Volume 2, No. 4, July-August 2011
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Implementation and Comparison of Black Hole and Gray Hole Attack in Wireless Mesh Network

Hina Wadhawan*
Department of Computer Science
Punjab Technical University
Mohali, India
hinawadhawan@gmail.com

Sandeep Kang
Department of Computer Science
Punjab Technical University
Mohali, India
cecm.cse.skang@gmail.com

Sahil Seth
Department of Computer Science
PEC University of Technology
Chandigarh, India
sahilseth.cs08@pec.edu.in

***Abstract*:** This paper analyzes the black hole and gray hole attack which are the possible packet dropping attacks in wireless mesh networks. In a black hole attack, a malicious node makes all the traffic travel through it, claiming to have the shortest route to all other nodes in the network and instead of forwarding the packets, a malicious node simply drops it. In a gray hole attack (selective forwarding attack) where a misbehaving mesh router just forwards a subset of the packets it receives but drops the others. In this paper we have shown that there is 100% packet loss and there is rigorous decrease in throughput and network performance as compared to gray hole attack. Simulations are done using Qualnet 5.0.

***Keywords*:** Black hole attack, gray hole attack, Wireless mesh networks (WMN).

I. INTRODUCTION

Wireless mesh networks are all about access to information. We generally access information from cell phones, TV, broadband, web browsers etc. but it is quite difficult to access information from the physical world. Taking example of a commercial building. A building has different sensors that people use to control to provide safety, security and energy efficiency. Sensors like temperature sensors, lightening sensors, energy consumption sensors, access control sensors and all these sensors are grounded to a central location where that information is used to reduce energy cost but the problem is getting access to this information becomes quite expensive due to cost of buying simple cells and then getting it installed. Also services like paint, dry walling increase expenses. So, WMN is a system that is connected to any kind of LAN or office LAN, access point(AP) and sensors that has distributed topology and these devices are connected to one to the next to the next to give a reliable wireless network. It is reliable because each device in a network has built in redundancy and talk to his neighbor.

WMN has emerged as a promising concept to meet the challenges in next-generation networks such as providing flexibility, adaptive and reconfigurable architecture while offering cost-effective solutions to providers [1][5]. It is different from traditional Wi-Fi networks in which each access point (AP) is connected to a wired network while in WMNs only a subset of the APs are required to be connected to a wired network. As shown in Figure1, the APs that are connected to the wired network are called the Internet Gateways (IGWs), while the APs that do not have wired connections are called the mesh routers. IGWs are further connected to the mesh routers using multi-hop fashion [2].

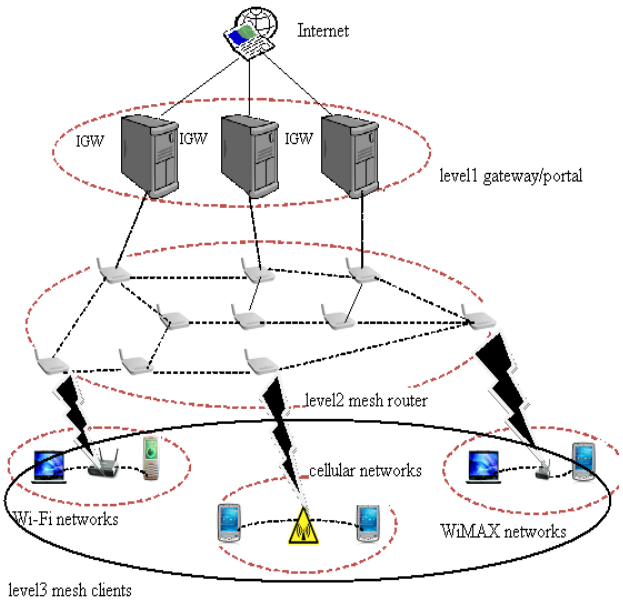

Figure1: The hierarchical architecture of a WMN

In multi-hop wireless networks, the packets from source to destination passes through one or more intermediate nodes. All nodes act as a router itself and there is no need for a base station or any specific architecture. Hence multi-hop wireless networks are also known as infrastructure-less networks. Some multi-hop networks include ad-hoc networks, sensor networks and WMNs [4].

Compared to wired networks, the WMNs are more likely to suffer from various packets dropping attacks, due to the inherent features such as open medium, dynamic topology and distributed architecture. These networks have been used in numerous applications such as in home networking, community and neighborhood monitoring, security and surveillance systems, disaster management and rescue operations etc [5][6].

A. Outline

This paper is based on the implementation of black hole and gray hole attack in wireless mesh networks. In Section II we discuss related work. Section III describes about Packet Dropping Attacks. Section IV presents methodology for wireless mesh networks. Section V explores the simulation results. Section VI finally gives the conclusion and discussion of future work of this review paper.

II. RELATED WORK

Jaydip Sen et al [8] presented an efficient algorithm for detection of selfish packet dropping nodes in wireless mesh networks. In this algorithm, a statistical theory of inference-based clustering is used for detection of selfish nodes in a WMN.A finite state machine model is developed on the AODV routing protocol based on the local observation in each node. To increase the reliability of clustering, an ANOVA test is applied and finally a new cross-checking mechanism is used by inserting extra fields in the AODV packet headers. This algorithm has better detection efficiency and reduced false alarm rates.

Yu Cheng [11] proposed a practical algorithm channel aware detection (CAD) to detect and isolate the selective forwarding attackers in the area of multihop networks such as WMNs. CAD mainly adopts two strategies for detection: hop-by-hop loss observation by downstream nodes and traffic monitoring by upstream nodes.

Nishant Sitapara [10] analysed the effect of the blackhole in an Ad-hoc On demand distance vector routing protocol (AODV). For this purpose, an implementation of an AODV protocol is done that behaves as blackhole in NS-2 (Network Simulator version). He simulated five scenarios where each one has 20 nodes that use AODV protocol and also simulated the same scenarios after introducing one blackhole node into the network.

Sukla Banerjee [9] proposed a mechanism to detect and remove the black hole and gray hole attacks. This technique is capable of cooperating malicious nodes which drop a significant fraction of packets in AODV protocol. In this technique, each node can locally maintain its own table of black listed nodes whenever it tries to send data to any destination node and it can also aware the network about the black listed nodes. This list of malicious nodes can be applied to discover secure paths from source to destination by avoiding multiple black/gray hoe nodes acting in cooperation.

III. PACKET DROPPING ATTACK

Packet dropping attack is basically a category of Denial of Service (DoS) attack. It occurs when a mesh router drops all of the packets or some of the packets.
Packet dropping attack consists of two types:

A. Black Hole Attack:

The malicious node always replies positively to a Route Request although it may not have a valid route to the destination.

Almost all the traffic within the neighborhood will be directed towards the malicious node, which may drop all the packets. Network performance degrades badly[4].

B. Gray Hole Attack:

In Gray Hole Attack, malicious node can selectively drop some of the packets instead of forwarding them to proper node. Performance degradation is inversely proportional to the percentage of packet dropping [3][9].

IV. METHODOLOGY

IEEE 802.11s defines a standard routing protocol called Hybrid Wireless Mesh Protocol (HWMP) for mesh networking which has following features:

A. It is based on Radio-Metric AODV (Ad-Hoc on-demand distance vector routing) (RF-3561) and Tree-based Routing.
B. It supports both broadcast/multicast and unicast delivery using “radio-aware metrics” over self-configuring multi-hop topologies.
C. It helps in congestion control and power save[7].

V. SIMULATION RESULTS

We have simulated an experiment to show packet dropping attack in Figure 4:

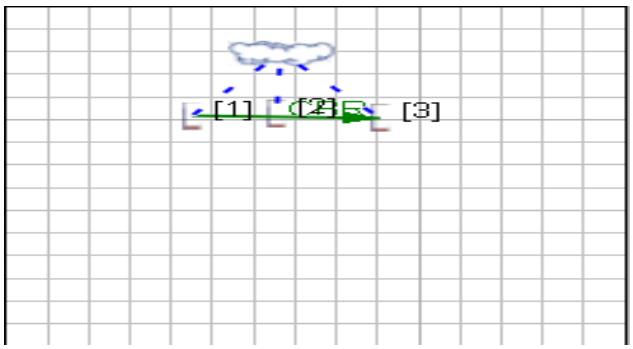

Figure 2: Simulation environment

Black hole attack is being performed since packets sent by the client has not been received at server end.

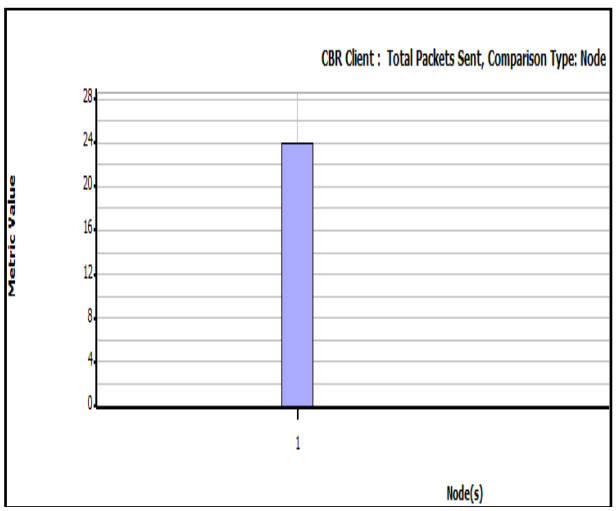

Figure 3: Total packets sent by client

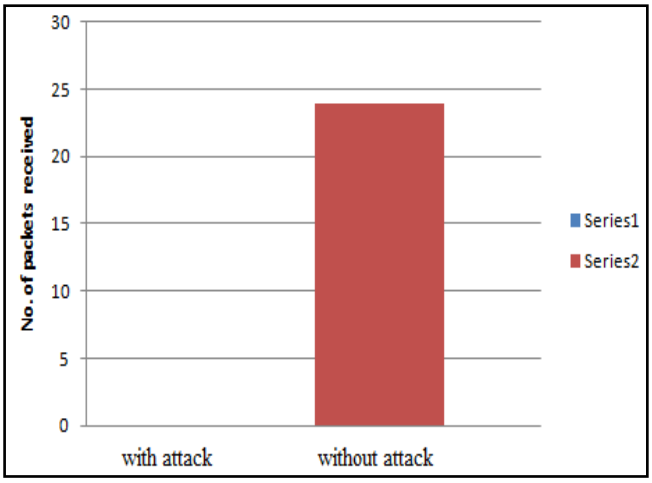

Figure 4: Black hole attack

Gray hole attack is being performed since some packets have been received at server end while some packets are being dropped by the intermediate node. Network performance is directly proportional to the percentage of packets dropped.

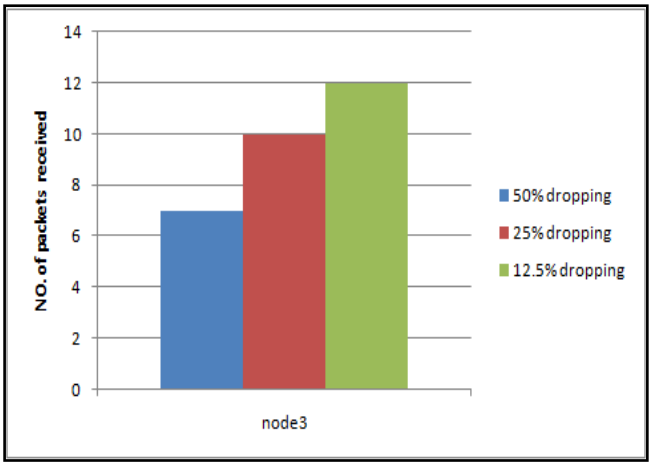

Figure 5: Packet loss on gray hole attack

Throughput:

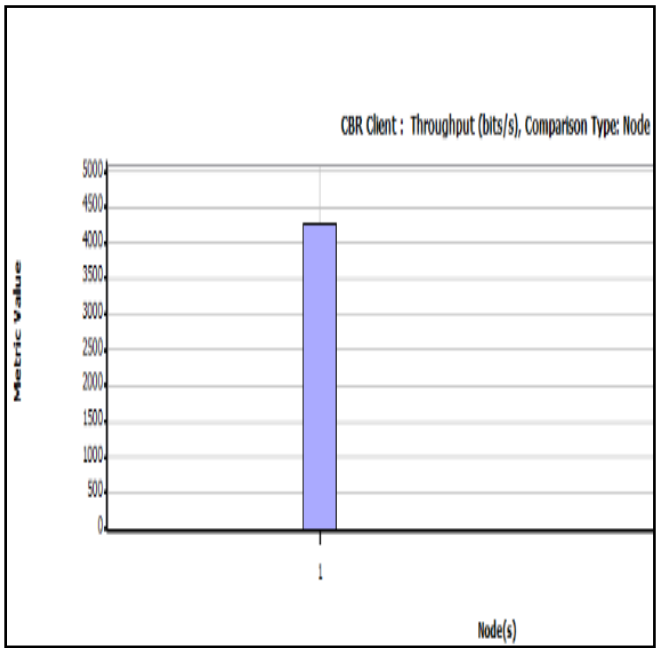

Figure 6 **:** Throughput sent by client

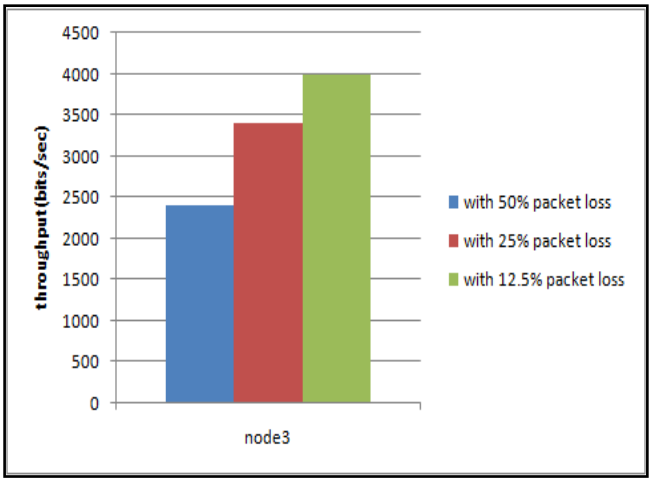

Figure 7 : Throughput by server on gray hole attack

A. Metrics

We evaluate our results using the following four metrics:

a. Data Packet Loss: Amount of packets dropped by the malicious node.

b. Throughput: This is the percentage of sent data packets actually received by the intended destinations.

VI. CONCLUSION

In this paper, we considered watchdog monitoring mechanism to implement black hole and gray hole attacks in the area of multihop networks such as WMNs. All the simulations presented in this paper use CBR data sources.
Our simulation results shows that there is increase in throughput in gray hole attack than in black hole attack. So network performance degrades badly in case of black hole while in case of gray hole, performance is inversely proportional to the amount of packet dropped. Also there is increase in overhead in black hole attack.

These results show that we can gain the benefits of an increased number of routing nodes while minimizing the effects of misbehaving nodes.

VII. FUTURE WORK

We simulated the black hole attack and gray hole attack in wireless mesh networks and investigated its effects. After implementing both the attacks now we need to develop the Intrusion detection system(IDS) for it.

VIII. REFERENCES

[1] Akyildiz, I.F.;Xudong Wang "A survey on wireless mesh networks" in communications Magazine,IEEE Volume 43, Issue 9,Page(s): S-23-S30,Sep 2005.

[2] Sahil Seth, Anil Gankotiya, Amandeep Jindal,"A Comparitive Study between Wireless Local Area Networks and Wireless Mesh Networks",2010.

[3] Anil Kumar Gankotiya, Sahil Seth, Gurdit Singh,"Attacks and their Counter Measures in Wireless Mesh Networks",2010.

[4] I.F Akyildiz,X.Wang and W. Wang,"Wireless Mesh Network: A survey", Computer Networks and ISDN Systems, Volume 47,Issue 4,March 2005.

[5] http://www2.cs.uh.edu/~rzheng/course/C0SC7397 /sp07/cunqing.ppt.

[6] Jangeun Jun, Mihail L. Sichitiu,"MRP: Wireless Mesh Networks Routing Protocol",Department of Electrical and Computer Engineering, North California State University.

[7] Prasant Mohapatra,"Wireless Mesh Networks", Department of Computer Science ,University of California,Davis.

[8] Jaydip Sen,"An Efficient Algorithm for Detection of Selfish Packet Dropping Nodes in Wireless Mesh Networks", International Journal of Computer Information Systems and Industrial Management Applications,ISSN 2150-7988 Vol3(2011) pp. 363-370.

[9] 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,WCECS 2008,October 22-24,2008, San Francisco, USA.

[10] Nishant Sitapara,"Detection and Prevention of Black Hole Attack in Mobile Ad-Hoc Networks",International Conference on Emerging trends in engineering organized by J.J. Magdum College of Engineering,Jasingpur",2010.

[11] Yu Cheng,Devu Manikantan Shila and Tricha Anjali, "Channel-Aware Detection of Gray Hole Attacks in Wireless Mesh Networks", Dept. of Electrical and Computer Engineering,Illinois Institute of Technology, Chicago,USA,2009.

.

