International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:8, No:1, 2014

A Comprehensive Survey and Comparative Analysis of Black Hole Attack in Mobile Ad Hoc Network

Nidhi Gupta, Sanjoy Das, Khushal Singh

Abstract**—**A Mobile Ad-hoc Network (MANET) is a self managing network consists of versatile nodes that are capable of communicating with each other without having any fixed infrastructure. These nodes may be routers and/or hosts. Due to this dynamic nature of the network, routing protocols are vulnerable to various kinds of attacks. The black hole attack is one of the conspicuous security threats in MANETs. As the route discovery process is obligatory and customary, attackers make use of this loophole to get success in their motives to destruct the network. In Black hole attack the packet is redirected to a node that actually does not exist in the network. Many researchers have proposed different techniques to detect and prevent this type of attack. In this paper, we have analyzed various routing protocols in this context. Further we have shown a critical comparison among various protocols. We have shown various routing metrics are required proper and significant analysis of the protocol.

Keywords**—**Black Hole, MANET, Performance Parameters, Routing Protocol.

I. Introduction

A Mobile Ad hoc Network (MANET) is a self governing network of mobile nodes connected through wireless links. Mobile ad hoc networks (MANET) are infrastructure less networks, dynamically formed by an autonomous system of mobile nodes that are connected via wireless links [1]. Each node in MANET operates not only as a host but also as a router that has the task to forward data. Mobile nodes only can communicate directly via wireless link if they are within each other's radio range otherwise, they depends on intermediate nodes to forward packets. The success of communication highly depends upon the cooperation of other nodes.

In MANET, data delivery is a major challenge. Due to unpredicted movement of mobile nodes topology of the network changes frequently. The primary goal of any routing protocol is establishing an optimal and efficient route between the communicating nodes. the past few years, much research efforts have been focused on this area and many different kinds of routing protocols have been put forward in the literature, such as Wireless Routing Protocol (WRP) [2], Dynamic Source Routing protocol (DSR) [3], Ad hoc On Demand Distance Vector protocol (AODV) [4] and Location Aided Routing [5]**.** However, from the beginning of its design, almost none of the routing protocols specify security measures.

To implement Security in MANETs is a complex issue. Nodes in the network are much more vulnerable to attacks compare to wired (traditional) networks due to the open medium, dynamically changing network topology, lack of centralized monitoring and management point, and lack of a clear line of defense. These factors have changed the battle field situations for the ad hoc wireless networks against the security threats. The ad hoc wireless networks the nodes communicate with each other on the basis of mutual trust without any a centralized administration. These characteristic makes ad hoc wireless networks more vulnerable to be exploited by an attacker inside the network. Wireless links also makes the ad hoc wireless networks more susceptible to attacks, which make it easier for the attacker to go inside the network and get access to the ongoing communication [6],[7].

There are different kinds of attacks by malicious nodes that can harm a network and make it unreliable for communication. One such kind of attack is black hole attack. A black hole attack is one in which a malicious node represents itself as having the shortest path to the destination. This can cause Denial of Service (DOS) [8] by dropping the received packets.

The paper is organized as follows. Section I discusses the introduction to MANETs. Section II presents Black Hole Attack Background and different techniques of black hole attack detection and prevention is discussed in Section III. In section IV a comparison is done among various techniques. Section V presents the conclusion and future direction.

II. Black Hole Attack

In black hole attack, [9], [10] a malicious node takes advantage of route discovery procedure of routing protocol, to show itself as having the shortest path to the destination node or to the node whose packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it [7].

Nidhi Gupta is a M.Tech scholar at Computing Science and Engineering Dept., Galgotias University, Greater Noida, India (Phone: 09457413221; e-mail: nidhiyashsinghal@gmail.com.)

Sanjoy Das and Khushal Singh are Asst. Professors at Computing Science and Engineering Dept., Galgotias University, Greater Noida, India (e-mail: sanjoy.das@galgotiasuniversity.edu.in,khushal.singh@galgotiasuniversity.edu .in)

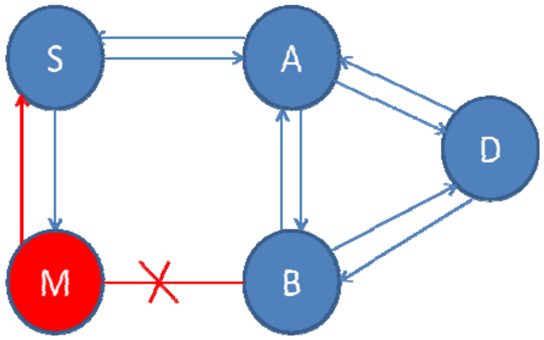

Fig. 1 Black hole attack

Fig. 1 shows how Black Hole problem arises, here node *S* wants to send data packets to node *M* and initiates the route discovery process. Now *M* will declare that it has an active route to the particular destination as soon as it receives RREQ packets from the source node. It will then send the response to node *S* before any other node. After getting response, node "*S*" will believe that this is the nearest active route to the destination thus active route discovery is complete. Node *S* will ignore all other replies and will start sending data packets to node *M*. *M* will drop all the data packets. Black hole Attacks are classified into two categories:

A. Single Black Hole Attack [11], [12]

In Single Black Hole Attack only single node behaves as malicious node within a network. It is also known as Black Hole Attack with single malicious node.

B. Collaborative Black Hole Attack [9], [10]

In Collaborative Black Hole Attack multiple nodes with in a network behave as malicious nodes. It is also known as Black Hole Attack with multiple malicious nodes.

III. Literature Review

Researchers and academician proposed various protocols to detect and prevent black hole attacks. Review of these protocols is presented below:

A. Deng's Solution

Deng et al. [13] have proposed a solution against black hole attack by modifying the AODV protocol. In this algorithm, each intermediate node has to include the address of the next hop node in RREP packets for checking whether the advertised route exists and is free of malicious nodes. On receiving a RREP packet, a node cross checks with the next hop on the route to the destination from an alternate path. This is to verify the existence of the next hope node and the routing metric value (i.e. the hop count) with the next hop node. The next hop node of the neighbor node replies the Further reply packet back to the source node to confirm the route information. If the next hop either does not have a link to the node that sent the RREP or does not have a route to the destination then the node that sent the RREP is considered as malicious. If both neighbor node and the next hop node are black hole nodes, the next hop node can response to the source node with falsified routing information.

1. Advantages

(i) This algorithm is very simple and easy to understand.

2. Disadvantages

(i) This solution is unable to detect cooperative black hole attack.

(ii) It has more routing overhead due to more number of messages exchanged.

B. Neighborhood-Based And Routing Recovery Scheme

Sun B et al. [14] proposed a detection system which uses neighborhood-based approach to identify the black hole attack. In this approach, source initiates a routing recovery process by sending RREQ, to discover the correct path to the destination. A method is designed to deal with the black hole attack, which is based on the neighbor set information and consists of two parts: detection and response. In detection procedure, two foremost steps are:

Step 1. To collect neighbor set information.

Step 2. To determine whether there exists a black hole attack.

In Response procedure, the source node sends a modify-RouteEntry (MRE) control packet to the destination node to create an accurate path by changing the routing entries of the intermediate nodes from source to destination.

1. Advantages

(i) This technique is very powerful to detect the black hole attack.

(ii) It improves the throughput at least 15%.

2. Disadvantages

(i) It becomes useless when the attacker agrees to forge the fake reply packets.

(ii) It announces more routing control overhead.

C. Redundant Route Method and Unique Sequence Number Scheme

Shurman et al. [15] proposed two procedures to avoid the black hole attack in MANETs. The first procedure is to find at least two routes from the source to the destination node. The working is as follow. Initially a RREQ message is sent to the destination by the source node then the receiver node with the route to the destination will send reply to this RREQ message and then the acknowledge examination is started at source node. After that the sender node will buffer the RREP packet sent by different nodes until there are at least three received RREP packets and after identifying a safe route, buffered packets are transmitted. It shows that there exits at least two paths for routing at the same time. The secure route is found by source node by counting the number of hops or nodes and as a result prevents black hole attack.

In the second technique, a sequence number which is unique is used. As sequence value is aggregated that's why it is always greater than the current sequence number. In this technique, two values are stored in two separate tables. These two values shows the last-packet-sequence-numbers which is used identify the last packet sent to and received from every other node. Each time a packet is sent or received; these two table values are updated automatically. These two table values help the sender to analyze whether there are malicious nodes in network or not. Second technique is considered to be good compared to first technique because of the sequence number which is included to every packet contained in the original routing protocol.

1. Advantages

(i) These techniques have less numbers of RREQ and RREP when compared to existing AODV.
(ii) These techniques have less network overhead due to less number of message transmission.

2. Disadvantages

(i) Both of these techniques fail to detect cooperative black hole attacks.
(ii) These techniques introduce more time delay.

D. Time-Based Threshold Detection Scheme

Tamilselvan L et al. [10] proposed a solution by the enhancement of the original AODV routing protocol. The main idea behind this approach is to set timer for collecting the requests from other nodes after receiving the first request. It records the packet's sequence number and the received time in a table named Collect Route Reply Table (CRRT). The route validity is checked based on the arrival time of the first request and the threshold value.

1. Advantages

(i) The PDR of this protocol is around 90 to100% when AODV is around 80%.

2. Disadvantages

(i) It is difficult to assign threshold value.
(ii) The end-to-end delay increases when the malicious node is away from source node.

E. Distributed Cooperative Mechanism (DCM)

Wu Chang et al. [11] proposed a distributed and cooperated "black hole" node detection mechanism which composes four sub-steps: (1) local data collection (2) Local detection (3) Cooperative detection (4) Global reaction. In first sub step, an estimation table is developed and maintained by each node in the network. Each node compares the information of overhearing packets to find out whether there is any malicious node. If there is one apprehensive node, the detect node initiates the local detection phase to identify whether there is possible black hole. Subsequently, the cooperative detection procedure is initiated by the initial detection node, which is started by broadcasting and notifying all the one-hop neighbors of the possible suspicious node to cooperatively participate in the decision process confirming that the node in question is indeed a malicious one If the inspection value is positive, the doubtful node is considered as a normal node. Otherwise cooperative detection procedure is started by the initial detection node and handles broadcasting and notifying all one-hop neighbors to participate in the decision making. A threshold viz. *thr* represents the maximum hop count range of cooperative detection message. Finally, the global reaction phase is executed to set up a notification system, and disseminate caution messages to all the nodes in the network. Global reaction phase consists of reaction modes. The first reaction mode notifies to the whole network, but might waste lots of communication overhead. In this method, each node only concerns its own black hole list and arranges its transmission route in other mode, however it might be broken by malicious nodes.

1. Advantages

(i) The Packet Delivery Ratio is improved by 64.14% to 92.93% when compared with AODV.

2. Disadvantages

(i) The first reaction mode notifies to the whole network, but might waste lots of communication overhead
(ii) It takes more operation time.
(iii) Network size is increased in this approach.

F. DRI Table and Cross Checking Scheme

Hesiri Weerasinghe et al. [16], [17] proposed an algorithm to identify Collaborative Black Hole Attack. In this the AODV routing protocol is little bit modified by adding an additional table i.e. Data Routing Information (DRI) table and cross checking using Further Request (FREQ) and Further Reply (FREP). If the source node (SN) does not have the fresh enough route entry to the destination in its routing table, the source node (SN) sends RREQ to each node, and sends packets to the node which replies the RREP packet. The intermediate node (IN) sends next hop node (NHN) and DRI table to the SN, then the SN again examines its own routing table and the received DRI table to determine the IN's honesty. After that, SN sends FREQ message to IN's NHN for asking its routing information, along with the current NHN, the NHN's DRI table and its own DRI table. Finally, the SN makes a comparison in the above information by cross checking to judge the malicious nodes in the routing path.

1. Advantages

(i) This protocol improves the throughput as compare to original AODV.

2. Disadvantages

(i) It wastes 5 to 8 % more communication overhead.
(ii) There is also increase in packet loss percentage due to secure route discovery delay.

G. Random Two-Hop Ack and Bayesian Detection Scheme

An approach is proposed by Djamel Djenouri et al. [18] to monitor, detect, and remove the black hole attack in MANETs. In the monitor phase, a competent technique of random two-hop ACK is used. A local judgment approach based on Bayesian technique is used for node allegation in the detection phase. Authors have proposed a witness-based protocol that forces the recognized node to ensure this decision from other nodes. Before separating the misbehavior node at the same time, the witness-based protocol forces the detector to accumulate minimum k witnesses. However, the decision of k value is a trade-off problem. A higher k value removes the false detection and attack possibility, but reduces the detection effectiveness, and vice versa. This solution deals with all kinds of packet droppers, selfish and malicious nodes launching a black hole attack. This solution detects the attacker when it drops packets. The solution utilizes cooperatively witness-based verification, yet, it's not easy to prevent collaborate black hole attack for the judgment phase is only running on local side. After determining a malicious node by the proposed detection scheme, all nodes have to prove this judgment.

1. Advantages
(i) It does not use any periodic packets exchanging, therefore the familiar overhead problem can be eliminated from this solution.
(iii) This technique detects all type of packet droppers like Byzantine attack.
(iv) It achieves lower false detection.

2. Disadvantages
(i) It does not detect cooperative black hole attack.

H. Bluff- Based Approach

Sharma et al. [19] proposed an algorithm which is designed using ZRP protocol. In this some extra code is integrated for bluff probe packet and for the detection and prevention of black hole attack. This algorithm is divided into following parts (i) when there is intra-zone communication (ii) when inter zone communication takes place. Bluff probe packet is broadcasted by source node for intra-zone communication and the bluff probe packet constitutes the address of destination node which really does not exist. On receiving this bluff probe packet the direct neighbor nodes check their routing table entries if they have entry for this non-existent destination node then they forward the packet to the next neighbor. If the non-existing node is assumed to be malicious node then they will give instant response to the source node through the intermediate node. According to the response, the source node declares it as a black hole node and blocks this node. Then after, the source node alert to the direct neighbors for altering their routing table entries.

1. Advantages
(i) This is a multi path routing protocol.
(ii) It improves the throughput and PDR of a network.

2. Disadvantages:
(i) It increase the overhead due to extra code required.
(ii) It introduces more time delay.

I. Resource-Efficient ACcounTability (REAct) Scheme Based On Random Audits

William Kozma Jr. et al. [20] propose a reactive misbehavior detection scheme called REAct scheme. When the performance between source and destination node decreases, the REAct is triggered automatically. REAct constitutes of three phases: (a) the audit phase, (b) the search phase and (c) the identification phase. The work of audit phase is to verify the packet forwarding from audited node to the destination node. The audit phase made up of three steps: (a) sending of an audit request. (b) Building up behavioral proof and (c) then processing of this build up behavioral proof. The search phase identifies the unreliable links i.e., the link in which packets are lost. The simulation shows that REAct scheme not only reduces the communication overhead, but enlarges the identification delay because REAct is based on reactive DSR routing protocol. Furthermore, there are some shortcomings in REAct. First, the REAct is designed for non-cooperative black hole attack only. It is unable to prevent collaborative black hole scenario because other malicious node is able to manipulate a fake proof and send to the audit node. Second, the behavioral proof only has the information of transmission packets not about the nodes. Finally, binary search method is used to find the attacker which is easily exposed to audit node's information. The attacker is able to cheat source node by changing its behavior dynamically.

1. Advantages
(i) It reduces the communication overhead.
(ii) It improves the network performance.

2. Disadvantages
(i) It enlarges the identification delay.
(ii) The binary search method is easily expose audit node's information.

J. Flow Conservation Based Approach

For detecting packet forwarding misbehavior Gonzalez et al. [21] presents an approach, which works on the principle of flow conservation in a network, which states that if all the neighbors of a node Nj are investigated for (i) the amount of packets sent to Nj to forward and (ii) the packets forwarded by Nj to them, the total amount of packets sent to and received from Nj must be identical. They assume a threshold value for non-malicious packet drop. A node Ni maintains a table with two metrics Uij and Vij, which contain an entry for each node Nj to which Vi has respectively transmitted packets to or received packets from. Node Ni increments Uij on successful transmission of a packet to Nj for Nj to forward to another node, and increments Vij on successful receipt of a packet forwarded by Nj that did not originate at Nj. Every node of the network uninterruptedly checks their neighboring nodes and bring up-to-date the list of that nodes which they have overheard freshly.

1. Advantages
(i) This algorithm does not need various nodes to overhear each other's received and transmitted packets so it has less overhead.

2. Disadvantages
(i) Low message authentication
(ii) Due to no collaborative compromise mechanism, this protocol may lead to false allegations alongside correctly behaving nodes.

K. Hash Based Scheme

Wang et al. [22] proposed hash based defending method to generate node behavioral proofs which uses the concept of involving the data traffic information within the routing path. This mechanism is for audit based detection of collaborative packet drop attacks. Firstly the weakness of the REAct system is studied and then illustrated that Collaborative adversary can compromise the attacker identification procedure by sharing Bloom filters of packets among them. The major difference between these two schemes is as follows. A hash based node behavioral proofs is proposed to defend the collaborative attacks. The audited node n_i is needed. Source node S settles by this audited node, and then S sends the sequence numbers of selected packets to auditing node. When source node transmits these packets, an additional random number t_0 is involved to the end of every packet. The intermediate node n_1 combines the received packet and its own random number r_1 to compute its value t_1, and this operation is persistent within every intermediate node until n_i receives the packet. No simulation is done for this approach so no results are available.

1. Advantages
(i) It overcomes the shortcomings of REAct system**.**
2. Disadvantages
(i) It consumes more resources like battery, bandwidth.
(ii) It introduces more identification delay.

L. Hashed-Based MAC and Hash-Based PRF Scheme

Zhao Min and Zhou Jiliu [23] proposed two hash-based authentication mechanisms, the message authentication code (MAC) and the pseudo random function (PRF). These two proposals are provided for fast message verification and group identification, detect the collaborative malicious nodes and determine the secure routing path to prevent cooperative black hole attacks.

Due to decentralized infrastructure, the public key infrastructure (PKI) is difficult to employ in MANET. To deserve to be mentioned, authors overcome this bottleneck by designing an authentication mechanism. The main point of this solution is that each node achieves a secret key K_i, and $K_i = G_k (r_i)$. The sharing key K_i is hidden to all other nodes; thus, it is formulated by choosing a random number r_i and persistently applying PRF on r_i by k times. When source node receives a packet, it checks $K_{i\text{-}d\ to}$ find whether the key used for the MAC is reveled or not, and checks the MAC when K_i is reveled. After checking the above two conditions, this packet is regarded as available packet and the route is confirmed as a secure route. On the other hand, authors propose the other solution based on time stamp method and global symmetric cryptosystem. However, we don't discuss this solution due to the time stamp method is familiar, and the global symmetric cryptosystem is designed based on accompanying the time delay range.

1. Advantages
(i) This protocol has the better packet delivery ratio than AODV routing protocol.
2. Disadvantages
(i) These solutions have higher control overhead.
(ii) Detection time is also increased due to raise in pause time.
(iii) Malicious node is able to forge the false reply packets and try to avoid the detection mechanism.

M. Detection, Prevention, and Reactive AODV (DPRAODV) Scheme

A new control packet called ALARM is used in DPRAODV which is proposed by Raj PN, Swadas et al. [24] by making use of threshold value. Unlike normal AODV, in DPRAODV an additional check is done to find whether the RREP_seq_no value is higher than the threshold value. If the RREP_seq_no value is greater than the threshold value, the node is considered to be malicious node. This malicious node is added to the black list. When the node finds out suspicious node, it transmits an ALARM packet to its neighbors. This ALARM packet has as a parameter, black listed node. The ALARM is sent to its neighbors which includes the black list. When a node receives the RREP from the other node receiving node checks the black list table, if the sender is malicious RREP is ignored and malicious node is blocked. On the other hand, the dynamic threshold value is changed by calculating the average of dest_seq_no between the sequence number and RREP packet in each time slot.

1. Advantages
(i) This scheme not only detects the black hole attacks but also prevents by updating threshold which responses the realistic network environment.
(ii) Packet delivery ratio is improved by 80-85% than AODV when under black hole attack, and 60% when traffic load increases.
2. Disadvantages
(i) It takes a little bit higher routing overhead and end-to-end delay.

N. SAODV Protocol

In method [25] Songbai Lu et.al proposed a secure and efficient routing protocol (SAODV) protocol by incorporating the random number generation mechanism at the nodes. In this protocol, process of route discovery is increased by verifying the destination node directly using exchange of random numbers. In route discovery phase, On receiving the RREP, source node will deposit the RREP in its routing table, and immediately a verification packet SRREQ with a random number (records as x) generated by a source node is sent to the destination node along the opposite direction route of RREP received. The destination node respectively sends confirmation packet SRREP to the source node immediately along corresponding opposite direction path of SRREQ with random number (records as y) generated by the destination node. Because of using the exchange of random numbers, the random number in the correct SRREP is generated by the destination node in each route discovery process. Even if the malicious node stores those random numbers, which used in the previous route discovery process, it cannot get the correct random number and send a correct SRREP to reply.

1. Advantages
(i) It improves the throughput and packet delivery ratio as compares to original AODV.
2. Disadvantages
(i) More time delay
(ii) Increase in network over head.

O. Mechanism Based On Judgment Process

A mechanism has been proposed by Medadian, M. et al. [26] to mitigate the Black hole attack through the judgment process which uses honesty of the nodes that is derived from the opinions of neighbor nodes of a node in a network. While transferring the data packets, each node must show its honesty. After receiving first RREP packet, a node forwards packets to source and starts judgment process on about sender of the received packet. The judgment process depends on the opinions of all nodes of the network about replier. The neighbors are requested to send their opinion about a node. After collecting all opinions of neighbors, it decides whether the replier is a malicious node or not, based on number rules.

1. Advantages

(i) This protocol is very simple and there is no time delay in it.

2. Disadvantages

(i) Opinions of neighbors may not correct always.

P. Detection Using Restricted IP Addresses

A mechanism is detected by Vishnu K. and Paul et al. [27] to detect and remove the black hole nodes. This solution also finds the collaborative malicious nodes which introduce huge packet drop percentage. An idea of the group of backbone nodes [28] used in MANET was originated.

Vishnu K. et al. refer this method to develop their algorithm, and also add a novel scheme known as restricted IP (RIP) to avoid collaborative black and gray attacks. The detailed procedure is defined as follows. In this solution, initially an ad hoc network of backbone nodes is established from a set of strong backbone nodes (BBNs). These trusted nodes have authority to allocate the RIP when there is new arrival node joining. A node gets a RIP which means that it is provided with the routing authority. Whenever a node wants to transmit data packets, it requests the nearest BBN for a RIP, and a RIP is assigned to the source node by BBN. Now the source node not only sends the RREQ for destination but also for RIP. If the source node only receives the RREP of destination node, it means that there is no black hole. In the case when RREP packet for RIP is also obtained, it implies that malicious node might be existed in the network. The RIP’s neighbor nodes change to promiscuous mode as a result of the source node sends monitor messages to alert them. These neighborhoods not only monitor the packets of designate nodes but also the suspicious nodes. Furthermore, the source node sends few dummy data packets to test the malicious node. The neighbor nodes monitor the data packet flow and regard it as a black hole if the packet loss rate exceeds the normal threshold, and inform the source node that it is a malicious attacker. Then the neighbor nodes broadcast this alert message through the whole network, and include the malicious nodes to the black hole list. Finally, the attacker’s authorization will be deleted and all of nodes drop the response from nodes in the black list.

1. Advantages

(i) It not only works for black hole but also grey hole attack, since it does not utilize trust based method.

(ii) It improves packet throughput and packet drop rate of the network.

2. Disadvantages

(i) The proposed system might be crashed if the numbers of attackers are higher than the numbers of normal nodes.

Q. Next Hop Information Scheme

A security approach is proposed by N. Jaisankar et al. [29] which is composed of two parts, detection and reaction. In the first part, the *field_next_hop* is attached to the RREP packet. Before the data packets are sent by the source node, the leading RREP packet is examined between intermediate node and destination node. A black identification table (BIT) is maintained by each node, and the fields which this table contains are <source, target, current_node_ID, Packet_received_count (PRC), Packet_forwarded_count (PFC), Packet modified count (PMC)>. Then the PMC is updated by tracing the BIT from their neighborhoods. If the node behaves properly, the subsequent count value multiplies. Now if the number of receiving packets differentiates from sending packets a malicious node can be found out. The second part is separating the black hole, thus each node maintains an isolation table (IT) and stores the black node ID. The ID is broadcasted to all nodes in order to remove the malicious node by checking the isolation table.

1. Advantages

(i) The PDR is improved by 40-50% and the number of packets dropped is decreased by 75-80% than AODV.

2. Disadvantages

(i) It includes some additional delay.

R. Nital Mistry et al.’s Method

Mistry N. et al. [30] proposed a solution for analyzing and improving the security of AODV routing protocol against Black hole Attack. The approach basically modifies the working of source node only, using additional function Pre_ReceiveReply. A table Cmg_RREP_Tab, a variable Mali_node and a new timer MOS_WAIT_TIME are also added to the default AODV. In the proposed solution, after receiving the first RREP the source node waits for MOS_WAIT_TIME and in the meantime it stores all the RREPs in the Cmg_RREP_Tab table until MOS_WAIT_TIME. In this technique the value of MOS_WAIT_TIME is considered to be half the value of RREP_WAIT_TIME. Now, the source node will analyze the stored RREPs and will discard the RREP which have high destination sequence number. The node which has sent these RREP with high destination sequence number is considered to be malicious node. This technique also records the identity of suspected malicious nodes as Mail_node, so that in future it can discard messages coming from that node.

1. Advantages

(i) It only needs changes in working of source node.

(ii) It improves PDR when network size and mobility is increasing.

2. Disadvantages

(i) Time delay is increased with varying size of network and mobility.

S. An Anti-Black Hole Mechanism (ABM) Using IDS

Ming-Yang Su [31] proposes an IDS scheme to solve the selective black hole attacks in MANET, and plants an anti-black hole mechanism (ABM) in all IDS nodes. The ABM employs two supplementary tables called RQ table and SN table. The RQ table stores the RREQ message within IDS node's transmission range. The contents including the source and destination ID, source sequence number, maximum hop count value, broadcasting node ID and expiration time. The IDS nodes use SN table to approximate the doubtful values nodes within its transmission range. The components of SN table including the node ID, doubtful values and status. If an intermediate node never broadcasts a RREQ for a route but sends a RREP packet, the doubtful value will be added one in the neighbor IDS node's SN table. Besides this, another new Block table is added into the original routing table in order to record the list of black holes.

The basic framework of proposed IDS is introduced as follow. In the beginning, the ABM function in a sniff mode is executed by the IDS nodes. According to the irregular difference between the routing information transmitted from a dubious node, ABM can estimate a value of the suspicious node. If the value exceeds the predefined threshold value, it can be regarded as a black hole. When a normal node receives a Block message broadcasted by the IDS node, this node adds the malicious node which is stored in the Block message into the Block table. After that, the normal node forwards RREP packet to establish the routing. If the RREP packet is obtained from its neighbor node which noted in the Block table, the normal node drops this RREP packet to prevent the malicious attack.

1. Advantages
(i) It is multipath protocol.
(ii) The packet loss rate can be decreased to 11.28% and 14.76%.

2. Disadvantages
(i) Cooperative isolation the malicious node, but failed at collaborative black hole attacks.
(ii) It adds more delay to the delay.

T. Algorithm Based On Preprocessor

An algorithm presented in [32] to detect the black hole attack in a MANET. This algorithm is based on the preprocessor called Pre_Process_RREP. The Process continues to accept RREP packets and calls a process called Compare_Pkts (packet p1, packet p2) which actually compares the destination sequence number of two packets and the packet with higher destination sequence number is selected if the difference between two numbers is not considerably high. A Packet which contains extremely high destination sequence number is assumed to be a malicious node and an ALERT message having the node identification is generated. This node ID is broadcasted to neighbor nodes so that the malicious node can be separated from the network and can maintain a list of such malicious nodes.

1. Advantages
(i) This algorithm is simple and does not affect workings of either intermediate or destination node.
(ii) It does not even modify the working of normal AODV.

2. Disadvantages
(i) This protocol does not work when malicious nodes are working cooperatively.

U. Mechanism Using recvReply() Function

Kamarularifin Abd et al. [33] have designed an ERDA solution to improve AODV protocol with minimum modification to the existing route discovery mechanism using recvReply() function. Authors introduce three new elements in modified recvReply() function namely: table rrep_table to store incoming RREP packet parameter mali_list to keep the record of detected malicious nodes identity and parameter rt_upd to control the process of updating the routing table. When source node initiates route discovery process by sending the RREQ packet to find a fresh route to the destination node, Source node will 874capture this received RREP packet into rrep_tab table. Since the malicious node firstly gives response to the source node, the routing table is updated with RREP information from malicious node. As the value of parameter rt_upd is „true‟, source node accepts the next RREP packet from other node to update the routing table although it arrives later and with a lower destination sequence number than the one in the routing table. The current route entry in routing table will be overwritten by the later RREP coming from other nodes. ERDA method provides a simple solution by eliminating the false route entry and replaced the entry with later RREP. The disadvantage of this method is that it cannot detect cooperative black hole attack.

1. Advantages
(i) This enhancement only involves a minimum modification and does not change the existing AODV protocol scheme.
(ii) This solution is very light and suitable for most resource constraint devices.

2. Disadvantages
(i) The major issue in this method is the latency time during the route discovery process since the source node has to wait until the waiting time period expired before the routing table can be updated. This issue is also exists even when there is no attack in network.

V. Protocol Based On Trusted Table

Yaser Khamayseh et al. [34] proposed protocol that modifies the behavior of the original AODV. This protocol introduces a data structure which is known as trust table at every node. This is the responsibility of the trust table to hold the addresses of the trusted nodes. An extra field, called trust field is added to RREP. If a node wants to add itself to the trust table of another node, it firstly requires passing the behavioral analysis filter. Once the behavior of the broadcasting node is normal, its entry is made in to the trust table of the receiving node. RREP with an extra trust field indicates the reliability of the replying node. The value of the trust field is initialized to zero by the replying node and might be modified by its previous hop during the trip of the RREP. The value of the trust field could be modified either to 2 if the replying node is the destination itself or to 1 if the replying node is not the destination but still exist in the trust table. On receiving the RREP, source node decides whether to transmit the data or to wait for another route. If the value of trust field is equal to 1 or 2, the source node sends, otherwise the source node waits for further route. Even though reliable routes are provided by this method but it consumes high network delay.

1. Advantages
(i) It improves the throughput, packet delivery ratio.
2. Disadvantages
(i) It introduces more time delay and network overhead.

V. Bait DSR (BDSR) Based On Hybrid Routing Scheme

Tsou P-C. et al. [35] design a novel solution named Bait DSR (BDSR) scheme to avoid the collaborative black hole attacks. The proposed solution utilizes the both proactive and reactive method to make a hybrid routing protocol in the beginning of routing stage, at first the source node sends bait RREQ packet before initiating route discovery. The target address of bait RREQ is arbitrary and non-existent. The same method as used in DSR is used here to avoid the traffic jam problem generated by bait RREQ. The forged RREP can be attracted by the initially sent bait RREQ and can easily remove malicious node to avoid black hole attack. In proposed mechanism, the generator of RREP is recorded in the RREP's additional field. Thus the source node can recognize the location of attacker from the reply location of RREP. All of the response sent by the adversaries should be dropped. After the completion of initial phase, authors employ the original DSR route discovery procedure.

1. Advantages
(i) BDSR has an increased packet delivery ratio more than 90 % when compared to existing DSR and WD approach.
2. Disadvantages
(i) Communication overhead is also lower than watch dog scheme but slightly higher than original DSR routing protocol.

W. CAODV Credit Based On AODV (CAODV)

Watchara Saetang and Sakuna Charoenpanyasak [36] proposed credit based mechanism to check the next hop whether it can be trusted or not. The credit is initiated in a route discovery phase. The credit is defined as followings:

Hop count*3; initial state
Credit = Credit+2; when destination node sends credit acknowledge
Credit-1; send 1 packet
Note: Credit Max = 5*(Hop count+2)

At first, a source node broadcasts RREQ to other nodes until it does not gets RREP from a destination node or node having a route to destination. The next hop node or who sent RREP will be assigned a credit by the receiving node. When a node in the path sends one packet, one credit is reduced from the next hop node. As soon as a destination node receives data packet, it will send Credit Acknowledge (CACK) back to a source node. A node within a way back will increase credit of the next hop by 2 to indicate a higher trust level of the next hop. Conversely, credit will be decreased if a node cannot receive CACK. When the credit of any node reaches to zero it will be untrusted and marked as a blacklist.

1. Advantages
(i) CAODV does not consume any extra resource like network bandwidth.
(ii) CAODV has improved the throughput up to 40% when compared to original AODV.
2. Disadvantages
(i) CAODV is unable to detect cooperative black hole attack.
(ii) It will increase the network overhead.

IV. Comparison

We have compared above discussed protocols based on various criteria, which are base protocol, single path or multi path, additional packet transmission, type of black hole detected and tool used. Table I shows the comparison.

TABLE I
COMPARISON AMONG VARIOUS MODIFIED PROTOCOLS

S. No.	Protocol	Base Protocol	Single Path/ Multi Path	Additional Packet Transmission	Type of Black Hole detected	Tools
1.	Deng's solution[13]	AODV	Single Path	YES	Single Black hole	--------
2.	Neighborhood-Based Approach[14]	AODV	Single Path	YES	Single black hole	NS-2
3.	Redundant Route Method[15]	AODV	Single Path	YES	Single black hole	NS-2
4.	Time-based Threshold Detection Scheme[10]	AODV	Single Path	YES	Single hole	Glomosim
5.	Distributed Cooperative Mechanism (DCM)[11]	AODV	Single Path	YES	Cooperative black hole	NS-2
6.	DRI Table and Cross Checking Scheme[16, 17]	AODV	Single path	YES	Cooperative black hole	Qualnet
7.	Random Two-hop ACK and Bayesian Detection Scheme[18]	AODV	Single Path	No	Single black hole	Glomosim
8.	Bluff- Based Approach[19]	ZRP	Multi Path	YES	Single black hole	Qualnet
9.	REAct Scheme based on Random Audits[20]	DSR	Single path	YES	Single black hole	Bloom Filters
10.	Flow Conservation based approach[21]	AODV	Single path	No	Cooperative black hole	NS-2
11.	Hash Based Scheme[22]	DSR	Single Path	NO	Cooperative black hole	No Simulation
12.	Hashed –based MAC and hashed based PRF scheme[23]	AODV	Single Path	NO	Cooperative black hole	NS-2
13.	(DPRAODV) Scheme[24]	AODV	Single Path	YES	Single Black hole	NS-2
14.	SAODV Protocol[2]	AODV	Single Path	YES	Single Black hole	NS-2
15.	Mechanism Based on Judgment Process[26]	AODV	Single Path	NO	Co operative black holes	NS-2
16.	Detection using restricted IP addresses[27]	AODV	Single Path	YES	Collaborative black hole	Opnet
17.	Nital Mistry et al.'s Method[29]	AODV	Single Path	No	Single black hole	NS-2
18.	Next Hop Information Scheme[30]	AODV	Single Path	YES	Single Black hole	NS-2
19.	An Anti-Black hole Mechanism (ABM) using IDS[31]	MAODV	Multi Path	YES	Multiple black holes	NS-2
20.	Algorithm based on Preprocessor[32]	AODV	Single Path	YES	Single Black hole	No Simulation
21.	Mechanism using recvReply() function[33]	AODV	Single Path	NO	Single Black hole	NS-2
22.	Protocol based on trusted table[34]	AODV	Single Path	NO	Single Black hole	GloMoSim
23.	BDSR based on Hybrid Routing Scheme[35]	DSR	Single Path	YES	Cooperative Black hole	QualNET
24.	Credit based on AODV (CAODV)[36]	AODV	Single Path	NO	Single Black hole	NS-2

V. CONCLUSION AND FUTURE SCOPE

Routing protocols because of their inherent infrastructure in MANET are vulnerable to black hole attack, many researchers have proposed different type of techniques to detect and prevent this kind of attack. In this paper, different kinds of the up to date routing methods of existing solutions are discussed for the detection and prevention of such attack which have better packet delivery ratio and correct detection probability but have high overhead. A comparison table has been provided for analyzing all the methods. The following are the main behavioral characteristics of the black hole node:

It snoops on its neighbors to discover which node is preparing to send a RREQ. For any received RREQ, the black hole node propagates a RREP claiming that it has a direct link to the destination.

It constantly attempts to locate itself within the transmission range of any source node in order to reply as quickly as possible.

There are various QOS parameters to measure the performance of network like throughput, end to end delay packet delivery ratio. While designing a new routing protocol in this context, researchers should also consider the following network parameters:

A. Scalability

Scalability is the ability of a routing protocol to perform efficiently as one or more inherent parameters of the network grow to be large in value.

B. Mobility

Mobility defines the movement of nodes from one place to another place.

For future direction the aim is to develop and analyze a routing protocol for detection and prevention of black hole attack and analyze the performance of that protocol under different network scenarios.

REFERENCES

[1] S. Basagni, M. Conti, S. Giordano, I. Stojmenovic, Mobile Ad Hoc Networking, *IEEE Press and John Wiley & Sons*, Inc., 2004.

[2] S. Murthy and J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks", ACM Mobile Networks and Applications Journal, vol.1, no.2, 1996, pp. l83-197.

[3] D. B. Johnan and D. A. Maltz, *"Dynamic Source Routing in Ad Hoc Wireless Networks*", Kluwer Academic Publishers, In Mobile Computing, edited by Tomasz Lmielinski and Hank Korth, chapter 5, 1996, pp. 153-181..

[4] C. E. Perkins and E. M. Royer, "Ad-Hoc On-Demand Distance Vector Routing," Proc. 2nd *IEEE Mobile Computer Systems and Applications*, 1999, pp. 90–100.

[5] Y. Ko and N.H. Vaidya.," Location-Aided Routing (LAR) in Mobile Ad Hoc Network", *ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM)*, 1998, pp. 66-75.

[6] P.V.Jani, "Security within Ad-Hoc Networks", Position Paper, *PAMPAS Workshop*, Sept. 16/17 2002.R. W. Lucky, "Automatic Equalization for Digital Communication," *Bell Syst. Tech. J.*, vol. 44, no. 4, pp. 547–588, Apr. 1965.

[7] K. Biswas and Md. Liaqat Ali, "Security Threats in Mobile Ad-Hoc Network", *Master Thesis*, Blekinge Institute of Technology Sweden, 22nd March 2007.

[8] B. Wu, J. Chen, J. Wu, M. Cardei, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks", *Wireless Network*

Security. On Signals and Communication Technology, Springer, New York, 2009.

[9] N. Bhalaji and A. Shanmugam, “A Trust Based Model to Mitigate Black Hole Attacks in DSR Based Manet”, *European Journal of Scientific Research*, vol.50 No.1, 2011, pp.6-15.

[10] L. Tamilselvan and Dr. V. Sankaranarayanan, “Prevention of Blackhole Attack in MANET”, *The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications*, 0-7695-2842-2/07, 2007.

[11] C. Wu Yu, T-K Wu, R. H. Cheng, and S. C. Chang, “A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks”, *PAKDD Workshops*, LNAI 4819, 2007, pp. 538–549.

[12] B. V. Santhosh Krishna, A.L Vallikannu, “Detecting Malicious Nodes For Secure Routing in MANETS Using Reputation Based Mechanism” *International Journal of Scientific & Engineering Research*, vol. 1, Issue 3, ISSN 2229-5518, December-2010.

[13] H. Deng, W. Li and D.P. Agrawal, "Routing Security in Wireless Ad Hoc Networks," *Communications Magazine, IEEE*, vol.40, no.10, October 2002, pp. 70- 75.

[14] B. Sun, Y. Guan, J. Chen , U.W. Pooch , “Detecting Black-hole Attack in Mobile Ad Hoc Networks”, 5th *European Personal Mobile Communications Conference, Glasgow*, United Kingdom, 22-25 April 2003.

[15] M. Al-Shurman, S-M Yoo, S. Park, “Black Hole Attack in Mobile Ad Hoc Networks”. 42nd *Annual ACM Southeast Regional Conference (ACM-SE’42), Huntsville, Alabama*, 2-3 April 2004

[16] H. Weerasinghe and H. Fu, “Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation*”, Intenation Journal of Software Engineering and Its Application*, Vol.2, No. 3, July, 2008, pp. 39- 54.

[17] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, K. Nygard, “Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks” *International Conference on Wireless Networks*, Las Vegas, Nevada, USA, June 2003, pp. 23-26.

[18] D. Djenouri, N. Badache, “Struggling against Selfishness and Black Hole Attacks in MANETs”, *Wireless Communications & Mobile Computing*, Vol. 8, No. 6, August 2008, pp 689-704.

[19] S.Sharma, Rajshree, R. Prakash, Vivek , “Bluff-Probe Based Black Hole Node Detection and prevention*”, IEEE International Advance Computing Conference*, 7 March 2009, pp. 458-461.

[20] W. Kozma, L. Lazos , “REAct: Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Networks Based On Random Audits” Second *ACM Conference on Wireless Network Security*, Zurich, Switzerland, March 2009, pp. 16-18.

[21] F. Oscar, Gonzalez, M. Howarth, and G. Pavlou, “Detection of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks”, 10th *IFIP/IEEE International Symposium Integrated Network Management, Centre for Communications Systems Research*, University of Surrey, Guildford, UK, May 21, 2007.

[22] W. Wang, B. Bhargava, M. Linderman, “Defending against Collaborative Packet Drop Attacks on MANETs” 2nd International *Workshop on Dependable Network Computing and Mobile Systems (in Conjunction with IEEE SRDS 2009)*, New York, USA, 27 September 2009.

[23] Z. Min, Z. Jiliu “Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks” International Symposium on Information *Engineering and Electronic Commerce*, Ternopil, Ukraine, 16-17 May 2009.

[24] P.N. Raj, P.B. Swadas, “DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET*”, International Journal of Computer Science*, Vol. 2, 2009, pp. 54–59.

[25] L. Songbai , L. Longxuan , L. Kwok, J. Lingyan, "SAODV: A MANET Routing Protocol That Can Withstand Black Hole Attack," *International Conference on Computational Intelligence and Security*, 2009. CIS '09, vol.2, 11-14 Dec. 2009, no., pp.421-425.

[26] M. Medadian, A. Mebadi, E. Shahri, "Combat with Black Hole Attack in AODV Routing Protocol*", IEEE 9th Malaysia International Conference on Communication*, vol.15, no.17, Dec.2009, pp.530-535.

[27] Vishnu K and Amos J Paul, “Detection and Removal of Cooperative Black/Gray Hole Attack in Mobile ADHOC Networks” *International Journal of Computer Applications* (0975 - 8887), Volume 1, No. 22, 2010, pp. 38-42.

[28] P. Agrawal, R. K. Ghosh, S. K. Das, “Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks”, 2nd *International Conference on Ubiquitous Information Management and Communication*, Suwon, Korea, 2008, pp. 310-314.

[29] N. Jaisankar, R. Saravanan , K. D. Swamy, “A Novel Security Approach for Detecting Black Hole Attack in MANET”, *International Conference on Recent Trends in Business Administration and Information Processing*, Thiruvananthapuram, India, 26-27 March 2010.

[30] N. Mistry, D. C. Jinwala, M. Zaveri, “Improving AODV Protocol Against Blackhole Attacks” *International Multiconference of Engineers and Computer Scientists*, Hong Kong, 17-19 March, 2010.

[31] M-Y Su, “Prevention of Selective Black Hole Attacks on Mobile Ad Hoc Networks Through Intrusion Detection Systems*”, IEEE Computer Communications*, vol. 34 issue 1, doi:10.1016/j.comcom.2010.08.007, January, 2011, , pp. 107-117.

[32] S. C. Mandhata, S. N. Patro, “A Counter Measure to Black Hole Attack on AODV- Based Mobile Ad-Hoc Networks*” International Journal of Computer & Communication Technology (IJCCT)*, Volume 2, Issue 6, 2011, pp. 37- 42.

[33] A. J. Kamarularifin, Z. Ahmad, J. A. Manan, “Mitigation of Black Hole Attacks for AODV Routing Protocol*”, Society of Digital Information and Wireless Communications*, Vol. 1, No 2, 2011, pp. 336- 343.

[34] Y. Khamayseh, A. Bader, W. Mardini, and M. BaniYasein, “A New Protocol for Detecting Black Hole Nodes in Ad Hoc Networks”, *International Journal of Communication Networks and Information Security*, Vol. 3, No. 1, April 2011, pp. 36- 47.

[35] P.C. Tsou, J. M. Chang, L, H. C. Chao, J. L. Chen , “ Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs”, 13th *International Conference on Advanced Communication Technology*, Phoenix Park, Korea, Feb. 2011, pp. 13-16.

[36] W. Saetang and S. Charoenpanyasak, “CAODV Free Blackhole Attack in Ad Hoc Networks” *International Conference on Computer Networks and Communication Systems*, IPCSIT vol.35, 2012, pp. 63- 68.