EXPLORING RESEARCH AND INNOVATIONS

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 4, April 2014)

Comparing Various Black Hole Attack Prevention Mechanisms in MANETs

Rahul Agarwal[1], Kriti Arora[2], Rajiv Ranjan Singh[3]

[1]*Research Scholar, Mewar University*

[2,3]*Assistant Professor, Department of Computer Science, Shyam Lal College, University of Delhi*

***Abstract* -- Mobile Ad-hoc Network is a temporary wireless network. It is a network which is self-configuring in which nodes moves freely and continuously. As a result the network topology also changes dynamically. Such networks are highly dynamic in nature and nodes communicate without a proper infrastructure. Various routing protocols employed by these nodes have various loopholes and hence vulnerable to attacks. One such attack is a BLACK HOLE ATTACK. A black hole attack in MANET is a malicious node that falsely replies for any route requests without having any active route to specified destination and drops all the packets received from other nodes. This Results in the degradation in** overall **packed delivery ratio and network performance. There have been various attempts to provide schemes to prevent black hole attack. This paper presents a comparative study of the different preventive mechanism available to cater the problem of BLACK HOLE ATTACK in Mobile Adhoc networks. The paper has compared various schemes such as DRI table , MN-ID broadcasting, BHS-ODMRP – Certificate chaining, RRT Table and Intrusion detection using anomaly detection. The comparison has been performed on certain network parameters such as PDR, EED as well as Throughput. The paper concludes that almost all the Black hole detection schemes have some overheads that make them susceptible to attacks from skilled attacker who can bypass these protocols.**

***Keywords* -- Mobile Ad hoc networks, Routing protocol, Black hole attack, Prevention from Black hole attack**

I. INTRODUCTION

Wireless adhoc network is a self-configuring network made up of mobile nodes or stations which are not physically connected and have limited bandwidth and processing power. These adhoc wireless networks are also known as Mobile Adhoc Networks or MANET. An adhoc network does not have fixed infrastructure such as access points and routers to connect these networks and the network is managed by the nodes inside the networks. Each node must route traffic unrelated to its own use thus acting as a host as well as a router. These wireless networks have dynamic topology as the nodes are free to move independently in any direction. Any node can join the network at any time and any node inside the network can leave the network at any time.

Due to these qualities, these networks can be used in places where establishing other types of fixed networks is not possible. In such networks the transmission is done through wireless medium with mutual trust and co-operation. Nodes help each other by transmitting information by keeping each other updated with the network information. Each node acts as a host as well as a router and sends and receives all packets from one node to another within the network. The lack of infrastructure and the dependence of transmission on cooperation from other nodes makes these networks vulnerable to various attacks and threats.

Black hole attack is one such attack which can impact Mobile Adhoc Networks severely. In black hole attack one or more nodes are under attack, which create black holes in network i.e. nodes that accept packets from other nodes for forward delivery but drop these packets instead of delivering them further. A node which is under attack falsely present itself as a node providing the shortest path to deliver the packets to the destination but in reality it drops all the packets it receives. As a result the Packet Delivery Ratio (PDR) and network efficiency and performance drops. Various mechanisms and protocols have been designed to avoid and prevent these black hole attacks. In this paper, a comparative study is done to discuss and compare the various mechanisms and protocols employed to avoid and prevent the Black hole attack. A brief overview of various routing protocols used in Wireless adhoc networks is discussed in section 2 with special mention of AODV and DSR protocols. In section 3 various types of black hole attacks is discussed. Section 4 discusses various schemes for detecting and preventing black hole attacks followed by a comparative analysis of these schemes based on their effectiveness on various network delivery parameters, advantages and drawbacks in section 5.

II. TYPES OF ADHOC WIRELESS ROUTING PROTOCOLS

There are many different routing protocols available for routing in MANET. Routing protocols can be classified into three main categories based on how they gather information about the network or how to find a path between any two nodes.

A. *Proactive (table-driven) Routing Protocol*

The proactive routing also called table-driven routing protocol requires mobile nodes to periodically broadcast their routing information to their neighbors. Each node maintains their routing table which records the information of all the neighboring and reachable nodes in the network together with the number of hops. These routing tables having topology information of the network are exchanged regularly between the nodes to maintain up to date routing information. The disadvantage is that it leads to a relatively very high overhead on the network as these routing tables are exchanged between all the nodes. The advantage of this protocol is that if any malicious attacker joins the network, its status can be immediately reported to the entire network. Some examples of proactive routing protocol are destination sequenced distance vector (DSDV) routing protocol and optimized link state routing (OLSR) protocol.

B. Reactive (on-demand) Routing Protocol

The reactive routing or on demand routing protocol finds a routing path as demand arises by flooding route request packets to the entire network. Under this routing technique the packets contains the address of next hop and destination. Unlike the proactive routing, the reactive routing protocol does not transmit packets regularly but initiates or starts the process whenever any node desires to transmit data packets across the network. The advantage of reactive routing is that the extra bandwidth usage which arises from the cyclically broadcast of route request packets can be reduced. The one drawback of this protocol is that passive routing method can lead to some packet loss, adding to the excessive flooding that can choke the network. Some reactive protocols are Ad hoc On Demand Distance Vector (AODV) and Dynamic source routing (DSR) are discussed below.

C. AD-Hoc On Demand Distance Vector (AODV) routing protocol

In AODV protocol a routing table is maintained by every node which contains information about the routes to other destinations. When a source node needs to transfer data to a destination node, it first checks its own routing table to determine whether a route to the destination node is already available in its routing table. If an existing route is found to the destination, the source node can use that route to transmit packets to the destination. It is a reactive protocol means that when a node wishes to send data to another distant node in the network to which it has no route; AODV will initiate a route discovery process.

AODV uses three different types of control messages to find a route to the destination node in the network. Route Request Message (RREQ) is broadcast by the source node wishing to communicate with the destination to find the path for the destination. Each middle node that receives RREQ investigates its own routing table. If middle node has a connecting node to the intended destination in its routing table or is the intended destination itself, it generates a Route Reply Message (RREP) and sends it to the source node, otherwise it relays or forwards the RREQ packet by re-sending it to its neighboring nodes. This process of forwarding RREQ packet goes on until the packet reaches the destination node or any middle node that knows a new route towards destination node. The destination node of this middle node then finally creates the RREP message. The node sending the RREP packet updates the information in its own routing table about the number of steps required in reaching the destination node and then updates a sequence number field maintained as a time stamp for indicating latest activity. The RREP packet is sent inversely to the source node through the reverse route thus completing the communication path between source and destination.

During the path discovery process, if there is any link failure at any middle node, that node generates a Route Error Message (RERR) and sends it back to the source node through the reverse path. RERR message is sent when there is a break in the link which causes the destination node to become unreachable from the middle node.

D. Dynamic Source Routing (DSR) protocol [1]

Dynamic Source routing protocol or DSR works on two mechanisms - Route Discovery and Route Maintenance. These two mechanisms allow the protocol to discover and maintain routes to arbitrary nodes in the network. In this protocol, when the source node needs to send data to destination node it creates RREQ message, thus recognizing the source and destination nodes. If middle node does not know any route to the destination node in its routing table, then it places the destination information in package header and distributes it generally to all its neighbors. When this RREQ packet is received by a destination node or middle node that knows a route toward destination, an RREP message is created, and this node inversely sends the RREP packet back to the source node by using information from the packet header. Therefore, when message is finally received by the destination node, it involves information of destination nodes and all nodes in the path from source to destination and their sequences.

This method is efficient, but requires high volume of data to be stored in packet headers. When the length of route increases, and there are too many nodes in the path from the source to destination, the size of packages increases, because information of many nodes should be included in packages header. This imposes too much load on the network due to big packet headers, and high bandwidth is required to transmit these packets. On receiving the RREP RREP packet, the source node will include all details of destination route in data package header (DATA). Therefore, middle nodes can find out that which packet should be sent to which node by checking the packet headers. For this reason, this protocol is called dynamic source routing protocol. In case a node is not able to send a packet to next node, it creates RERR packet and returns it inversely back to the source node. In this way, it informs the source node about route disconnection, and the process of route discovery is re-initiated.

E. Hybrid Routing Protocol

Hybrid Routing is a third type of Adhoc Mobile network routing algorithm. The hybrid routing protocol makes use of the advantages of both the proactive routing method and reactive routing method to overcome the defects of both the protocols. It blends the technique of distance-vector routing method, in which each node shares its knowledge of the entire network with its neighbors only and link-state routing method in which every node shares the knowledge of their closest neighbors with every router on the network. Hybrid routing requires less processing power and memory as compared to link-state routing. In the beginning phase, proactive routing method is used to gather the unknown routing information, then the reactive routing method is used to update the routing information whenever there is a change in network topology. Some examples of the hybrid routing protocols are zone routing protocol (ZRP) and temporally-ordered routing algorithm (TORA), Enhanced Interior Gateway Routing Protocol (EIGRP), developed by Cisco, Optimized Link State Routing (OLSR).

III. Black Hole Attacks

In WAoN (Wireless Adhoc Network) nodes are constantly moving and the network itself is highly dynamic in nature. The existing node may leave and new nodes keep joining the network. To deliver the packet from the source to the destination the information of delivery path is required. For this each node is having information of its neighboring nodes. Before transmission route must be known and to get this, various routing protocols are used.

In Black hole attack one or more malicious nodes within the network become attack points by not behaving according to network rules. All network traffic gets redirected to these malicious nodes that actually drop the transmitted packets causing the packets to disappear. As the network packets disappear into these malicious nodes, they are called Black hole nodes analogous to the Black holes where all matter disappear in the universe. A Black hole node has two properties – first it attracts network traffic by advertising itself as having the shortest valid route to a destination node even though that route does not exist or is spurious, with the intention of misleading packets and second the black hole node will eventually drop or consume the packets causing packet loss from the network. There can be one or more such Black hole nodes in the network. When only one node is acts as a Black hole node it is known as Single Black hole attack. When more than one malicious nodes collaborate together to provide fabricated route information and misguide network traffic, the damage to network transmission can be very serious. This type of attack is called a Collaborative Black hole attack.

Types of Black hole attacks - Black hole attacks in AODV routing protocol can be classified into two categories based on the various messages generated by the malicious node: first is the RREQ Black hole attack and second is the RREP Black hole attack.

A. Black hole attack caused by RREQ [2][4]

In this attack the attacker sends fake RREQ messages to cause Black hole attack [2]. The attacker creates fake RREQ messages with non-existent node address and pretends to rebroadcast it further to the network. It sets the originator IP address and destination IP address in RREQ packet to the originating node’s IP address and destination node’s IP address respectively. It sets the source IP address to a non-existent IP address and increases the source sequence number in the packet by at least one or decreases the hop count by 1 making it look like a correct route request. Other nodes take input from this fake RREQ message and update their routing tables considering the non-existent node as a valid middle node to reach the destination node. The nonexistent node address misleads the packets thus causing breakdown of the normal route. The attacker forms a black hole attack between the source and destination node by faked RREQ message as shown in Figure 1 below.

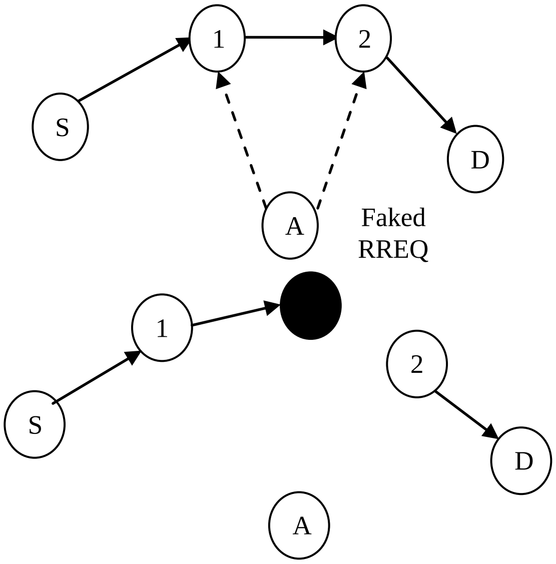

FIG 1. BLACK HOLE FORMED BY FAKED RREQ [2]

B. Black hole attack caused by RREP [2][4]

In this attack the attacker generates a fake RREP message to cause the Black hole attack. It creates a fake RREP message by setting the IP address of the originating node as the originator IP address and the IP address of the destination node as the destination IP address in the RREP packet. It sets the source IP address to a non-existent IP address (of a black hole) and increase the destination sequence number by 1 and set the hop count field to 1. Thus the originating node gets the impression that packets will be delivered to the destination in one more hop. On receiving the faked RREP message, the originating node updates its routing table entry to the destination node passing through the non-existent node getting the impression that the packet has been delivered but actually the packets have been dropped by the non-existent black hole nodes. The RREP Black hole attack is shown in Fig 2 below.

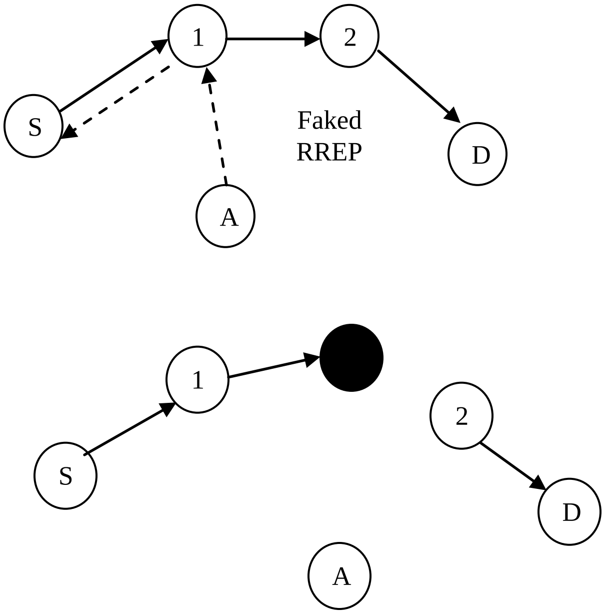

FIG 2. BLACK HOLE FORMED BY FAKED RREP [2]

IV. CURRENT BLACK HOLE DETECTION/PREVENTIVE MECHANISMS

Several mechanisms and schemes have been devised and employed to detect and prevent Black hole attacks in MANETs. These mechanisms have been devised to work with various routing protocols and use different types of schemes to prevent and detect Black hole attacks. Some of these schemes and methods have been studied and analyzed in this paper as given below.

A. Data Routing Information and Cross Checking[3][4][8]

This method suggested by H. Weerasinghe and H. Fu[8] and Sanjay Ramaswamy and H. Fu [9] requires each node to maintain a data routing information (DRI) table.

This table keeps a record of the data transfers done by a node with its neighbors. Each table entry contains information about one neighboring node and specifies if the node has transmitted data through this neighbor earlier or not and if the node has received data from this neighbor earlier or not. This table contains fields for node id, data transfer done from and through nodes as shown in Table 1. The from field contains information on routing data packets from the neighboring nodes (in the node id field) passed on to this node while the through field contains information on routing data packets through the neighboring nodes (in the node id field). The from and through fields take values 0 or 1 depending on whether any data transfer has been done from or through that neighboring node. For node 3 the from entry is 1 implying that this node has transmitted data packets earlier received from node 3 and the through entry is 0 implying that this node has not transmitted any data packet through node 3. Similarly for node 6, the from as well as through entry is 1 which means that this node has transmitted data packets successfully from and through neighboring node 6.

TABLE I.
EXAMPLE OF DRI TABLE [3]

Node Id	**Data Routing Information – From**	**Data Routing Information – Through**
3	1	0
6	1	1
2	0	0

This DRI table is updated with entries for all intermediate nodes in the path when any node receives data packet from any of its neighbors or any node sends data packets through one of its neighboring nodes. Initially, when the source node (SN) does not know the route to the destination node, it broadcasts a RREQ (Route Request) message to find out a secure route to the destination node. Any intermediate node that receives this RREQ either replies to this request if it has the route to the destination node or again broadcasts the RREQ message to its neighbors if it does not have route details for the destination node. If the intermediate node (IN) knows the route to the destination node it generates the Route Reply (RREP) packet, and provides its next hop node (NHN) i.e. the next node to which packets will be routed and the DRI table entry for the next hop node. On receiving RREP message from IN, the source node will confirm the reliability of IN by consulting its own DRI table. The IN is considered to be a reliable node if the source node has used it to route data earlier. If IN is found to be reliable, source node will again confirm that IN is not a black hole.

If the value in Through field of the DRI table entry from the Intermediate Node is equal to 1 (i.e. IN has routed data through the NHN), and the From field of the DRI table entry from the NHN is equal to 0 (ie. NHN has routed data from IN), that Intermediate node is a black hole. In this way DRI table is used to identify black hole nodes. If this condition is not satisfied then IN is not a black-hole and NHN is considered as a reliable node and the route is considered to be secure. Once RREP message is received and secured path is found, the source node will first send a message to establish the secured route to IN node following the route that RREP came through and then update its DRI table entry for IN node with 01, before it starts to send data packets through this route. If IN is found to be a black-hole, the source node marks all the nodes along the reverse path from IN to the node that generated the RREP as black hole nodes. Once marked as black holes, the source node will ignore any other RREP from these black hole nodes and broadcasts the list of black holes to all other nodes in the network.

Analysis – The DRI table and cross checking mechanism is able to handle most of the single as well as collaborative Black hole attacks. The process of cross checking the intermediate nodes is done only once. It can be minimized further by letting the nodes share their trusted nodes list (DRI table) with each other. The main drawback of this mechanism is the overhead of maintaining the extra DRI table is high for all the nodes. Another issue comes whenever the black hole node takes part in two or more transmission paths, it takes more time to discover the black hole node. Therefore the delay in performance is high and loss of packets can take place.

B. Broadcasting of MN-ID [4]

Antony Devassy & K. Jayanthi has proposed this solution. Under This solution, Malicious Node ID (MN-ID) broadcasting method is used to prevent Black hole attacks. This method is mostly used along with a reliable Black hole detection method. In this method, the malicious nodes are identified first using another black hole detection scheme, then the id of those malicious nodes is sent or broadcasted to the entire network. Therefore even if the malicious nodes take part in two or more routing paths, packets do not move towards malicious nodes because the entire network knows about the malicious nodes. Now the packets are routed through an alternative path (that does not include the black hole node) from the source node to the destination node instead of passing through the black hole node.

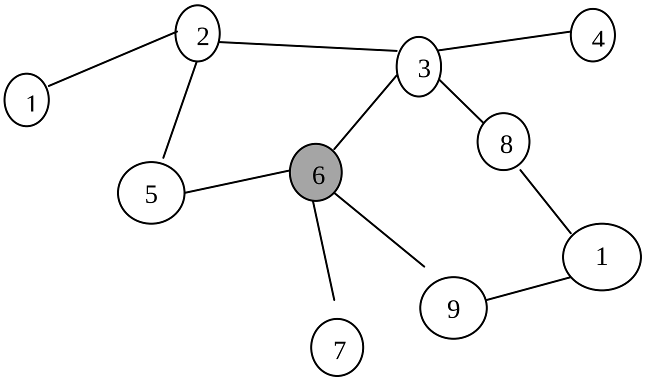

FIG 3. MN-ID BROADCASTING METHOD [4]

In Figure 3 node 1 is the source node, node 9 is the destination node and node 6 is represented as the black hole node. When the packet transmission takes place source 1 transmits packets to destination node 9. When node 1 tries to send packets to node 9 and the transmission reaches the black hole node 6 it drops all received packets. Now the protocol identifies node 6 as the black hole node and finds an alternative longer path to destination as 1-2-3-8-12-9. Now it transmits all its packets to node 9 through this long route rather than the short route 1-2-5-6-9. Hence the packet transmission takes place through the path 1-2-3-8-12-9 and reaches the proper destination node 9.

Analysis – The MN-ID broadcasting method is able to handle most of the single as well as cooperative Black hole attacks. For optimum performance it needs to be paired with any efficient Black hole detection method. It provides improved performance of throughput and packet delivery ratio when compared with DRI table method. The packet loss is very less as compared to DRI routing table method. Also the overhead for setting up the DRI table and cross checking is not there in this method making faster and easier to implement.

C. Preventing black hole using certificate chaining [5]

This solution of certificate chaining also called BHS-ODMRP is proposed by E.A.Mary Anita & V.Vasudevan.[5] for multicasting routing protocols. It provides a security mechanism for On Demand Multicast Routing ODMRP protocol by working along with the route discovery process of ODMRP. ODMRP is a mesh based routing protocol in which only a subset of nodes forward the multicast packets through shortest known routes between different node pairs to build a forwarding mesh network for each multicast group.

When a Multicast source needs to send packets in ODMRP, it initiates a route discovery process. It broadcasts a JOIN REQUEST packet periodically to the entire network. Intermediate nodes receive this JREQ packet and store the upstream node ID that forwarded this packet and rebroadcasts the packet forward. Passing through various intermediate nodes when finally this packet reaches the destination node, the destination node creates a JOIN REPLY (JREP) packet and sends the reply packet to its neighbors. All intermediate nodes receiving the JREP packet check if the next node id in reverse path of JREP match their own id. If a match is found, it knows that it forms a part of the forwarding mesh network, then it sets its flag and broadcasts its JREP forward through the path following the matched node id entries. This JREP packet is thus forwarded by each path group member to reach the source node via the shortest path. The route from sources to receivers thus built from tracing JREP’s path builds a mesh of nodes called forwarding group. A secure route is established in this way by the route establishment and route construction process, which can now be used by a multicast source to transmit packets to receivers via these selected routes and forwarding groups.

ODMRP does not have any provisions for providing security to the network, hence making it vulnerable to both internal and external attacks. Certificate chaining provides security mechanism for the ODMRP protocol. Certificate chaining employs a self-organized Public key infrastructure (PKI) authentication of nodes without the use of any trusted third party. Here authentication is verified through a set of digital certificates that form a chain. Any node on the network can issue certificates to any other node within its communication range. A certificate encapsulates a node, its public key and the security parameters together as one entity. Every node authenticates its neighbors, creates and issues certificates for its neighbors and maintains the details of certificates it has issued. The criteria for issuing certificates is based on the security parameters of the node. Certificates are provided to nodes by other nodes, but the nodes themselves store and distribute the certificates issued to them. Every node has a local repository to store certificates issued by this node to other neighboring nodes and it also stores the certificates issued by other nodes to this particular node. Hence each certificate is stored twice, once by the issuer issuing the certificate and secondly by the other nodes to whom the certificate is issued.

In this proposed solution BHS-ODMRP protocol is used where route discovery is followed by certification phase and authentication phase.

In certification phase there are three steps (i) key generation and certificate issuing, (ii) certificate update, (iii) certificate revocation. First a route is established between the source and destination. Once the route between the source and destination are established, the source node checks the authenticity of each node on the route by checking their certificates issued to them. In the first phase of certification it requests the identity and security parameters of the next hop node. If the issuer is convinced about the reliability of the next hop node from its security parameters, it generates a unique public key certificate based on its identity and security parameters.

The security parameters used to confirm if a given node is reliable and not a black hole are node id, location of the node and the time taken in processing the JREQ packet by the node. The malicious nodes reply immediately and delay in reply to JREQ packet is zero since these malicious nodes respond immediately with a JREP message without referring their routing table. The legitimate nodes would take some time in referring their routing tables and hence would have certain delay in sending the reply. The certificate contains the security parameters of the node and the public key of the node signed by the neighboring nodes through which it wants to route its packet. Every intermediate node in the route has to establish its identity and reliability and get a certificate from its neighboring node thus authenticating that it is a reliable node for routing. These certificates are issued in the certification phase and checked in the authentication phase. When a source node A wants to send packets to a destination node D, it has to find a chain of valid public key certificates for all nodes in the path leading to destination node D. The security level of each node is set to 1 initially implying that the issuer node is convinced of the reliability and security parameters of the routing node. But if some ambiguity or abnormality is found in security parameters, the security level parameter S is set to zero value. A node having a certificate with the value of security parameter set to zero is identified as a malicious black node and it is blacklisted in the repository of each node. The certificates are issued for a given time period and renewed from time to time based on the current security parameters. In some cases a reliable legitimate node may turn malicious over a period of time. In such cases the node's abnormal behavior and security parameters would be tracked and their certificate would not be renewed after it has expired, thus prohibiting the node from further participation in the transmitting data.

Analysis – Chained certificates mechanism or BHS-ODMRP is very effective in sustaining Single as well as collaborative Black hole attacks.

The BHS-ODMRP protocol reduces the packet loss caused due to black holes by about 20% which is quite higher compared to ODMRP protocol. This authentication mechanism removes the need for a centralized trusted authority which is difficult to maintain and implement in MANETs due to their self organizing nature. This black hole prevention method protects the network through a self organized, fully distributed and localized procedure. The main drawback of this method is the high overhead for generating Private keys, issuing certificates and authenticating certificates which requires extra resources, cost and implementation and can cause time delays.

D. Checking of sequence numbers

This solution is proposed by Pooja Jaiswal & Dr.Rakesh Kumar [6]. This method works for AODV and DSR protocols and is based on the sequence numbers stored on transmitted packets. It prevents Black hole attacks by checking whether there is large difference between the sequence number of source nodes and intermediate node that sent the RREP message. In this method, initially when the source node needs to send data to destination node it creates RREQ message, thus recognizing the source and destination nodes. When a RREQ message is broadcasted by a source node to find the route to the destination, other nodes respond by either sending the RREP message if they have a fresh route available to destination or they broadcast the RREQ message to further neighboring nodes if they do not know the route to the destination. When a RREP packet is received its sequence number is stored in a Route Request Table (RRT). All route replies received are stored in the RRT table together with the sequence number of nodes that sent them. The stored sequence number is checked with the first entry in the route request table because the malicious node will generally be the first to reply to the RREQ message as it does not check its lookup routing table before responding. When an intermediate node generates RREP packet, RRT table entry is checked for all neighboring nodes to find out what data is sent and what data is received from the neighboring nodes. If the sequence number of destination node is much greater than the sequence number of the first source node from the RRT table, then that node is marked as a malicious node and its entry is removed from RRT table. The contents of RRT table are sorted from time to time according to their destination sequence numbers (DSN).

Analysis – This mechanism achieves effective protection against Single black hole attacks by identifying the black hole nodes in initial stage itself without letting it harm the network.

The overhead for memory and time required for implementing this method is also low. One drawback in this solution is that a malicious node can play a role of SN collector in order to get the SN of as many other nodes as possible by broadcasting RREQs with high frequency to different nodes in a MANET so that this collector always keeps the freshest SN of other nodes. Another issue is of false alarms caused by highest DSN under normal circumstances.

E. Black hole Prevention using anomaly detection[7]

Also called Intrusion Detection using Anomaly Detection (IDAD) this solution is proposed by Yibeltal Fantahun Alem & Zhao Cheng Xuan. Intrusion detection is a process of detecting an adversary by checking information about all its network activities and identifying malicious nodes from this information. Intrusion Detection (ID) can be classified as Network-based and Host-based. Network-based ID can be installed on the point of network where data flow is high such as switches, routers etc. Whereas Host-based ID can be installed on host side so it can keep a check on the activities and of a host. This system assumes every activity of nodes or system can be monitored and deviating activities of a malicious node can be identified from other normal activities. Hence, by identifying anomalies or abnormal activities of an attacker node, it is possible to detect an intrusion and isolate the malicious node. For this IDAD needs a pre-collected set of data for normal and deviating activities, called audit data (AD). Once Audit data is collected and given to the IDAD system, the system then compares every activity of host with audit data. If any activity of a host (node) resembles the data for deviating activities listed in the audit data, the IDAD system isolates that particular node by denying further interaction. Generally the Black hole attack is employed by sending fake RREQ or RREP packets by the Black hole nodes. The various data entries on the RREP and RREQ packets can be monitored closely to differentiate anomaly activities from normal activities thus forming Audit data. This system works on a principle, trust no one. This means a node do not rely on other nodes to prevent intrusions. It only checks its network data to determine whether it's a malicious node.

Analysis – The IDAD method provides very efficient security against Single and collaborative Black hole attacks. To avoid false positive alarms of intrusion detection, this technique checks multiple anomaly conditions. Hence false alarms are very less. It also minimizes the number of extra routing packets generated as a result of communication between mobile nodes. The reduction in the number of routing packets in turn minimizes network overhead and facilitates a faster communication. It can achieve high PDRs in the range of 95% and more.

V. Comparison Of Various Black Hole Prevention/Detection Schemes

The comparative results for various Black hole prevention/detection schemes studied have been summarized in the Table 2A and Table 2B:–

TABLE II A
COMPARISON OF VARIOUS BLACK HOLE DETECTION/PREVENTION MECHANSMS

Prevention /Detection Scheme	Routing protocol	Black hole detection type	Effectiveness against attack
DRI table – Data Routing Information table	Unicasting protocols - AODV DSR	Single and collaborative	Moderately effective. Packet loss can happen.
MN-ID broadcasting	Unicasting protocols - AODV DSR	Single and collaborative	Highly effective. No packet loss once MN-ID is detected.
BHS-ODMRP - Certificate chaining	Multicasting protocol – ODMRP	Single and collaborative	Highly effective. Almost no packet loss
RRT table = checking sequence numbers	Unicasting protocol – AODV	Single only	Moderately effective
Intrusion detection using Anomaly detection	Unicasting protocols - AODV DSR	Single and collaborative	Highly effective. Can be further improved easily by the right choice of Audit data.

TABLE II B
COMPARISON OF VARIOUS BLACK HOLE DETECTION/PREVENTION MECHANSMS

Prevention /Detection Scheme	Improvement in Network parameters (PDR, EED, Throughput)	Ease of Implementation	Drawbacks/ Overheads
DRI table – Data Routing Information table	Considerable improvement in PDR, EED, Throughput	Difficult and time taking	Delay in identifying black hole can cause packet losses. Overhead of keeping DRI table by all nodes.
MN-ID broadcasting	Large improvement in PDR, EED, Throughput	Easy to implement	Need to be paired with an efficient Black hole Detection scheme
BHS-ODMRP - Certificate chaining	Large improvement (90% PDR) in PDR and throughput	Difficult as it involves Private key generation and authentication	Overhead in implementing Private keys, issuing and checking certificate makes it costly and difficult and causes delay of about 15%
RRT table = checking sequence numbers	Considerable improvement in PDR, EED, Throughput	Easy to implement	No overheads. Malicious node can act as source node and break security. Problem of False alarms in a big network.
Intrusion detection using Anomaly detection	Huge improvement in PDR (95%), EED and throughput	Easy to implement.	Overhead in keeping Audit data is small. No false alarms and no delays.

The various Black hole prevention/detection schemes mentioned above were studied, analyzed and compared for their behavior, effectiveness, ease of implementation, advantages and drawbacks to find out the most suitable Black hole prevention scheme under various situations. The various Network parameters used in evaluating performance are –

- **Packet Delivery Ratio(PDR)** - It is the ratio of the total number of data packets delivered to the destination node to the total number of data packets generated by the source nodes. This evaluates the ability of the protocol to deliver data packets to the destination in the presence of malicious nodes
- **End-to-End Delay(EED) -** This is the average time difference or delay between the time the packet is sent by the source node and the time the packet is received by the destination node. It means it is the difference between the receiving time and sending time of packets. This includes all possible delays caused by various steps in the routing process like data buffering, route discovery, packet queuing, packet processing at intermediate nodes, retransmission delays, propagation time, etc.
- **Throughput** - Throughput is the average rate of successful message delivery over a communication channel.

VI. CONCLUSION

Various techniques have been proposed and employed by researchers to detect and prevent Black hole attacks to work with various MANET protocols in varied network environments. Five such mechanisms for detection and prevention of Black holes have been studied, analyzed and compared on the basis of their effectiveness, performance on various network parameters, ease of implementations, advantages and drawbacks. Intrusion detection using Anomaly detection is the most suited Black hole prevention scheme for Unicasting networks. IT provides a very high degree of protection against Black hole attacks by identifying the malicious nodes in the initial stages itself. It is cost effective, easy to implement and can be further tuned for performance by the right choice of audit data. For multicasting networks Chaining certificates provide a reliable though expensive method for preventing Black hole attacks. Based on our analysis, we can safely conclude that all the Black hole detection schemes mentioned above have some overheads that make them susceptible to attacks from skilled attacker who can bypass these protocols.

REFERENCES

[1] Iman Zangeneh, Sedigheh Navaezadeh, Abolfazl Jafari (2013), Investigating the Effect of Black Hole Attack on AODV and DSR routing protocols in Wireless Ad Hoc network. Journal of Advances in Computer Research (Vol. 5, No. 1,)

[2] Sharma, S., & Gupta, R. (2009), Simulation study of black hole attack in the mobile ad hoc networks. Journal of Engineering Science and Technology, 4(2), 243-250.

[3] Tseng, F. H., Chou, L. D., & Chao, H. C. (2011), A survey of black hole attacks in wireless mobile ad hoc networks. Human-centric Computing and Information Sciences, 1(1), 1-16.

[4] Devassy, A., & Jayanthi, K., Prevention of Black Hole Attack in Mobile Ad-hoc Networks using MN-ID Broadcasting

[5] Anita, E. M., & Vasudevan, V. (2010), Black Hole Attack Prevention in Multicast Routing Protocols for Mobile Ad hoc networks using Certificate Chaining, International Journal of Computer Applications, 1(12), 21-2.

[6] Jaiswal, P., & Kumar, R. (2012), Prevention of Black Hole Attack in MANET, International Journal of Computer Networks and Wireless Communications (IJCNWC), 2(5).

[7] Alem, Y. F., & Xuan, Z. C. (2010, May), Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection, Future Computer and Communication (ICFCC), 2010 2nd International Conference on (Vol. 3, pp. V3-672). IEEE.

[8] H.Weerasinge and H.Fu(2008), Preventing Black Hole Attack in Mobile Ad hoc Networks: simulation, implimentation and evaluation, International Journal of software engg. and its applications,vol2,no3

[9] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks, 2003 International Conference on Wireless Networks (ICWN'03), Las Vegas, Nevada, USA