ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 6, June 2016

An Approach To Get Rid Of Gray Hole Attack

Rinki Bhati [1], Dr. Deepti Sharma[2]

M-Tech Student[1],HOD. [2] & Department of CSE
Advanced Institute of Technology & Management
Palwal, Haryana, India

Abstract
Mobile ad hoc networks (MANET) are broadly utilized in places where there is less or no infrastructure. A no. of people with mobile devices may link together to make a huge group. Later on they may divide into smaller groups. This dynamically changing network configuration of MANETs builds it susceptible for a broad range of attack. In this paper we introduce a entire protocol for detection & elimination of networking Black/Gray Holes by employing OPNET network modeler 14.5; it is the latest version of simulation software. Generally, OPNET permits you to make a network with a range of simulated "real-life" resources, so various configuration options can be analyzed. And assuming two different networks with 15 nodes and 35 nodes in network and measuring a security attack against MANET as a network, several statistics or performance metrics i.e. packet delivery ratio, Packet loss and Average end to end delay has been utilized.

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

I.INTRODUCTION

The word mobile indicates the meaning of moving and the word ad hoc indicates the meaning of temporary or do not have any type of constant infrastructure, therefore mobile-adhoc-networks implies the networks that are temporary and allows the nodes to move within the network without any centralized administration [1]. Ad-Hoc Network make a system in such circumstance where making the base is impossible.In all correspondence systems, security is the significant concern, yet because of reliance on different hubs for transmission, Ad-Hoc system faces many difficulties. Numerous analysts have proposed answers for alleviating and recognizing the single gray hole node. Gray Hole Attack is one of the assault in system layer which goes under security attacks. The packet delivery proportion will diminished in the event that some attacker hub is in the way of destination hub. To get rid from this problem ,identification of misbehaved nod is necessary. To enhance the execution of system, trust esteem for hub is presented[6]. MANET can be utilized as a part of various applications, for example, front line correspondence, crisis alleviation situation and so forth. The nature of MANET is a powerfully evolving process, because of its powerfully changing procedure its helpless for extensive variety of assault[8].

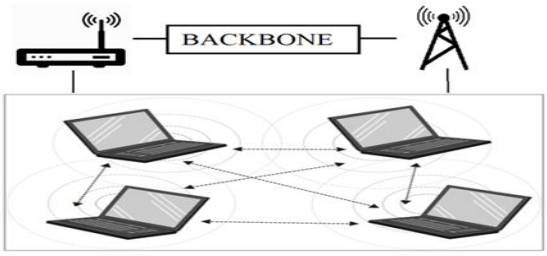

Figure1: Mobile Adho Ntwork

II. Gray Hole Attack

In computer networking, a packet drop attack or black hole attack is a sort of denial-of-service assault in which a switch that should hand-off parcels rather remove them. This typically happens from a switch getting to be traded off from a number of various reasons. One reason said in exploration is through a denial-of-service attack on the switch utilizing a Distributed Denial of Service instrument. Since packets are routinely dropped from a flossy system, the packet drop assault is difficult to distinguish and avert. The malignant switch can likewise achieve this assault specifically, for case, by dropping packets for a specific system destination, at a particular time, a parcel each n parcels or each t seconds, or a haphazardly chose part of the parcels. This is known

as a Gray hole attack. On the off chance that the pernicious route drops all the coming packets, the assault can really be found decently fast through basic systems administration devices for example, follow course. Likewise, when different switches watch that the arranged switch is dropping all movement, they will by and large begin to expel that switch from their sending tables and at long last no movement will stream to the assault. Be that as it may, if the pernicious switch begins dropping packets on a particular time period or over each n bundle, it is for the most part harder to distinguish in light of the fact that some movement still streams over the system Gray hole is a node/hub that can change from carrying on accurately to carrying on like a black hole that is it is really an aggressor and it will go about as an ordinary hub. So we can't recognize effortlessly the assailant since it carries on as a typical hub. Each hub keeps up a directing table that stores the following jump hub data which is a course packets to destination hub The gray hole attacks has two stages:

Stage 1:

A pernicious hub performs the AODV Protocol to advance itself as having a legitimate course to destination hub, with the expectation of interfering with parcels of spurious course.

Stage 2:

In this stage, the hubs has been dropped the hindered bundles with a specific likelihood and the discovery of gray hole attack is a troublesome procedure. Ordinarily in the gray hole attack the assailant carries on noxiously for the time at whatever point the parcels are not dropped and after that change to their ordinary conduct. Both typical hub and assailant are same. Because of this conduct, it is elusive out in the system to make sense of such sort of assault. The other name for Gray hole attack is node misbehaving attack[7].

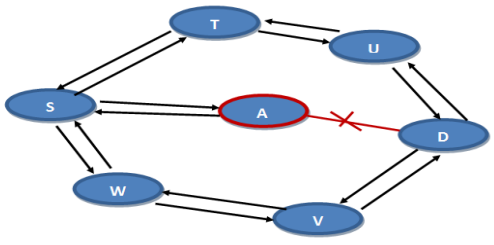

Fig 2.5: Grayhole Attack

In above figure

- **S- Source**
- **D- Destination**
- **T- Node, U- Node, W-Node ,V-Node**
- **A-Malicious Node**

III. LITERATURE REVIEW

Ankit Mehto et al[1]:In this paper the creators examined the diverse assaults and talked about the best approach to enhance the execution of the remote network. It needs security to execute the remote environment and serves clients with wellbeing and non security applications. Numerous types of assaults against MANET have developed as of late that endeavour to trade off the security of such systems. In MANET every hub capacities as a host and also switch, sending bundles for another hub in the system. MANET is powerless against different sorts of assaults. These incorporate dynamic course meddling, curse and disavowal of administration. Dark gap assault is one of numerous conceivable assaults in MANET. In this assault, a malignant hub sends a manufactured Route REPLY (RREP) parcel to a source hub that starts the course disclosure keeping in mind the end goal to put on a show to be a destination hub. The vindictive hub dispatches this assault by publicizing new course with slightest jump tally and most noteworthy destination arrangement number to the hub which begins the course revelation. Portability is the primary issue in system. Because of their dynamic nature, it will require higher security. After this study it is by all accounts that there are such a variety of assaults are accessible with a specific end goal to do the pernicious movement in the portable specially appointed system.

Rashmi Vishwakarmaet al[3]:Here the authors examined the Wireless ad hoc network. . It is autonomous system which can dynamically form the network which has self- configuring capability and infrastructure less network. Due to its dynamic behavior it is more vulnerable to severe threats such as Sybil, wormhole, byzantine, hello flood, denial of services etc. which can influence the performance of the system. Authors proposes a novel method to detect and find a secure route against Black hole attack in ad hoc network. Black hole attacks are serious problems that need to be addressed in wireless network security. Although significant research has been done to defend black hole attacks, with use of this method one can detect black hole nodes in wireless ad hoc network. A secure and flexible technique is proposed using the blacklist criteria as well as miss activity node identification based method which can be tuned to meet desired security and performance constraints. These methods are performed well with low operating cost and resist the described attack. The simulation result the proposed methodology is done by using different

performance metrics parameter in which the work shows that it enhances the performance of the mobile ad-hoc network in the respect of overall performance like high PDR and minimum routing load maintenance

Ravinder Kaur et al[4]:Here the creators analyzed the Adhoc organize and examined abot the systems to keep the systems from attacks .As security is the most vital worry in system Because of nonattendance of any sort altered foundation and open remote medium security usage is troublesome. In MANET every hub capacities as a host and additionally switch, sending parcels for another hub in the system. MANET is defenseless against different sorts of assaults. These incorporate dynamic course meddling, curse and disavowal of administration. Dark gap assault is one of numerous conceivable assaults in MANET. In this assault, a pernicious hub sends a manufactured Route REPLY (RREP) bundle to a source hub that starts the course disclosure with a specific end goal to put on a show to be a destination hub. The malignant hub dispatches this assault by promoting new course with slightest bounce check and most astounding destination grouping number to the hub which begins the course disclosure. Versatility is the principle issue in system. Because of their dynamic nature, it will require higher security.

Sonal Shrivastava etal[5]:Here the creators examined about the directing convention AOMDV and IDS and comparison between them ..The Ad hoc On interest Multipath Routing (AOMDV) convention is consider for steering furthermore to enhances the directing quality as contrast with single way directing convention. The aggressor is influenced all the conceivable ways that is chosen by sender for sending information in system. The malevolent hubs are forward idealistic answer at the season of directing by that their ID is additionally a perplexing strategy. The proposed Intrusion Detection System (IDS) plan is distinguished the assailant data through jump tally component. The directing data of real information is come to which moderate hub and the following bounce data is exist at that hub is affirm by IDS plan. The dark opening aggressor hub Identification (ID) is forward in system by that in future assailant is not taking an interest in directing technique. The proposed security plan recognizes and gives the prevention against directing bad conduct through malevolent assault. The directing execution of AOMDV convention and IDS plan on AOMDV is verging on equivalent that implies about the system is gives identical execution. In assailant module debases the entire execution of system however in nearness of aggressor their exercises are totally hindered by IDS plan in the wake of recognizing them in system. In addition after dump the execution of system by assailant proposed IDS plan recoups 95 % of information misfortune as contrast with ordinary AOMDV.

Varsha Patidar et al[6]: Here the creator examined about the Security in MANET , the most imperative sympathy toward the essential usefulness of system. Creators assess the protected way for transmission through Digital Signature. Computerized Signature is the check procedure. Different security issues of MANET are contemplated and agreeable dark gap assault is alsostudied. A malignant hub can decrease the proportion of end to end conveyance. At the point when the suspicious estimation of hub surpasses a sift hold esteem, the identified IDS telecast the Block message to all hubs to seclude the noxious hub by every single other hub in the system. In spite of the fact that their exist numerous systems for distinguishing dark gap hub yet all have either additional time defer or system overhead because of numerical computations or recently presented bundles in the system. Different recommendations are given for identifying and forestalling of dark gap assaults by different creators.

IV. NETWORK MODEL & ASSUMPTION

We address this issue by choosing some nodes which are powerful and trustworthy in terms of battery power and range. These nodes which are called as Back Bone Nodes (BBN) will make a Back Bone network and has particular functions unlike normal nodes. For the co-ordination between the normal nodes and Back Bone Nodes (BBN), it is considered that the network is partitioned into many grids. It is considered that the nodes, when initially enters the network is able of determining their respective grid locations. It is also considered that the no. of normal nodes are more than the no. of black/gray nodes at any point of time.

4.1 Core Maintenance of the Allocation Table:-

In this mechanism only the backbone network in MANET is allowed to choose the IP addresses for un-configured hosts. The approach depends on assigning a conflict free address to all newly reached nodes by utilizing several disjoint address spaces [6]. Every BBN in MANET has responsibility for assigning a range of addresses disjoint from the ranges of all other BBN. In other words every BBN creates no. that is unique for that host. Each host in the MANET must have the probability to arrive one of the Backbone Nodes (BBN) all the time.

V. METHODOLOGY & ALGORITHM

In this exposition, to identify the malevolent hub in system digital signatures are utilized. Digital

signature is the one of the check procedure. All hubs have honest to goodness Digital signature . In AODV the course demand is send to neighbor hubs by the source hub. In the event that destination hub is one of them then alright generally course ask for telecast to next hub until the destination is found. The course ask for (RREQ) parcel header contains the data of going to (hub id) in hub data segment and jump tally section which contains the quantity of going to hubs utilized as a part of way. At the destination TTL plan is utilized. the destination hub select the most limited way with least number of hubs. the destination hub unicast the answer whose header contain the section of hub id that contains the id of all hubs utilized as a part of that way and digital signature segment in which every meeting hub includes its advanced mark. At the point when the getting hub got parcel analyze the Digital signature of the past hub from its database. on the off chance that the mark is match then that hub is honest to goodness generally that hub is considered as malevolent hub. At the point when vindictive hub is identified then that information is telecast to the neighbors. This procedure is rehashed until the protected way is not found.

5.1 Algorithm

Algorithm:To detect and prevention from attack.
Type of attacker = Black hole as a Malicious attacker

Steps:
1)Begin
i)Establish a network for n number of nodes.
ii)Define sender, receiver nodes.
iii)Find out all neighbors of source node.

2)For sender to receiver
i) Sender Send Route Request message to neighbor nodes for finding the destination
ii) If next node is destination Then direct path is established
iii)Else Broadcast the RREQ to next neighbors and maintaining the hop count information.
iv)If destination(receiver) is found then select the route of minimum hop count and deliver data through that minimum hop count path h.
a)Multiple paths are selected on the basis of hop counts h1, h2, h3…….. hn, n=1,23…
b) Σ Hn = (h1, h2, h3…….. hn) up to destination is Minimum then select for data sending and next route of hop count h1, h2, h3 …….. hn ≥ Min is select for multiple path.

3) For destination to source
i)Select the path with minimum hop counts
ii)Unicast RREP to pervious node with digital signature
iii) Verify digital signature
iv) If (all signatures are valid)
v) Establish a path for data transfer.
vi) If (Any intermediate or destination node is malicious node)
vii)Then add the malicious node information in malicious node column and again rebroadcast Route request (RREQ) .

VII. IMPLEMENTATION AND ANALYSIS

6.1 Implementation

Simulation utilizing OPNET Simulator was utilized to inquire the performance effect of a co-operative black hole attack on a mobile ad hoc network. Packet delivery ratio, Network throughput and end-to-end delay are the performance metrics utilized in our result analysis. Depending on the analyses of performance metrics built, we observed the consequences of a co-operative black hole attack on MANET.
In our introduced work we assume three metrics to measure the performance specified below –
Performance Metrics
In measuring a MANET routing protocol as well as measuring a security attack against MANET as a network, several statistics or performance metrics are utilized. In this subsection, we talk about the necessary metrics needed to measure and determine the probability of several node attacks on a MANET. The performance metrics:
5.1.1 Network throughput
5.1.2 End to end delay
5.1.3 Packet delivery ratio

6.1.1 Network throughput

A network throughput is the normal rate at which message is effectively conveyed between a recipient (target node) and its sender (source node). It is likewise alluded to as the proportion of information got from its sender to the time the last obtained from its sender to the time the last packet arrives its target node. Throughput can be expressed as bits per second (bps), packets per second or packet per time slot and OPNET Simulator represents it utilizing bits per second. For a network, it is needed that the throughput is at high-level. Some factors that influence MANET's throughput are specified in: these are unreliable communication, changes in configuration, limited bandwidth and energy.

6.1.2 End-to-end delay

Packet end-to-end delay is the time delay it considers a network source to deliver a packet to its destination node. Hence, the packets end-to-end delay is the total amount of delays detected in the entire network at each hop going to its destination node. In MANETs,

this type of delay is often caused by specific link tearing or/and the signal strength between nodes been low. The flexibility of a routing protocol can be determined by its end-to-end delay on a network, hence a steadfast MANET routing provides low packet end-to-end delay.

6.1.3 Packet delivery ratio

This refers to the ratio of the total no. of data packets that arrives the recipient (targeted node) to the total no. of data packets forwarded by the source node. This is another performance metric that is utilized to determine the accuracy and efficiency of MANET's routing protocol because it is utilized to compute the rate of dropping packets. Same as the network throughput, packet delivery ratio (PDR) is required to be high.

Scenarios

Several scenarios can be generated in a simulation in OPNET. We generated various scenarios during the simulation model for providing another step of designed project space that we utilized for several experiments and results analyses. Another cause for having various scenarios is to enable us to detect the consequences of mobile network under regular operation, under co-operative attack and in terms of changing network size. Here, we show the various results achieved in our two main scenarios and describe every scenario.

Scenario 1: 15-Node MANET Network

First scenario is small network simulation of 15 mobile nodes. In this scenario, we conducted two different simulations. The first simulation in this scenario is making a regular MANET in terms of observing the outcome and nodes behavior of the mobile ad-hoc network without any kind of attack launched on them. This would enable us to take note and evaluate the network impacts when there is an attack (in second simulation). We conducted several simulations that were run many times to ensure the results and we were capable to present related and comparable results.

Figure-1 Scenario-1 workspace with 15-nodes

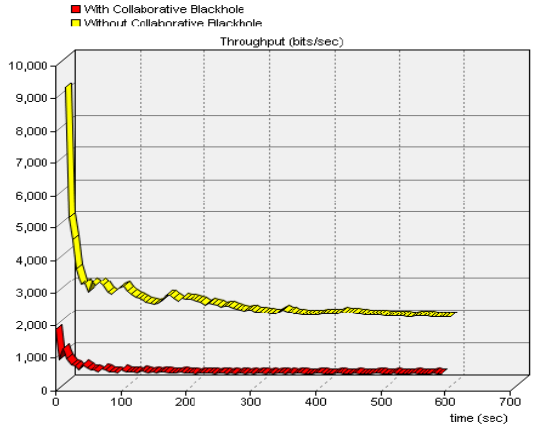

Figure a) Throughput of 15-node MANET Network

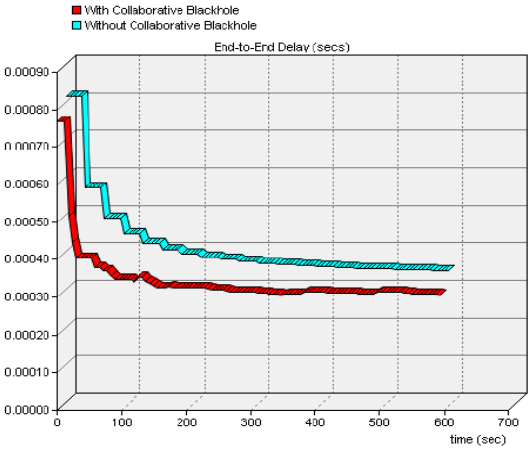

Figure b) Packet Delivery Ratio of 15-node MANET Network

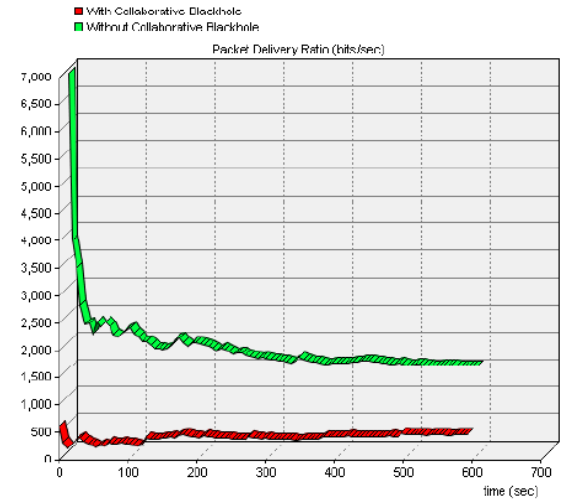

Figure c) End-to-End Delay of 15-node MANET Network

Scenario 2: 35-Node MANET Network

In the second scenario; a simulation of a larger network in term of size compared to the first scenario. The network atmosphere is still the same 1

x 1 km square pace of a campus network but the network size is larger; having 35 mobile nodes in comparison of the earlier two simulations with 15 mobile nodes. Here, we show two simulations in which the first is a MANET network under regular operation while the latter is a MANET network under direct cooperative attack and both involve 35 nodes. The model layout in this scenario is same as that shown in fig 2 except that it consist mobile nodes 0 to 34.

Figure-2 Scenario-2 workspace with 35-nodes

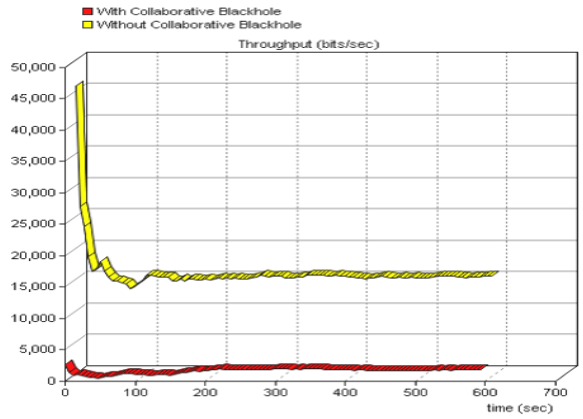

Figure a) Throughput of 35-node MANET Network

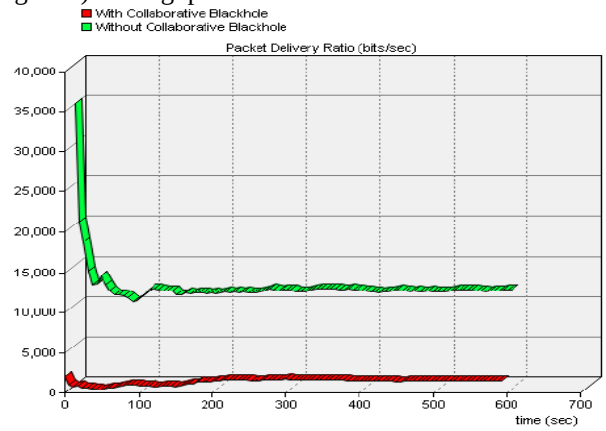

Figure b) Packet Delivery Ratio of 35-node MANET Network

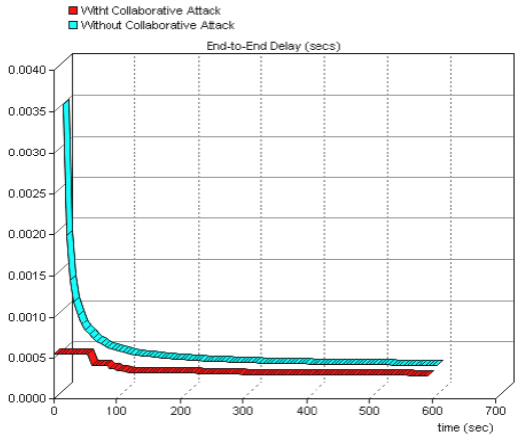

Figure c) End-to-End Delay of 35-node MANET Network

6.2 ANALYSIS

5.2.1 Scenario 1 vs. Scenario 2

In comparing scenarios 1 and 2 with all the results shown and also when comparing the data in tables 1 & 2; we note that our measurement depends on some metrics; packet delivery ratio, throughput and end-to-end delay, scenario 2 has larger network performance both when the MANET was without and with collaborative black hole attack. This is required due to the obvious cause that scenario 2 has larger no. of mobile nodes in comparison of scenario 1. On the other side, comparing the margins of every performance parameter of the several scenarios, we note that the rate of reduction and collaborative impacts of the dangerous nodes build the data margin of scenario 2 to be broader. This is as a result of the collaborative black hole attack, which influences more nodes in comparison of the no. of nodes influenced in scenario 1. For finding differences in the simulation results and to be capable to compare results, our simulation was done in two scenarios depending on various network sizes. Every scenario has first experiment for MANET regular operation and second experiment for MANET operation under a cooperative black hole attack. Our experiments represent encouraging results achieved from the two simulation scenarios. The regular MANET outperforms the MANET under attack in terms of packet delivery ratio and throughput. These results represent the impact of the collaborative black hole attack on MANET because the throughput and packet delivery ratio of a good network is often high. On the other side, in terms of the end-to-end delay performance metric, the result achieved when the MANET was under collaborative black hole attack represents there was a little reduction in the delay because the malicious nodes offer a quick route response to the source node claiming to be benign

nodes and having the shortest route to the needed target node. In conclusion, we find that the larger the MANET network size is in terms of the no. of nodes, the more nodes that would be compromised and hence malicious; the more powerful the impact of the collaborative attack would be in terms of performance reduction.

VII. CONCLUSION AND FUTURE WORK

The simulation results are examined to get the final conclusion about two different network scenarios with 15 and 35 nodes. These results represent the impact of the collaborative black hole attack on MANET because the throughput and packet delivery ratio of a good network is often high. On the other side, with respect to the end-to-end delay performance metric, the result achieved when the MANET was under collaborative black hole attack represents there was a little reduction in the delay because the dangerous nodes (Black/Gray holes) offer a quick route response to the source node claiming to be benign nodes and having the shortest route to the required target node. Comparing the margins of every performance parameter packet delivery ratio, throughput and end-to-end delay of the various scenarios, we note that the rate of reduction and collaborative impacts of the malicious nodes build the data margin of scenario 2 to be broader. This is as a result of the collaborative black hole attack, which influences more nodes in comparison of the no. of nodes influenced in scenario1.

VIII.REFERENCES

1) Ankit Mehto,, Prof. Hitesh Gupta," A Review: Attacks and Its Solution over Mobile Ad-Hoc Network", International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue 5- May 2013,pp-2009-2011.

2)Prachi Sharma, Kalpana Rai, Deepak Jain and B L Rai."Hybrid Method for MANET Security against Blackhole and DoS"International Journal of Computer Applications 139(11):20-24, April 2016. Published by Foundation of Computer Science (FCS), NY, USA.

3) Rashmi Vishwakarma , Moh. Imran Hashiam," An Enhancement of Security level under varying Black Hole attacks in Mobile ad-hoc Network", International Journal of Electrical, Electronics, and Computer Engineering ,Volume 4(1), 2015,pp-57-65

4) Ravinder Kaur Jyoti Kalra ,"Detection and Prevention of Black Hole Attack with Digital Signature ",International Journal of Advanced Research in Computer Science and Software Engineering , Volume 4, Issue 8, August 2014 ,pp-843-847.

5) Sonal Shrivastava,Chetan Agrawal &Anurag Jain "An IDS scheme against Black hole Attack to Secure AOMDV Routing in MANET "Radharaman Institute of Technology & Science Bhopal, India .

6) Varsha Patidar1, Rakesh Verma2,"Black Hole Attack and its Counter Measures in AODV Routing Protocol", International Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5,pp-1612-1614.

7) Madhuri Gupta, Krishna Kumar Joshi," An Innovative Approach to Detect the Gray-Hole Attack in AODV based MANET " International Journal of Computer Applications Volume 84 – No 8, December 2013 44 ,pp-0975 – 8887.

8)] G.S Mamatha , Dr.S.C. Sharma "A Highly Secured approach against attacks in MANETS" IJCTE Vol.2,No.5, Oct.