Volume 5, Issue 7, July 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Positive Vote Count and Secure Path for Black Hole and Gray Hole in MANET

Shweta Goswami*, Nidhi Bajpai, Brajesh Kumar Shrivash
Department of CSE & GITS Gwalior,
M.P., India

Abstract— Mobile ad hoc networks (MANET) are widely used in places where there is little or no infrastructure. A number of people with mobile devices may connect together to form a large group. Later on they may split into smaller groups. This dynamically changing network topology of MANETs makes it vulnerable to a wide range of attack. In this paper, we propose a complete protocol for detection & removal of networking Black/Gray Holes.

Keywords— Mobile Ad-hoc Networks, Black Holes, Gray Holes, Routing Table.

I. INTRODUCTION

Mobile ad hoc network is a wireless ad hoc network. In an ad-hoc network mobile nodes are in touch with each other with multihop wireless links. MANET does not rely on fixed infrastructure. The infrastructure of MANET is not preset it changed very frequently because of dynamic topology. In MANET all nodes act as a router and forwards data packets to supplementary notes. MANET has a lot of applications for instance, in military rescue operations, commercial environments and etc. Mobile ad-hoc networks have several safety issues due to their normal nature, such as open medium, frequently changing topology, not have centralized control, restricted battery power and narrow bandwidth. Routing in a MANET is a difficult work. The major reason for this is the steady changes in network topology due to the mobility of nodes. For this reason there are present several attacks that can be easily launched on an ad hoc network. In Mobile Ad-Hoc Network nodes communicate with each on the basis of common trust. MANET is self configuring and spread network.

II. AODV PROTOCOL

The (Ad hoc On-Demand Distance Vector) AODV is a routing protocol. AODV is designed for ad hoc mobile networks and of both routing, that is unicast and multicast routing. AODV establish routes between different nodes as needed by source nodes. There are three messages which are defined by AODV. These messages are Route Errors (RERRs), Route Request (RREQs) and Route Replies (RREPs). For discovering and maintaining routes in the network these three messages are used, by using UDP packets from source to destination. A node uses its IP address as the source address in the IP header of a message when its request for a route, and for broadcast 255.255.255.255. Route Request Message RREQ Source node that needs to communicate with another node in the network transmits the RREQ message. AODV floods RREQ message, using the expanding ring technique. There is a time to live (TTL) value in every RREQ message, the value of TTL states the number of hops the RREQ should be transmitted. Route Reply Message RREP A node having a requested identity or any intermediate node that has a route to the requested node generates a route reply RREP message back to the originator node. Route Error Message RERR Every node in the network keeps monitoring the link status of its neighbor nodes during active routes. When the node detects a link crack in an active route, Route error (RERR) message is generated by the node in order to notify other nodes that the link is down.

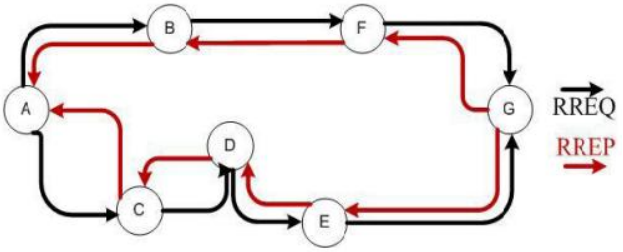

Figure 1. AODV Route Discovery [1]

When there is a link down or a link between destinations is broken that causes one or more than one links unreachable from the source node or neighbor nodes, the RERR message is sent to the source node. When RREQ message is broadcasted for locating destination node, i.e. from node "A" to the neighbor nodes, at node "E" the link is broken between "E" and "G", so a route error RERR message is generated at node "E" and transmitted to the source node informing the source node a route error. The scheme is shown in the Fig 2. Below.

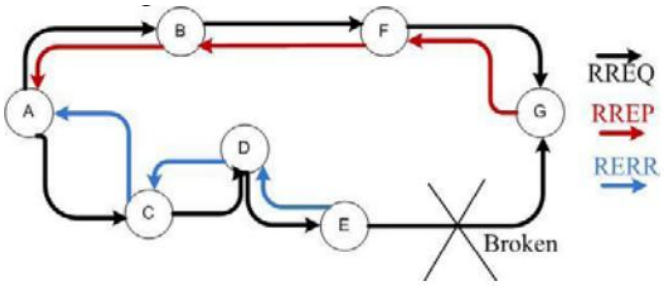

Figure 2. Route Error Message in AODV [1]

III. BLACK HOLE ATTACK

A malicious (node) hub uses its directing convention (routing protocol) with a specific end goal to advertise itself for having the most brief way to the destination hub or to the bundle it needs to block. This hostile hub promotes its accessibility of fresh courses, regardless of checking its directing table. Along these lines aggressors hub (attacker node) will dependably have the accessibility in answering to the course demand and consequently capture the information packet and return it. In based on flooding, the malicious node reply will be received by the requesting nod in light of the flooding, the malevolent hub answer will be gotten by the asking for hub before the gathering of answer from the real hub; henceforth a noxious and manufactured course is made. As this course is perceived, now its up to the hub whether to drop every one of the parcels or forward it to the obscure location. This technique how malicious node fits in the information routes varies. Fig. 3 show how the (black hole) difficulty arise, here node "A" want to send data packets to node "D" and initiate the route discovery process. So if node "C" is a malicious node, then it will claim that it has an active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node "A" before any other node. In this way node "A" will think that this is the active route and thus the active route discovery is complete. Node "A" will ignore all other replies and will start seeding data packets to node "C". In this way all the data packets will be lost, consumed or lost.

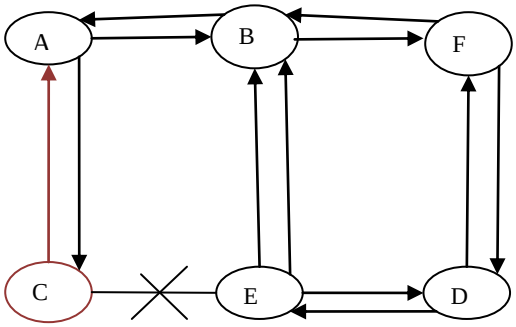

Fig 3: Black Hole Problem [1]

IV. GRAY HOLE ATTACK

The Gray hole attack is a selective packet dropping attack. In this attack a malicious node becomes a part of the route selected by the source node as it replies that it has a valid shortest path. After establishing the spurious route, it forward all packets to certain nodes but drop packets coming from or destined to specific nodes or the node that may behave maliciously for some time but later on it behaves absolutely normally. Due to this uncertainty in behavior of gray hole, this type of attack is more difficult to detect when compared to black hole attack [2]. This attack is also known as Misbehaving attack [3]. If the single malicious node is responsible to accomplish this attack, then it is called as a Single Gray hole attack. In Fig. 4 nodes G is the Gray hole node which acts normal for other nodes in the network and drop packets destined to node D or drop packets coming from source node S.

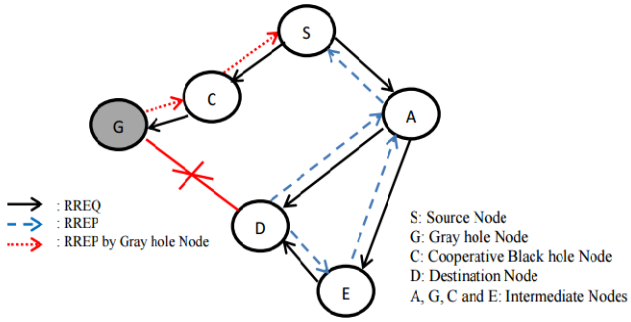

Fig.4: Gray hole Attacks in Mobile Ad hoc Network [4]

V. RELATED WORK

Onkar V. Chandure and V. T. Gaikwad [5] proposed a technique to detect malicious node in the network using DRI table. In this technique security procedure is called by a node when it founds a suspicious node by checking its DRI table. The

node that initiates the procedure is known as the Initiator Node (IN). The IN initially choose a Cooperative Node (CN) in its area, based on its DRI records and then broadcasts a RREQ message to only 1-hop neighbors requesting for a route. In reply of this RREQ IN will take delivery of a number of RREP communication from its nearest nodes. It determination also receive a RREP message from the Suspected Node (SN) which, the latter is a gray hole. As RREP is gotten from the SN, the IN sends an inquiry bundle to the CN through the SN. After sooner or later to live estimation of the inquiry parcel is finished, the IN checks the CN whether it has gotten the question bundle or not. In the event that the answer to this inquiry is sure, then the IN changes DRI table. On the other hand, if the question parcel is discovered to be not coming to the CN, the IN builds its stage of disbelief in relation to the Suspected Node and begins the suspicious hub acknowledgment technique [13]

R. H. Jhaveri, S. J. Patel, D. C. Jinwala, proposed AODV convention [6], when a node gets a RREP, it checks the sequence number in the routing table. In the event that the sequence number is more noteworthy than the one in the RREP, the RREP packet is acknowledged as it is disposed of. The route discovery process transforms in this is done in the presence of a malicious node. Source node broadcast RREQ to the node inside of its neighborhood zone or sort correspondence range. At the point when a neighbor node gets the RREQ and rebroadcasts RREQ to their neighbors until a node having a legitimate course to the destination or destination itself gets RREQ packets. This node sends RREP to the source node on the converse way on which RREQ sent. The malicious node sends RREP with higher, however the created arrangement number of the source. Also, another RREP is sent from destination hub, having really a higher sequence number. As malicious node sends RREP with a higher sequence number than the normal node, the source node chooses the way through malicious node to exchange information. Furthermore, malicious node can drop some or every single got packet, which leads system to the execution. Likewise, in this the moderate node alternately computes a PEAK value after settling time interim. This uses three parameters for count, i.e. RREP sequence Number, Number of answers Received amid the time interim and Routing table arrangement number.

Sukla Banerjee [7] has proposed an algorithm for location & evacuation of Black/Gray Holes. As indicated by the algorithm proposed the aggregate information movement was isolated into little measured squares, as opposed to sending immediately, in the trust that the malicious node can be identified and evacuated in between transmission. Stream of movement is observed by the neighboring node. The destination node sends acknowledgment and source node utilizes this acknowledgment, to check for data loss and assesses the plausibility of a dark opening. However, in this component may bring about false positives and the calculation may report that a non malicious node is misbehaving.

Hesiri Weerasinghe [8] used a technique to detect collaborative black hole nodes that are working collaboratively or as a collection to begin cooperative black hole attacks. In this technique author used (Data Routing Information) DRI chart and irritated checking using the Further Request (FREQ) and Further Reply (FREP) to produce a slightly modified version of ADOV protocol. In this paper, the focus has been on the cooperative black hole attacks in MANET routing.

Shalini Jain Mohit Jain Himanshu Kandwal [9] in this they have proposed an algorithm to find a chain of supportive malevolent node in an ad - hoc network that disrupts broadcast of data by feeding wrong routing data along with the discovery algorithm. They also advised a mechanism to notice and take away the black and gray hole attacks. Their method is based on distribution information on conditions on equivalent other than little sized blocks instead of distribution whole of information in one nonstop stream. The flow of communication is monitored separately in the area of both source and target. The theoretical results indicate that node operators under this algorithm have the possibility of the over half of the real nodes comprised by the attack. Lastly, they also projected a possible solution for discovery and taking away of chain of supportive attack (black and gray hole) during an AODV procedure with enhanced complexity O (n) which is semi of the preceding complexity O(n2) in previous work. In their solution every node can nearby keep up its own table of black listed nodes at any time it tries to send data to any target node and it can also conscious the network about the black listed nodes.

Deepali Raut and Kapil Hande [10] have proposed a technique. 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 the effect has been analyzed using the NS2 simulator**.** Wireless mobile Ad Hoc system is predictable to be attacked by the (black hole and gray hole) attack. To explain this difficulty, 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 a warm hole attack.

Neelam Khemariya, Ajay Khuntetha [11] in this paper a competent approach for the improvement and exclusion of (the Black hole) attack in the (Mobile Ad Hoc Networks) MANET is described. The algorithm is implemented in (AODV) Ad hoc on demand Distance Vector Routing protocol. In this exploration paper a proficient methodology for the identification of the Black opening assault in the MANET (Mobile Ad Hoc network) on AODV routing protocol is projected. The beauty of this algorithm is that it can detect the black hole nodes in both of the cases when a node is not idle and when node is idle(i.e., there is no communication for a defined interval). And it detects the single Black hole node and cooperative Black hole nodes.

Antony Devassy, K. Jayanthi [12] here the proposed technique transmit the MN-ID to the entire nodes in the system. This technique prevents the black hole attack forced with both single and numerous black hole nodes. The instrument used to apply the projected algorithm is NS2, which is an entity slanting event drive software enclose. In this paper, we studied the difficulty of supportive black hole attacks in MANET routing. The MN-ID broadcasting method provides

improved performance of throughput, packet release ratio and condensed packet loss comparing with H. Weerasinge and H. Fu technique. Therefore MN-ID broadcasting means provides improved network presentation and least amount packet loss in the packet diffusion.

VI. PROPOSED WORK

The proposed method for Black hole and Gray hole attacks, provides the framework for developing a complete solution to combat against the different types of Black hole and Gray hole attacks possible in the MANET.

Step1: Initialization of Network.

Step2: Broadcast RREQ

Step 3: Receive Reply Packet from Neighbor Nodes.

Step 4: Source node wait for TTL.

Step 5: Initialized Threshold value, Wait time = current time + TTL.

Step 6: If (threshold > Wait) then start voting process and goon to step 8.

Step 7: Path is secure, data drop by other condition then follow path.

Step 8: On the basis of ack, start voting.

Step 9: On the basis of +ve and –ve votes, we decrease the trust of their nodes.

Step 10: If +ve votes are approximate equal to –ve nodes, then send data by using all available paths to the destination.

Step 11: If Ack is not received from path where node exist, then mark that node as a malicious node.

Step12: Now broadcast id of malicious node and tell everyone in the network about malicious behavior of the node.

Step 13: Repeat the above process after a time interval t, so that we can find out malicious nodes behaving like gray hole.

VII. RESULT ANALYSIS

A. Packet delivery ratio:

The packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated from the sources. Mathematically, it can be defined as:

PDR= S1÷ S2

Where, S1 is the sum of data packets received by the each destination and S2 is the sum of data packets generated by the each source. The graphs show the fraction of data packets that are successfully delivered during simulation time versus the number of nodes.

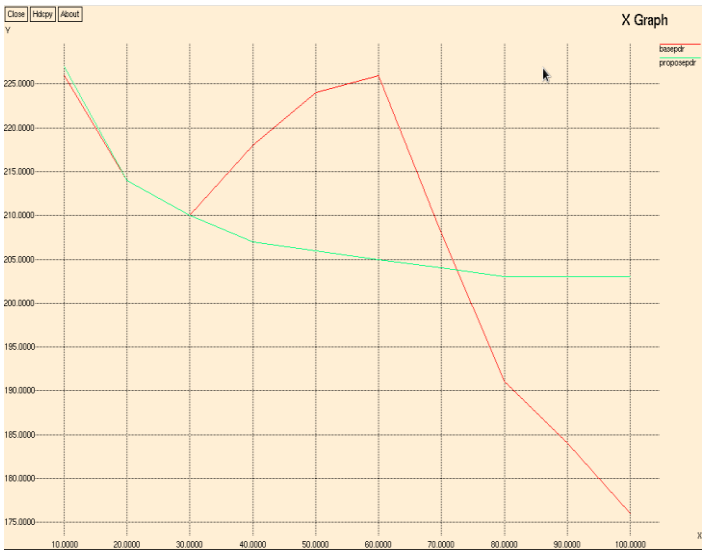

Fig 5: Shows Comparison between base (red) and Proposed (green) values in PDR.

In this graph1 shows when the simulation start maximum packet delivery ratio is 226 and minimum is 203 of proposed and the other end base maximum packet delivery ratio is 226 and lowest is 175. In real time base work value drastically fall that is not good where as proposed value after some points vary.

B. Throughput:

It is defined as the total number of packets delivered over the total simulation time. The throughput comparison shows that the three algorithms performance margins are very close under traffic load of 50 and 100 nodes in MANET scenario and have large margins when the number of nodes increases to 200. Mathematically, it can be defined as:

Throughput= N/1000

Where N is the number of bits received successfully by all destinations.

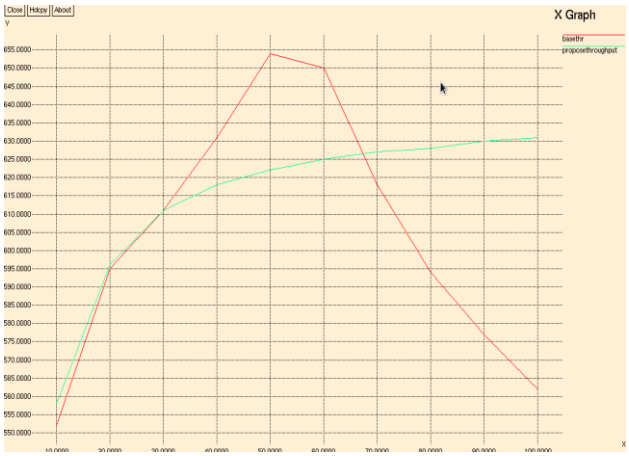

Fig 6: Shows Comparison between base (red) and Proposed (green) values in Throughput.

In graph2 shows the comparison between base and proposed values in throughput. When simulation starts the throughput of proposed work start with 559 and goes to maximum value 631 and the value of base work start with 552 and reached up to 654 then constantly low. In this way it's not good in real time scenario.

C. Routing Overhead:

Routing overhead refers to metadata and network routing information sent by application, which uses a portion of the available bandwidth of communications protocols. This additional information, make up the procedure headers and a purpose-specific data are referred to as transparency, because it doesn't throw into the substance of the communication. Protocol overhead can be expressed as a percentage of non-application bytes (protocol and frame synchronization) divided by the total number of bytes in the message.

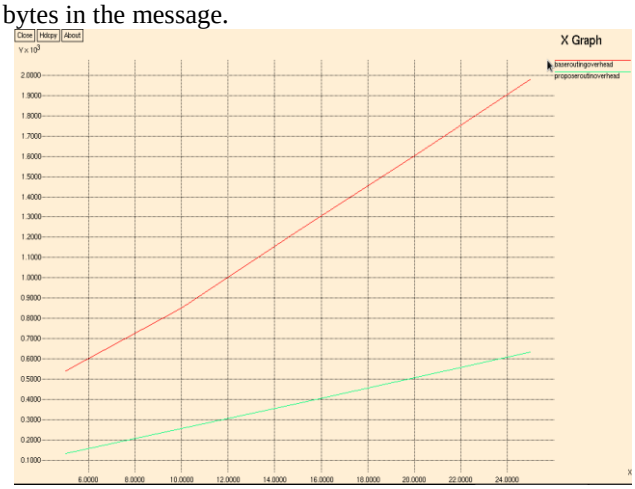

Fig 7: Comparison between base and proposed values in routing overhead.

In graph 3 shows the comparison of routing overhead. When simulation start the proposed value is 0.1500 and increased up to 6500, whereas the values of base work is higher.

D. Forward Packet:

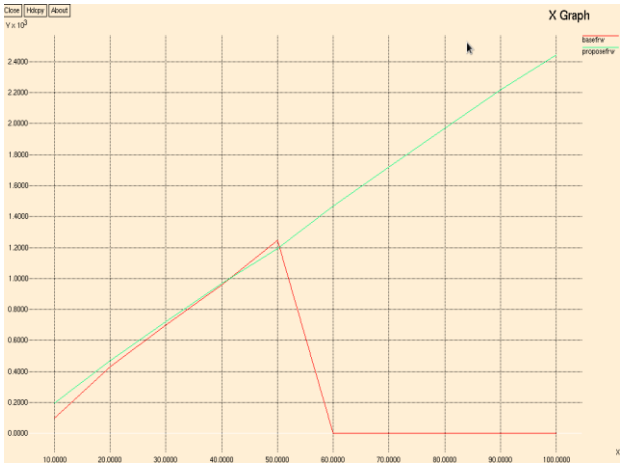

Fig 8: Comparison between base and proposed values in Forward packet.

In graph 4 shows the comparison of forward pocket. When simulation start the proposed value is 0.2000 and increased up to 2450, whereas the values of base work at starting 0.700 and maximum up to 1.2100 and then lower down.

E. Receive Packet:

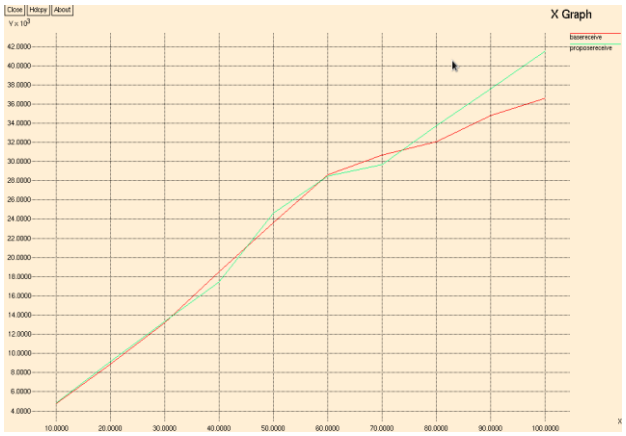

Fig 9: Comparison between base and proposed values in Receive packet.

In graph 5 shows the comparison of receive packet. When simulation start the proposed value is 5 and increased up to 41, whereas the values of base work is 5 and increased up to 37 not good enough to receive more no. of the packet.

VIII. CONCLUSIONS

Wireless Ad Hoc network is likely to be attacked by the black and gray hole attack. In this paper, we have presented a feasible solution to detect 2 types of malicious nodes(Black/Gray Hole) in the ad hoc network. The proposed solution can be applied to identify and remove any number of Black Hole or Gray Hole Nodes in a MANET and discover a secure path from source to destination by avoiding the any type of malicious nodes.

REFERENCES

[1] Romina Sharma, Rajesh Shrivastava "Modified AODV Protocol to Prevent Black Hole Attack in Mobile Ad-hoc Network" IJCSNS International Journal of Computer Science and Network Security, VOL.14 No.3, March 2014.

[2] Garima Neekhra, Sharda Patel, Ashok Varma, "A Literature Review on Detection of Gray Hole Attack in MANET AODV Routing Protocol", International Journal of Emerging Technologies and Engineering (IJETE) Volume 1 Issue 7, August 2014, ISSN 2348 – 8050, 186-189

[3] V. Shanmuganathan, Mr.T.Anand, "A Survey on Gray Hole Attack in MANET", IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501, Vol.2, No6, December 2012, 647-650.

[4] S.V. Vasantha , Dr. A. Damodaram "A Defense Model for Black hole and Gray hole attacks in MANET" IJCSMC, Vol. 3, Issue. 11, November 2014, pg.570 – 576.

[5] Onkar V. Chandure, V. T. Gaikwad, "Detection & Prevention of Gray Hole Attack in Mobile Ad-Hoc Network using AODV Routing Protocol", International Journal of Computer Applications(0975-8887), Volume 41-No.5, pp. 27-32, March 2012

[6] R. H. Jhaveri, S. J. Patel, D. C. Jinwala, "A novel approach for Grayhole and Blackhole attacks in Mobile Ad-hoc Networks", Second International Conference on Advanced Computing & Communication Technologies, IEEE, pp. 556-560, 2012.

[7] Sukla Banerjee "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks" Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA.

[8] Hesiri Weerasinghe, 2011, on Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks Proceedings of the IEEE International Conference on Communications, Jun. 24-28.

[9] Shalini Jain Mohit Jain Himanshu Kandwal "Advanced Algorithm for Detection and Prevention of Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks" ©2010 International Journal of Computer Applications (0975 – 8887) Volume 1 – No. 7

[10] Deepali Raut, Kapil Hande " Performance analysis and Prevention of Gray Hole and Black Hole Attack in MANET" Volume 4, Issue 7, July 2014 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering.

[11] Neelam Khemariya, Ajay Khuntetha " An Efficient Algorithm for Detection of Blackhole Attack in AODV based MANETs" International Journal of Computer Applications (0975 – 8887) Volume 66– No.18, March 2013

[12] Antony Devassy and K. Jayanthi " Prevention of Black Hole Attack in Mobile Ad-hoc Networks using MN-ID Broadcasting" International Journal of Modern Engineering Research (IJMER) www.ijmer.com Vol.2, Issue.3, May-June 2012 pp-1017-1021 ISSN:2249.

