Elimination of Gray Hole Attack in Wireless Mesh Network by Enhanced Multipath Security Approach

Renu Bala [1], Sarika[2]

M-Tech Student[1,] Assit. Prof. [2] & Department of CSE
Delhi Institute of Technology, Management & Research
Faridabad, Haryana, India

***Abstract*— Wireless mesh network is a wireless communication among various nodes which are self-configured and self-organized in a dynamic manner. The nodes in the network mechanically demonstrating an ad-hoc network and holding the mesh connectivity, nodes interact with each other by propagating data packets to other network nodes. But in comparison of wired networks, WMNs are greatly prone to various security attacks because of its distributed architecture, open medium nature, and dynamic configuration. DoS attacks are most general attacks in networks which link to internet and since WMNs are primarily designed for long and fast distance internet access. We primarily focus our study on gray hole attacks in our work. Wireless mesh networks are composed of both mesh clients and mesh routers. We limit our studies to static mesh routers. We carry out gray hole attack in mesh routers and study the network delivery ratio without and with the existence of attack routers. By modeling the scenario with AODV protocol we analyzed the delay and throughput of packets and determine how it is influencing the network in the existence of an attacker router. After analyzing the results we suggest a new detection and prevention algorithm depending on overhearing the adjacent node to which the packet is propagating. By holding the past knowledge of number of packets routed and the number of packets overheard the algorithm finds out the number of packets lost and find the possibility of attack. This probability is examined with the threshold value of probability and finds out whether a router is behaving badly or not. We also taken into account the possibility of false positives and considered essential measures in the algorithm to minimize it. If a router is detected behaving badly it is discarded from the network and barred from further propagating the packets. We examine our algorithm in the existence of an attack router and determine the attack router and study the enhancement in the delivery ratio. By simulation we measure and enhance the WMN performance by considering our algorithm utilizing delay and throughput as an performance metrics.**

Keywords: DOS, AODV, WMN, GH

I. INTRODUCTION

Wireless mesh networks (WMNs) provide multi-hop wireless interaction between different nodes which are self-configured and self-organized in a dynamic way. WMNS are developed as a promising idea to fulfill the issues in wireless networks i.e. adaptability, flexibility, reconfigurable architecture etc [1]. WMNs are composed of two types of nodes: mesh clients and mesh routers. Mesh routers are routers which makes the static or minimum mobile part of the mesh network with less power constraint and make the important part of the mesh network. Mesh clients are nodes which are not static in the network with power constraints. Since mesh clients can also perform routing by propagating packets to the adjacent node in mesh networking, the software and hardware platform are much simpler for them as compared to mesh routers. Mesh routers can perform all the bridge/gateway functions similar to traditional wireless router, it also have extra functions to support mesh routing. They can provide support to multiple wireless interfaces made on either the different or same wireless access technologies. Therefore mesh routers are devoted and static nodes for routing functions with low power constraint. Mesh clients are nodes which do not perform bridge/gateway functions and only one wireless interface is required in mesh clients. Wireless mesh networks can be combined with other networks due to the gateway/bridge functions offered by the mesh router. The availability of mesh routers and hop by hop propagation in WMNs provide several benefits in comparison of traditional ad-hoc network i.e. low up-front cost, easy network maintenance, higher scalability, reliable, robustness and require less transmission power. A wireless mesh network makes capable ad-hoc mode peer to peer interconnection between mesh clients are known as client meshing [1]. With client meshing, mesh routers that remain beyond the radio coverage of a mesh router can depend on other intermediary clients to pass packets to them to obtain WMN access network connections. Therefore packets from a mesh client which remains far away from the mesh router has to traverse multi hop client-to-client and client-to-router wireless connection before arriving its destination node. The number of hops is found by the geographical position of the client and also the configuration structure of the access network. The wireless mesh networks architecture can be categorized in to three important groups depending on the functionalities of the nodes such as client WMNs, infrastructure/backbone WMNs, and Hybrid WMNs. In infrastructure WMNs wireless mesh routers will make a mesh of self-organizing, These routers can be linked to the internet with gateway functionality. This method offers backbone for traditional clients and enables combination of WMNs with available wireless networks, through bridge/gateway functionalities in mesh routers.

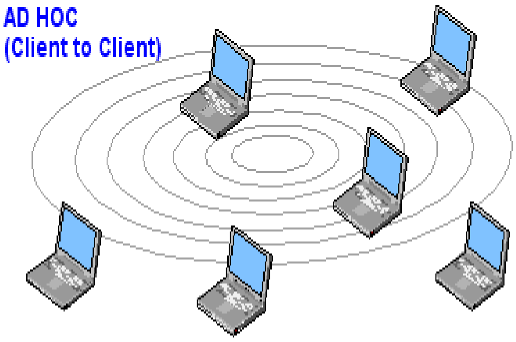

Figure 1 Wireless Mesh Network

II. GREY HOLE ATTACK

In gray hole attack, a node that is a part of the network, receives RREQ packets and forms a path to destination node. After forming the path, it losses some of data packets. This type of dropping against Gray hole does not loss all data packets. Attacker drops packets sometimes. It means attacker sometimes behaves like a normal node and other times as a harmful node.

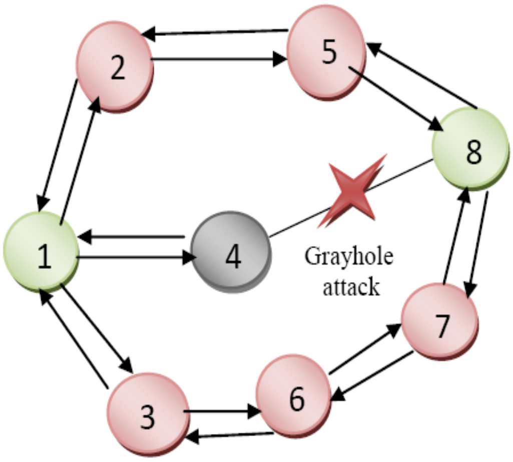

Figure 2: Gray Hole Attack

The Gray Hole attack has two stages. Firstly, a harmful node feats the AODV protocol to populate itself as having a legal path to a destination, with the objective of disrupting packets, even though the path is unauthentic. Secondly, the node drops the disrupted packets with a limited possibility. This attack is more complicated to determine as compared to the Gray Hole attack where the harmful node drops the obtained data packets with surity. A Gray Hole may show its harmful behavior in several techniques. It simply losses packets coming from (or destined to) certain particular node(s) in the network while propagating all the packets for another nodes. Another kind of Gray Hole attack is a node acts harmfully for some specific time duration by losing packets but may switch to normal behavior after some time. A Gray Hole may also show a behavior which is a integration of the above two, thus forming its detection even more complicated.

III. PROBLEM STATEMENT

Formerly the works performed on security issues such as attack (Gray Hole attack) included in WMN were based on reactive routing protocol i.e. Ad-Hoc On Demand Distance Vector. Gray Hole attack is analyzed under the AODV routing protocol and its impacts are worked out by telling how this attack affects the WMN performance. Very less attention has been provided to the fact to study the effect of Gray Hole attack in WMN employing both proactive and Reactive protocols in very large number of nodes.

IV. RELATED WORK

Marti et al. [2] introduced a method that utilizes Path rater and Watchdog to determine black hole attacks. The Watchdog makes capable neighboring nodes to overhear and determine harmful nodes. Watchdog forms it possible to determine harmful nodes by determining nodes that are intentionally dropping packets. Path rater allocates a default value to every node and then analyzes the transmitting behavior of every node. The value for every node changes depending on the node transmitting behavior. After some time, if the value for a node is below a particular threshold, the node will be summed to the list of black hole nodes. These techniques have the similar defection to detect harmful node, when the neighboring node react wrong observing message. In other way, this technique cannot manage collaborative attacks. If the neighboring nodes collude with each other, they may be able to avoid detection.

Lu et al. [3] suggested the SAODV black hole detection strategy for MANETs that is planned to present some of the security issues of AODV and withstand black hole attacks.
Deswal and Singh [4] generated an improved version of the SAODV protocol that involves password security for each of the routing nodes and routing tables that are modified depending on timeliness.

Ramaswamy et al. [5] suggested a mechanism for detecting multiple black hole nodes. They were the first to suggest a solution for cooperative black hole attacks. They slightly changed the AODV protocol by presenting a Data Routing Information (DRI) table and a cross checking method. Every entry of the node is kept by the table. This mechanism utilizes the reliable nodes to transport the packets.

V. METHODOLOGY USED

This research is related to offering solution for the gray hole problem by employing multipath algorithm resulting in finding of the mean no. of hops by barring the attacker nodes. Research has began with generating a WMN in the OPNET modeler by employing Random Waypoint mobility Model for offering mobility with AODV as routing protocol Basic simulation parameters such as speed of nodes, buffer size, mobility rate energy carrying capacity and average error rate for AODV have been utilized that described in Table 1. Random waypoint model is used for mobility of all nodes and the trajectory chosen for the nodes movement is Vector.

Table 1: Simulation Parameters

Examined Protocols Cases	AODV with and without Gray Hole Attack
Number of Nodes	100 and 150
Types of Nodes	Vehicular
Simulation Area	55*55 km
Simulation Time	1800 seconds
Mobility	Uniform(50-100) m/s
Pause Time	100 seconds
Performance Parameters	Throughput, Delay, Network load
No. of Gray Hole Node	10
Trajectory	VECTOR
Data Type	Constant Bit Rate (CBR)
Packet Size	1024 bytes
Traffic type	FTP, Http
Active Route Timeout(sec)	3
Hello interval(sec)	1,2
Hello Loss	3
Timeout Buffer	2
Physical Characteristics	Extended rate IEEE 802.11g (OFDM)
Data Rates(bps)	54 Mbps
Transmit Power	0.005
RTS Threshold	1024
Packet-Reception Threshold	-95
Performance Parameters	Throughput, Delay, Network load
Trajectory	VECTOR
Long Retry Limit	4
Max Receive Lifetime (seconds)	0.5
Buffer Size(bits)	25600

VI. RESULTS

After showing the general results of all simulations conducted in both scenarios we examine and talk about all these results. The performance metrics gathered and shown in our results are either depending on the global statistics or object statistics of the WMN model i.e. the whole network.

6.1 Throughput:

A high throughput is absolute need in each network. In figure the graph sows the throughput in bits/ seconds. The x-axis represents the simulation time in minutes and the y-axis represents throughput in bits/ seconds.

In first scenario of 100 nodes of work, packets travels are represented as throughput with maximum value of nearly 825367 bits per seconds and it is measured as bits per second. In second scenario which is with gray hole attack, packets drops which are shown as throughput, reduces to value of nearly 99815 bits per second. . In first scenario of 150 nodes of our work, packets travels are represented as throughput with maximum value of nearly 35345630 bits per seconds and it is shown as bits per second. In second scenario which is with gray hole attack, packets loss which are shown as throughput, reduces to value of nearly 1522434 bits per second.

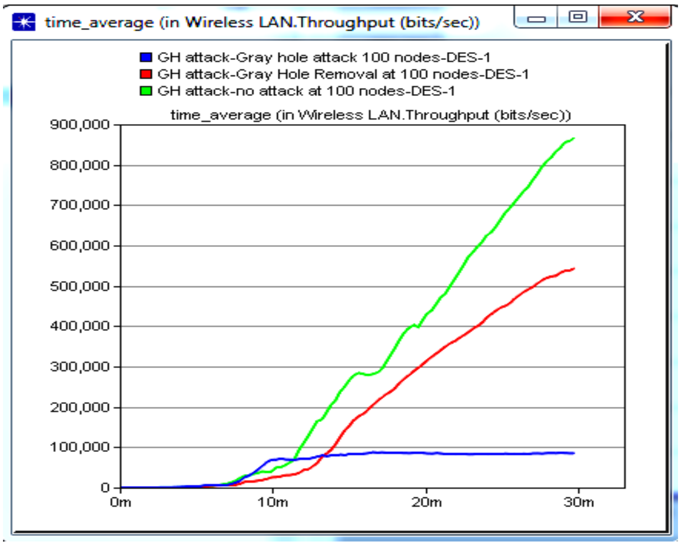

Figure 6.1 Throughput of all three scenarios at 100 nodes

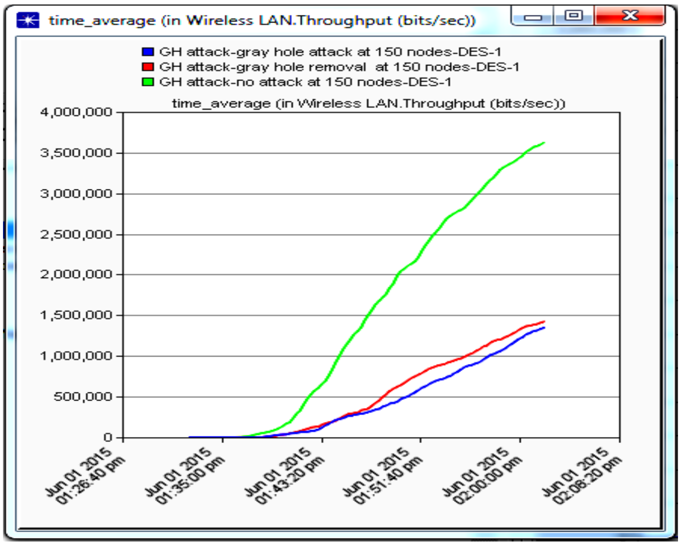

Figure 6.2 Throughput of all three scenarios at 150 nodes

6.2 End to End Delay:

In first scenario of 100 nodes of our work, packets Delay are represented as figure 5.3 with maximum value of nearly 0.459 seconds. In second scenario which is with gray hole attack, packets delay Increases to value of nearly 0.00030 seconds. In first scenario of 150 nodes of our work, packets delay are nearly 0.001 seconds. In second scenario which is with gray hole attack, packets delay increases to value of nearly 0.25 seconds.

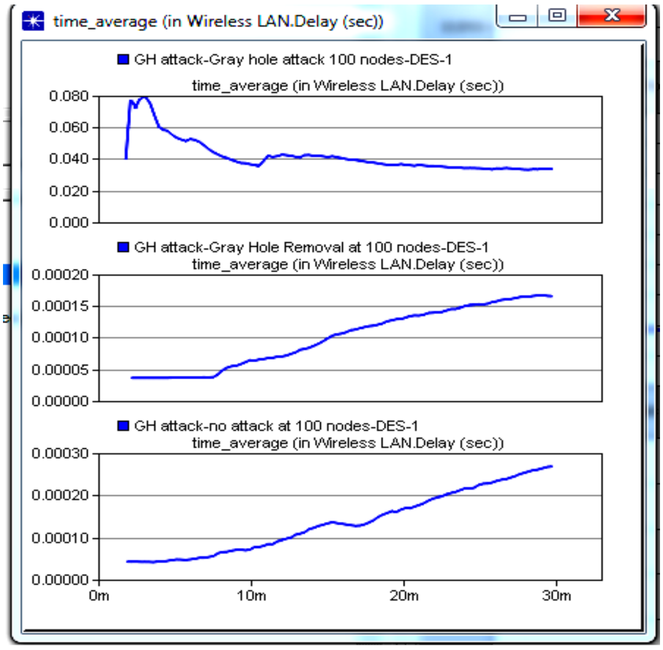

Figure 6.3 Delay of all three scenarios at 100 nodes

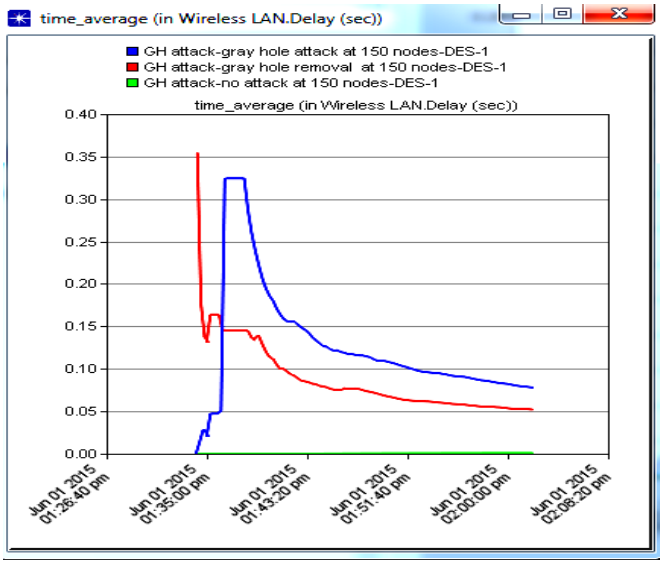

Figure 6.4 Delay of all three scenarious at 150 nodes

CONCLUSION AND FUTURE SCOPE

With the significance of Wireless Mesh Networks (WMN) relative to its broad potential still it has many issues left in order to resolve. Security of WMN is one of the significant characteristics for its deployment. In our work we suggested a feasible solution for the AODV protocol. The primary concern of this work to show the AODV performance under normal environment, under gray hole attack and performance after removal of gray hole attack in term of throughput, delay and traffic obtained. The performance of network with gray hole attack in order of throughput reduces around bits per second. By our suggested method, we have regained around in throughput. The performance of network with gray hole attack in order of end to end delay increases around 12% and with our suggested method, we have regained around 10% in delay. Concept has represented enhanced results after removal of the gray-hole attack in the simulation. Removal of harmful nodes occurs on Network layer by flooding the information of harmful nodes. Overall, removal of gray hole attack has been performed so that ad-hoc interaction can be normalized as normal interaction. It will be very significant in preserving a lot of resources for mobile ad-hoc communication as we have utilized unicasting process rather than broadcasting which preserves resources as harmful nodes are only determined through partial multicasting method.

REFERENCES

[1] Uma mani, Ramasamy chandrasekaran and V. R Sharma" Study and analysis of routing protocols in Vehicular ad hoc networks" in Proceedings of Journals of Computer science, 2013, pp. 1519-1525.

[2] Chen Y. S., Y. W. Lin, and S. L. Lee, "A mobicast routing protocol for Vehicular ad hoc networks," in Proceedings of ACM/Springer Vehicular Networks and Applications, Vol. 15, 2010, pp. 20-35.

[3] Skordylis A. and Trigoni N., "Delay-bounded routing in Vehicular ad-hoc networks (WMN)," in Proceedings of ACM International Symposium on Vehicular Ad hoc Networking and Computing, 2008, pp. 3020-3026.

[4] Tonguz, J. S. Parikh, F. Bai, P. Mudalige, and V. K. Sadekar, "On the broadcast storm problem in ad hoc wireless networks," in Proceedings of International Conference on Broadband Communications, Networks and Systems, 2006, pp. 1-11.

[5]Tonguz, F. Bai, P. Mudalige, "Broadcasting in WMN," in Proceedings of IEEE Vehicular Networking for Vehicular Environments, 2007, pp. 7-12.

[6] Amit Kumar Saha, David B. Johnson. "Modeling mobility for Vehicular ad-hoc networks". In Proceedings of the first ACM workshop on Vehicular ad hoc networks. Philadelphia, PA, USA, Oct. 2004, pp. 22-34.

[7] Shastri A., R. Dadhich and Ramesh C. Poonia" Performance analysis of on-demand routing protocols for Vehicular ad hoc networks" in Proceedings of International Journal of wireless and Vehicular networks, Vol. 3,2011, pp. 103-109.

[8] Yamaguchi H., K. Yukimasa, and S. Kusumoto, "QOS routing Protocol for Vehicular ad hoc networks," in Proceedings of IEEE International Workshop on Quality of Service, 2006, pp. 132-139.

[9] Pooja Gupta and Rajesh Kumar Tyagi" A significant study and comparison of DSDV, AODV and DSR protocols in WMN using NS-2" in Proceeding of International Journal of Engineering Research and technology, Vol. 2, Issue 3, 2013, pp. 1-8.

[10] Vidhale, B., Dorle, S.S., "Performance Analysis of Routing Protocols in Realistic Environment for Vehicular Ad Hoc Networks," In Proceedings of Systems Engineering (ICSEng), 2011 21st International Conference on , vol.2, Aug. 2011, pp.267-272.

[11] Artimy M.M., W. Robertson, and W. J. Phillips. "Connectivity in inter-vehicle ad hoc networks". In Proceedings of Engineering Canadian Conference on Electrical and Computer, Volume: 1, May 2004, pp. 110-112.

[12] Zhao J. C. and Josh Broch "Vehicle-Assisted Data Delivery in Vehicular Ad Hoc Networks" in Proceedings of 25th IEEE International Conference on Computer Communications. Proceedings, April 2006, pp. 6-12

[13] Saha A. K. and Johnson D.B., "Modeling the mobility for Vehicular ad hoc networks(WMN)," In Proceedings of The ACM International Workshop on Vehicular Ad Hoc Networks,2004, pp. 91-96.

[14] T. Taleb, E. Sakhaee, K. Hashimoto, N. Kato, and Y. Nemoto, "A stable routing protocol to support ITS services in WMN networks," In Proceedings of IEEE Transactions on Vehicular Technology, Vol. 56, 2007, pp. 3337-3347.

[15] Naumov V. and Gross T., "Connectivity-aware routing (CAR) in Vehicular ad hoc networks," in Proceedings of IEEE International Conference on Computer Communications, 2007, pp. 1919-1927.