ISSN 2277-3061

Detection and Prevention of Gray Hole and Black Hole Attack in MANET

Deepali Raut [1], Kapil Hande [2]
[1] PG student, Department of Computer Science & Engineering, PBCE, RTMNU, Nagpur
[2]Assistant Professor, Department of Computer Science & Engineering, PBCE, RTMNU, Nagpur

ABSTRACT

An Ad hoc network is the network with no fixed infrastructure. There is no central administrator so any node can come and move in and outside of the network in a dynamic manner. This makes it more dynamic and complex which makes it more prone to attacks. They can attack either active or passive. Some effects of malicious nodes are Denial of service, Routing table overflow, Impersonation, Energy consumption, Information disclosure etc. A black hole attack node attracts all packets by falsely claiming a fresh route to the destination node and absorbs them without forwarding them to destination. In this work the effect of Black hole and Gray Hole attack on DSR protocol has been considered. Simulation has been performed on the basis of performance parameters and effect has been analyzed using NS2 simulator.

Indexing terms/Keywords

DSR Protocol, Black Hole, Gray Hole Attack,False Positive Rate, MANET.

Council for Innovative Research
Peer Review Research Publishing System
Journal: INTERNATION JOURNAL OF COMPUTERS AND TECHNOLOGY
Vol. 13, No. 9
editorijctonline@gmail.com
www.ijctonline.com, www.cirworld.com

ISSN 2277-3061

I. INTRODUCTION

Wireless ad-hoc networks are composed of autonomous nodes that are self- managed without any infrastructure. They usually have a dynamic topology such that nodes can easily join or leave the network at any time and they move around freely which gives them the name Mobile Ad hoc Networks or MANETs. They have many potential applications, especially in military and rescue operations such as connecting soldiers in the battle or establishing a temporary network in place of one which collapsed after a disaster like an earthquake. In these networks, besides acting as a host, each node also acts as a router and forwards packets to the correct node in the network once a route is established. To support this connectivity nodes use routing protocols such as AODV (Ad- hoc On-Demand Distance Vector) or DSR (Dynamic Source Routing). Wireless ad-hoc networks are usually susceptible to different security threats and black hole attack is one of these. In this type of attack, a malicious node which absorbs and drops all data packets makes use of the vulnerabilities of the on demand route discovery protocols, such as DSR. In the route discovery process of DSR protocol, intermediate nodes are responsible to forward the packets through a fresh path to the destination, sending discovery packets to the neighbour nodes. Malicious nodes abuse this process and they immediately respond to the source node with false information as though they have a fresh enough path to the destination. Therefore source node sends its data packets via this malicious node assuming it is a true path. Black hole behaviour may also be due to a damaged node dropping packets unintentionally [1]. In any case, the end result of the presence of a black hole in the network is lost packets.

In this study, black hole and gray hole attacks are simulated in wireless adhoc networks and evaluated their effects on the network performance are evaluated. This paper, propose a new approach to detect black hole and gray hole attacks by modifying the detecting threshold according to the network's overload. The simulation is made using ns-2 (Network Simulator version 2). Having implemented a new routing protocol which simulates the black hole and gray hole behaviour in ns-2, different tests are performed to compare the network performance with and without black hole and Gray hole in the network. As expected, the throughput in the network deteriorated considerably in the presence of a black hole or gray hole. Also the proposed a solution based on ignoring the established route to reduce the adverse effects of the black hole node in an ad-hoc network using DSR as a routing protocol.

The remainder of this paper is organized as follows:Section II explain black hole and gray hole attack Section III presents DSR protocol working. Section IV presents the related researches. In Section V, black hole and gray hole detection and prevention algorithm over DSR protocol is presented. In Section VI, simulation results are discussed followed by conclusion.

II. BLACK AND GRAY HOLE ATTACK

The Black Hole attack is a powerful attack in MANET. In this Malicious Node attract all traffic by claiming the route to the destination which then absorbs the packets without forwarding them to the destination. Co-operative Black hole means the malicious nodes act in a group. The attacker injects falsified routing packets to attract traffic. The attacker intercepts or drops control as well as data packets to deny services to authentic nodes. This attack can be prevented by establishing routes free of such nodes or by removing them from existing routes [8]. In the following illustrated fig. 1, imagine a malicious node M. When node A broadcasts a RREQ packet; nodes B, D and M receive it. Node M, being a malicious node, does not check up with its routing table for the requested route to node E. Hence, it immediately sends back a RREP packet, claiming a route to the destination. Node A receives the RREP from M ahead of the RREP from B and D.

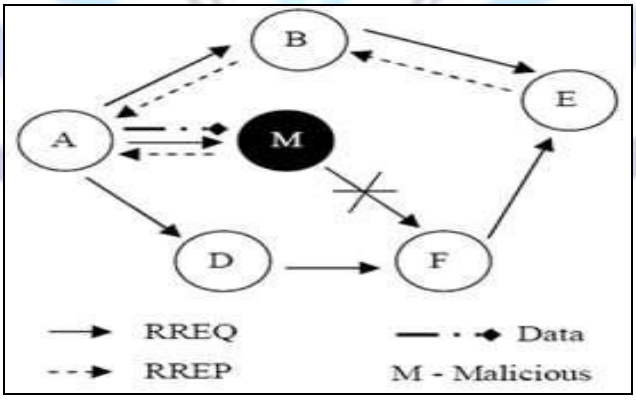

Figure 1: Black hole Attack

Node A assumes that the route through M is the shortest route and sends any packet to the destination through it. When the node A sends data to M, it absorbs all the data and thus behaves like a Black hole. Researchers have proposed solutions to identify a single black hole node. However in that solution next-hop also behaves as a malicious node they cannot identify it.

As for gray hole, its activities are similar to a black hole. A gray hole does not drop all data packets but just part of packets. The Gray Magnitude is defined as the percentage of the packets which are maliciously dropped by an attacker. For example, a gray hole is gray magnitude of 60% will drop a data packet with a probability of 60% and a classical black hole has a gray magnitude of 100%. The black and gray hole attack will bring great damage to the performance of MANETs.

III. DSR PROTOCOL

The Dynamic Source Routing Protocol is a source-routed on-demand routing protocol[15]. A node maintains route caches containing the source routes that it is aware of. The node updates entries in the route cache as and when it learns about new routes.DSR does not rely on functions like periodic routing advertisement, link status sensing or neighbour detection packets and because of the entirely on demand behavior, the number of overhead packets caused by DSR scales down to zero. Route Discovery and Route Maintenance, which are the main mechanisms of the DSR protocol, allows the discovery and maintenance of source routes in the ad hoc network's works entirely on an on-demand basis. As DSR works entirely on demand and as nodes begin to move continuously, the Routing packet overhead automatically scales to only that needed to react to changes in the route currently in use. In response to a single Route Discovery if a node learns and caches multiple routes to a destination, it can try another route if the one it uses fails. The overhead incurred by performing a new Route Discovery can be avoided when the caching of multiple routes to a destination occurs. and Mobile IP routing and supports internetworking between different types of wireless networks.

DSR Route Discovery

The header of the packet, which originates from a source node S to a destination node D, contains the source route, which gives the sequence of hops that the packet should traverse. A suitable source route is found normally when searching the Route Cache of routes obtained previously but if no route is found then the Route Discovery protocol is initiated to find a new route to D. Here S is the initiator and D the target. Node A transmits a ROUTE REQUEST message, which is received by all the nodes in the transmission range of A.

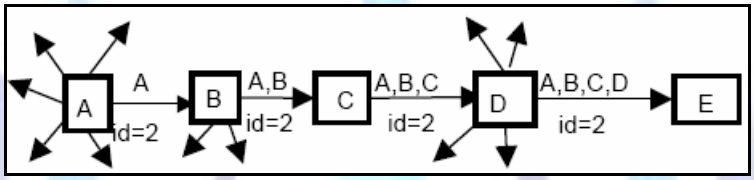

Figure 2: Node A is the initiator and Node E is the target

Each ROUTE REQUEST message identifies the initiator and target of the Route Discovery and also contains a unique request ID, determined by the initiator of the REQUEST. Each ROUTE REQUEST also contains a record listing the address of each intermediate node through which this particular copy of the ROUTE REQUEST message has been forwarded. The initiator of the Route Discovery initializes the route record to an empty list. [15] When the target node receives the ROUTE REQUEST message, it returns a ROUTE REPLY message to the ROUTE Discovery initiator with a copy of the accumulated route record from the ROUTE REQUEST. This route is cached in the Route Cache when the initiator receives the ROUTE REPLY and is used in sending subsequent packets to this destination. When the target node finds a ROUTE REQUEST message from the same initiator bearing the same request ID or if it finds its own address is already listed in the route record of the ROUTE REQUEST message, it discards the REQUEST. If the target node does not find the ROUTE REQUEST message from the initiator, then it appends its address to the route record in the ROUTE REQUEST message and propagates it by transmitting it as a local broadcast packet. When Route Discovery is buffer called Send Buffer. The Send Buffer contains copies of each packet that cannot be transmitted by the sending node. The packets are kept until a source route is available or a timeout or Send Buffer overflow occurs. As long as a packet is in the Send Buffer, the node should initiate new Route Discovery until time out occurs or overflow of Buffer occurs. An exponential Back off algorithm is designed to limit the rate at which new ROUTE Discoveries may be initiated by any node for the same target.

DSR Route Maintenance

When a packet with a source route is forwarded, each node in the source route makes sure that the packet has been received by the next hop in the source route. The confirmation of receipt will be received only by re-transmitting the packet for a number of times[15]. Node A is the originator of a packet to the desired destination E. The packet has a source route through intermediate nodes B, C and D. Node A is responsible for receipt of the packet at B, node B at C, node C at D and node D at E.

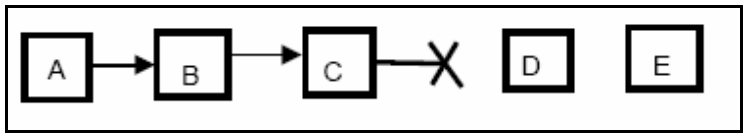

Figure 3: Node C is unable to forward a packet from A to E over the next

Node D Node B confirms receipt of packet at C by overhearing C transmit the packet to forward it to D. The confirmation of acknowledgement is done by passive acknowledgements or as link-layer mechanisms such as option in MAC protocol. The node receiving the packet can return a DSR specific software acknowledgement if neither of the acknowledgements is available. This is done by setting up a bit in the packet's header and then requesting a DSR specific software acknowledgement by the node transmitting the packet. When a node is unable to deliver a packet to the next node then the node sends a ROUTE ERROR message to the original sender of the packet. The broken link is then removed from the cache by the originator of the packet and retransmissions to the same destination are done by upper layer protocols like TCP[15].

Route maintenance is also carried out also by both ROUT E REQUEST and ROUTE REPLY packets, when they traverse form each node the data from the option header of these packets which contain the link information of the nodes are updated in the nodes route cache**.**

IV. RELATED WORK

Following are the black hole and gray hole attack detection techniques:

Neighborhood-based Technique:

In neighborhood based technique once the normal path discovery process is finished, the source node sends a special control packet to request the destination to send its current neighbor set. The neighbor set of a node is defined as all of the nodes that are within the node's radio transmission range[1]. They claim this metric provides a good "identity" of a node, that is if the two neighbor sets received at the same time are different enough, it can be concluded that they are generated by two different nodes. They verified their claim through the following two experiments:

- They measured the neighbor set difference of one node at different time instants *t* and *t*+1 seconds under different moving speeds and network sizes. The result shows that there is not much change of a node's neighbor set during a route discovery process.
- They examined the neighbor set difference of two different nodes at the same time, that is (({A's neighbor set} U {B's neighbor set}) – ({A's neighbor set} ∩ {B's neighbor set})). The result shows that the probability that node A's neighbor set is the same as that of node B is very small.

Detection: After source node receives the neighbor set information, it analyses them by measuring the neighbor set difference. If the difference is larger than the predefined threshold values, the source node knows that current network has black hole attacks and responds to it accordingly.

Response: They proposed a routing recovery protocol, with the following two-step approach:

- When a black hole attack is identified, the source node uses a cryptography-based method to authenticate the destination,
- once verified, the source node sends a control packet to destination node to form a correct path by modifying the routing entries of the intermediate nodes between them.

Reputation based Technique :

CONFIDANT [9](Cooperative of Nodes, Fairness In Dynamic Ad-hoc Networks) is an extended version of Watchdog and Path rater. It is also implemented on unicast routing protocol such as DSR. Each node monitors the behavior of its next-hop neighbors. If a suspicious event is detected, the information is given to the reputation system. If the event is significant for the node, it is checked whether it has occurred more often than a predefined threshold, which is high enough to distinguish deliberate malicious behavior from simple coincidences such as collisions. If the occurrence threshold is exceeded, the reputation system updates the rating of the node that caused the event. If the rating turns out to be intolerable, the information is relayed to the path manager, which proceeds to delete all routes containing the intolerable node from the path cache. The node continues to monitor the neighborhood, and an ALARM message is sent by the trust manager component. This message contains the type of protocol violation, the number of occurrences observed, whether the message was self-originated by the sender, the address of the reporting node, the address of the observed node, and the destination address. When the monitor component of a node receives such an ALARM message, it passes it on to the trust manager, where the source of the message is evaluated and the report is forwarded to the reputation system. Reputation system shares this information with all nodes present in network. CONFIDANT is suitable for small networks with low mobility; however it might be less efficient for large networks since each node needs to maintain a huge table for reputation purposes. Likewise, the high mobility of nodes increases significantly the communication overhead. Additionally, this protocol inherits all the problems of passive-feedback based schemes since it uses this mechanism for the monitoring function.

Digital Certificate based Technique:

In Digital Certificate based Technique the nodes authenticate each other by issuing security certificate in digital form to all the other nodes in the network[18]. It uses the route discovery scheme of DSR to issue security certificates. Every node participating in certificate chaining must be able to authenticate its neighbors, create and issue certificate for neighbors and maintain the set of certificates it has issued. The issue of certificates can be on the basis of security parameters of the node. Each node has a local repository consisting of certificates issued by the node to other nodes and certificates issued by others to the particular node. Therefore each certificate is stored twice. The extended route discovery process of DSR consists of the original route discovery process followed by an authentication phase. To overcome black hole attack, source node does not initiate the data transfer process immediately after the routes are established. Instead it waits for the authenticated reply from the destination. The destination node sends authenticated messages appended with certificates taken from the corresponding node's repository. Since the security levels of participating nodes are updated based on their faithful participation in the network, any malicious nodes between the source and destination can be very well isolated from the network as these nodes would not be able to produce the certificates to be appended with the RREP message.

Hybrid Routing Technique :

Hybrid routing approach is designed to prevent the collaborative black hole attacks. The proposed mechanism is composed of proactive and reactive method to form a hybrid routing protocol, and the major essence is the DSR on-demand routing. This solution is briefly introduced as below. In the beginning of routing stage, the source node sends bait RREQ packet before starting route discovery. The target address of bait RREQ is random and nonexistent. To avoid the bait RREQ inducing the traffic jam problem, BDSR use the same method with DSR[20]. That is all bait RREQ packets only survive for a period time. The malicious nodes are easily expelled from the initial phase, because the bait RREQ is able to attract the forged RREP from black hole node. In authors' mechanism, the generator of RREP is recorded in the RREP's additional field. Therefore the source node can recognize the location of attacker from the reply location of RREP. Compare with the primitive DSR scheme and watch dog method, the simulation results show that BDSR provides an excellent packet delivery rate. The packet delivery ratio of BDSR is 90% which is more superior to DSR and WD approach. Moreover, the communication overhead is also lower than watch dog scheme but slightly higher than original DSR routing protocol.

V. MODIFIED DSR ALGORITHM

The algorithm is based on a course based scheme. That is, a node does not observe every node in the neighbour, but only observes the next hop in current route path. For example, in Figure 4, S is the source node; D is the destination node; and P is a gray hole. Node S is sending data packets to node D through the course S, P, Q, D. In this system, Node S only watches Node P, which is the next hop; but does not care Node 1 and Node 2.

The algorithm is represented for finding the intentional selective dropping attack by a node and if all the packets are dropped will identify the attack as a black hole attack by checking the forwarding of packets by the immediate neighbor downstream node to which the data is sent.

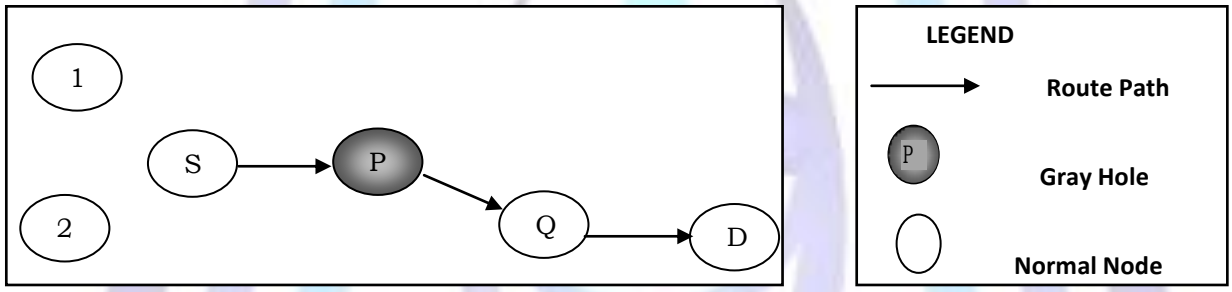

Figure 4: A course based detection scheme

In the algorithm at each node, the router will maintain a packet count history of the number of packets it has forwarded to the downstream node and also the number of packets it has overheard for the forwarded packets.

The algorithm is divided into three steps:

i) When a router forwards a packet to the downstream node, the number of packet sent is incremented and also buffers the packet for a certain time period. Then it overhears the packet which is forwarded by the downstream node and compares with the packet in the buffer.

ii) When a match is found the number of packets forwarded by downstream node is increased. Once the match is found or if the time period is over the packet is deleted from the buffer.

iii) If the packet forwarding is not heard within the time period the algorithm assumes that the packet is dropped by the downstream node.

If the overhear rate of next hop is less than threshold value (TH) then the node is considered as Black Hole. After applying detection algorithm the performance of the network is further improved by applying dynamic threshold method. The node at which the attack is detected keeps the track of Black hole detection time. If Detection Time is less than Expected Time then threshold values are updated. Due to dynamic threshold values the performance of network increases.

Proposed algorithm isolates the black hole or gray hole node from path construction phase. To prevent Black hole node, the detecting node reroute the packet to another available path till no black hole or gray hole node is detected in path. DSR protocol sends the route Request for the packet and starts the route discovery process again.

The overall detection and removal algorithm is represented with the help of following pseudo code:

Start

1. Deploy mobile adhoc network with finite number of mobile nodes
2. The source flood route request packets in the network
3. Source get various route reply packets
4. At each node,

   If (overhear rate of next node < threshold value)

   { That node will be detected as BH node or GH node }

   Else

   { Source assume that no attack node exist in the network }
5. If (BH or GH nodes == exists)

   { Source will not select the path in which BH or GH node exists }
6. Secure path is selected between source and destination

   For any node,

   If (Attack Detection Time < Expected Time)

   { Update threshold values and reroute the packet }

   End

VI. ANALYSIS OF SIMULATION RESULTS

The simulation has been carried out using NS-2.34. In ns2, two languages are used, tcl-tool command language as front end and c++ as back end .The user writes in tcl script, are interpreted by network simulator and give two output files. They are NAM and tr files.NAM is for visual animation of output and tr is the large text trace file consists of simulation Results. In this simulation 25 mobile nodes are considered in the terrain area of 1186 x 584 meters. Simulation parameters are considered as shown in the Table.1

TABLE 1: SIMULATION PARAMETERS

Parameters	Values
Examined Protocol	DSR
Topology size	1186 X 584 m
Simulation time	100 seconds
Number of Nodes	25
Transmission Range	1.5 m
Movement Model	Random way point
Traffic Type	CBR(UDP)
Payload size	1000 bytes
Pause Time	0.001 s
Malicious nodes	1

Performance of proposed DSR can be analyzed by different simulation metrics such as throughput, end to end delay, energy and etc...

Throughput

Throughput is the number of bits received over the time difference between the first and the last received packets. Throughput graph is plotted in presence of Black hole attack and after removal of Black hole attack. Presence of black hole node in MANET degrades the performance of DSR. Comparison of the graphs in fig.5 shows that the proposed DSR method has good throughput than original DSR with Black hole attack.

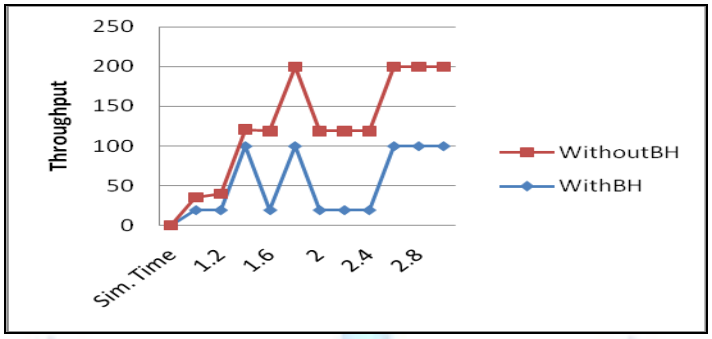

Figure 5: Comparison of Throughput of DSR with and without BH

Average End To End Delay

It is the average time taken by the data packets travel from source to destination. This includes all types of delay caused by buffering of data, Route Discovery latency, queuing, processing at intermediate nodes, retransmission delays, propagation time and etc [13].

End to end delay must be low to get better performance of DSR. Fig.6 shows that the proposed DSR method has lower End to end delay than original DSR with Black hole.

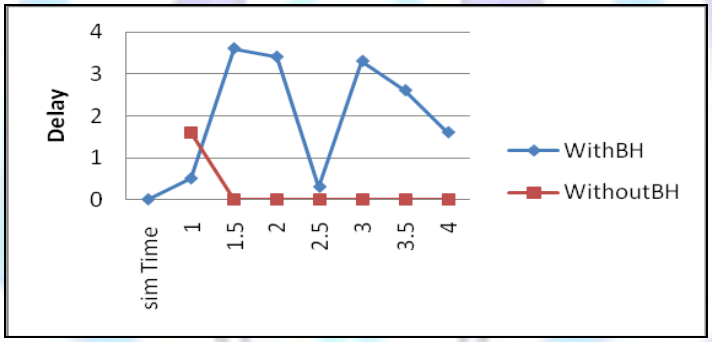

Figure 6: Comparison of Delay of DSR with and without BH

Network Energy

Devices in a mobile network may rely on batteries or other exhaustible means as their power source. For these nodes, the conservation and efficient use of energy may be the most important system design criteria. Power consumption is the total consumed energy divided by the number of delivered packet. Fig.7 shows that the proposed DSR method saves more energy as compared to original DSR with Black hole.

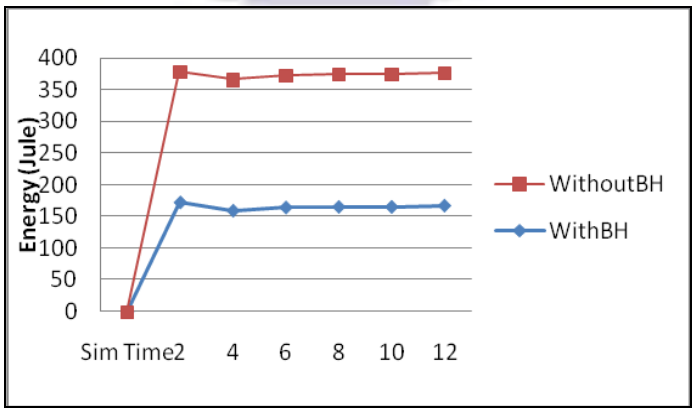

Figure 7: Comparison of Network Energy of DSR with and without BH

Analysis of Gray Hole Attack:

The Gray hole attack is analyzed against different percentage of gray magnitude. Following Graphs show the performance of proposed algorithm against DSR with Gray Hole. Modified algorithm's performance is better as compared to DSR with Gray Hole attack.

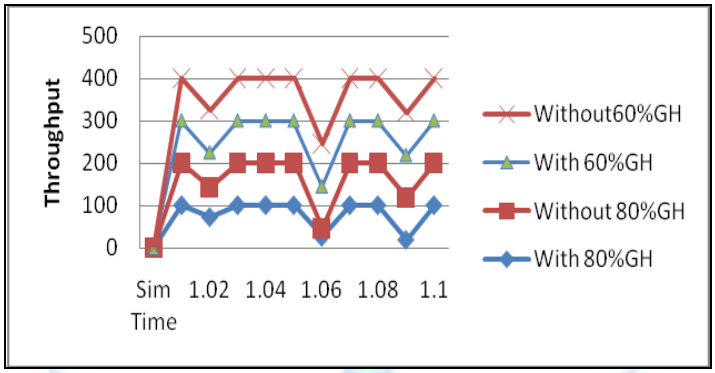

Figure 8: Comparison of Throughput of DSR with and without GH

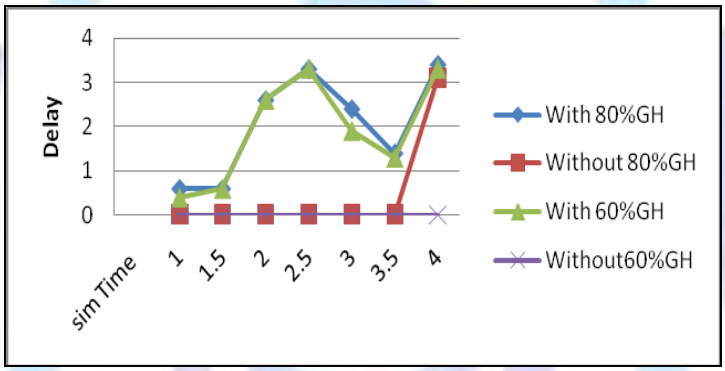

Figure 9: Comparison of Delay of DSR with and without GH

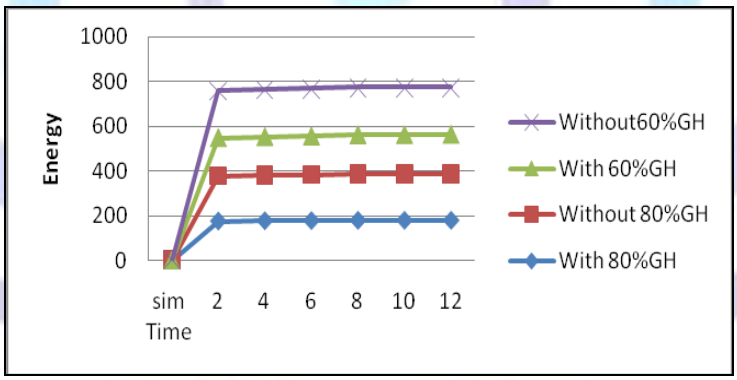

Figure10: Comparison of Network Energy of DSR with and without GH

Analysis of False Positive Probability:

One problem of this detection method is that it suffers from a high false positive probability under high network overload if a constant threshold is used. False positive probability is the ratio of number of honest nodes incorrectly detected as malicious and the total number of honest nodes.

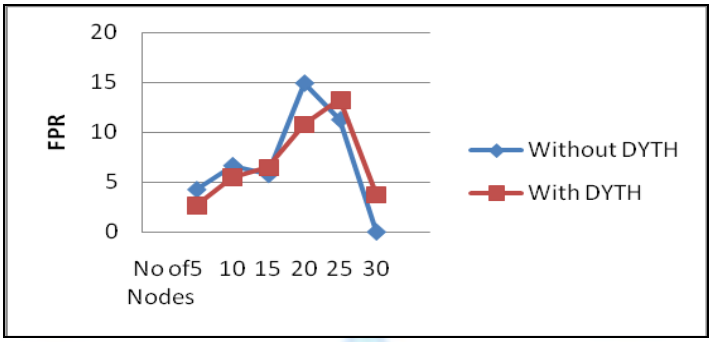

Figure 11: Comparison of False Probability Ratio against No. of Nodes

In case of network failure, nodes may be falsely accused of misbehavior. The false positive should be kept low.Fig.11 shows that by applying dynamic threshold values false probability ratio decreases. Thus ultimately it will result into the improved security of MANETs.

VII. CONCLUSION AND FUTURE WORK

Wireless mobile Ad Hoc network is likely to be attacked by the black hole and gray hole attack. To solve this problem, a course based method is presented to detect black and gray hole attack. The proposed solution is simulated using ns-2 and compared the modified DSR with original DSR in terms of throughput, end to end delay and network energy. Simulation results show that the proposed method has good performance against Black hole attack without much overhead. This solution holds good for gray hole attack also. In the future, the work may extend to propose a feasible solution which will strengthen original DSR against different types of attacks as warm hole or sinkhole attack.

REFERENCES

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

[2] Patcha; A. Mishra; Patcha and Mishra “Collaborative Security Architecture for Black Hole Attack Prevention in Mobile Ad HocNetworks” IEEE Transactions on Wireless Communications,Pg. 7803-7829, 2003

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

[4] I.F. Akyildiz; X. Wang A Survey on Wireless Mesh Networks IEEE Communications Magazine, 43 (9), 23-30, (2005).

[5] Tamilselvan, L. and Sankaranarayanan, V., “Prevention of Blackhole attack in MANET”, The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications. Aus Wireless, 21-21, 2007.

[6] D.Johnson, Y. Hu, and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4", RFC 4728, 2007.

[7] Chang Wu Yu, Wu T-K Chang, “A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network”, Emerging Technologies in Knowledge discovery and Data Mining, Vol, 4819, Issue 3, 2007.

[8] Raja Mahmood RA, Khan Al. “A Survey on Detecting Black Hole Attack in AODV-based Mobile Ad Hoc Networks”. International Symposium on High Capacity Optical Networks and Enabling Technologies, Dubai, United Arab Emirates, 18-20 November 2007.

[9] Sonja Buchegger and Jean-Yves Le Boudec, “Performance analysis of the CONFIDANT protocol” Proceedings of the 3rd ACM international symposium on Mobile Adhoc networking &computing’ 2002. p.p:226–236.

[10] H.Weerasinghe H. Fu., “Preventing Cooperative Blackhole Attack in Mobile Ad Hoc Networks, Simulation, Implementation and Evaluation”. International Journal of Software Engineering and Its Application vol.2, No.3, 2008.

[11] B. Wu, J. Chen, J. Wu, and M. Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks," in Wireless/Mobile Network Security, Springer 2008.

[12] D.M. Shila; T. Anjali; “Defending selective forwarding attacks in WMNs, IEEE International Conference on Electro/Information Technology”, 96-101,2008.

[13] J.W. Cai; P. Yi, Y. Tian, Y.K. Zhou, N. Liu, “The Simulation and Comparison of Routing Attacks on DSR Protocol”, WiCOM 2009, in press.

[14] Kozoma W, Lazos L, “REAct: Resource- Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits”. Second ACM Conference on Wireless Network Security, 16-18 March 2009.

[15] Charles. E ,.Perkins. *AdHoc Networking,* Addison Wesley, 2001.

[16] Wang W, Bhargava B, Linder man M, “Defending against Collaborative Packet Drop Attacks on MANETs”, 2nd International workshop on Dependable Network Computing and Mobile Systems, 27 September 2009.

[17] Saini A, Kumar H, “Comparison between Various Black Hole Detection Techniques in MANET”. National Conference on Computational Instrumentation, Chandigarh, India, 19-20 March 2010.

[18] K.Selvavinayaki, K.K.Shyam Shankar, Dr.E.Karthikeyan “Security Enhanced DSR Protocol to Prevent Black Hole Attacks in MANETs” International Journal of Computer Applications (0975 – 8887) Volume 7– No.11, October 2010

[19] Jaydeep Sen, Sripad Koikonda, Arjit Util, “ A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Network”, *Second International Conference on intelligent system, Modeling and Simulation*, IEEE 2011 .

[20] Tsou P-C Chang, “Developing a BDSR Scheme to Avoid Black hole Attack Based on Proactive and Reactive Architecture in MANETs” *13th International Conference on Advanced Communication technology*, Phonix Park Korea, 13-16 Feb 2011.

[21] IETF MANET work group. [online] Available at : http://www.ietf.org