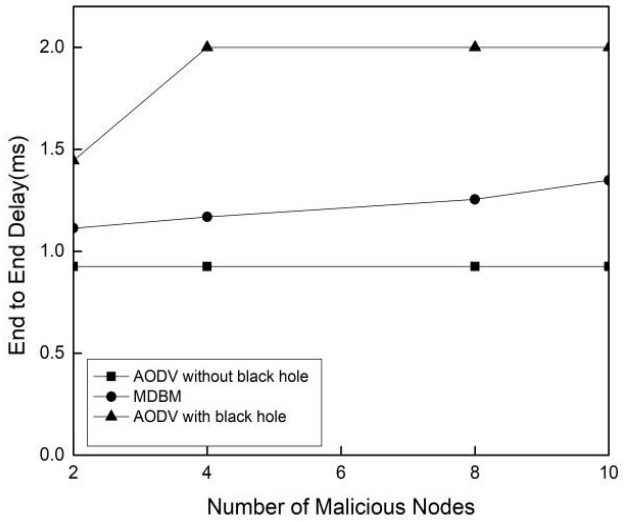

Fig. 9. End to End Delay Versus Number of Malicious Nodes.

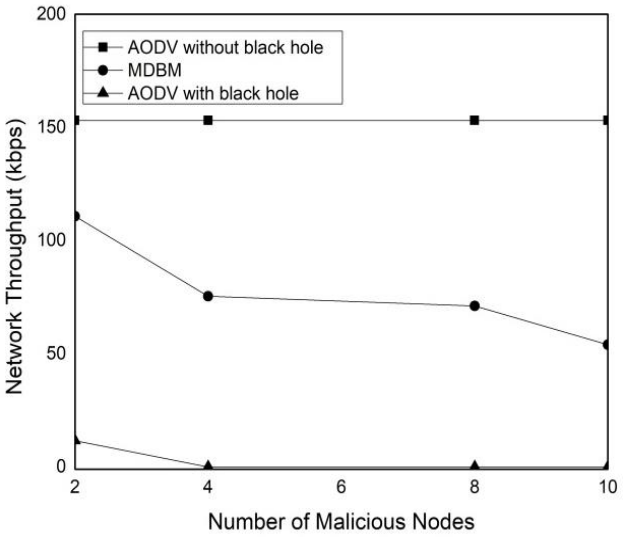

Fig. 10. Network Throughput versus Number of Malicious Nodes.

VI. Conclusion

Black-hole attack is included in the category of DOS attacks that can seriously harm the performance of MANETs. Detection of black hole node during early stages is of much importance in order to prevent the network failures. Accordingly, the authors developed a scheme for detecting and managing different kind of black hole attacks in MANET. Over a minimum amount of overhead, the proposed scheme can efficiently detect the black hole attacks and prevent the network from their harm. In the proposed MDBM, the authors introduced a simple and innovative mechanism for detecting the black hole nodes in AODV-based MANETs by using fake RREQ packet in order to bait the black hole nodes during early stages. This scheme was verified and implemented on AODV protocol. As the proposed scheme doesn't generate any extra control packets or any mathematical calculations during routing, the results of the simulations reveal that the performance of proposed scheme is very much similar to the native AODV in terms of delay. By doing some changes, the

proposed scheme can be applied to DSR protocol. Furthermore, the proposed scheme can be tested on worm-hole and gray hole attacks, as these attacks function similar to black-hole.

REFERENCES

[1] Conti, Marco, Andrea Passarella, and Sajal K. Das. "The Internet of People (IoP): A new wave in pervasive mobile computing." Pervasive and Mobile Computing 41 (2017): 1-27.

[2] Zhou, Yifeng. "A Routing and Interface Assignment Algorithm for Multi-Channel Multi-Interface Ad Hoc Networks." Mobile Networks and Applications (2018): 1-12.

[3] Jisha, G., Philip Samuel, and Varghese Paul. "Maintaining connectivity of mobile nodes using MANET gateway nodes." IJCNDS 19, no. 3 (2017): 288-311.

[4] Njilla, Laurent, Harold Ouete, Niki Pissinou, and Kia Makki. "Game theoretic analysis for resource allocation in dynamic multi-hop networks with arbitration." In Systems Conference (SysCon), 2017 Annual IEEE International, pp. 1-8. IEEE, 2017.

[5] Pathan, Muhammad Salman, Nafei Zhu, Jingsha He, Zulfiqar Ali Zardari, Muhammad Qasim Memon, and Muhammad Iftikhar Hussain. "An Efficient Trust-Based Scheme for Secure and Quality of Service Routing in MANETs." Future Internet 10, no. 2 (2018): 16.

[6] Mandhare, V. V., V. R. Thool, and R. R. Manthalkar. "A novel approach to improve quality of service in MANET using cache update scheme for on-demand protocol." International Journal of Communication Networks and Distributed Systems 18, no. 3-4 (2017): 353-370.

[7] Anjum, Shaik Shabana, Rafidah Md Noor, and Mohammad Hossein Anisi. "Review on MANET based communication for search and rescue operations." Wireless Personal Communications 94, no. 1 (2017): 31-52.

[8] Salman, M. Al-Shehri and Pavle, Loscot "Enhancing Reliabilty of Tactical Manet by Improving Routing Decisions." Journal of Low Power Electron and Applications 8, (2018): 1-15.

[9] Sandeep, J., and J. Satheesh Kumar. "Efficient packet transmission and energy optimization in military operation scenarios of MANET." Procedia Computer Science 47 (2015): 400-407.

[10] Anand, M., and T. Sasikala. "Efficient energy optimization in mobile ad hoc network (MANET) using better-quality AODV protocol." Cluster Computing (2018): 1-7.

[11] Prabha, Jyoti, Dinesh Goyal, Savita Shivani, and Amit Sanghi. "Prevention of Conjunct Black Hole MANET on DSR Protocol by Cryptographic Method." In Smart Trends in Systems, Security and Sustainability, pp. 233-240. Springer, Singapore, 2018.

[12] Usman, Muhammad, Mian Ahmad Jan, Xiangjian He, and Priyadarsi Nanda. "QASEC: A secured data communication scheme for mobile Ad-hoc networks." Future Generation Computer Systems (2018).

[13] Chaurasia, M., & Singh, B. P. (2018). Prevention of DOS and Routing Attack in OLSR under MANET. In Proceedings of International Conference on Recent Advancement on Computer and Communication (pp. 287-295). Springer, Singapore.

[14] Hemalatha, P., J. Vijitha Ananthi, and R. Kalaivani. "Analysis of reverse tracing algorithm for the detection of DOS attacks in MANET." International Journal of Autonomic Computing 2, no. 4 (2017): 311-322.

[15] Yaseen, Qussai M., and Monther Aldwairi. "An Enhanced AODV Protocol for Avoiding Black Holes in MANET." Procedia Computer Science 134 (2018): 371-376.

[16] Dorri, Ali. "An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET." Wireless Networks 23, no. 6 (2017): 1767-1778.

[17] Gupta, Prakhar, Pratyaksh Goel, Pranjali Varshney, and Nitin Tyagi. "Reliability Factor Based AODV Protocol: Prevention of Black Hole Attack in MANET." In Smart Innovations in Communication and Computational Sciences, pp. 271-279. Springer, Singapore, 2019.

[18] Gurung, Shashi, and Siddhartha Chauhan. "A dynamic threshold based approach for mitigating black-hole attack in MANET." Wireless Networks (2017): 1-15.

[19] Singh, Moirangthem Marjit, and Jyotsna Kumar Mandal. "Impact of black hole attack on reliability of mobile ad hoc network under DSDV routing protocol." International Journal of Systems, Control and Communications 9, no. 1 (2018): 20-30.

[20] Mukherjee, Saswati, Matangini Chattopadhyay, Samiran Chattopadhyay, and Pragma Kar. "EAER-AODV: Enhanced Trust Model Based on Average Encounter Rate for Secure Routing in MANET." In Advanced Computing and Systems for Security, pp. 135-151. Springer, Singapore, 2018.

[21] Patel, Suchita, Priti Srinivas Sajja, and Samrat Khanna. "Enhancement of Security in AODV Routing Protocol Using Node Trust Path Trust Secure AODV (NTPTSAODV) for Mobile Adhoc Network (MANET)." In International Conference on Information and Communication Technology for Intelligent Systems, pp. 99-112. Springer, Cham, 2017.

[22] Anand, M., and T. Sasikala. "Efficient energy optimization in mobile ad hoc network (MANET) using better-quality AODV protocol." Cluster Computing (2018): 1-7.

[23] Fang, Weidong, Wuxiong Zhang, Jinchao Xiao, Yang Yang, and Wei Chen. "A Source Anonymity-Based Lightweight Secure AODV Protocol for Fog-Based MANET." Sensors 17, no. 6 (2017): 1421.

[24] Jhaveri, Rutvij H., Aneri Desai, Ankit Patel, and Yubin Zhong. "A Sequence Number Prediction Based Bait Detection Scheme to Mitigate Sequence Number Attacks in MANETs." Security and Communication Networks 2018 (2018).

[25] Mai, Yefa, Fernando Molina Rodriguez, and Nan Wang. "CC-ADOV: An effective multiple paths congestion control AODV." In Computing and Communication Workshop and Conference (CCWC), 2018 IEEE 8th Annual, pp. 1000-1004. IEEE, 2018.

[26] Bhagat, Swapnil P., Puja Padiya, and Nilesh Marathe. "A generic request/reply based algorithm for detection of blackhole attack in MANET." In Smart Technologies For Smart Nation (SmartTechCon), 2017 International Conference On, pp. 1044-1049. IEEE, 2017.

[27] Singh, Kulwinder, and Shilpa Sharma. "A new technique for AODV based secure routing with detection black hole in MANET." In 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), pp. 1528-1534. IEEE, 2017.

[28] Shashwat, Yugarshi, Prashant Pandey, K. V. Arya, and Smit Kumar. "A modified AODV protocol for preventing blackhole attack in MANETs." Information Security Journal: A Global Perspective 26, no. 5 (2017): 240-248.

[29] Khan, Danista, and Mahzaib Jamil. "Study of detecting and overcoming black hole attacks in MANET: A review." In Wireless Systems and Networks (ISWSN), 2017 International Symposium on, pp. 1-4. IEEE, 2017.

[30] Kolade, A., Yafi, E., & Zheng, L. "Performance analysis of black hole attack in MANET". In Proceedings of the 11th International Conference on Ubiquitous Information Management and Communication. ACM, Newyork, USA, 2017.

[31] Gurung, Shashi, and Siddhartha Chauhan. "A review of black-hole attack mitigation techniques and its drawbacks in mobile ad-hoc network." In Wireless Communications, Signal Processing and Networking (WiSPNET), 2017 International Conference on, pp. 2379-2385. IEEE, 2017.

[32] Gurung, Shashi, and Siddhartha Chauhan. "Performance analysis of black-hole attack mitigation protocols under gray-hole attacks in MANET." Wireless Networks (2017): 1-14.mnm mnm

[33] Jhaveri, Rutvij H., and Narendra M. Patel. "A sequence number based bait detection scheme to thwart grayhole attack in mobile ad hoc networks." Wireless Networks 21, no. 8 (2015): 2781-2798.

[34] Kumar, Sudheer, and Nitika Vats Doohan. "A modified approach for recognition and eradication of extenuation of gray-hole attack in MANET using AODV routing protocol." In Colossal Data Analysis and Networking (CDAN), Symposium on, pp. 1-5. IEEE, 2016.

[35] Yasin, Adwan, and Mahmoud Abu Zant. "Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique." Wireless Communications and Mobile Computing 2018 (2018).

[36] Tamilselvi, P., and C. Ganesh Babu. "An efficient approach to circumvent black hole nodes in manets." Cluster Computing (2017): 1-9.

[37] Dorri, Ali, Soroush Vaseghi, and Omid Gharib. "DEBH: detecting and eliminating black holes in mobile ad hoc network." Wireless Networks 24, no. 8 (2018): 2943-2955.

[38] Noguchi, Taku, and Mayuko Hayakawa. "Black Hole Attack Prevention Method Using Multiple RREPs in Mobile Ad Hoc Networks." In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pp. 539-544. IEEE, 2018.

[39] Deshmukh, Sagar R., and P. N. Chatur. "Secure routing to avoid black hole affected routes in MANET." In Colossal Data Analysis and Networking (CDAN), Symposium on, pp. 1-4. IEEE, 2016.

[40] Kamel, Mohammed Baqer M., Ibrahim Alameri, and Ameer N. Onaizah. "STAODV: a secure and trust based approach to mitigate blackhole attack on AODV based MANET." In IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference, pp. 1278-1282. 2017.

[41] Dumne, Pradeep R., and Arati Manjaramkar. "Cooperative bait detection scheme to prevent collaborative blackhole or grayhole attacks by malicious nodes in MANETs." In Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO), 2016 5th International Conference on, pp. 486-490. IEEE, 2016.