Performance Evaluation of Black Hole Attack and Prevention Using AODV on MANET

[1]Priyanka Sonal Sao, [2]Jageshwer Shriwas, [3]Rohit Miri

[1] Mtech Scholar, CSE Department, Dr.C.V.Raman University, Chhattisgarh, India
[2] Assistant Professor, CSE Department, Dr.C.V.Raman University, Chhattisgarh, India
[3] HOD, CSE Department, Dr.C.V.Raman University, Chhattisgarh, India

---***---

Abstract- *An Ad-hoc network is a part of a network that is use for as requirement. It's a LAN i.e. built spontaneously as devices connect. A wireless Ad-Hoc network is decentralized type of wireless network i.e. access from anywhere. It's a geographical independent. In the Ad hoc network, security issue is more because of it's without infrastructure. The threat can be arise on the MANET (MOBILE Ad hoc Network). The most of the security issue is black hole. In the MANET most common and useful protocol is AODV (Ad hoc On demand Distance Vector). The AODV is a threatened by Black hole. In the black hole the malicious node is absorb all data packets. To avoid this problem we can give sequence number to each data packet and find more than one route for each packet .*

Key Words- MANET (Mobile Ad hoc Network), AODV (Ad hoc On demand Distance Vector), Black hole.

I. INTRODUCTION

A wireless network is a connectionless network. Here connectionless it means no need to connect with cables and other physical device except some require physical device. The wireless network is a geographical independent method. Wireless networks can be classified in two types [1].

1) Infrastructure Networks
The infrastructure network is a wired based network. Each node is a communicate via bridge. It's a infrastructure based network i.e. depends on various network topology like a star, mesh, hybrid etc. The communication device move geographically. It has 1 base station and multiple node [2].

2) Infrastructure-Less (Ad hoc) Networks
It's a connectionless network i.e. dynamically connected in an arbitrary manner. Its also called MANET(Mobile Ad hoc Network). MANET are significantly difference from wired network[2]. This network is a easy to use and less maintaining problem. Nothing to vary about geographical problem. We can access network from anywhere. But in the MANET security is big challenge for the user. Most of the problem is "Black hole" problem [3].

MANET –
Mobile Ad hoc Network are decentralized wireless systems and private network. MANET is consist with mobile nodes that are freely moving in the geographical surface in and out in the network. Nodes can be either mobile phone, tablet, laptop, personal digital assistance, MP3 players etc. Internet Engineering Task Force (IETF) have MANET working group i.e. for developing IP routing protocol [4].
Characteristics of MANET-
Autonomous and infrastructure less: MANET is a well organized, infrastructure less and autonomous network, independent of any organized infrastructure and centralized network administration. In the MANET each node operates all the function and works as a router [5].
Multi-hop routing: In the MANET there is no dedicated router, so that the every node of MANET is acts as a router and forwarding packets to the destination using shortest path. Hence, data sharing among mobile nodes is made easier and available [6].
Dynamic network topology: If there is any mobile node move frequently the MANET, the MANET topology are also change randomly and regular routing of data packet will be changes, network partitions, and possibly data packet will be loss [7].
Variation on link and node capabilities: Every In the MANET every node is a device with different radio frequency for having varying transmission and receiving capabilities. All devices are operating on multiple and difference frequency bands. Asymmetric links may be in the heterogeneity in the radio capabilities [8].
Energy-constrained operation: The Each mobile device has limited power supply so that the processing power of each node is restricted.
k scalability: In the MANET application it's a wide range applications can involve bulky networks with plenty of nodes especially that can be found in strategic networks. Scalability is crucial to the flourishing operation of MANET.

© 2015, IRJET.NET- All Rights Reserved

Overview of AODV protocol-

The Ad-hoc on demand Distance Vector routing algorithm is a designed for ad hoc mobile network. It's a routing protocol i.e. determine the appropriate path from the source to destination. The AODV is capable to route both unicast and multicast. These protocols are broadly divided into two categories [9].

a) Table-driven routing protocols or proactive routing protocol.

b) Source-initiated on-demand driven routing protocols or reactive routine protocol.

Table-driven routing protocols are also known as proactive routing protocols. The proactive routing protocol are maintain table of all routing information. These protocols desire to maintain unique, exact and all routing information in the network. All the nodes exchange routing information periodically and also there is even a minor change in the network topology and thus, every node in the network maintains one or more routing table are stores routing information about every other node in the network [10].

Source-initiated on demand driven routing protocols are also known as reactive routine protocol. AODV is a reactive routing protocol used to search a route between source and destination and establish new route and give new route path. In this order it is manage route and different types of link is establish, information are exchange. Its find route when necessary[11]. The drawback of this routing protocol is delay due to route discovery.

II. BLACK HOLE ATTACK

Black hole – In the black hole the malicious node produce himself as a node for routing to the destination node. When source node send request the malicious node receive it and send response to him and create shortest path. The malicious node create fake route for destination node. When the malicious node insert itself between communication route, it is able to drop the data packet, it is retrieve information from the data packet and can be modify it. He can do anything in that communication route. And the data packet never reaches to the destination.

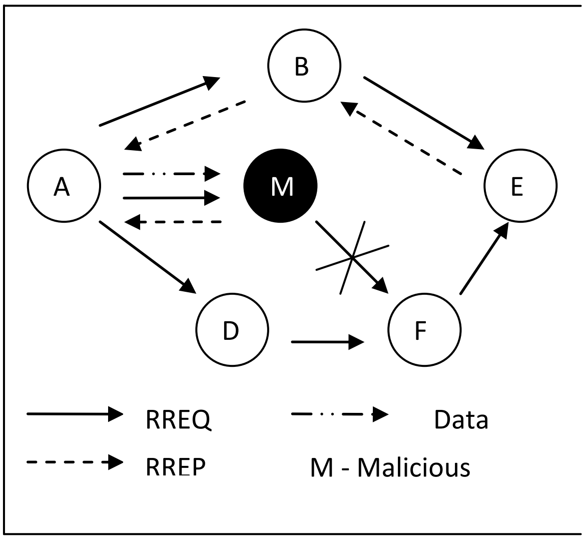

Figure 1: Black hole Attack

In the following figure the malicious node is act as like a intermediate node. Node "A" want send data packet to node "D". But in the between A and D,B is a malicious node. It will act like a active node and receiving RREQ (route request) from the node A. And send response to the node A. node A is think the route is a active and ok, I got response from node D and start to send data packet but data packet are received by node B and node D doesn't know about the data packet. And all data packet are lost.

III.PROBLEM IDENTIFICATION

Performance Evaluation of Black Hole Attack and Prevention Using AODV on MANET. To avoid black hole problem the AODV routing protocol is commonly and main routing protocol i.e. used. The performance of black hole attack and prevention is most common use the AODV routing protocol. The AODV is capable to route both unicast and multicast. So that the black hole problem can be easily removed from MANET. The AODV is on demand routing protocol it can arise when it require.

IV. PROPOSED APPROACH

NS (version 2) is an object- oriented and developed at UC Berkeley written in C++ and OTCL. It is a discrete event driven network simulator. NS is primarily helpful for one thing native and wide space Network Simulator (Version 2), widely referred to as NS2, is solely a happening driven simulation tool that has proved helpful in finding out the dynamic behavior of linking networks. Simulation of wired similarly as wireless network functions and protocols (e.g., routing algorithms, TCP, UDP) might be completed using NS2 [12]. In general, NS2 gives to users with how of specifying such network routing protocols and combinations their corresponding behaviors'. Attributable to its easiness, flexibility and modular nature, NS2 has gained constant popularity within the networking analysis community since its birth in 1989. Ever since, many changes and repetitions have marked the increasing maturity of the tool, due to substantial contributions from the players within the field. Among these are the University of California and Cornell University who developed the important network simulator, the inspiration that NS relies on. Last however not the smallest amount, the cluster of researchers and developers within the community are constantly operating to stay NS2 sturdy and versatile. Again, the most objective of this book is to supply the readers with insights into the NS2 design. This chapter offers a quick introduction to NS2. NS2 Beginners are suggested to travel through the detailed introductory on-line resources [13].

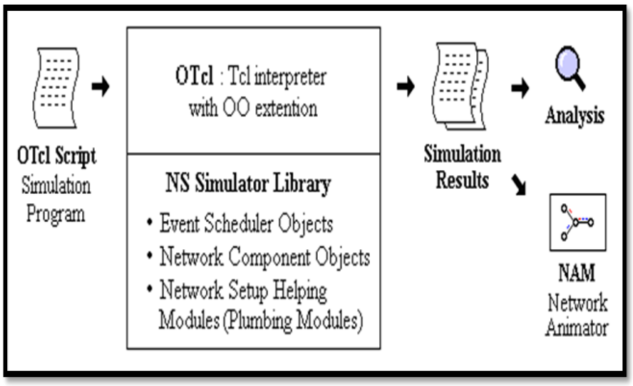

Figure 21: NS2 Architecture

4.1 Structure of Ns2

NS-2 is constructed using object oriented strategies in C++ and OTCL (object oriented variant of Tcl).NS-2 interprets the simulation scripts written in OTCL. A user should set the various parts (e.g. event scheduler objects, network parts libraries and setup module libraries) up within the simulation setting. This leads into the actual fact that ns may be a discrete event simulator wrote in C++, with an OTCL interpreter as a front-end. The simulator supports a category hierarchy in C++ (we conjointly decision it the compiled hierarchy), and an analogous category hierarchy among the OTCL interpreter (we conjointly decision it the interpreted hierarchy). The 2 hierarchies are closely associated with one another. From the user's perspective, there's a one-to- one correspondence between a category within the interpreted hierarchy and one within the compiled hierarchy. the basis of this hierarchy is that the category Tcl Object Users creates new simulator thing via the interpreter; these things are instantiated among the interpreter, and are that clearly mirrored by a corresponding object within the compiled hierarchy. The interpreted category hierarchy is automatically established through strategies outlined within the category Tcl category. User instantiated objects are mirrored through strategies outlined within the category TCL object [14].

NS uses 2 languages as a result of the simulator has 2 totally different sorts of things it must do. On the one hand, detailed simulations of protocols need a systems programming language which might efficiently manipulate bytes, data packet headers, and implement algorithms that run over giant knowledge sets. For these tasks, the run-time speed necessary is vital is very important} and also the turn-around time is a smaller amount important. On the opposite hand, an outsized a part of network analysis using few thing varying parameters or configurations, or quickly exploring variety of eventualities. In these cases, the iteration time is additional necessary. Since configuration runs once (at the start of the simulation), the run time of this a part of the task is a smaller amount necessary. C++ is quick to run however slower to alter, creating it appropriate for detailed protocol implementation. OTCL runs abundant slower however will be modified terribly quickly (and interactively), creating it ideal for simulation configuration.

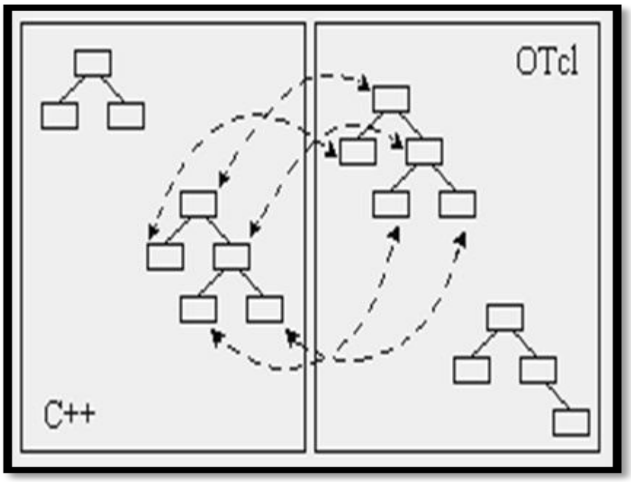

Figure 3: C++/OTCL duality

Protocols like TCP and UPD, traffic supply behavior like FTP, TELNET and CBR, router we currently briefly

© 2015, IRJET.NET- All Rights Reserved

examine what data is stored during which directory or file in ns- NS (version 2) is an object- oriented, and discrete event driven network are simulator developed at UC Berkeley written in C++ and OTCL. NS is primarily helpful for one thing native and wide space networks. It implements network queue management mechanism like Drop Tail, RED and CBQ, routing algorithms like AODV, DSR, and more. NS conjointly implements multicasting and a few routing algorithms like AODV, DSR and a lot of. NS conjointly implements multicasting and a few of the Media Access Control layer protocols for LAN simulations [15].

Below are the running screenshot of the simulation.

Simulation is started and the aodv as per the normal procedures proceeds for route discovery. All the procedures are followed exactly same manner and the nodes start communicating with each other.

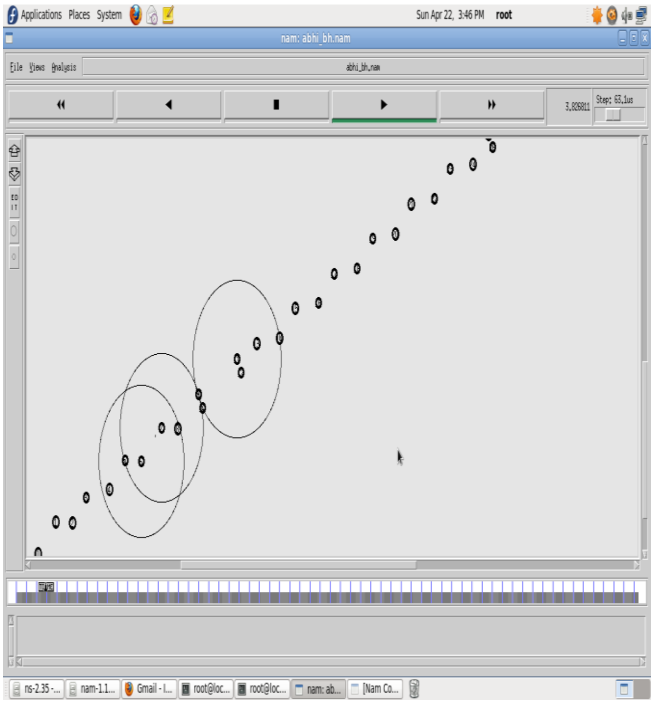

Figure 4: Simulation

After 3.0 sec the Black hole is introduced to the network with three black hole nodes in it. Node 8, Node 11 and Node 15 are the black hole nodes in the simulation.

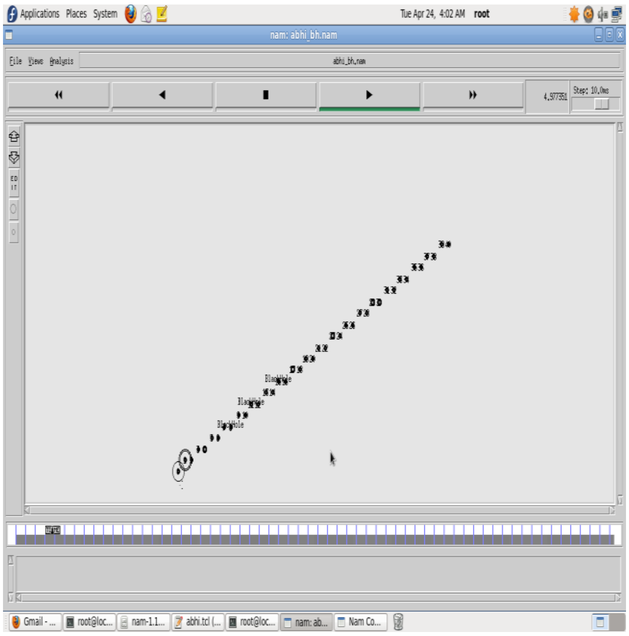

Figure 5: Black hole nodes introduced

The nodes are labeled as the Black hole and can be seen in the figure 14. The data will not flow beyond the black hole nodes.

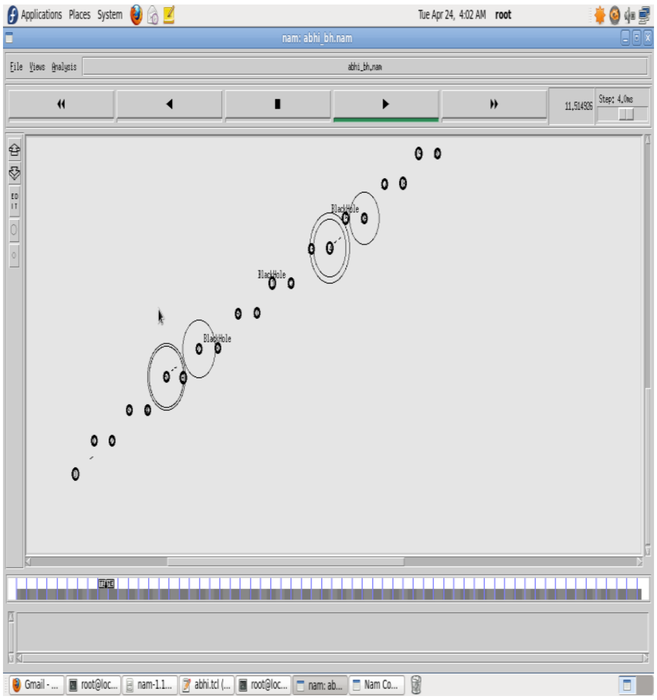

Figure 6: Packet Travelling

© 2015, IRJET.NET- All Rights Reserved

Packets travelling through various paths.

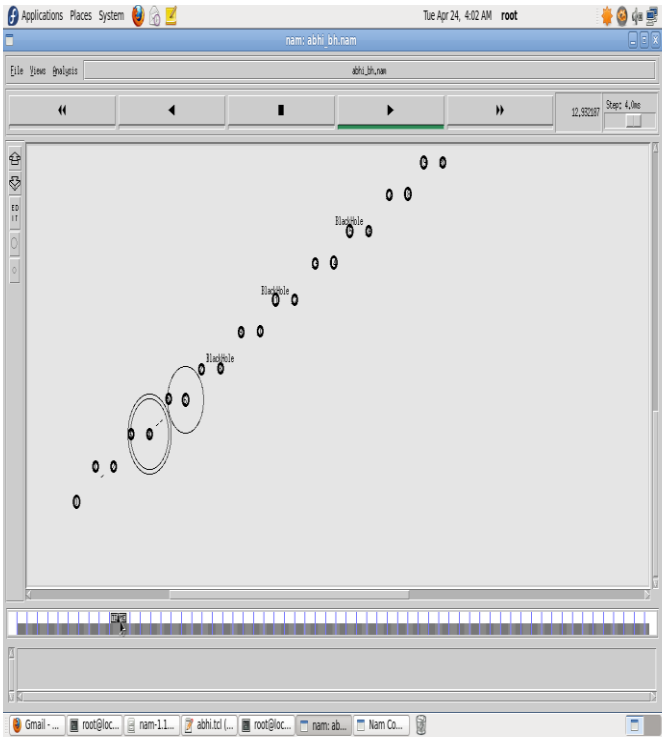

Figure 8: Packet not going beyond Black hole

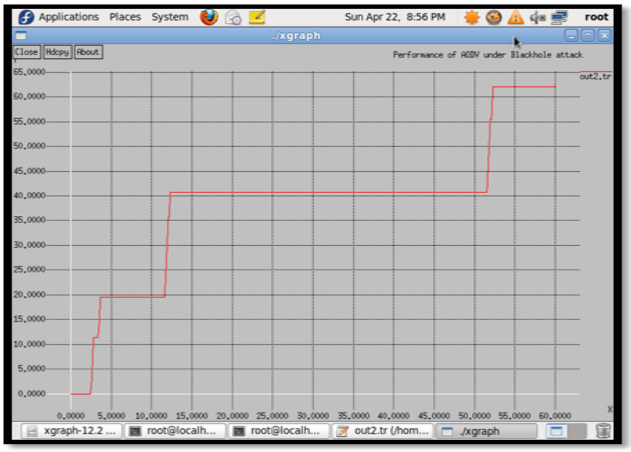

Figure 7: Throughput VS Time Graph

Figure 18 shows the throughput graph of the simulation representing the Time on the x-axis and throughput percentage on the y-axis. The graph is plotted on the x graph included with NS2-35 all-in-one. At time 5 the throughput is 20% as the system is just started sending the data packets and Black hole nodes have been initialized. Similarly by the end of the simulation the performance is reached up to 63% only which is far below the level of the aodv which is over 90% in highly dense environments.

V. RESULT

Time	Throughput
10	20.0 %
20	40.0 %
30	41.0 %
40	42.35 %
50	42.36 %
60	63.0 %

Table 1: Result Analysis Figure 18

VI. CONCLUSION

The performance of the AODV is very good as it provides more than 90 % throughput under dense traffic circumstances also. The AODV is simplest of the routing used by the Mobile Ad-Hoc Networks.

The attack simulated significantly hampered by the Black hole Attack.

1. In the first scenario of 30 nodes with 2 black hole nodes the performance of the aodv reached till 62% maximum. With the average being 46%.
2. In the second scenario of 40 nodes with 3 black hole nodes the performance of the aodv reached till 65% maximum. With the average being 48%.

The scenario and the results supports that the Black hole attack severely hampers the performance of the AODV or any other Ad-Hoc network in which there is no security mechanisms and detection of such types of nodes and attacks.

VII.APPLICATION

❖ MANET could be setup quickly to facilitate communications in different fields such as:-

a) Military
- Rapidly deployable battle-site networks

b) Disaster management
- Disaster saving teams that cannot rely on all ready existing infrastructure

c) Neighborhood area networks (NANs)
- Shareable Internet access in high density urban settings

d) Impromptu communications among groups of people
- Meetings/conferences

© 2015, IRJET.NET- All Rights Reserved

❖ Advantages of MANET

These are many advantage of MANET but here we are giving following advantages of MANETs:

a. They are giving service to access the information and services regardless of geographic position.
b. These networks can be configure at any place and time.
c. These networks work without any pre-existing infrastructure.

VIII. FUTURE WORK

We observed that the effect of the Gray Hole attack is less as compared to the Black Hole attack. We have also floated an idea for detection of these attacks. In future, we plan to develop and simulate the detection technique on these lines.

IX. REFERENCES

[1] Meenakshi Tripathi,M.S.Gaur,V.Laxmi, Comparing The Impact Of Black Hole And Gray Hole Attack On LEACH In WSN, The 8th International Symposium On Intelligent Systems Techniques For Ad Hoc And Wireless Sensor Networks (IST-AWSN), Procedia Computer Science 19 (2013) 1101 – 1107

[2] Mayuri Gajera1, Sowmya K. S2, Prevention of Black Hole Attack in Secure Routing Protocol,International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064

[3] Jaya Jacob*, V.Seethalakshmi**, Performance Analysis and Enhancement of Routing Protocol in Manet, International Journal of Modern Engineering Research (IJMER), Vol.2, Issue.2, Mar-Apr 2012 pp-323-328

[4] Tarun Kumar Mishra1, Bhupendra Singh2, Arun Kumar3, A Security Scheme for Mobile Ad-hoc Network with Reduced Routing Overhead,International Journal of Advanced Research in Computer Science and Software Engineering,Volume 3, Issue 8, August 2013

[5] R.Kumar, Performance Evaluation of Gateway Discovery Approaches in the Integrated Mobile Ad Hoc Network (MANET)-Internet Scenario,International Journal of Computer Technology and Electronics Engineering (IJCTEE), Volume 2, Issue 3, June 2012

[6] Mohammad Al-Shurman and Seong-Moo Yoo "Black Hole Attack in Mobile Ad Hoc Networks" Electrical and Computer Engineering Department The University of Alabama in Huntsville.

[7] IRSHAD ULLAH and SHOAIB UR REHMAN " Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols" Electrical Engineering Thesis no: MEE 10:62 June, 2010 School of Computing Blekinge Institute of Technology Box 520 SE – 372 25 Ronneby Sweden.

[8] FIHRI Mohammed, OTMANI Mohamed and EZZATI Abdellah " The Impact of Black-Hole Attack on AODV Protocol" Mathematics and Computer Science Dept, LAVETE Laboratory Faculty of Sciences and Technical Settat, Morocco.

[9] Prof. Dhaval Thakar and Prof. Nainesh Prajapati "A Modified AODV – Algorithm for prevention of Black hole attack in Mobile Adhoc Networks" Asso. professor, Dept of Information Technology A D Patel institute of Technology, A D Patel institute of Technology, New VVNagar-388121, Gujarat.

[10] Mayuri Gajera and Sowmya K. S "Prevention of Black Hole Attack in Secure Routing Protocol" Dayanand Sager College of Engineering, Bangalore, India

[11] Jyoti and Ms Rashmi Kushwah "Performance Analysis of Black-Hole Attack in MANET" M.Tech. Scholar,Assistant Professor Of CSE, P .D.M College of Engineering, Bahadurgarh, Haryana (India)

[12] Jaspal Kumar, M. Kulkarni, and Daya Gupta "Effect of Black Hole Attack on MANET Routing Protocols" I. J. Computer Network and Information Security, 2013, 5, 64-72Published Online April2013 in MECS,DOI:10.5815/ijcnis.2013.05.08

[13] Ajay Sharma "Performance Evaluation of AODV under Black hole attack in MANET using NS2 simulator" ISSN: 2278 – 1323 International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 8, October 2012

[14]MONIKA ROOPAK " BLACK HOLE ATTACK IMPLEMENTATION IN AODV ROUTING PROTOCOL" International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013 402 ISSN 2229-5518

[15] Vasanthavalli.S, R.Bhargava Rama Gowd and Dr.S.Thenappan "Peruse Of Black Hole Attack and Prevention Using AODV on MANET" ISSN: 2319-8753 Vol. 3, Issue 5, May 2014

© 2015, IRJET.NET- All Rights Reserved