International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878
Volume 1 Issue 3, November 2013

Performance Analysis of Mobile Ad Hoc Network in the Presence of Sink Hole attack

Nisha Puri[1], Simranjit Kaur[2], Sandeep Kumar Arora[3]

[1, 2] SSCET, PTU University, Badhani, Pathankot, India

[3]LPU, LPU University, Phagwara, Jalandhar, India

Abstract: ***A mobile ad-hoc network (MANET) is an example of wireless mobile communication. It is a temporary network set up by the collection of multi-hop and self-configured mobile nodes without any network infrastructure or access points. Due to its unique characteristics such as dynamic topology, infrastructureless, node mobility, self-configured and self-organizing makes it different from other networks but these types of networks are more vulnerable to various security threats. One of the major security attacks is denial of service (DoS) attack. In this paper we study the effects of two types of DoS attacks namely gray hole attack and black hole attack in MANET using reactive routing protocol. Due to gray hole attack and black hole attack in the network there is an impact on the different performance metrics of the network such as throughput, packet delivery ratio and normalized routing load. All simulation is done by network simulator (NS-2).***

Keywords: MANET, AODV, Gray hole attack, Black hole attack, NS-2.

1. Introduction

Mobile Ad Hoc Network is one kind of new wireless network. A MANET is an infrastructure-less network consisting of set of mobile nodes or mobile devices, communicate with each other via shared wireless medium. It is self-configuring network, means there is no dedicated router, each node act as a router as well as host because of absence of centralized administration. Unlike traditional Wireless LAN solutions, all nodes are movable and the topology of the network is changing dynamically in an Ad Hoc Networks, which brings various challenges to the security of Ad Hoc Network. As a result, attackers can take advantage to carry out various attacks. Black hole attack and gray hole attacks are two classical attacks [1] under Ad Hoc networks, which could disturb operation of routing protocol and bring enormous damage to the network's topology.

The paper is organized as follows: Section 2 gives details about related work on security of MANET by routing attacks. Section 3, describes fundamental working of AODV routing protocol. Section 4 we sink hole Attack. Section 5 provides methodology for adding malicious code in AODV and 6 presents the simulation set up and performance metrics. Sections 7 discuss important results analysis and Section 8 describes the conclusion and the direction for future work.

2. Literature review

The whole life cycle of mobile ad-hoc networks can be characterized into first, second and third generation. The history of wireless ad-hoc networks can be traced back to 1970's. The packet radio networks (PRNET) was the first ad-hoc network system in 1970. In the early 1980's, the PRNET is evolved into survivable adaptive radio networks (SURAD) programs to providing packet switched networking in infrastructreless environments. By growing interest in ad-hoc networks, more developments took place in 1990's onwards. Lidong Zhou et. al. [2] analyzes the security threats an ad hoc network faces and presents the security objectives that need to be achieved. On the other hand, ad hoc networks are inherently vulnerable to security attacks. It take advantage of the inherent redundancy in ad hoc networks - multiple routes between nodes - to defend routing a against denial-of-service attacks. Animesh Patcha et. al. [3] he presents some extensions to the watchdog concept in scenarios where there is no a priori trust relationship between the nodes. The Black hole attack is an important problem that could happen easily in ad hoc network especially in popular on demand protocols like the Ad hoc On-demand Distance Vector routing. Gonzalez et al [4] presents a methodology, for detecting packet forwarding misbehavior, which is based on the principle of flow conservation in a network. The problem of security and cooperation enforcement has received considerable attention by researchers in the ad hoc network community. Sukla Banerjeez et. al. [5] shows how address the problem of packet forwarding misbehavior and propose a mechanism to detect and remove the black and gray hole attacks. Technique is used is capable of finding chain of cooperating malicious nodes which drop a significant fraction of packets. He proposed a feasible solution for detection and removal of chain of cooperative black and gray hole attack in AODV protocol. Ashok M. Kanthe, et. al. [6] Explain that MANET is vulnerable to different types of DoS attack in which packets are drop. Black hole attack, packet drop attack and gray hole attack are an event that eliminates a network's capacity to perform its expected function**.** He proves that the numbers of malicious nodes are increases the performance on the MANET goes down.

In [7], authors explained about various attacks in AODV like black hole, DDoS, malicious node etc. and discussed about security issues in MANETs, code implementation of the said

attack in AODV and provided solutions to prevent these attacks.

3. Fundamental Working of AODV

AODV belongs to the class of distance vector (DV) routing protocol. It is one of the most popular reactive routing protocols. AODV also known as pure on-demand routing protocol because route create only when a node has data to transmit to other nodes. Due to its features life dynamic self-starting, multi-hop routing, quick aging, link breakages efficiently repaired, it most widely used in networks. AODV uses sequence number i.e. created by destination for maintaining each route entry. A requesting node always selects that route which has highest sequence number. AODV protocol contains 3 set of message types like route request (RREQ), route reply (RREP) and route error (RRER). These messages are control messages used for establishing a path to the destination. When a source node wants to transmit or communicate with other node, it broadcasted RREQ messages across the network. This control message is forwarded to the neighbours, and those node forward the control message to their neighbours' nodes. If any intermediate node has the path to the destination with a sequence number equal to or greater than the last known sequence number indicated by the RREQ source it generates a route reply (RREP) message and sends to source node only if it is destination node and route become active to the destination. Once the route is established between nodes they can communicate with each other. If a link breaks down while route is active then the node upstream of the break, propagates a RRER message to source node to inform it of the now unreachable destination. After receiving RRER message by the source node, it generates a new RREQ message [8]. HELLO messages are used for broadcasting information, detecting and monitoring links to neighbours.

4. Sink Hole Attack

Sinkhole attack is one of the severe attacks in wireless Ad hoc network. In sinkhole Attack, a compromised node or malicious node advertises wrong routing information to produce itself as a specific node and receives whole network traffic. Gray hole attack and black hole attack are most popular examples of sink hole attack.

4.1 Gray Hole Attack

The gray hole attack is also a kind of Denial of service (DoS) attack. Gray hole attack is an extension of black hole attack in which malicious node behaviors and activities are exceptionally unpredictable. Gray hole attacks is an active attack type, which lead to dropping of messages. It is act as a slow poison in the network side means we can't say that probability of losing the data. In gray hole attack, a malicious node misleads the network by agreeing to forward the packets in the network. As soon as malicious node receive the packets from the neighboring node and simply drops them [9]. In this type of attack, attacker selectively drops the packets originating from a single IP address or a range of IP addresses and forwards the remaining packets. In MANETs gray hole nodes are very effective.

4.2 Black Hole Attack

A black hole attack is an active denial of service attack in which a malicious node can attract all packets by falsely claiming a fresh route to the destination and then absorb them without forwarding them to the destination. In black hole attack, a malicious node advertises itself for having the shortest path to the destination node in order to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request message and thus intercept the data packet and retain it. There are two types of black hole attack can be described in AODV in order to distinguish the kind of black hole attack.

- **Internal black hole attack -**In this type of black hole attack has an internal malicious node which fits in between the routes of given source and destination. As soon as it gets the chance this malicious node make itself element of an active data route.
- **External black hole attack**- External attacks physically stand outside of the network and try to access network traffic or creating congestion in network or by disrupting the process of entire network

5. Methodology

The implementation phase of the Gray hole and Black hole behaviour to the AODV protocol written using C++. In this project, the nodes that exhibit gray hole and black hole behaviour in wireless ad-hoc network used AODV protocol. All routing protocols in NS are installed in the directory of "ns-2.35". The project was started by duplicating AODV protocol in this directory and changing the name of directory as "grayholeaodv". Names of all files that are labelled as "aodv" in the directory are changed to "grayholeaodv" such as grayholeaodv.cc, grayholeaodv. h, grayholeaodv.tcl, grayholeaodv_rqueue.cc, grayholeaodv_rqueue.h etc. in this new directory except for "aodv_packet. h". All classes, functions, structs, variables and constants names in all the files in the directory except struct names that belong to AODV packet.h code are changed. After the above changes, two common files that are used in NS-2 are changed globally to integrate new grayholeaodv protocol to the simulator. The First file modified is "\tcl\lib\ ns-lib.tcl" where protocol agents are coded as a procedure as shown in figure 5.1.

Second file which is adapted is "*makefile*" in the root directory of the "**ns-2.35**". After all implementations are ready, we have to compile NS-2 again to create object files. We have added the below lines in figure 5.2 to the "*makefile*" for gray hole attack. After all implementations are ready, NS-2 is compiled again to create object files. So far, a new routing protocol which is labeled as gray hole

AODV was implemented. We used same scenarios for black hole AODV as we used for gray hole attack.

```
grayholeAODV {
set ragent [$self create-grayholeaodv-agent $node]
}
Simulator instproc create-grayholeaodv-agent { node } {
set ragent [new Agent/grayholeAODV [$node node-addr]]
$self at 0.0 "$ragent start" # start BEACON/HELLO
Messages
$node set ragent_ $ragent
return $ragent
}
```

Figure 5.1: "grayholeaodv" protocol agent is added in "\tcl\lib\ ns-lib.tcl"

```
grayholeaodv/grayholeaodv_logs.o grayholeaodv/grayholeaodv.o \
grayholeaodv/grayholeaodv_rtable.o grayholeaodv/grayholeaodv_rqueue.o\
```

Figure 5.2: Addition to the "*makefile*" for gray hole attack

6. Simulation Set Up and Performance Matrices

6.1 Simulation Environment

The simulations were performed using Network Simulator-2 (NS-2.35). Mobility scenarios are generated by using a Random waypoint model by varying 20 to 40 nodes moving in a terrain area of 600m x 600m. We setup 1 Mbps IEEE 802.11 protocol at the MAC layer, AODV protocol at the network layer with the random way point model at the physical layer. CBR agents are used to simulate normal and attack traffic. The MANET environment is summarized in Table 1.

6.2 Performance Metrics

For performance comparison, we considered various types of performance metrics for our evaluation. In our work, we use only three performance parameters. They are as follow:

Table 1: MANET Environment

Property	*Values*	*Description*
Channel type	Wireless channel	Channel used
Propagation model	Two ray ground	Radio propagation model used
Antenna type	Omni antenna	Type of antenna
Interface queue type	Drop Tail/PriQueue	Queue used
MAC type	802.11	MAC layer protocol used
Maximum packets in queue	50	Packets in Queue
Topology area	600m*600m	Area of simulation
Mobility scenario	10 m sec^{-1}	Nodes' mobility
Mobility model	Randomwaypoint	For mobility of nodes

- **Average Throughput:** It is measured as the ratio of amount of received data to the amount of simulation time. A higher throughput implies better QoS of the network. The throughput is measured in bits per second (b/s).
- **Packet Delivery Fraction-** Packet delivery fraction is calculated by dividing the number of packets received by the destination through the number of packets originated by the application layer of the source (i.e. CBR source).

Packet Delivery Fraction=Dr/Dt

- **Normalized Routing Load-** Normalized routing load is the ratio between the total numbers of packets transmitted from routing layer of the source to the total number of packets received at the application layer of the destination. It characterizes the protocol routing performance under congestion. NRL is determined as:

NRL = Pc/Pd

7. Result Analysis

This paper mainly focusing on the effect of gray hole attack or black hole attack on MANET. Result is analyzed by the comparing the performance metrics of the normal AODV, gray hole attack & black hole attack.

7.1 Evaluation of Throughput for Normal AODV, Gray hole and for black hole attack

Throughput is defined as amount of data transferred from sender to receiver in a given amount of time. In this, throughput is calculated for the network in normal condition, then in the presence of the attacks. Throughput values for 20, 30 and 40 nodes for normal AODV, grayholeaodv and for blackholeaodv are plotted in graph as shown in figure 7.1. Based on simulation results we can analyze that, the throughput of network under black hole and gray hole attacks decreases when compared to the network under normal conditions because of the packets discarded by the malicious node.

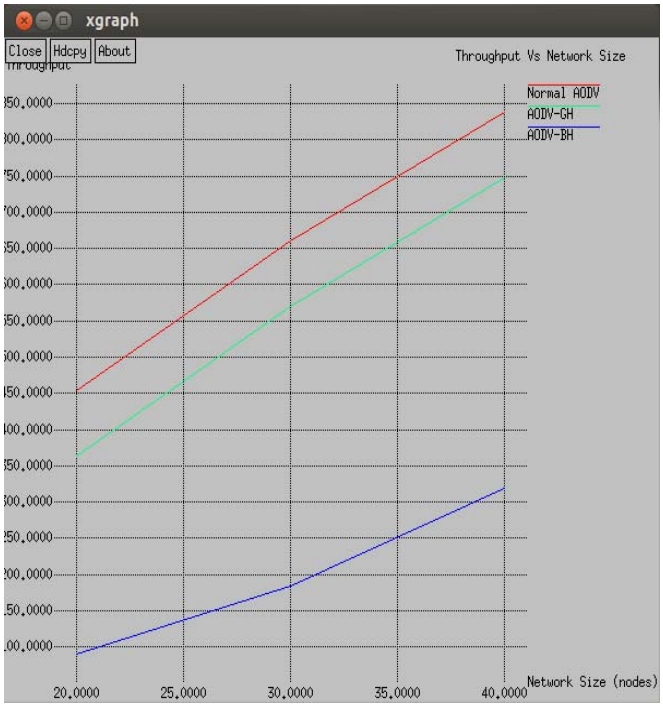

Figure 7.1: Comparison of Throughput

7.2 Evaluation of Packet delivery ratio for Normal AODV, Gray hole and for black hole attack

Packet delivery fraction in case of attacks and without attack depends on the protocol routing procedure and number of nodes involved. PDR is calculated by considering number of nodes 20, 30 and 40 for different routing protocols are plotted in graph as shown in figure 7.2.

Figure 7.2: Impact of attacks on PDR

The average results from the comparison diagram show the PDR decreases to 12% from 100% for 20 nodes, 28% for 30 nodes and 35% for 40 nodes when the IDS is implemented PDR increases to nearby 98% for all number of nodes. It means that PDR value of network in normal condition is higher than the network under attack.

7.3 Evaluation of Normalized routing load for Normal AODV, Gray hole and for black hole attack

In this normalized routing load values for 20, 30 and 40 nodes for normal AODV, grayholeaodv and for blackholeaodv are plotted in graph as shown in figure 7.3.

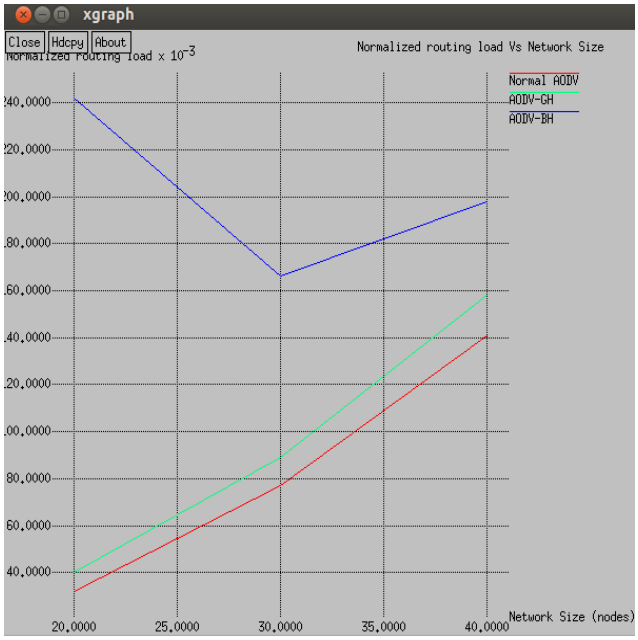

Figure 7.3: Comparison of routing load

From the Fig. 6.3, it can be visualized that due to the black hole in the network it generates unnecessary routing packets due to which ROH is more under attack condition.

8. Conclusion and Future Scope

Mobile ad hoc network (MANET) has been gained attention from past few years due to its application in military, disaster management and civilian communication. But it poses various security issues than traditional networks due to its unique characteristics such as open medium, lack of centralized monitoring, dynamic topology, lack of central management etc. in this paper, we analyzed the impact of gray hole attack and black hole attack on the AODV routing protocol. The analysis is done by using highly reliable and commercial tool like NS-2. Here we summarize the network performance in the case of normal AODV protocol, Gray hole attack and black hole attack. During implementing attack on AODV, we realized the weakness of AODV. From simulation results it can be concluded that throughput value in the normal condition is higher than the network under attack. It means network working level is better in normal condition. As similar we see in the case of packet delivery ratio, PDF is lies between 90% to 100% without attack but when attack is applied it decreases and routing load is very lower in normal condition than under attack. From analysis

we observed that network performance in the case of gray hole is better than in the presence of black hole attack. In future work, we will focus on detecting and preventing other malicious attack in MANET. This proposed method will implement by using NS-3 simulation tool which is easy to understand than NS-2.

References

[1] Y.C. Hu; A. Perrig, A Survey of Secure Wireless Ad Hoc Routing[J], IEEE Security and Privacy, 2(3), 28-39, May 2004.R. Caves, Multinational Enterprise and Economic Analysis, Cambridge University Press, Cambridge, 1982. (book style)
[2] L.Zhou and Z.Haas, "Securing ad hoc network (1999)," IEEE Network Magazine, Special issue on network security, Vol. 13, No. 6, pp. 24-30.
[3] Animesh Patcha (2003), "Collaborative Security Architecture for Black Hole Attack Prevention", in Radio and Wireless Conference, pp. 490-495.
[4] Oscar F. Gonzalez, Michael Howarth, and George Pavlou, "Detection of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks", Center for Communications Systems Research, University of Surrey, Guildford, UK. Integrated Network Management, 2007. IM '07. 10th IFIP/IEEE International Symposium on May 21, 2007.
[5] Sukla Banerjee (2008), "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks" Proceedings of the World Congress on Engineering and Computer Science WCECS 2008, San Francisco, USA, October 22 – 24.
[6] Ashok M.Kanthe, Dina Simunic and Ramjee Prasad (2012), "Effects of Malicious Attacks in Mobile Ad–hoc Networks", IEEE International Conference on Computational Intelligence & Computing Research (ICCIC), pp. 1-5.
[7] Harris Simaremare and Riri Fitri Sari," Performance Evaluation of AODV variants on DDOS, Blackhole and Malicious Attacks", IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.6, June 2011.
[8] Mr. L Raja 1, Capt. Dr. S Santhosh Baboo (2013)," Comparative study of reactive routing Protocol (AODV, DSR, ABR and TORA) in MANET", International Journal of Engineering and Computer Science, ISSN: 2319-7242 Volume 2 Issue 3, pp. 707-718.
[9] Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG and Ning LIU (2010), "An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network", 24th IEEE International Conference on Advanced Information Networking and Applications, pp. 775-780.

Author Profile

Nisha Puri received her Bachelor Degree in ECE from RIEIT, Railmajra, PTU University, INDIA in 2010. She is also pursuing a Master Degree in ECE from SSCET, Badhani, PTU University. Her fields of interest include computer network and mobile ad-hoc network.

Simranjit Kaur received Bachelor degree in ECE from GNIT greater Noida, INDIA in 2007 and Master degree in ECE from DIET Kharar INDIA in 2012. She has 4 years teaching experience. Her research area includes optical communication and computer networks.

Sandeep Kumar Arora received Bachelor degree from CTIEMT Jalandhar in 2008 and Mater degree from LPU Jalandhar (2012), INDIA. He is Assistant Professor in LPU. He has 2 years experience as a network administrator in LPU (2008-2010), 1.5 years experience as a lecturer in Rayat and Bahra Engineering. College (2010-2011). His research area includes Computer and Wireless Networks, Network Security, Traffic Engineering, Ad-hoc networks.