A Survey on Black Hole Attacks on AODV Protocol in MANET

Madhusudhananagakumar KS
P.G Student,
Department of Computer Science,
School of Engineering & Technology,
Pondicherry University.

G. Aghila
Professor
Department of Computer Science,
School of Engineering & Technology,
Pondicherry University.

ABSTRACT
Mobile Ad hoc Network (MANET) is a collection of mobile nodes that dynamically form a temporary network without infrastructure. It has many number of applications mainly in the areas of Sensor Networks (SN), medical, military and rescue operations. Routing is an important component in mobile ad hoc networks and it has several routing protocols, which are affected from different attacks. Ad hoc On demand Distance Vector (AODV) is one of the most suitable routing protocol for the MANETs and it is more vulnerable to black hole attack by the malicious nodes. A malicious node that incorrectly sends the RREP (route reply) that it has a latest route with minimum hop count to destination and then it drops all the receiving packets. This is called as black hole attack. In the case of multiple malicious nodes that work together with cooperatively, the effect will be more. This type of attack is known as cooperative black hole attack. In this paper, we have surveyed and compare the existing solutions to black hole attacks on AODV protocol and their drawbacks.

Keywords
MANET, AODV, Black Hole, DPRAODV, MAODV, SAODV.

1. INTRODUCTION
In recent years mobile ad hoc network [2] (MANET) has a great impact on wireless networks. In MANET, there are no basic network devices, such as routers or access points to transfer data among nodes. Instead, each node acts as a router to establish a route and transfer data by means of multiple hops. Due to the mobility nature of nodes, the network topology changes rapidly and erratically over time. MANETs have many potential applications, like Sensor Networks, Medical Service, Personal Area Network, especially in military and rescue operations such as connecting soldiers in the battlefield or creating a temporary network in place of one, which collapsed after a disaster like tsunami. Mobile ad hoc networks are more vulnerable to security problem than the wired networks and there are several security issues [24] such as no predefined boundary, Adversary inside the network, No centralized control facility, Limited energy resource and changing scale. The network is less centralized, where mobile the nodes are must carry out network organization and delivery of packets themselves. When a node wants to transfer data to another node, packets are transferred through the intermediate nodes, thus, searching and establishing a route from a source node to a destination node is an important task in MANETs. A number of routing protocols have been developed for execute this task. Since, wireless networks came into existence, routing in mobile ad hoc networks has been a challenging task. The major reason for this is the constant changes in network topology due to the mobility of nodes. The available routing protocols are mainly categorized into proactive routing protocols, reactive routing protocols and hybrid routing protocol. In proactive routing protocols, the routing information of nodes is exchanged, sporadically, such as DSDV. In reactive routing protocols, nodes exchange routing information when it is needed such as AODV and DSR. Some ad-hoc routing protocols are a combination of the above two categories which we called as hybrid routing protocols. The primary goal of such an ad hoc network routing protocols are correct and efficient route establishment between a pair of nodes so that messages can be delivered in a timely manner.

The rest of the paper is organized as follows. Section 2 provides an overview of AODV protocol and some of the attacks performed at network layer, section 3 describes how the black hole attack is performed on AODV, Section 4 deals with several solutions to black hole attack, section 5 presents a comparison table among the solutions and finally, conclude the paper with plan for future work in Section 6.

2. OVER VIEW OF AODV ROUTING PROTOCOL
The Ad-hoc On-Demand Distance Vector (AODV) [1][29] is a reactive routing protocol designed to have intention for use in mobile ad hoc networks. It finds a route to a destination when a node likes to transfer a packet to that destination. Routes are maintained by the source node as long as they needed. Route discovery process is based on the route information is stored in all intermediate nodes along the route in the form of route table entries. Every node has routing table, it has the fields like destination, next hop, number of hops, destination sequence number, active neighbors and lifetime respectively. AODV uses several control packets like route request packet (RREQ) is broadcasted by a node requiring a route to another node, routing reply message (RREP) is unicasted back to the source of RREQ, and route error message (RERR) is sent to notify other nodes of the loss of the link. HELLO messages are used to find active neighbors. Sequence numbers are used to find the freshness of routes towards the destination. When a route is not available for the destination, a route request packet (RREQ) is flooded throughout the network. The RREQ contains source address

along with request ID is incremented each time the source node sends a new RREQ and identifies it uniquely. On receiving a RREQ packet, each node checks the source address and the request ID. If the node has already received a RREQ with the same pair of parameters the new RREQ packet will be discarded Otherwise the RREQ will be either forwarded (broadcast) or replied (unicast) with a RREP packet: once a RREP packet is received, the route is established . A source node may receive multiple RREP packets with different routes. It then updates its routing entries if and only if the RREP has a greater sequence number, i.e. fresh information. While transmitting RREQ packets through the network, each node notes the reverse path to the source. When the destination node is found, the RREP packet will travel along this path.

Recently, most research on ad-hoc routing protocols, has been assumed trusted environment but, many usages of ad-hoc network run in untrusted situations. Therefore, most ad hoc routing protocols are vulnerable to different types of attacks. These attacks are divided into two categories, called external attacks and internal attacks. Internal attacks are done by authorized node in the network, where as external attacks are performed by the node that they are not authorized to participate in the network. Another classification of attacks is related to protocol stacks, for instance, network layer attacks and some network layer attacks [18] are listed below in Table1.

Table1: Attacks at the network layer

Type of Attack	**Description**
Wormhole	Tunneling the packets using private high speed network.
Byzantine	Selectively drop packets by making routing loops, forwarding packets through non-optimal paths with compromised nodes.
Rushing	Quickly forwards the control messages to gain access to the network.
Resource consumption	It injects the packets to get more network resource.
Location disclosure	Attacker discloses the privacy of a network by knowing the location of a node.
Black hole	Drops the packets by sending false route reply messages to the route request.

3. BLACK HOLE ATTACK ON AODV PROTOCOL

To perform black hole attack, malicious node waits for RREQ messages from neighboring nodes. When the malicious node receives an RREQ message, immediately sends a false RREP message with a high sequence number and minimum hop count without checking its routing table to make an entry in the routing table of the source node, before other nodes replies to absorb transmitted data from source to that destination and drop them instead of forwarding. Black hole attack [4] in AODV protocol can be performed in two ways: black hole attack caused by RREP and black hole attack caused by RREQ are described in table2 as follows:

Table2: Black hole attack

Caused by RREQ	**Caused by RREP**
Set the originator IP address in RREQ to the originating node's IP address.	Set the originator IP address in RREP to the originating node's IP address.
Set the destination IP address in RREQ to the destination node's IP address	Set the destination IP address in RREP to the destination node's IP address.
Set the destination IP address of IP header to broadcast address	Set the destination IP address of IP header to the IP address of node that RREQ has been received
Set the source IP address of IP header to its own IP address	Set the source IP address of IP header to its own IP address.
Put high sequence number and low hop count in RREQ field	

4. SOLUTIONS TO BLACK HOLE ATTACK IN MANET

In this section, we will review the several solutions to black hole attacks**.**

Deng et.al. [11] have proposed a solution against black hole attack by modifying the AODV protocol. This approach avoids malicious nodes advertising the route that is not existed. In order to check whether the route advertised is existed and free of malicious nodes, each intermediate node has to include the address of the next hop node in RREP packets. Once the source node received the RREP packet, it extracts the details of the next hop node and sends a further request to the next hop node. 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 neighbour node replies the Further reply packet back to the source node to confirm the route information. If the source does not receive the Further reply, the route contains the malicious nodes and the route is removed from the routing table. However, this solution is vulnerable to cooperative black hole attacks. If both neighbour node and the next hop node are black hole nodes, the next hop node can response to the source node with falsified routing information. Therefore, this solution is still vulnerable to a cooperative black hole attack.

Al-Shurman et.al. [5] have proposed two solutions designed to target on black hole attacks on AODV protocol. The first proposed solution is to find more than one route to the destination. Source node unicasts a ping packet to the destination node. The receiver and the malicious in addition to intermediate node will reply to this ping packet. The source node receives an acknowledgement pinging back from different routes and it will check to find the safe routes. In the second solution, in order to find the malicious node, each node needs to maintain two tables to store sequence numbers of last packet sent to every node and last packet received from every sender

respectively and compare the last sequence number which is extracted from RREP at source node. If it matches, data will be forwarded to that route otherwise an alarm message is broadcasted to isolate the malicious node in the network. However, the two solutions has time delay as the drawback. According to proposed solution [23] by Tamilselvan et.al, the source node has to wait for other replies with next hop information without sending the data packets to the destination. Once it receives the first RREP it sets timer in the 'TimerExpiredTable', to collect the further RREP's from different nodes are stored in 'Collect Route Reply Table' (CRRT) with the 'sequence number', and the time at which the packet arrives. In order to calculate the 'timeout' value, uses arrived time of the first RREP. It first checks in CRRT whether there is any repeated next hop node. If any repeated next hop node is present, in route reply paths it assumes the paths are correct or the chance of malicious paths is limited. The disadvantages of the proposed solution are time delay, since source node has to wait for other route replies and it cannot detect cooperative black hole attack.

In [26] this paper authors Satoshi Kurosawa et.al. have introduced an anomaly detection scheme to detect black hole attack using dynamic training method in which the training data is updated at regular time intervals. They use the features to express the state of the network. In this scheme, the average of the difference between the Dst_Seq in RREQ packet and the one held in the list are calculated and this operation is executed for every received RREP packet. The average of this difference is finally calculated for each timeslot and it taken as the feature; hence, it consumes considerable amount time to do calculations for every RREP packet.

Latha Tamilselvan, Dr. V Sankaranarayanan [9] proposed a better solution with the modification of the AODV protocol, which avoids multiple black holes in the group. It uses Fidelity table where every node that is participating is given a fidelity level that will provide reliability to that node. Any node having 0 value is considered as malicious node and is eliminated from the network. The fidelity levels of nodes are updated based on their trusted participation in the network. Upon receiving the data packets, the destination node will send an acknowledgement to the source, thereby the intermediate node's level will be incremented. If no acknowledgement is received, the intermediate node's level will be decremented. The main drawback of this solution is processing delay in the network

Zhao Min et.al [27] have discussed an authentication mechanism for identifying black hole nodes in MANETs. An authentication mechanism is constructed based on the concept of the hash function, MAC, and PRF, which is used for checking the RREPs at source node to send the data packets. The proposed mechanism eliminates the need for a PKI or other forms of authentication infrastructure, however it needs to be discuess, how to handle unlimited message authentication by switching one-way-hash chains and how to prevent a malicious node cannot forge a reply if the hash key of any node is to be disclosed to all nodes.

In [25] Authors Ming-Yang Su et.al discussed a mechanism, called an ABM (Anti-Black hole Mechanism), which is mainly used to estimate the suspicious value of a node according to the amount of abnormal difference between RREQs and RREPs transmitted from the node. When a suspicious value exceeds a threshold level, the nearby IDS broadcasted a block message with id of IDS, the identified black hole node and the time of identification will place the malicious nodes on their blacklists to isolate the malicious node in the network cooperatively. The advantage of this method is that it can be able to detect cooperative black hole nodes in the MANETs. The main drawback of this technique is that mobile nodes have to maintain an extra database for training data and its updations, in addition to the maintenance of their routing table.

In [22] authors Alem, Y.F et.al. proposed a solution based on Intrusion Detection using Anomaly Detection (IDAD) to prevent attacks by the both single and multiple black hole nodes. IDAD assumes every activity of a user can be monitored and anomaly activities of an intruder can be identified from normal activities. To find a black hole node IDAD needs to be provided with a pre-collected set of anomaly activities, called audit data. Once audit data collected and it is given to the IDAD system, which is able to compare every activity with audit data. If any activity of a node is out of the activity listed in the audit data, the IDAD system isolates the particular node from the network. The reduction of the number of routing packets in turn minimizes network overhead and facilitates a faster communication.

Medadian, M et.al. [28] have proposed an approach to mitigate the Black hole attack through the judgment process by using honesty of a nodes, which, is derived from the opinions of a neighbor nodes of a node in a network. In order to transfer the data packets, a node must show its honesty. If a node is the first receiver of a RREP packet, it forwards packets to source and initiates judgment process on about replier. The judgment process was depends on opinion of network's nodes about replier. These neighbors are requested to send their opinion about a node. When a node collects all opinions of neighbors, it decides if the replier is a malicious node based on number rules. The biggest drawback of this solution is that the opinions of neighbors may not correct always.

XiaoYang Zhang et.al. [15] introduced a new detection method based on checking the sequence number in the Route Reply packets by making use of a new message originated by the destination. In this method, when an .intermediate node unicasts a RREP packet, the node also unicasts a newly defined control message to the destination node to request for the up-to-date SN. Upon receiving, the destination node unicasts a reply message to inform the source node of the up-to-date SN. This reply from the destination node enables the source node to verify if the intermediate node has sent a faked RREP message by checking if the SN in the RREP message is larger than the up-to-date SN. This method has more network overhead and time delay since node in the network generates new packets.

In method [10] Songbai Lu et.al proposed a secure and efficient routing protocol (SAODV) protocol by incorporating the random number generation mechanism at the nodes. SAODV increases the process of route discovery by verifying the destination node directly using exchange of random numbers. In route discovery phase, when the source node in MANET receives a RREP, it will deposit the RREP in its routing table, and immediately sends a verification packet SRREQ with a

random number (records as x) generated by a source node 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.

In solution [12] the source node stores all the RREPs in the table called Cmg_RREP_Tab until receiving first RREP packet waits for MOS_WAIT_TIME. Meanwhile, the source node analyses all the stored RREPs from Cmg_RREP_Tab table, and discard the RREPs having a very high destination sequence number. Every node in the network maintains a table called Mali_node for storing the malicious node details to isolate the malicious node in the network. Moreover, in order to maintain freshness, the Cmg_RREP_Tab is flushed once an RREP is chosen from it. However, this solution fails to detect co-operative black hole attack and it has high processing delay.

In [16] Yaser khamayseh et.al. proposed protocol and modifies the behavior of the original AODV by introducing a data structure referred as trust table at every node. This table is responsible for holding the addresses of the reliable nodes. The RREP is extended with an extra field called trust field. In order for a node to be added to the trust table of another node, it needs firstly to pass the behavioral analysis filter. Once the behavior of the broadcasting node is normal, it is added to the trust table of the receiving node. RREP is overloaded with an extra field to indicate 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. Upon the RREP is received by the source node, it decides whether to send the data or to wait for further route. In case the trust field value equals to 1 or 2, the source node sends, otherwise the source node waits for further route. Although the proposed method gives reliable routes but it consumes high network delay.

The proposed solution in [8] modifies the behavior of AODV to include a mechanism for checking the sequence number of the received RREP. As the source node receives the RREP it compares the sequence number of the received RREP to a threshold value. The replying node is suspected to be a black hole if its sequence number is greater than the threshold value. The source node adds the suspected node to its black list, and propagates a control message called an alarm to publicize the black list for its neighbors. The threshold is the computed average of the difference between the destination sequence number in the routing table and the destination sequence number in the RREP within certain periods of time. The main advantage of this protocol is that the source node announces the black hole to its neighbors in order to be ignored and eliminated.

The proposed architecture AODVR [14] has introduced several modules such as Packet Classifier, Extractor, Blacklist Tester, RREP sequence number Tester, Threshold Tester and ALARM broadcaster. As the packet arrives in the system, Packet Classifier classifies it to be RREQ, RREP secure, RERR, ALARM and HELLO packet. AODVR modifies the content and format of RREP and includes a new type of packet ALARM. Extractor extracts required contents of all types of packets other than HELLO. However, the procedure of formulating the threshold is a bit overwhelming, hence it results network delay. Formulations of correct threshold range keep black holes from intrude; while a wrong formulation may restrict an authentic node thereby disgrace it to be a black hole.

An algorithm presented in [21] to detect the black hole attack in a MANET based on the preprocessor called Pre_Process_RREP and it is simple and does not change workings of either intermediate or destination node. It does not even modify the working of normal AODV. 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 selects the packet with higher destination sequence number if the difference between two numbers is not significantly high. Packet containing exceptionally high destination sequence number is suspected to be a malicious node and an ALERT message containing the node identification is generated which is broadcasted to neighbor nodes so that it can be isolated from the network and can maintain a list of such malicious nodes. This solution has more network delay and cannot detect cooperative black hole nodes.

Lalit Himral et.al [20] have proposed method to find the secured routes and prevent the black hole nodes (malicious node) in the MANET by checking whether there is large difference between the sequence number of source node or intermediate node who has sent back first RREP or not. Generally, the first route reply will be from the malicious node with high destination sequence number, which is stored as the first entry in the RR-Table. Then compare the first destination sequence number with the source node sequence number, if there exists much more differences between them, surely it is from the malicious node, immediately remove that entry from the RR-Table. The proposed method cannot find multiple black hole nodes.

In paper [19] authors K. Lakshmi et.al. have proposed and discussed a feasible solution for the black hole attacks that can be implemented on the AODV protocol. In this solution, compare the first destination sequence number with the source node sequence number, if there exists much more differences between them, surely that node is the malicious node, immediately remove that entry from the RR-Table. Final process is selecting the next node id that have the higher destination sequence number, is obtained by sorting the RR-Table according to the DSEQ-NO column, whose packet is sent to Receive Reply method to continue the normal AODV process.

Herminder Singh et.al. [17] have discussed the AODV protocol suffering from black hole attack and proposed a feedback solution which comparatively decreases the amount of packet loss in the network. The black holes by examining the no of sent

packets at that node which will always be equal to zero for most of the cases. After the malicious black nodes have been detected, we can adopt a feedback method to avoid the receptance of incoming packets at these black holes. The packets coming at the immediate previous nodes to black nodes are propagated back to the sender and the sender follows an alternative safer route to the destination. However, it cannot detect black hole nodes when they worked as a group.

In [13] Kamarularifin Abd et.al. have designed an ERDA solution to improve AODV protocol with minimum modification to the existing route discovery mechanism recvReply() function. There are three new elements introduced in modified recvReply() function namely: table rrep_table to store incoming RREP packet parameter mali_list to keep the detected malicious nodes identity and parameter rt_upd to control the process of updating the routing table. When RREQ packet is sent out by the source node S to find a fresh route to the destination node D. RREP packet received by node S will be captured into rrep_tab table. Since the malicious node M is the first node to response, the routing table of node S is updated with RREP information from node M Since the value of parameter rt_upd is 'true', node S 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 node. ERDA method offers a simple solution by eliminating the false route entry and replaced the entry with later RREP. However, it cannot detect cooperative black hole attack.

The authors Sen, J et.al. have proposed mechanism [7] for defending against a cooperative black hole attack. This proposed mechanism modifies the AODV protocol by introducing two concepts, such as (a) data routing information (DRI) table and (b) cross checking. In the proposed scheme, the nodes that respond to the RREQ message of a source node during route discovery process send two bits of additional information. Each node maintains an additional DRI table. In the DRI table, the bit 1 stands for 'true' and the bit 0 stands for 'false'. The first bit 'From' stands for the information on routing data packet from the node (in the Node filed), while the second bit 'Through' stands for information on routing data packet through the node. In this mechanism source node (SN) broadcasts a RREQ message to discover a secure route to the destination node. The intermediate node (IN) replies with Next Hop and the DRI of Next Hop Node (NHN) to the source node. Upon receiving the replies from the IN, the source node checks its own DRI table for the reliability of the IN node. If it is present in the DRI table, SN starts sending the data packets through the IN node, otherwise SN sends FREQ to the NHN for the reliable IN. after receiving the DRI of its NHN and DRI of IN, the source node again checks its own DRI table for the reliable IN. If reliable IN presents, the source node (SN) starts sending data packets through that IN node. Otherwise, again source node sends a further request for the reliable intermediate node. However, this mechanism cannot detect black hole nodes completely that act as cooperatively.

All the above approaches can only check whether the route to the destination node is valid or not. But, they cannot check the quality of the route. In paper [6] described a solution to counter black hole attacks on the ETX metric acquisition process which is based on the quality of the routes between the source and the destination nodes. The solution is called the Secure ETX (SETX) protocol. The protocol, instead of allowing individual nodes to advertise their respective delivery ratios (as in ETX) it will, allows nodes to measure neighbors' delivery ratios directly. The algorithm makes use of the ETX metric value to find a detection threshold value (d_{thresh}). The main idea used in the design of the SETX protocol is to let a sending node to calculate both d_r and d_f values themselves, rather than relying their neighboring nodes to calculate the d_f value. To allow this, a sending node, called an initiator, I, generates and broadcasts probes to its neighboring nodes. Each of these probes contains a stream of random value. The neighboring nodes will need to return the probes received back to the initiator. The probes which are sent back to the initiator are called acknowledge probes. The initiator calculates the d_f value by working out the ratio between the number of authentic acknowledge probes (i.e. the probes that can pass the verification) received and the number of probes that were broadcast. In the SETX protocol, two types of buffers are introduced, an Advertised Probe Buffer (APB) and Received Probe Buffer (RPB). An APB is a probe buffer used to store probes that have been advertised, and a RPB is used to store the probes received from a given neighbour node. The size of APB and RPB are denoted as the PROBE_BUFFER_SIZE, and its default value is 10 probes to maintain only the latest probes in the buffers. The SETX protocol does not allow neighbors to send their respective d_f values to its initiator. Rather, the neighbors have to send back the initiator all the probes they receive from the initiator. These returned probes serves as the evidence of the quality of the link concerned. As the probes contain random numbers, if a neighbour node had not received a valid probe, it would be difficult for the node to forge one that could pass the verification in order to forge up the d_f value for the link. Therefore, we could say that, with the SETX protocol, it is difficult for a neighboring node to launch black hole attacks by fabricating the d_f value.

5. COMPARISON OF VARIOUS SOLUTIONS TO BLACK HOLE ATTACK

The various solutions to black hole attacks proposed by several authors are analyzed and made a comparison based on important parameters and depicted in Table3.

6. CONCLUSION

This paper has amalgamated various works related to black hole attack detection mechanism in AODV-based MANETs. The various authors have given several proposals for detection and prevention of black hole attacks in MANET but every proposal has its own disadvantages in their respected solutions and we made a comparison among the existed solutions. We observe that the mechanisms detects black hole node, but no one is reliable procedure since most of the solutions are having more time delay, much network overhead because of newly introduced packets and some mathematical calculations. For future work, to find an effective solution to the black hole attack on AODV protocol.

Table 3: Comparison of available solutions to black hole attacks on AODV

Technique proposed by	Techniques / Solutions	Introduced new packets (yes/no)	Modifies AODV/ Routing tables(yes /no)	Type of black hole attack	Drawbacks
Osathanunkul, K.; Ning Zhang; April 2011 [6].	Secured ETX metric (Expected Transmission Count)	yes	yes	Co- operative black holes	Time delay and overhead due to much calculations.
Sen, J.; Koilakonda, S.; Ukil, A.; 2011 [7].	Data Routing Information(DRI) table of Next hop node	yes	yes	Co-operative black holes	Maintenance of DRI tables apart from normal routing information.
Kamarularifin Abd. Jalil, Zaid Ahmad, Jamalul-Lail Ab Manan, 2011 [13].	Enhance Route Discovery for AODV(ERDA)	no	yes	Single black hole	Co operative black holes
Herminder Singh, Shweta, June 2011[17].	Feedback solution based on the no. of packets sent from the nodes	yes	no	Single black hole	always it doesn't works i.e. when congestion occurs
Lalit Himral, Vishal Vig, Nagesh Chand, May 2011 [20]	Checking SN's of source node and first route reply.	no	yes	Single black hole	Time delay, co-operative black hole nodes
Subash Chandra Mandhata, Dr.Surya Narayan Patro, 2011 [21].	Compares SN's of more than one RREP's at source node	yes	no	Single black hole	Cannot detect co-operative black hole nodes.
Mohammad Abu Obaida, Shahnewaz Ahmed Faisal, Md. Abu Horaira, Tanay Kumar Roy, 2011 [14]	Compares the RREP sequence numbers. with threshold value and selects the routes	yes	no	Single black hole	Cannot detect co-operative black hole nodes.
Payal N. Raj1 and Prashant B. Swadas2, 2008 [8].	Compares the RREP sequence numbers with threshold value using dynamic learning method	yes	no	Single black hole	Time delay, co-operative black hole nodes
N. Bhalaji, A. Shanmugam, 2011 [3].	Association based route selection based on the trust value	no	yes	Co operative black holes	Time delay
Yaser khamayseh, Abdulraheem Bader, Wail Mardini, and Muneer BaniYasein, April 2011 [16].	Behavioral analysis filters and trust values.	no	yes	Single black hole	Network overhead and time delay
Alem, Y.F.; Zhao Cheng Xuan; May 2010 [22].	Intrusion detection using anomaly detection (IDAD)	yes	no	Single black hole	Neighbor nodes may give false information
Ming-Yang Su; Kun-Lin Chiang; Wei-Cheng Liao, Sept. 2010 [25].	An Anti-Black hole Mechanism (ABM) using IDS	yes	yes	Multiple black holes	Time delay
Nital Mistry, Devesh C Jinwala, Mukesh Zaveri, 2010 [12].	Compare RREPs and discards the high destination seq- number RREP.	no	yes	Single black hole	Time delay
K. Lakshmi1, S.Manju Priya2 A.Jeevarathinam3 K.Rama4, K. Thilagam5, 2010 [19].	Using Prior_ReceiveReply method	no	yes	Single black hole	Time delay, Multiple Black hole nodes
Songbai Lu; Longxuan Li; Kwok-Yan Lam; Lingyan Jia, Dec. 2009 [10].	Using SRREQ and SRREP based on the random numbers generation	yes	no	Single black hole	Time delay, Network overhead
XiaoYang Zhang; Sekiya, Y.; Wakahara, Y., March 2009 [15].	IN node generates SREQ to the desti-nation for fresh SN.	yes	no	Single black hole	Time delay, multiple black holes.

Zhao Min; Zhou Jiliu, May 2009 [27].	Authentication mechanisms based on the hash function, MAC and the PRF	no	no	Co operative black hole	Low message authentication, may forge RREP with hash key of node
Medadian, M.; Mebadi, A.; Shahri, E., Dec 2009 [28].	Uses honesty of a nodes and opinions from neighbor nodes.	no	no	Co operative black holes	Opinions of neighbor's may not correct always
Latha Tamilselvan, V. Sankaranarayanan, May 2008 [9].	Fidelity table based on the acknowledgements received by the source node.	yes	yes	Co operative black holes	Time delay
Tamilselvan, L.; Sankaranarayanan, V., August 2007 [23]	Collect Route Reply Table' (CRRT)	yes	yes	Single black hole	Time delay
Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, Yoshiaki Nemoto, Nov. 2007 [26].	A new detection method based on dynamically updated training data.	no	no	Single black hole	Network delay
Al-Shurman, M., Yoo, S. and Park, S, 2004 [5].	Checks the shared hops from RREP's and maintains last packet sequence numbers that are sent and received	yes	yes	Single black hole	Time delay
Deng H., Li W. and Agrawal, D.P., October 2002 [11].	Further route request and reply to next hop node	yes	no	Single black hole	Routing overhead, Cannot prevent cooperative black holes.

7. REFERENCES

[1] Raja Mahmood, R.A.; Khan, A.I.; , "A survey on detecting black hole attack in AODV-based mobile ad hoc networks," High Capacity Optical Networks and Enabling Technologies, 2007. HONET 2007. International Symposium on , vol., no., pp.1-6, 18-20 Nov. 2007

[2] Hao Yang; Haiyun Luo; Fan Ye; Songwu Lu; Lixia Zhang; , "Security in mobile ad hoc networks: challenges and solutions," Wireless Communications, IEEE , vol.11, no.1, pp. 38- 47, Feb 2004.

[3] N. Bhalaji, A. Shanmugam, "A Trust Based Model to Mitigate Black Hole Attacks in DSR Based MANET", European Journal of Scientific Research, Vol.50 No.1, pp.6-15, 2011.

[4] H.A. Esmaili, M.R. Khalili Shoja, Hossein gharaee, "Performance Analysis of AODV under Black Hole Attack through Use of OPNET Simulator", World of Computer Science and Information Technology Journal (WCSIT), Vol. 1, No. 2, 49-52, 2011.

[5] Al-Shurman, M., Yoo, S. and Park, S, "Black hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference, pp. 96-97, 2004.

[6] Osathanunkul, K.; Ning Zhang; , "A countermeasure to black hole attacks in mobile ad hoc networks," Networking, Sensing and Control (ICNSC), 2011 IEEE International Conference on, vol., no., pp.508-513, 11-13 April 2011.

[7] Sen, J.; Koilakonda, S.; Ukil, A.; , "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks", Intelligent Systems, Modelling and Simulation (ISMS), 2011 Second International Conference on , vol., no., pp.338-343, 25-27 Jan. 2011.

[8] Payal N. Raj1 and Prashant B. Swadas2, "DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET", IJCSI International Journal of Computer Science Issues, Vol. 2, 2009.

[9] Latha Tamilselvan, V. Sankaranarayanan, "Prevention of Co-operative Black Hole Attack in MANET", Journal of Networks, Vol 3, No 5, 13-20, May 2008

[10] Songbai Lu; Longxuan Li; Kwok-Yan Lam; Lingyan Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack," Computational Intelligence and Security, 2009. CIS '09. International Conference on, vol.2, no., pp.421-425, 11-14 Dec. 2009.

[11] Deng H., Li W. and Agrawal, D.P., "Routing security in wireless ad hoc networks," Communications Magazine, IEEE, vol.40, no.10, pp. 70- 75, October 2002.

[12] Nital Mistry, Devesh C Jinwala, Mukesh Zaveri, "Improving AODV Protocol against Blackhole Attacks", proceedings of the International Multi Conference of Engineers and Computer Scientists 2010 Vol II, IMECS 2010.

[13] Kamarularifin Abd. Jalil, Zaid Ahmad, Jamalul-Lail Ab Manan, "Mitigation of Black Hole Attacks for AODV Routing Protocol", Society of Digital Information and Wireless Communications (SDIWC) Vol01_No02_30, 2011.

[14] Mohammad Abu Obaida, Shahnewaz Ahmed Faisal, Md. Abu Horaira, Tanay Kumar Roy, "AODV Robust (AODVR): An Analytic Approach to Shield Ad-hoc Networks from Black Holes" International Journal of Advanced Computer Sciences and Applications, Vol: 2 Issue: 8 Pages: 97-102, 2011.

[15] XiaoYang Zhang; Sekiya, Y.; Wakahara, Y., "Proposal of a method to detect black hole attack in MANET," Autonomous Decentralized Systems, 2009. ISADS '09. International Symposium on, vol., no., pp.1-6, 23-25 March 2009

[16] Yaser khamayseh, Abdulraheem Bader, Wail Mardini, and Muneer BaniYasein, "A New Protocol for Detecting Black Hole Nodes in Ad Hoc Networks", International Journal of Communication Networks and Information Security (IJCNIS) Vol. 3, No. 1, April 2011.

[17] Herminder Singh, Shweta "An approach for detection and removal of Black hole In MANETS" International Journal of Researh in IT& Management (IJRIM) Volume 1, Issue 2 (June, 2011).

[18] Praveen Joshi, "Security issues in routing protocols in MANETs at network layer", Procedia Computer Science 3 (2011) 954–960, World Conference on Information Technology 2010.

[19] K. Lakshmi1, S.Manju Priya2 A.Jeevarathinam3 K.Rama4, K. Thilagam5, "Modified AODV Protocol against Blackhole Attacks in MANET", International Journal of Engineering and Technology Vol.2 (6), 2010.

[20] Lalit Himral, Vishal Vig, Nagesh Chand, "Preventing AODV Routing Protocol from Black Hole Attack" International Journal of Engineering Science and Technology (IJEST) Vol. 3 No. 5 May 2011.

[21] Subash Chandra Mandhata, Dr.Surya Narayan 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-VI, 2011.

[22] Alem, Y.F.; Zhao Cheng Xuan; , "Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection," Future Computer and Communication (ICFCC), 2010 2nd International Conference on , vol.3, no., pp.V3-672-V3-676, 21-24 May 2010.

[23] Tamilselvan, L.; Sankaranarayanan, V., "Prevention of Blackhole Attack in MANET," Wireless Broadband and Ultra Wideband Communications, 2007. Aus Wireless 2007. The 2nd International Conference on, vol., no., pp.21, 27-30 Aug. 2007.

[24] Sheikh, R.; Singh Chande, M.; Kumar Mishra, D.;, "Security issues in MANET: A review," Wireless And Optical Communications Networks (WOCN), 2010 Seventh International Conference On , vol., no., pp.1-4, 6-8 Sept. 2010.

[25] Ming-Yang Su; Kun-Lin Chiang; Wei-Cheng Liao, "Mitigation of Black-Hole Nodes in Mobile Ad Hoc Networks," Parallel and Distributed Processing with Applications (ISPA), 2010 International Symposium on, vol., no., pp.162-167, 6-9 Sept. 2010.

[26] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, Yoshiaki Nemoto, "Detecting Black hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method" International Journal of Network Security, Vo l.5, No .3, P P.338–346, Nov. 2007.

[27] Zhao Min; Zhou Jiliu, "Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks", Information Engineering and Electronic Commerce, 2009. IEEC '09. International Symposium on, vol., no., pp.26-30, 16-17 May 2009.

[28] Medadian, M.; Mebadi, A.; Shahri, E., "Combat with Black Hole attack in AODV routing protocol", Communications (MICC), 2009 IEEE 9th Malaysia International Conference on, vol., no., pp.530-535, 15-17, Dec.2009.

[29] Perkins, C.E.; Royer, E.M.; "Ad-hoc on-demand distance vector routing," Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on , vol., no., pp.90-100, 25-26 Feb 1999.