



Detection and Prevention of Gray Hole Attack in MANET

Pooja Jangra¹ and Chander Diwakar²

Department of Computer Science & Engineering
University Institute of Engineering and Technology
Kurukshetra University, Kurukshetra
INDIA

¹poojajangra012@gmail.com, ²chander_cd@rediffmail.com

Abstract: A MANET (mobile ad hoc network) is an association of mobile nodes collaborates in packets which are sending on in a multi hop manner with no centralized administration. There is no right security solution for MANET that is why it is prone to attacks. The harmful node in the network will behave as a strong node which produce the selective forwarding attack named as gray hole attack. In this a new PSO technique is simulated. This technique observe and remove gray hole attack and evaluation of this is done using some parameters like packet delivery ratio, end-to-end delay and throughput of the network.

Keywords: Gray hole, MANET, routing protocols, node.

I. Introduction

An accumulation of several mobile nodes sustaining the capability to exchange information with each other without any fixed infrastructure is known as MANET (Mobile Ad-hoc Network). The nodes in the ad-hoc networks are collected of self-managed nodes which grasp a dynamic topology which can merely link up or leave the network at any time. The nodes are directed in decentralized modes which signify no central authority, self-organizing, self-managing networks and also capable of modeling a communication network [1].

In a MANET, mobile nodes admit and route traffic from their intermediate nodes to the target, intends the nodes can work as both routers and hosts. A lot continual connection conceited and re-consistency commit an energy restriction on the mobile nodes [2].

Its routing protocol's expertness is determined by its battery power usage of a node contribution and routing of traffic into the network [3].

MANET is a mobile multi-hop which is wireless shared network and self-organized in character. The main idea of routing protocol is to find the route. The routing protocol for MANET begins to establish and keeps up routes between nodes [4]. In MANET, breaking of link and non-validation of an end-to-end route passes due to continuously switching network topology. There is extremely dynamic character of wireless network allots drastic limitations about routing protocols [5].

II. Gray Hole vs. Black Hole Attack

A change in the black hole attack is the gray hole attack, in which the nodes will drop the selecting packets. Selective forward attack is of two sorts they are [6]:

- i) Forwarding the TCP packets and dropping UDP packets
- ii) Dropping half of the packets or dropping them with a probabilistic distribution. These are the attacks that look to disturb the system without being distinguished by the efforts to establish security.

III. Literature Review

Jain *et al.* [7], proposed an algorithm to observe a chain of cooperative harmful nodes in ad hoc network which interrupts broadcasting of data by generating false routing information along with detection algorithm. The author as well proposed an algorithm to observe and wipe out the black hole and gray hole attack in MANET. In this work the complexity of network is improved.

Arya and Jain [8], proposed a methodology using three different protocols and then differentiating results. Each protocol being simulated utilizing the uniform parameters which is throughput, routing load and packet delivery ratio between different protocols with certain simulation to produced correct results. Another goal is to find the performance and QoS of the various matrices and overcome the destroyed packet and drop fee, Transmission expenses of these three matrices and compare with the AODV protocols.

Jhaveri *et al.* [9], proposed a mechanism in which an arbitrate node getting defective routing data by its neighbour node believes that neighbour node as a malicious node. Once routing call is broadcast, a number of malicious nodes are affixed to the packet and all nodes getting the packet advances its routing table to assure the enrolled

node as malicious. Afterwards controlling nodes routing table; the node thus assures additional nodes not to believe the routing data getting from the malicious node.

Kanthe *et al.* [10], a mechanism is planned on practice the efficient techniques to allowing the security in AODV in opposition to grey hole attack. This mechanism is operated to discover the grey hole attack and terminate the fresh nodes with the higher sequence number value to get into the black list. Once the process of route discovery initiates, the nasty nodes are being recognized. To make the mechanism more efficient, execution of new approach of current elapsed and effective use of peak value is considered.

Kumar and Chawla [11], applied a detection based algorithm when numerous one malicious nodes are introduced in mobile ad hoc network. The algorithm holds three steps. In initial step it puts the RREP packet on preceding node. Second step assures two hop distance of a distrusted node and third step holds the rejection of RREP packet. Kariya *et al.* [12], proposed an adaptive technique to observe malicious node in MANET supported cross-layer design in a network layer and a course-based technique to overhear the adjacent hop's valid activity. For execution of this algorithm it is necessary for all nodes to keep up a packet digest buffer called as FwdPacketBuffer. Once the packet is sent away, its digest is brought into the FwdPacketBuffer and the observing node overhears. When the process that the adjacent hop sends on the packet is overhead, the digest will be released from the FwdPacketBuffer. In a limited time period, the observing node ought to figure out the overhear rate of its adjacent hop and equate them with a threshold.

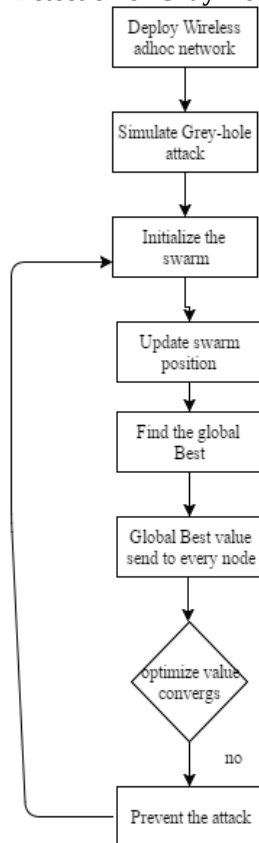
Makwana and Vaghela [13], proposed an algorithm which observes and eradicates gray hole attack applying dynamic credit based technique using AODV routing protocol. The gray hole node are observed based on credit value which step-ups and step-downs. The simulation outcomes are equated with distinct position and undertake to make better operation of AODV protocol for various parameters like packet delivery ratio, throughput and end-to-end delay. Afterwards, analyze the performance parameters of the network.

Dhaka *et al.* [14] proposed an outline in which broadcasting a control sequence to the nearest nodes and then awaiting the nodes response then based on that response observing the harmful nodes. In this looked into different existing solutions and present a novel approach to anticipate these harmful attacks that efficiently finds out short and safe route to the destination.

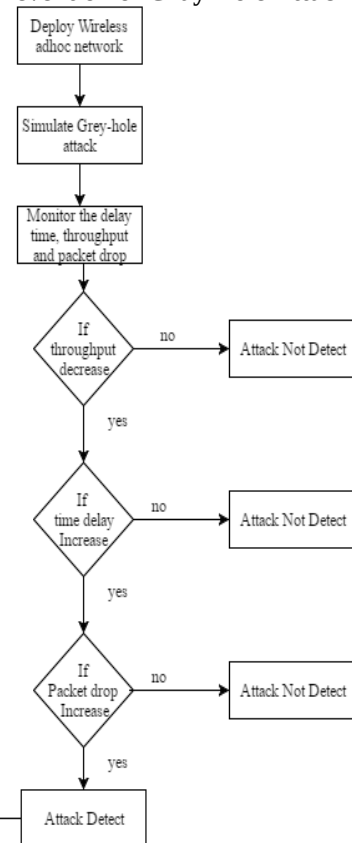
IV. Proposed Work

The proposed work contains the PSO technique to observe and eliminates the Gray hole attack. The simulation process includes the various parameters which evaluates the performance of the network with and without gray hole attack in MANET.

a. Detection of Gray Hole Attack



b. Prevention of Gray Hole Attack



The parameters which are applied to examine the performance are network throughput, packet delivery ratio and end-to-end delay in the network.

V. Simulation Analysis

In this chapter, concentrates on the outcomes and the analysis is depends on the simulation executed on NS2 simulator. To evaluate the behavior of stimulated Grey-hole attack, considered the performance metrics of the packet delivery ratio, End-to-End delay and throughput.

i) *Packet Delivery ratio*: Packet drop is considered for 10 nodes in this simulation process. The packet delivery ratio with and without the attack is shown in figure below.

Fig 1.1 Packet delivery ratio (with attack)

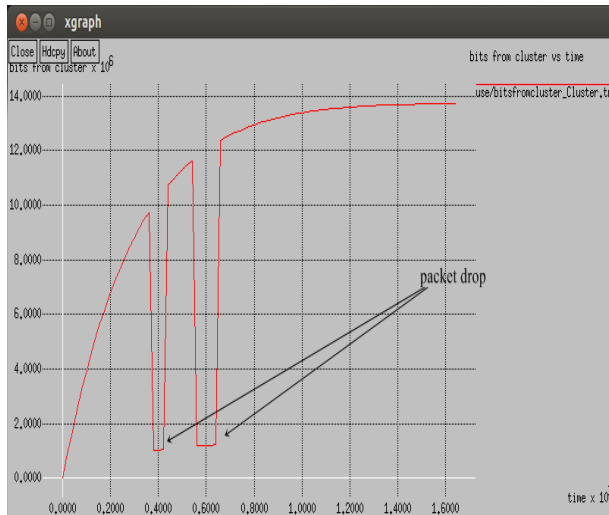


Fig. 1.2 Packet delivery ratio (without attack)

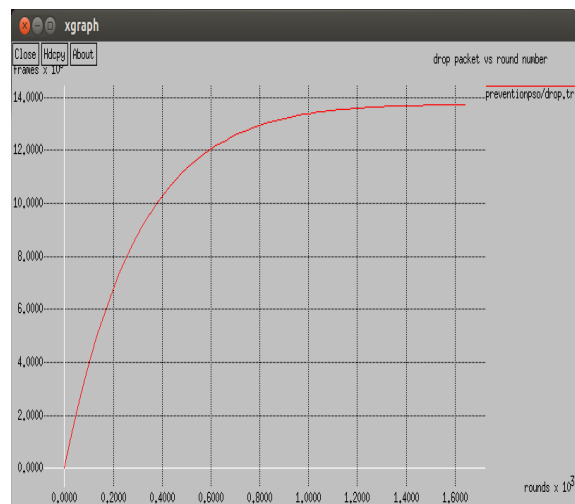


Figure 1.1 shows that there is some dropping of packet occurs in the network. The reason that malicious node does not send any data within the network because it drops some packets in the network. Then the figure 1.2 shows that when the attack is detected and then removed it using the simulation process then there is no dropping of packet occurs and the data is delivered to the destination node from the source of the data in the network.

ii) *End-to-End Delay*:

Fig 1.3 End-to-End delay (with attack)

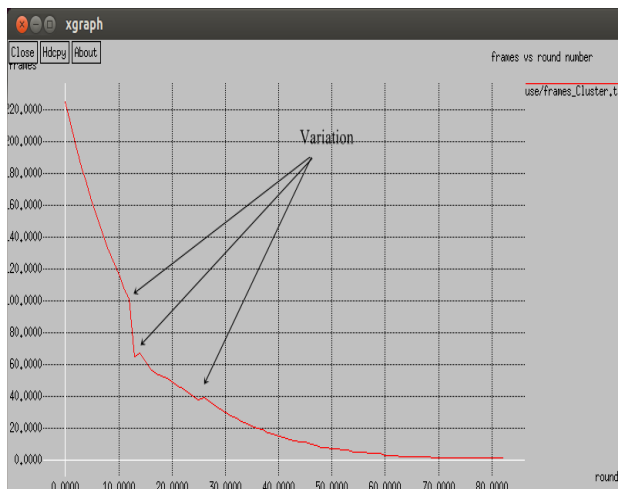
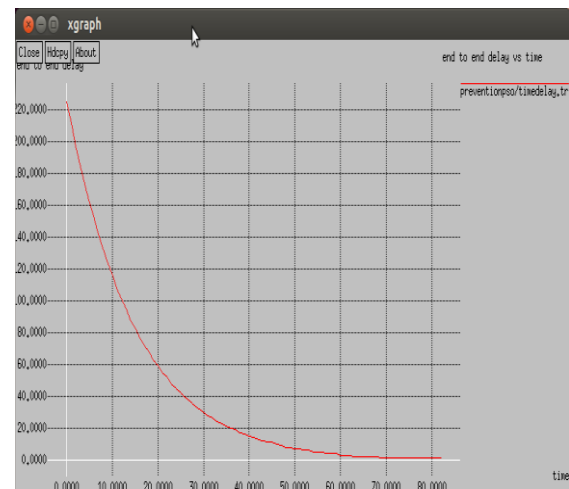


Fig. 1.4 End-to-End Delay (without attack)



The behavior of attack i.e. grey-hole attack also depends on protocols, routing procedure, and number of nodes involved. The figure 1.3 shows that the numbers of alive nodes that remain in the network after the simulation process finished. The figure shows that the alive node decreases as per the simulation process reaches its end point. There is corresponding delay occurs when attack is found in the network. In figure 1.4 shows there is delay occurs without any variation i.e. without any attack.

iii) *Throughput*: Figure 1.5 shows that the throughput for the 10 nodes when the attack occurs in the network. This is because the fewer routing forwarding and routing traffic. Here the harmful node throws out the data rather

than pass it to the destination node, thus effecting of throughput. Figure shows the little fluctuations in the throughput when the grey-hole happens in the network.

Fig. 1.5: Throughput (with attack)

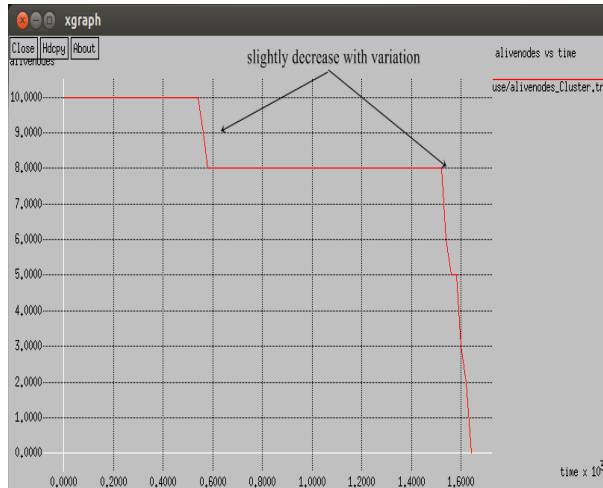
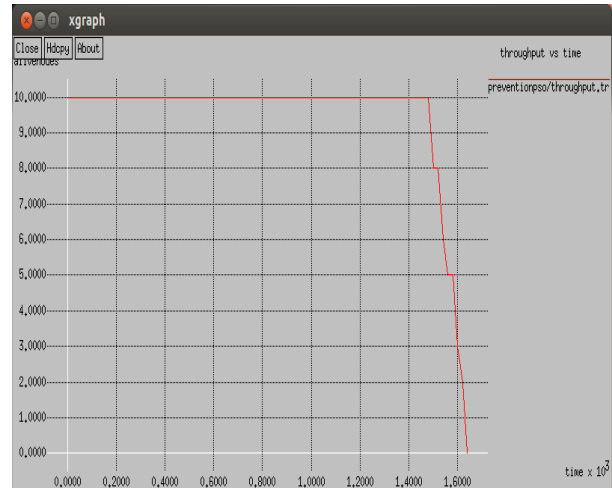


Fig. 1.6 : Throughput (Without attack)



VI. Simulation Results

The breakdown of simulation outcomes performed is based on the standard metrics of packet delivery ratio, end to end delay and the throughput of the network. Simulation area is the main parameter which is varying in simulation process.

Fig. 1.7: Sending Information through

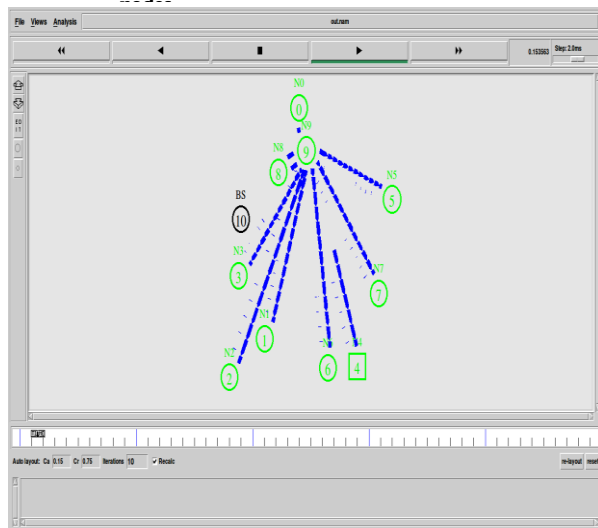
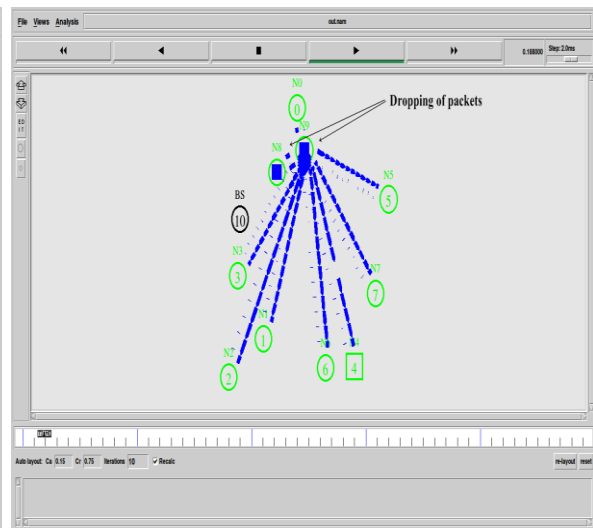


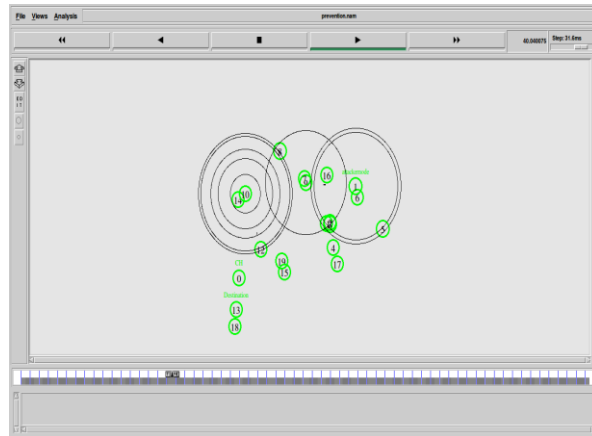
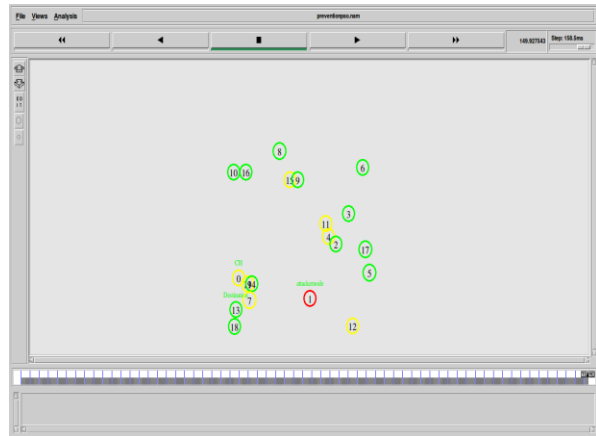
Fig. 1.8: Grey-hole attack with 10 mobile nodes and dropping of packets



This figure shows that the network structure and the flow of information through the nodes in the network. There are 10 nodes in the network which is denoted by 1-10. The blue arrows denotes that the flow of information through the nodes. Initially, there is smooth flow of information through every node to its neighboring nodes. Then in the next image it is shown that how the dropping of packets occurred when the attack happens in the network. The dropping of packets occurs from the nodes which are affected by the gray hole attack and there is information loss occurs and the information can't be able to reach destination node.

The figure represents that the dropping of packets in the node denoted with circle on the node in the network. The range of circle is analyzed by the neighboring nodes in the network.

The figure shows that the gray hole attack detected in the network. The yellow circle nodes are the nodes which are supposed to be malicious node but after the simulation process done there is malicious node detected which is circled with red in the figure.

Fig. 1.9: Grey-hole with 10 mobile nodes with certain drop of packets**Fig. 1.10: Grey-hole detect in red circle node and yellow nodes who are supposed to be malicious node**

VI. Conclusion and Future Scope

MANET holds the potential to situate the network where a traditional network infrastructure environment cannot feasible be situated. MANET is open to a variety of attacks. The harmful node creates the harm to the nodes and to the packets also. A new PSO technique is used to detect and remove the gray hole attack in Network. In future work, the count of nodes used in the simulation process can be raised with the larger count of nodes. The harder is network, the more chance of occurrence of an attack. It is very important to prevent the attack in earliest stage otherwise it tends to lose all information which has to be sent to destination node. There can be more than one grey-hole attack in existence of one network.

VII. References

- [1] A. Rana, V. Rana and S. Gupta, "EMAODV: Technique to Prevent Collaborative Attacks in MANET's", Proc. 4th International Conference on Eco-friendly Computing and Communication Systems, ICECCS, Vol. 70(2015), pp. 137-145, 2015.
- [2] D. Wadbude and V. Richariya, "An Efficient Secure AODV Routing Protocol in MANET", Proc. of International Journal of Engineering and Innovative Technology (IJEIT), Vol. 1, pp. 274-279, 2012.
- [3] J. Hoebeke, I. Moerman, B. Dhoedt and P. Demeester, "An Overview of Mobile Ad Hoc Networks: Applications and Challenges", Journal Communication Network, Vol. 3(3), pp.60-66, 2005.
- [4] A. Desai and P. Ramanuj, "Agent based mechanism for gray hole detection in MANET", Proc. International Journal of Innovative Research & Studies, Vol. 2(5), pp.441-452, 2013.
- [5] B. Wu, J. Chen, J. Wu and M. Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", Book on Wireless/Mobile Network Security, Springer, 2006.
- [6] V. Shanmuganathan and T. Anand M. E., "A Survey on Gray Hole Attack in MANET", Proc. International Journal of Computer Networks and Wireless Communications, Vol. 2(6), 2012.
- [7] S. Jain, M. Jain and H. Kandwal, "Advanced Algorithm for Detection and Prevention of Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks", Proc. of International Journal of Computer Applications, Vol. 1(7), 2010.
- [8] M. Arya and Y. K. Jain, "Gray hole Attack and Prevention in Mobile Ad Hoc Network", Proc. of International journal of Computer Applications, Vol. 27(10), 2011.
- [9] R. H. Jhaveri, S. J. Patel and D. C. Jinwala, "DoS attacks in mobile ad-hoc network: A Survey", Proc. 2nd International Conference on Advanced Computing and Communication Technology, 2012.
- [10] A. M. Kanthe, R. Prasad and D. Simunic, "A Mechanism for Gray hole Attack Detection in Mobile Ad-Hoc Networks", Proc. International Journal of Computer Application, Vol. 53(16), 2012.
- [11] A. Kumar and M. Chawla, "Destination based Group Gray Hole Attack Detection in MANET through AODV", Proc. International Journal of Computer Science Issue, Vol. 9(4), 2012.
- [12] D. G. Kariya, A. B. Kathole and S.R. Heda, "Detecting Black and Gray hole Attacks in Mobile Ad Hoc Network Using an Adaptive Method", Proc. of International Journal of Emerging Technology and Advanced Engineering, Vol. 2(1), 2012.
- [13] S. Makwana and K. Vaghela, "Detection and Elimination of Gray Hole Attack using Dynamic Credit based Technique in MANET", Proc. International Journal of Computer Applications, Vol. 125(4), 2015.
- [14] A. Dhaka, A. Nandal and R. S. Dhaka, "Gray and Black Hole Attack Identification using Control Packets in MANETs", Proc. 11th International Multi-Conference on Information Processing, Vol. 54, 2015.