AMSE JOURNALS –2015-Series: Advances D; Vol. 20; N° 1; pp 35-46

Submitted April 2015; Revised Sept. 21, 2015; Accepted Nov. 30, 2015

Analysis of Black Hole and Gray Hole Attack in MANET based on Simulation through NS2

* J. K. Mandal , ** Khondekar Lutful Hassan

*Department of Computer Science and Engineering, University of Kalyani,
Kalyani, Nadia-741235, West Bengal, India, (jkm.cse@gmail.com)
** Department of Computer Science, Vidyasagar University,
Midnapore-721102, West Bengal, India, (klhassan@yahoo.com)

Abstract

In this paper simulation based analysis of Black and Gray hole attack has been performed in MANET. Ad Hoc On-Demand Distance Vector (AODV) routing protocol is taken as routing protocol and simulation has been carried out with Network Simulator 2(NS2.34). Node density and types of attack are considered for the purpose of analysis and comparisons based on variable node density and mobility. In all scenarios 5% nodes are taken as effected with each type of attacks. Performances analysis based on packet generated, average end to end delay, throughput, drop packet and goodput are made. Based on the analysis it is seen that Black hole attack affects the performance of a network more than a Gray hole attack.

Key words

Mobile ad-hoc network, MANET, NS2, AODV, Black hole Attack, Gray hole attack.

1. Introduction

Mobile Ad-Hoc Network (MANET1) [1,2,3,4] is combination of a set of mobile nodes, which is infrastructure less. Mobility is the main characteristics of MANET [1,2,3,4]. It is very difficult to maintain the security in MANET [1,2,3,4] than wired network because any node can enter the network and as well as leave the range of network at any moment. There are three types of routing protocol in MANET [1,2,3,4]. They are proactive routing protocol, reactive routing protocol and hybrid routing protocol. Proactive routing protocols create the routing tables before transmitting data. It is also called table driven routing protocol. DSDV [1,2,3,4] is the example of proactive routing protocol. Reactive routing protocols are those routing proctors which create the route when it is required or it create the route at the time of data transmission. AODV[1,2,3,4,7] is the example of reactive routing protocol. Hybrid routing protocol is the combination of reactive and proactive routing protocol. ZRP [1,2,3,4] is the example of hybrid routing protocol.

Ad-Hoc On Demand distance Vector (AODV) [1,2,3,4] is a reactive routing protocol which create the route at the time of data transmission. When a sender want to send data to the destination it will broadcast the RERQ (route request) message to its neighbor. In response of RERQ message RERP (route reply) message is received by sender for a valid routing path. With the help of RERP message sender node creates the route and sends data towards the destination. There are various types of attacks are possible in MANET [1,2,3,4].These attacks are classified broadly into two categories namely active attack and passive attack. Active attacks are those attacks which drop the packets and interrupt the data transmission in the network. Black hole attack and Gray hole attack are examples of this type of attacks. Passive attack is under the category where the attacker will not interrupt the network traffic but it will manipulate the data in the network. Snooping and Traffic analysis are examples of passive attack.

Black hole attack [9,10,11,13,14] is a kind of Denial-of-Service (DoS) attack where a sender sends a RERQ (route request) packets to create route at that time the malicious node replies to the sender with a false RERP (route reply) message as a request the sender node accept it as real route and interpreted that route has been discovered and it will ignore other RERP message which is send by original destination node, and sender node send the packets through the malicious node. Malicious node then drops all the packets. On the other hand the Gray hole [15,16] attack is also a kind of Black hole attack where the malicious node drops the selective packets. Here the malicious node act as normal node and drop the specific packets. So identifying of these types of malicious node is difficult. Gray hole attack has two phases, in the first phase the malicious node exploits the sender to advertise itself as having a valid route to a destination node like Black hole attack and in the second pass the malicious node drop the packets with the certain probability or selectively.

In this paper analysis of Black hole and Gray hole attack has been done through simulation of the same using NS2 environment.

Section two of the paper deals with the simulation environment. Section three deals with methodology. In section four, simulations Parameters are described. Section five deals with results, analysis and comparisons, and conclusion are drawn in the last section.

2. Simulation Environments

There are various tools for simulations of MANET. NS2 (2.34) [6,8] is taken as simulation for analysis. NS2 [6,8] is an event driven simulation tool for networking. It consists of two types of languages, C++ and Otcl. In the back end C++, which defines the internal mechanism of the simulation object, and the front end Otcl set up simulation by assembling and configuring objects as well as scheduling discrete events. On completing of each simulation it will generate two types of file one is trace (.tr) file, which is used for statically analysis and another is nam (.nam) which is used for graphical animation.

To configure Black hole and Gray hole attack, AODV [1,2,3,4,7,8]] routing protocol has been initiated in NS2 package. In NS2 package two replica of modified AODV routing protocol has been added, one for Black hole attack and another is for Gray hole attack. The attack of both types modified AODV has been added separately with AODV protocol within the TCL scripts.

3. Methodology

To configure Black hole and Gray hole attack in NS2, AODV routing protocol is cloned with BlackholeAODV and GrayholeAODV and both protocols is placed in the main folder of NS2 (/nsallinone/ns2.34/). For adding these protocols some major files of NS2 packages are modified and configured. On modifying and configuring those file of NS2 packages, make is performed for compilation. In BlackholeAODV "recv" function is defined in BlackholeAODV/BlackholeAODV.cc file. When "recv" function received a packet it will check whether the packet is management packets or data packets. If the packet is data packet then normal AODV function sends the packets to the destination but BlackholeAODV drop all the data packets as along as data packets come to that malicious node itself. Malicious node will check whether it is destination node or not. If it is destination node then it will drop the packets. BlackholeAODV check whether it is the management packet (RERQ) or not. If it is so then it will reply immediately with RERP packet by recvReply function. On the other hand same process is followed in GrayholeAODV partially for dropping selective packets. But in Gray hole attack sequence number is consider as destination sequence number which is considered as highest sequence number (4294967295) whereas in Grayhole attack sendReply(rq->rq_src) function is totally omitted .

4. Simulations Parameters

For the purpose of simulation six parameters are taken as common in each case. Table 1 shows the details of the parameters of the simulations

Table 1: Parameters (fixed) of the simulations

Routing protocols	AODV
Percentage of node mobility	40 %
Maximum packets in IFQ	50
Speed of the nodes	100 m/s
Time of simulation	10 sec
% of affected node	5% node

Number of nodes and type of attacks are taken as variable parameters .Maximum nodes is considered as 100 and that of minimum number of node is 20 and variation is made with gradation of 20. Two types of attacks are considered i.e. Black hole and Gray hole attack. A nam view of the simulation is shown in figure 1.

Variable parameters are

i. Number of nodes which varies from 20 to 100 using a difference of 20

ii. Types of attack : Black hole attack and Gray hole attack

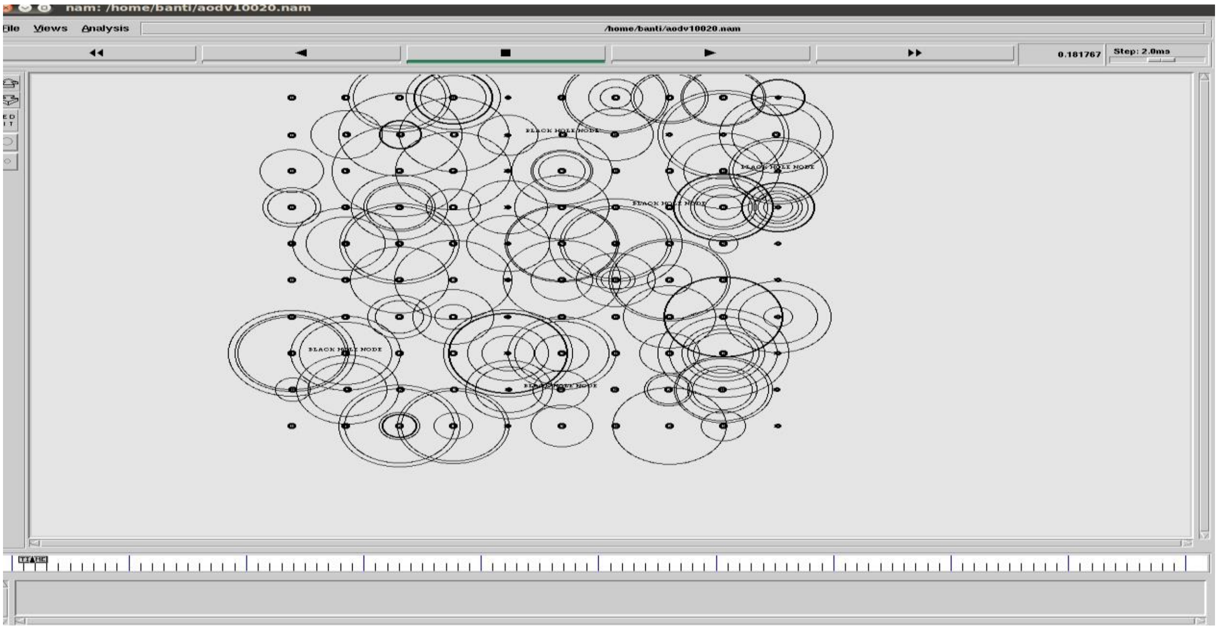

Fig.1. Snapshot of Simulation in Network Animator (NAM)

5. Results, analysis and Comparisons

Comparison of performance is measured with the following parameters.

i. *Generated packets* :Number of total packets generated by all nodes during the simulation time

ii. *Drop packets* : Number of total packets drop by all nodes during simulation times

iii. *Throughput at sender side* : rate of sending data(Bytes/sec) by all nodes in unit of times

iv. *Average End to End Delay* : average end to end delay by all nodes during the simulation time

v. *Goodput* : application level throughput (Bytes/second) in the receiving end

Results are obtained considering the variable parameters like number of nodes, types of attacks (Black hole and Gray hole). Numbers of nodes are taken 20, 40, 60, 80 and 100. Five percent of nodes have been taken as malicious. These are discussed in section 5.1 to 5.6

5.1 Generated Packet:

Various numbers of packets are generated during simulations of each scenario with different numbers of nodes. It is seen that number of generated packet is directly proportional to the number of mobile nodes. When node number is minimum number of generated packets is also minimum. When node number is maximum numbers of generated packets are also maximum. It is seen that network which is affected by Gray hole attack generates more packets than the network which is affected by Black Hole attack. As Black hole attack drops all type of packets as a result it will generate less packets. But Gray hole attack drop only the specific type of packets. Thus Black hole attack effect the performance of the network more than Gray hole attack. Figure 2 shows the total number of packet generated by all the nodes during simulation time (10 sec)

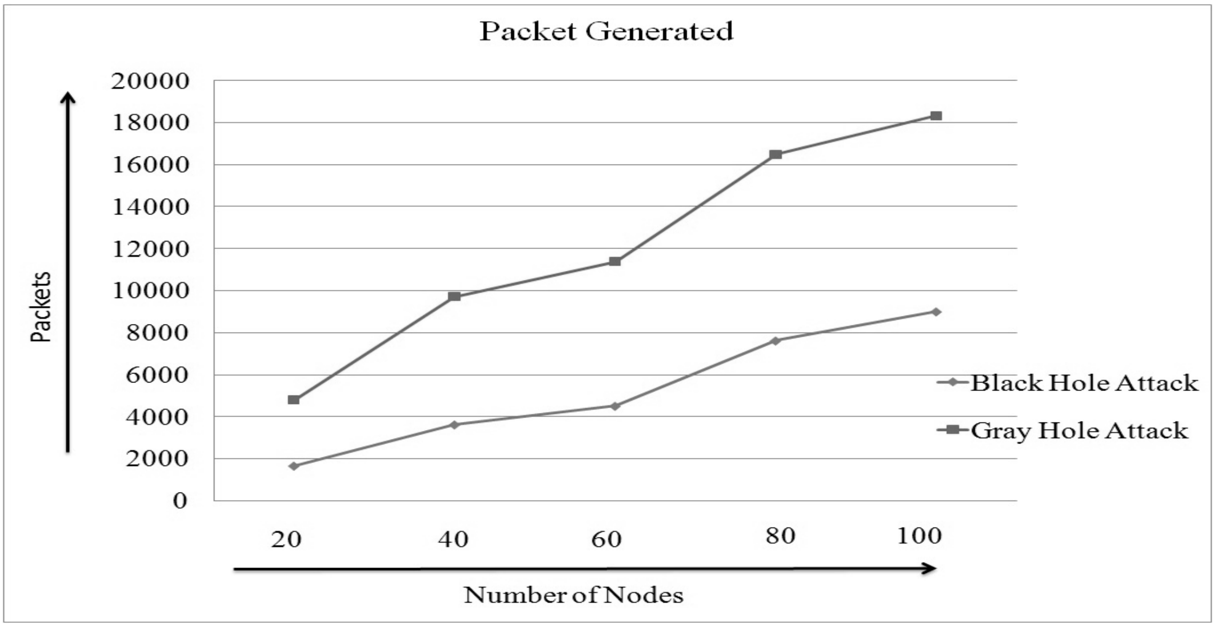

Fig.2. Comparison of total generated packets by all nodes in both type of attack

The Figure 2 shows that the network which is affected by Gray hole attack generated more packets than the Black hole affected network.

5.2 Drop Packet:

Various numbers of packets are generated during simulations of each scenario with various numbers of nodes. As Black hole attack drop all type of packets so it block the network traffic and various type of packets including management packets and acknowledgement packets also(from other node which sends the packets through the malicious node). Thus the total number of generated packets by the network affected by Black hole attack is less than by the network affected by Gray hole attack. So the total number of drop packets by the network which is affected by Black hole attack which is less than the network which is affected by Gray hole attack. Figure 3 shows the total number of drop packets by all nodes during simulation time (10 sec)

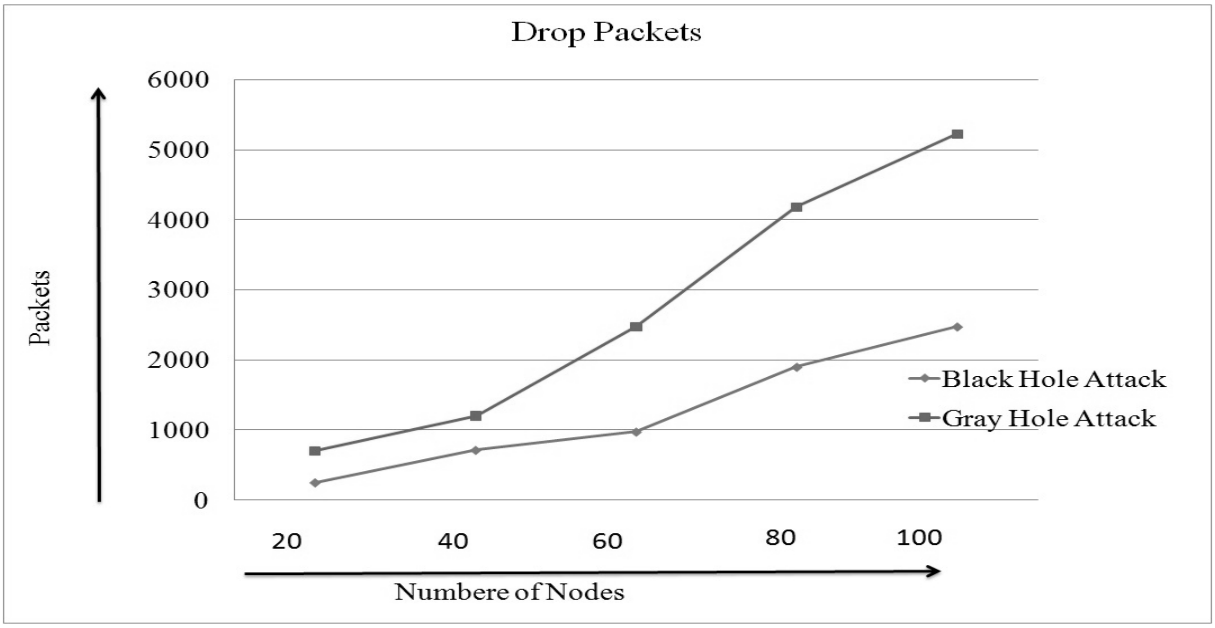

Fig. 3. Comparison of total number packets drop in both type of attack

Figure 3 shows that number of drop packets of the network which affected by Gary hole attack is higher than the network which is affected by Black hole attack.

5.3 Throughput at sender side:

Throughput at sender side is defined as the rate of sending data (Bytes/sec) by all nodes in unit of times. In Black hole attack the malicious node drop all type of packets which passes through it. In the other hand in Gray hole attack the malicious node drop specific type of packets(it may be control packet or data packets in probabilistic nature), so few packets passes through the malicious node. That is why the total communication breakdown in Black hole attack, but in Gray hole attack partial communication breakdown (due to dropping of specific type of packets in probabilistic nature). So through put of the network affected by Black hole attack is less than the throughput of the network affected by Gray hole attack. Figure 4 shows the throughput at sender side during simulation time (10 sec)

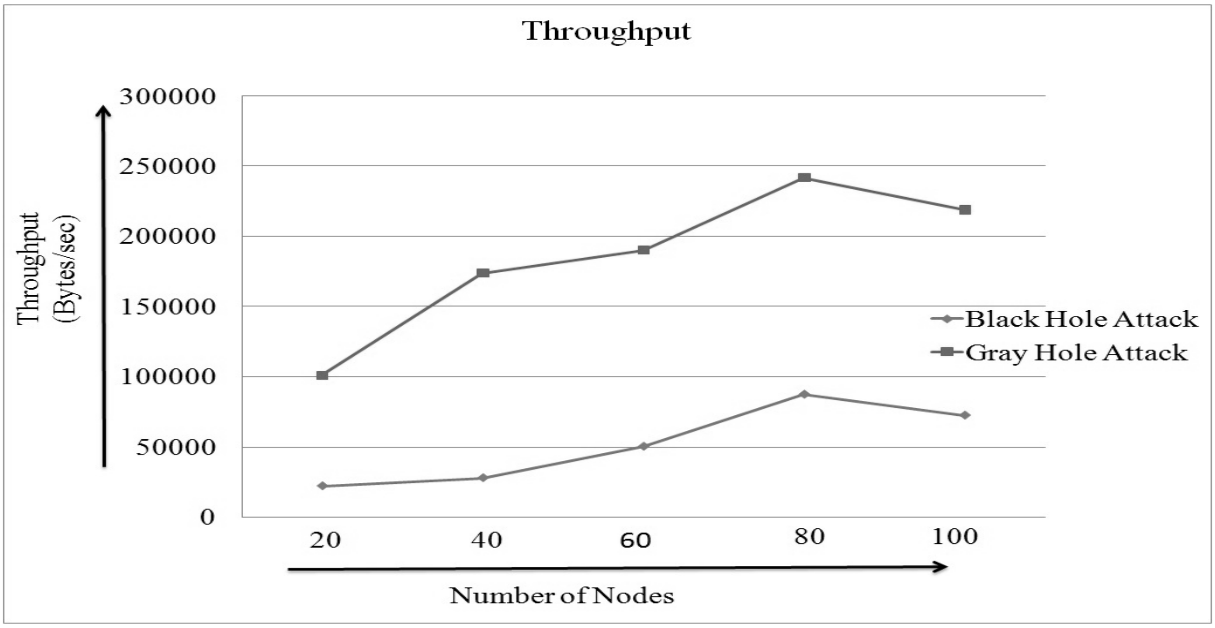

Fig.4. Comparison of throughput in sender side in both type of attack

Figure 5 shows the comparison of Throughput at the sender side within the network affected by both types of attacks. In the figure it is seen that throughput of sender side of the network affected by Gray hole attack is greater than the throughput of the sender of the network affected by the Black hole attack.

5.4 Average End to End Delay:

In Black hole attack when a packet reach to the malicious node it drops the packet instantly without taking any decision in the other hand when a packet reaches to the malicious node at that time it may drop that packet or forward that packets because Gray hole attacks belongs the nature of dropping of specific type of packets in probabilistic nature. So average end to end delay of the network which is affected by Black hole attack is less than average end to end delay of the network which is affected by Gray hole attack. Figure 5 shows the average end to end delay of the various simulations of both attacks.

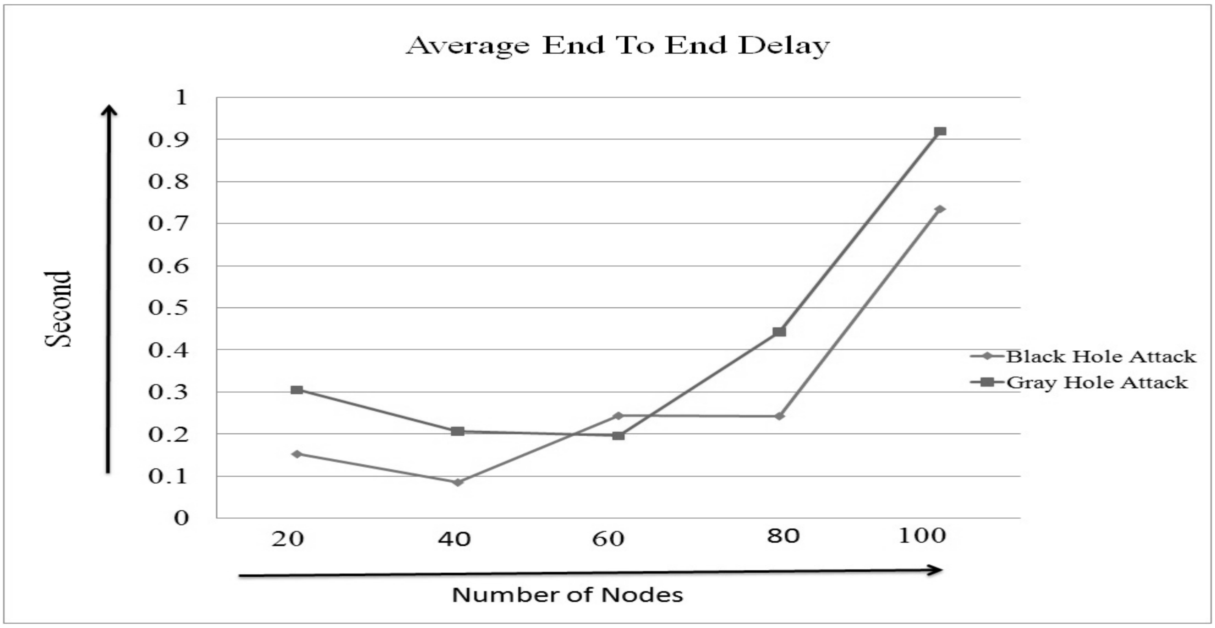

Fig.5. Comparison of average end to end delay in both type of attack

From the above figure 5 it is seen that average end to end delay in Gray hole attack is higher than Black hole attack. Only when the node number is 60 at that time average end to end delay of Black hole attack is a little greater than Gray hole attack. It can be happen due to other parameters, like mobility of the nodes.

5.5 Goodput:

Goodput is defined as application level throughput (Bytes/second) in the receiving end. In Black hole attack the malicious node drop all type of packets which passes through it. In the other hand in Gray hole attack the malicious node drop specific type of packets(it may be control packet or data packets in probabilistic nature), so few packets passes through the malicious node. That is why the total communication breakdown in Black hole attack, but in Gray hole attack partial communication breakdown (due to dropping of specific type of packets in probabilistic nature). So goodput of the network affected by Black hole attack is less than the goodput of the network affected by Gray hole attack like throughput at sender side .Figure 6 shows the goodput at the receiving end by all nodes of the network affected by both attacks.

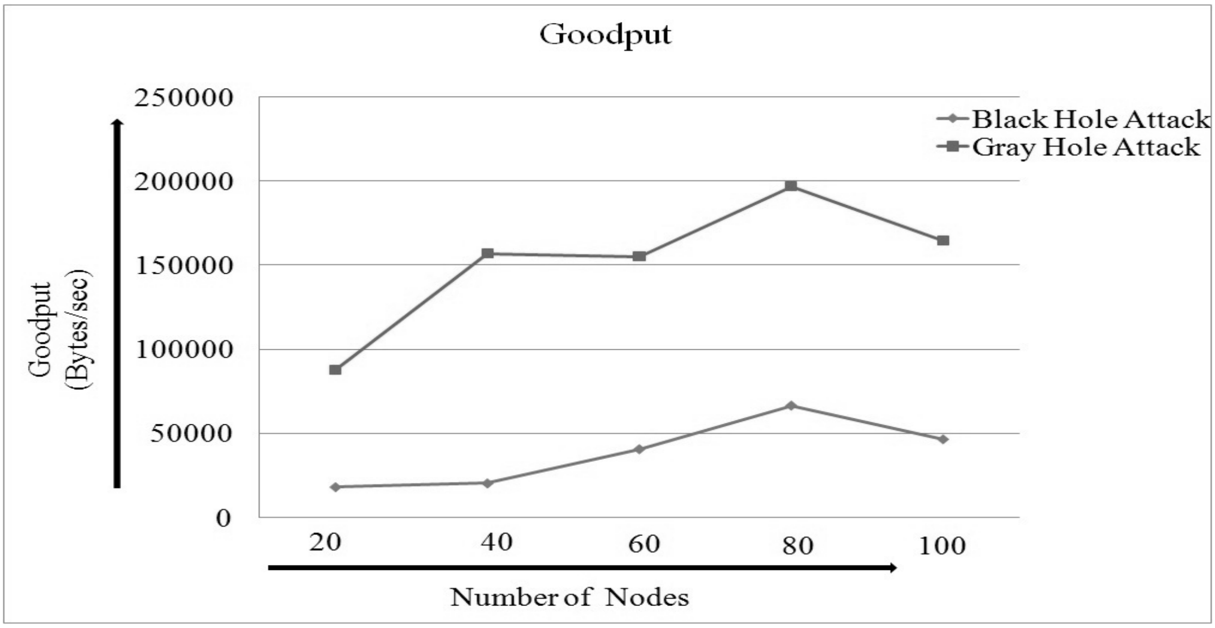

Fig.6. Comparison of goodput at receiving side in both type of attack

It is very much clear from figure 6 that good put of the network which is affected by Gray hole attack is higher than the good put of network which affected by Black hole attack

Conclusions

From the result and analysis it is seen that black hole attack is more effective than gray hole attack in any network, because Black hole attack drops all the packets which passes through the malicious node but in the other hand Gray hole attack drop the selective packets which passes through the malicious node. When a packet comes to the Black hole node it drop that packet immediately without justifying the packets in the other hand when a packet comes to the Gray hole node at that time the node will justify wheatear the packet is to be transmitted or dropped that is why the average end to end delay of the network which is affected by Gray hole attack is higher than the network which is affected by Black hole attack. Black hole attack breaks down the network traffic. As Gray hole attack drop selective packets so identifying of malicious node (Gray hole attack) is quite difficult than Black hole attack in the network.

Acknowledgements

The authors express deep sense of gratuity towards the Dept of CSE University of Kalyani where the computational resources are used for the work and the PURSE scheme of DST, Govt. of India

References

1. C.Siva Ram Murthy and B.S Manoj “Ad Hoc Wireless networks architecture and protocols” Pearson education, India, ISBN13:9780131470231, ISBN10:0-13-147023-X, 2004.
2. Chai-Keong Toh “Ad hoc mobile wireless networks: protocols and systems” Prentice Hall., ISBN13: 9780130078179, ISBN10: 0-13-007817-4, 2001.
3. Prasant Mohapatra, Srikanth Krishnamurthy “Ad hoc Networks: Technologies and Protocols” Springer, eBook ISBN: 0-387-22690-7 Print ISBN: 0-387-22689-3, 2005.
4. Sarkar, S.K., Basavaraju, T.G., Puttamadappa, C. “Ad hoc Mobile Wireless Networks: Principles, Protocols and Applications”. 1st ed. Auerbach Publications, Boca Raton (2008)
5. Amitava Mishra “Security and Quality of Service in Adhoc Wireless Network”, Cambridge University Press. ISBN-13: 9780521878241, 2008.
6. Teerawat Issariyakul, Ekram Hossain “Introduction to Network Simulator NS2” Springer ISBN-13: 978-1489986917, 2012.
7. Shanthi N, Ganesan L, Ramar K “Secure multicast route path formation in A-Hoc on-demand distance rector protocol.” AMSE journals; Advances D (Computer Science and Statistics), Vol. 15; N° 1-2, pp 30-44, 2010.
8. Mubashir Husain Rehmani, Sidney Doria, and Mustapha Reda Senouci “A Tutorial on the Implementation of Ad-hoc On Demand Distance Vector (AODV) Protocol in Network Simulator (NS-2)” Version 1 , 28th June 2009, http://arxiv.org/pdf/1007.4065v2.pdf ,(last access on 28.10.2015 at 11:54 P.M (GMT+5.30)). .
9. Dokurer, S. Ert, Y.M. ; Acar, C.E.” Performance analysis of ad-hoc networks under Black hole attacks”, 22-25 March 2007; DOI:10.1109/SECON.2007.342872 In proceeding of: SoutheastCon, Proceedings. IEEE, Richmond, Varginia, pp. 148 – 153, 2007.
10. Ananthakumaran, S, Vidhyalakshmi M, Angel A “A secure randomized routing selection strategy against black hole attack” journal of Computer Science and Statistics , Association for the Advancement of Modelling and Simulation Techniques in Enterprises (AMSE) , France, Vol. 16 N° 1-2, Issue 2 , 2011.
11. Dr.J.K.Mandal and Khondekar Lutful Hassan“A Novel Technique to Detect Intrusion in MANET” International Journal of Network Security & Its Applications (IJNSA), ISSN 0974 - 9330 (Online);0975 - 2307 (Print), Vol.5, No.5, September 2013.

12. Deng H, Li W, Agrawal D,"Routing Security in Wireless Ad Hoc Networks" IEEE Communication Magazine (October 2002) pp. 70-75, 2002.

13. Al-Shurman, M., Yoo, S., Park, S., "Black hole Attack in Mobile Ad Hoc Networks", 42nd Annual Southeast Regional Conference (2004) Huntsville, Alabama, Pp. 96-97, April 2 – 3, 2004.

14. Usha, Bose “Understanding Black Hole Attack in Manet” European Journal of Scientific Research, ISSN 1450-216X Vol.83 No.3 (2012), pp.383-396.

15. V. Shanmuganathan, Mr.T.Anand “A Survey on Gray Hole Attack in MANET” International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501Vol.2, No6, December 2012.

16. Nisha,Simranjeet Kaur, Sandeep Arora “Analysis Of Black Hole And Gray Hole Attack On RPAODV In MANET” International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181. Vol. 2 Issue 8, Pp-192-196 August – 2013.