Study of Black Hole and Gray Hole Attacks in MANET

R.Saranya¹ and Dr.R.S.Rajesh²

¹,²Department of Computer Science & Engineering, Manonmaniam Sundaranar University, Tirunelveli-627012, India

Abstract
This article analyzes the trust parameters which are used for detecting the attacker node in Mobile Adhoc Network (MANET) based on simulation. MANET is vulnerable to various attacks due to a lack of central examining control. But this article only inspects the black holes and gray hole attacks in various scenarios. The Dynamic Routing Protocol (DSR) protocol is used for routing and simulation is performed with the Network Simulator 2 (NS2.34). The scenarios are formed by changing the number of nodes, the speed of the nodes and the flows number. In the entire scenarios, 5% of nodes are considered as the attacker node with every attack type. For analyzing the performance, the trust parameters like Packet Delivery Ratio, Delay, throughput, packet drop, control overhead, the packet generated, energy consumption and normalized routing overhead are taken. The experimental results provide a detailed analysis of MANET's performance with black holes and green hole attacks for various scenarios. Based on the analysis of attacks, black hole affects the network performance rather than the gray hole and also using these trust parameters, the attacker nodes in MANET are easily and effectively detected.

Keywords: NS2, MANET, Black Hole Attack, Gray Hole Attack, DSR, Trust Parameters, Attacker Node

1. INTRODUCTION
Dynamic Traffic Source Protocol (DSR) is an effortless and well-organized routing protocol which is developed particularly of a movable node in MANET. The DSR permits the network to be self-contained fully in a structured and organized way without the necessity for existing network infrastructure or administration. For that reason, this ad hoc network can be employed for military communications and disaster relief and further special circumstances.

The Ad Hoc Network is a multi-hop wireless network with an automated mobile node connecting each other through a wireless environment with no permanent infrastructure. This is a quick, easy-to-implement situation that cannot create a more streamlined fixed-line network used in other applications in a variety of key scenarios such as battlefields, emergency disaster relief, and conference. A mobile ad hoc network (MANET) can be characterized by the mobile node which has the freedom to move at any direction and has the ability of self-configuring, self-maintaining and self-organizing themselves within the network by means of radio links without any fixed infrastructure like the based station, fixed link, routers, and centralized servers. As in the network, there is no base station or central coordinator exists, so the individual node plays the responsibility as a router during the communication has to be played by each and every node, participating in the network communication. Hence all the nodes are incorporated with a routing mechanism in order to transmit a data packet from source to destination. Nodes are operated by a battery which is having limited capacity and they all suffer from severe battery consumption, especially when they participate in data communication for various sources and destinations.

MANET workgroup of IETF has been focusing on the research of routing protocol for Ad Hoc network, and many protocol draft plans were proposed, such as Dynamic Source Routing protocol (DSR) which is a kind of simple and efficient routing protocol designed for Ad Hoc network. This related high-performance algorithm behaves well in some highly mobile network.

The current mobile ad-hoc networks vulnerable to many different types of attacks. Although the analogous exploits also exist in wired networks but it is easy to fix by infrastructure in such a network. Current MANET's are mainly vulnerable to two different types of attacks. Black hole attack and Gray hole attack are one of them. Gray hole attacks have two stages. In the initial stage, malicious nodes use the AODV protocol to properly propagate to the target node, with the intention of intercepting packets, even though the route is spurious. In the second phase, the node drops the intercepted packets with a certain probability. This attack is more difficult to detect than the black hole attack where the malicious node drops the received data packets with certainty. A gray hole may exhibit its malicious behavior in different ways. It may drop packets coming from (or destined to) certain specific node(s) in the network while forwarding all the packets for other nodes. Another type of gray hole node may behave maliciously for some time duration by dropping packets but may switch to normal behavior later. A gray hole may also exhibit a behaviour which is a combination of the above two, thereby making its detection even more difficult.

Black Hole Attack is a DoS attack that the sender sends a Route Request (RERR) package to create a path when the malicious body responds to the sender using the Route Reply (RERP) message. The sender node allows it as genuine route and proceeds that route has been revealed in addition to it will disregard another RERP message which sent through original destination node, as well as sender node sends the packets via the malicious node. The malicious node then drops all the packets. In this paper examination of the Blackhole and Gray hole, the attack has been completed through NS2 simulator. The following section summarizes previous related work.
2. RELATED WORK

For security in MANETs, many routing protocols have been designed based on the DSR protocol in order to provide protection against the possible attacks. The secured routing protocols designed based on the DSR protocol are:

SRP [1], prevents spoofing attack and vulnerable to wormhole attack. Intermediary nodes are not authenticated and invisible node attacks. EndairA [2] was later proposed using TIK (TESLA with instant key disclosure) protocol. It prevents adversarial nodes from impersonation, forging, deleting any node from the node list carried by the RREP packets or even rendering them. In ARAN [3], the attacks of integrity and non-repudiation are mitigated using the public key cryptography scheme. The conclusion is that the protocol results in a route disruption, route diversion or creation of incorrect routing state and also vulnerable to the wormhole attack.

ADSR [4], this protocol employs elliptic curve cryptography to sign the route discovery packets. It also uses the aggregate signature scheme which allows us to connect M signatures of M different signers, in one single signature. Its drawback is that checking would have to be done in blocks. e-ARAN [5], e-ARAN was designed to detect and handle authenticated selfish nodes, based on reputed OCEAN scheme. Offers authentication, confidentiality, message integrity, and non-repudiation by utilizing certificate infrastructure. It protects the network against fabrication, modification, spoofing, and denial of service attack. Schemes used are currency based scheme and reputation based scheme. A Temporal table Authenticated Routing Protocol for Ad hoc networks [6]. In this, temporal table-based techniques are applied to the ARAN protocol to detect selfish nodes and improve the performance. ARAN- authenticated routing protocol is a secure protocol which provides security for attacks using modification, fabrication, impersonation and securing shortest paths [7]. BDADSR [8], a protocol that proposed a scheme that detects and avoids the black hole node in the network before the actual routing starts by using fake RREQ packets. The protocol is an extended version of DSR. The fake RREQ packets are sent before the routing process starts in order to identify the malicious nodes. This mechanism is performed before actual routing so that the network is protected against the damage due to the malicious nodes. In this, an acknowledgement scheme is also used, in which data packets are routed only after receiving the acknowledgement by the source node. This process of sending fake RREQ packets for finding the black hole node in the network is similar to the actual DSR RREQ packets. The only difference is that the destination address used is a fake i.e. invalid address which really does not exist and only lives for a certain time. When the source node receives a reply for this fake RREQ, it checks for the node that initiated this packet and records the address of that node in the list of malicious nodes. After that, a normal DSR routing process is started. The protocols given above provides authentication, integrity, some protection against the DoS (Denial Of Service) attacks, non-repudiation, some presented schemes to protect against wormhole attack like using TESLA scheme and secured message transmission scheme is also provided. There is also a protocol that protects against blackhole attack. But [9] introduces a new attack named deep blackhole attack that not only introduces fake RREP for the RREQ packets but also interrupts and modifies the valid RREP originated from the target node. The [9] is to provide a method to protect against deep black hole attack. S-PDSR [10] proposes enhancements in Preemptive DSR to provide secured route discovery. This protocol evaluates the integration of Secured Routing Protocol (SRP) and Secured Message Transmission (SMT) with Preemptive Dynamic Source Routing (PDSR) to get Secured PDSR (SPDSR), which is capable of secured route discovery. No security association is there in P-DSR. PDSR also needs a random id of traversed nodes in the route request packet. At the destination, it first verifies the authenticity of the packet, by calculating MAC. S-PDSR retains the basic functionality of PDSR and integrates the security aspects based on SRP. The secured route discovery of multiple routes is achieved in S- PDSR with minimum modifications in the methodology of PDSR and SRP.

Priya Jeego Payyappilly et al [11], proposed a new approach which is used to detection and prevention of collaborative black hole attack. A trust value is used to distinguishing the malicious node from the genuine node. At starting, each node act as equally and trusted. Trust is based on RREQ sent, RREP received and received data packets. Trust is decreased when RREP is received before a predefined time. To identify black hole node DSN (destination sequence number) is used. For prevention, malicious node removes from its routing table. Ravinder Kaur, et al [12] proposed a digital signature which is a verification technique to detect the malicious node in the network. The source node sends a route request to neighbor nodes in AODV. If destination node received that request then OK otherwise route request broadcast to next nodes until the destination is found. RREQ packet header contains information regarding visiting node (node-id) in node info column which also contains the number of visiting nodes used in the path. TTL scheme is used at the destination site. According to this scheme, the destination node selects the shortest path with less number of nodes. The destination node unicasts the reply whose header contains all information of visiting nodes or digital info column which contains the genuine digital signature of all nodes. Receiving node received data packets & verifies or compare with a digital signature from its database. If the signature is a match then that node is genuine otherwise considered as a malicious node. After detection of the malicious node, this information is broadcast to all the neighbors.” The process is repeated until the secure path is not found. Romina Sharma et al [13], proposed modifying the AODV protocol to prevent black hole attack. According to this, adding next hop information in the RREP message and two other control message including further route request and further route reply. The source node broadcasts RREQ. RREP will receive by a source with next hop information. After that, the source node sends further route request (FRREQ) to all next hop nodes. After receiving FRREP source node sends data packets to the destination with the shortest path. If next hop node is a black hole, FRREQ will not reach to next hop node & no FRREP will send to the source node. So source node not sends data packets to the path which is suggested by black hole node. Muhammad Sajjada et al. [14] proposed intrusion detection model based on
neighbor node trust estimation process to detect the malicious nodes from the network. Each node will estimate the trust value of its neighboring nodes by using both the direct and indirect trust estimation. Depending upon the measured trust value the nodes can be classified either as a trustworthy or malicious node. Moreover, the trustworthy nodes are updated the forwarding engine for the packet forwarding activity. The main advantages of their model are to detect the hello flood attack, jamming attack and selective forwarding attack by analyzing the malicious activity of the nodes and the network statistics.

Mohanapriya and Krishnamurthi in [16] presented a Modified Dynamic Source Routing Protocol (MDSR) to detect and prevent selective black hole attack. The source node selects the first shortest path to the destination, to intimate the no. of data packets it sends to the destination. The source node then selects the second shortest path for the actual transmission of data. Then packet count and transmitted data both are compared. If the difference is significant i.e. abnormality is detected the nearby IDS node broadcast a message informing all nodes to obscure all nodes from the network. In [17], a Routing Security Scheme based on Reputation Evaluation (RSSRE) is proposed. The reputation evaluation mechanism is built on the basis of correlation among nodes that need to be evaluated. It has the mechanism to promote the cooperation of cluster members for forwarding data packets to execute improved routing when there are malicious nodes in hierarchical Ad Hoc networks. In [18], authors proposed checkpoint-based Multi-hop Acknowledgement Scheme, for detecting selective forwarding attacks which can select the intermediate nodes randomly as checkpoint nodes which will generate acknowledgments for each packet received. Intermediate node has to send the acknowledgment for every packet that it is receiving; the algorithm has to suffer from overhead. Moreover, the channel is assumed perfect. Gao and Chen [19] proposed three security algorithms such as full proof algorithm, check-up algorithm, and diagnosis algorithm. The full proof algorithm was for creating a proof and the check-up algorithm was for checking up source route nodes, and the diagnosis algorithm was for locating the malicious nodes in the network. In approach [20], Jaisankar et al. presented that each node should have Blackhole Identification Table (BIT) that contains source, target, current node ID, Packet received count (PRC), Packet forwarded count (PFC). If the difference between PRC and PFC is significant, then the node is identified as malicious and is isolated from the network. In [21], Chavda and Nimavat proposed an algorithm to remove the black hole attack at the cost of overhead. The source node continues to accept RREP packets from the various nodes and compares RREP (RREP R1, RREP R2) which actually compares the destination hop count of two route replies and selects the route reply with high destination hop count if the difference between two hop counts is not significantly high. In [22] Wang et al. proposed an approach basis of cooperation between nodes to improve the scalability and efficiency of MANETs by arranging the nodes on the basis of the trust mechanism.

3. DYNAMIC SOURCE ROUTING PROTOCOL (DSR)

The dynamic source routing is the simple and efficient routing protocol. It follows the source routing technique. At this point, the sender of the packet decides the entire sequence of nodes by which the packet is forwarded. This route is listed in the packet header and each hop is identified by the address of the next node and the packet is transmitted to the destination host.

DSR is completely self-organizing and self-configuring and requires no existing network infrastructure. The DSR protocol allows to dynamically discover a source route across multiple network host to any destination in the network. Two mechanisms that make up the operations of DSR are Route Discovery and Route Maintenance. But before continuing some assumptions are made.

Assumptions made are

- All nodes wishing to communicate with other nodes within the ad-hoc network are willing to participate fully in the protocols of the network. In other words, nodes should be willing to forward packets to other nodes.
- The diameter of the ad-hoc network is the minimum number of hops traveled by a packet from any node located at one end to a node located at the other extreme end. Thus the diameter will often be small (e.g perhaps 5 to 10 nodes) but may often be greater than 1.
- The speed with which the nodes move is moderate with respect to the packet transmission latency. Nodes should not move continuously as to make every individual packet the only possible routing protocol.
- The nodes may be able to enable promiscuous receive mode on their wireless network interface hardware. The hardware should deliver each and every packet to the network driver software without filtering based on link layer destination address.

3.1 ROUTE DISCOVERY

Route discovery allows to dynamically discover a route to any other host in the ad hoc network. The source initiating a route discovery broadcasts a route request packet. The route request packet identifies the destination host, referred to as the target of the route discovery, for which the route is requested. If the route discovery is successful the initiating host receives a route reply packet. The packet contains a list of a sequence of network nodes through which it may reach the target. Each route request packet also contains a unique request id, set by the initiator from a locally-maintained sequence number. The original route request packet is received only by those hosts within wireless transmission range of the source host. Each host receiving the packets transfers the request if it is not the
When node S sends a message to the destination node D, it first queries about routing buffer in the route from S to D. Afterwards, the source node S sends a message according to the route. Otherwise, route discovery program is launched, meanwhile source node S floods route request packet RREQ, when intermediate nodes receive the RREQ message, and they test RREQ for the repetition of message. If repetition of the request message is found, they are abandoned, otherwise, attach their address to the route record in the head part of the packet, and then send this packet to all the neighbor nodes. When the last destination node finally receives RREQ packet, it copies and reverses the route record of the RREQ packet and sends the route reply message RREP to the source nodes, and returns route response message RREP to source node S. Source node buffers the route information locally for future use when receives the RREP packet, this process is shown on the Fig 1.

3.2 ROUTE MAINTENANCE

Route maintenance is carried out by continuously sending periodic routing updates. If the status of a link or router changes the changes will be reacted to all other routers,
presumably resulting in the computation of new routes. The route maintenance procedure monitors the operation of the route and informs the sender of any routing errors. Wireless networks are inherently less reliable than wired networks. Many wireless networks follow a hop-by-hop acknowledgment in order to provide early detection and retransmission of lost or corrupted packets. In these networks, route maintenance can be easily provided, since, at each hop, the host transmitting the packet for that hop can be determined if that hop of the route is still working. If a transmission problem is reported for which a node cannot recover this host sends a route error packet to the original sender of the packet encountering the error. The route error packet contains the addresses of the hosts at both ends of the hop in error: the host that detected the error and the host to which it was attempting to transmit the packet on this hop. On receiving the route error packet the node in error is removed from this hosts route cache, and all routes which contain this hop must be truncated at that point. The route maintenance flow diagram of DSR protocol is shown in Fig.2.

3.3 BLACK AND GRAY ATTACKS IN DSR

Black hole attacks breach the routing protocols through confusing the nodes for path information. The black hole node employs in the subsequent method: After receiving the RREQ and RREP messages, the attacker responds directly to the RREP message and assumes that this is the target node. The source node may get pseudo-RREP from the attacker prior to returning the real RREP. Beneath these conditions, the source node transmits the data packet to the black hole in place of the target node. When the source node delivers a packet of data via a black hole, an attacker abandons that packet without sending a RERR message. For gray holes, its behavior is alike to a black hole. The gray hole does not drop all the packets but only the part of the data packets. Gray degree is described as a percentage of randomly attacked packets. For instance, in gray holes, 60% of packets will be dropped with a chance of 60% and a standard black hole have 100% gray degree. Attacks on Black and Black Pit will cause serious damage to the Adhoc Network. The level of malicious drop value is determined proportionally between the total number of dropped packets and the total number of received packets. Particularly, the drop value of malicious in black holes is a hundred percentage.

4. EXPERIMENTAL EVALUATION

The proposed system is implemented using Network Simulator (NS2). NS2 is an event-impersonating tool for networking. There are two languages, C ++ and Otcl. At the back of C ++, which determine the internal mechanics of the experimental object, the front edge of Otcl creates a simulation by installing and configuring the object as well as organizing each event. At the end of each experiment, it creates two types of files: one is a tracing file (.tr) used for static analysis and the other is nam (.nam) used for animation.

In the simulation experiments, several parameters are used. They are listed in Table.1 given as follows.

<table>
<thead>
<tr>
<th>Table 1: Different Parameters Used In the Simulation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>No of Nodes</strong></td>
</tr>
<tr>
<td><strong>Area Size</strong></td>
</tr>
<tr>
<td><strong>Target Size</strong></td>
</tr>
<tr>
<td><strong>Simulation Duration</strong></td>
</tr>
<tr>
<td><strong>Speed of Nodes</strong></td>
</tr>
<tr>
<td><strong>Queue Size</strong></td>
</tr>
<tr>
<td><strong>Packet Size</strong></td>
</tr>
<tr>
<td><strong>Packet Interval</strong></td>
</tr>
<tr>
<td><strong>Communication Range</strong></td>
</tr>
<tr>
<td><strong>Buffer Size</strong></td>
</tr>
<tr>
<td><strong>Percentage of Attacker node</strong></td>
</tr>
</tbody>
</table>

The black and gray hole attacks have a severe impact on the performance of the wireless ad hoc networks. The trust parameters that credit the network performance are Delivery Ratio, Delay, throughput, packet drop, control overhead, the packet generated, energy consumption and normalized routing overhead. The black and gray hole attack can cause an adverse effect on these performance metrics. A brief discussion on the parameters is given below.

1. Packet Delivery Ratio

This is the ratio between the number of packets distributed to the target and the source sent by the source. \( \frac{\sum \text{Number of the packet received}}{\sum \text{Number of packet sends}} \). The packet delivery ratio decreases when there is a malicious node in the network because some of the packets are dropped by the black hole and gray hole node.

2. Delay

The average time is taken by a data packet to reach the destination node. It includes the delay in the pathfinding process and in the queue. The end to end delay decreases with black hole attack as the black node replies immediately without checking the routing table.

3. Packet Drop

It is the total number of packets dropped due to reasons like time expiration, collision, and congestion in the queue. The packet drop is very high when a black-hole node is present in the network as the black and gray hole node consumes the packets.
4. Throughput
Throughput is the amount of data transferred from source to destination in a given amount of time. It is measured in kbps. The throughput of the network decreases considerably due to the black and gray hole effect.

5. Control Overhead
It is the ratio of the control packets to the total number of the received data packets.

6. Normalized Routing
It is the average ratio of total routing control packets transmitted to the total data packets received at the destination. It should be lower for efficient network and it increases with black and gray hole attack.

7. Energy Consumption
It is the average energy used by the node in the network. It decreases with black hole attack because the packets transmitted between source and destination gets dropped which leads to less transmission between the nodes.

8. Generated Packet
A variety of packets are produced for the period of simulations of every scenario with dissimilar numbers of nodes. It can be seen that the number of the produced packet is straightly proportional to the number of mobile nodes.

5. EXPERIMENTAL RESULTS
5.1 Experiment No: 1 Analysis the Performance of Black Hole Attack

Variation in the Network Traffic
The effect of changing network traffic on performance parameters is investigated. The traffic is changed by changing the number of flows that have a total of 150 nodes in a motionless state. Links are fixed at 2, 3, 4 and 5. The evaluation metrics like Packet Delivery ratio, Packet Drop, Throughput and delay are examined for black hole attack and no attack condition. Black holes are also kept in motion. From the simulation, it is clear that the overall throughput and delay ratio increase with the number of streams, but decrease with the attack. Delay reduction with an attack when the black hole sends the highest target number without having to check the route to the destination. The packet drop boost with the attack. The results are depicted on the Fig.3 (a), (b), (c) & (d).

![Fig.3 (a). Variation of Network Parameters with Varying Traffic](image1)

![Fig.3 (b). Variation of Network Parameters with Varying Traffic](image2)

![Fig.3 (c). Variation of Network Parameters with Varying Traffic](image3)
Variation in the Network Size

The size of the network is changed by changing the number of nodes to 75, 100 and 150. All nodes are fixed and the connection number is fixed as 3. Experiments show that throughput, PDR and control overhead reduces the size of the network due to congestion and average delay diminishes with black hole attacks as black nodes forwards RREP without exploring the path. Normal network load has also increased with black hole attacks. The results are depicted in Fig.4 (a), (b), (c), (d) & (e).

Variation in the Mobility Speed

The simulations are carried out for different mobility speeds of the nodes. The speeds are fixed to 0 m/s, 5 m/s and 10 m/s. The number of nodes, pause time and flows are fixed to 150, 10s and 3 respectively. As the mobility varies the delay and
packet drop increases but the packet delivery ratio and throughput decrease as the nodes move randomly in all directions degrading the performance. The results are shown in Fig.5 (a), (b) and (c).

5.2 Experiment No: 2 Analysis the Performance of Black Hole and Gray Hole Attack

Generated Packet: Different packages are created during the test of each scenario with different numbers of nodes. It can be seen that the number of generated packages is proportional to the number of mobile nodes. When nodes are the minimum number of packages that have been created, then there is a minimum attack. When Number is the maximum number of packets created, it is also the maximum number. It can be seen that networks affected by gray hole attacks create more network packets affected by black attacks. Since the attack, black hole uploads all kinds of packages, it will create few packages. But attacks on gray holes have dropped only a specific package. In this way, black hole attacks affect the network work more than the gray hole attacks. Fig. 6 depicted the total number of packages created by all nodes during the experiment (10 seconds).

The Fig.6 depicted that the network which is exaggerated by Gray hole attack produced additional packets than the Blackhole affected network.

Drop Packet: Different packages are created during the test of each scenario with different numbers of nodes. Due to black hole attacks, it reduces all kinds of packets, it blocks traffic, networks, and various types of packets, including management packets and acknowledgment packets (from other nodes that forwarded packets by malicious node). In this way, the total number of network packets created by black hole attacks is smaller in the network affected by gray hole attacks. So the total number of dropped packets through the network that was affected by the black hole attacks, which is smaller than the network that suffered a gray hole. Fig 7 depicted the total number of dropped packets of all nodes during the experiment (10 seconds).
Fig. 7. Total Number Packets Drop in Both Types of Attack.

Fig. 7 depicted that amount of drop packets of the network which exaggerated through Gary hole attack is superior to the network which is exaggerated through Blackhole attack.

Throughput at sender side: The sender's throughput is defined as the rate of data transmission (bytes) of all nodes per unit of time. In this malicious nodal attack, the node omits all sorts of packets that pass through it. In other situation in the gray hole attack, the malicious node drops a particular packet type (this can be a control packet or a probabilistic nature packet of data), so less number of packet goes through the malicious node. So, the total breakdown of communication in a black hole, but in gray holes, partial communication breakdown occurs (due to the dropping of a particular type of probabilistic nature packets). Thus, the throughput of the network affected by the "black hole" attacks, is less than the throughput of the network affected by the black hole attacks. Fig 8 depicted the sender's throughput through the system execution time (10 seconds).

Fig. 8. Throughput in Sender Side in Both Type of Attack

Fig. 8 depicted the assessment of Throughput at the sender side inside the network exaggerated by two types of attacks. In the Fig.8, it is proved that the throughput of sender side of the network affected by Gray hole attack is superior to the throughput of the sender of the network affected by the Blackhole attack.

Average End to End Delay: When the attack comes on a black hole, when the package reaches the malicious node, it dropped the packet immediately, without deciding the packet launches the other hand, when it reaches the malicious nodes at that moment, may drop these packets or forward because of gray hole attacks fits in the manner of dropping of a particular type of packet in a probabilistic manner. So average end-to-end delay of the network affected by this black hole is less than a black hole. Fig.9 depicted the average end-to-end delay of the various experiments of the two attacks.

Fig.9. Average End to End Delay in Both Type of Attack

From the above Fig.9, it is proved that the average end to end delay in Gray hole attack is superior to Blackhole attack. Merely when the node number is 60 at that time average end to end delay of Black hole attack is slightly superior to Gray hole attack. It is able to be occurred because of other parameters, similar to the mobility of the nodes.

6. CONCLUSION

In this paper simulation based trust parameter analysis of attack has been performed in Mobile Adhoc Network. In all the scenarios simulated and studied, it is noticed, with the black hole attack the network parameter degrades. With the increase in network traffic, throughput and PDR increases and packet drop decreases under no attack condition. It is also observed that when the attacker is near the source the impact is severe than it is farther. Similarly, as the number of black and gray hole increases, PDR and throughput decrease. In all the simulations the proximity of attacker to the sending node has an impact on the average delay and it decreases with black and gray hole attack. This is due to the fact that the black hole sends the RREP with highest destination sequence number without verifying for a route in its routing table. Finally, it is concluded that these trust parameters are definitely produced high performance in the attacker nodes detection.
REFERENCES

[1] [Huabing Yang, Xingyuan Zhang, and Yuanyuan Wang “A Correctness Proof of the SRP Protocol” 1L-4244-0054-6/06/$20.00 ©2006 IEEE.


