IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume3, Issue1)
Available online at: www.ijariit.com

Cooperative Black Hole Attack Prevention by Particle Swarm Optimization with Multiple Swarms

Suman Brar
Department of Computer Science and Engineering, GCET, Gurdaspur- 143521

Mohit Angurala
Department of Computer Science and Engineering, GCET, Gurdaspur- 143521

Abstract*— MANET (Mobile Ad Hoc Network) is a type of ad hoc network that can change locations and configure itself, because of moving of nodes. As MANETs are mobile in nature, they use wireless connections to connect various networks without infrastructure or any centralized administration. Open medium, dynamic topology, distributed cooperation are the characteristics of MANET and hence ad hoc networks are open to different types of security attacks. A Grey hole is a node that selectively drops and forwards data packets after advertises itself as having the shortest path to the destination node in response to a route request message. Our mechanism helps to protect the network by detecting and reacting to malicious activities of any node. The results enable us to minimize the attacks on integrated MANET-Internet communication efficiently. Simulation will be carried out by using network simulator tool so as to address the problem of detection & prevention of grey hole attack in mobile ad-hoc network. In this thesis uses Particle swarm optimization(PSO).Which monitors by changing its values because of adhoc nature ,if node converge then it change its value infinite and prevent the node to send packet.

***Keywords*— MANET, Black hole attack, Gray hole attack, malicious node, simulation.**

I. Introduction

A Mobile ad hoc network (MANET) is a self-organized system which doesn't have any pre-defined network infrastructure where mobile devices are connected by wireless links. Hence, a MANET can be constructed quickly at a low cost, as it doesn't rely on existing network infrastructure. The configuration required in network deployment is minimal where the individual node acts as routers. MANET allows intermediate parties to relay data transmissions by dividing MANET into two types of networks, namely, single-hop and multi-hop. A communication session is achieved either through single-hop transmission if the recipient is within the transmission range of the source node, or by relaying through intermediate nodes otherwise.

Mobile Ad hoc Network (MANET) is a robust infrastructure less wireless network. It can be formed either by mobile nodes or by both fixed and mobile nodes. Nodes are randomly connected with each other and forming arbitrary topology [1]. Theses nodes can act as both routers and hosts. Those have ability to self-configure makes this technology suitable for provisioning communication to, for example, disaster-hit areas where there is no communication infrastructure or in emergency search and rescue operations where a network connection is urgently required. In MANET routing protocols for both static and dynamic topology are used [2].

An ad-hoc network is a wireless network describe by the nonexistence of a centralized and fixed infrastructure. In the absence of an infrastructure in ad hoc networks poses great challenges in the functionality of these networks. Therefore, a wireless ad hoc network with mobile nodes as a MANET discussed here. In a MANET, mobile nodes have the capability to accept and route traffic from their intermediate nodes towards the destination, i.e., mobile nodes can act as both routers and hosts. More frequent connection tearing and re-associations place an energy constraint on the mobile nodes [4].

As MANETs are illustrate by limited bandwidth and node mobility, there is demand to take into account the energy efficiency of the nodes, topology changes and unreliable communication in the design. There are many types of protocol are available in MANET. Its efficiency of a routing protocol is determined by its battery power consumption of a participating node and routing of traffic into the network [3].

MANET is a mobile multi-hop which is wireless distributed network and self-organized in nature. The primary objective of routing protocol is to discover the route. In the routing protocol for MANET undertakes to setup and maintain routes between nodes [6]. In MANET, constantly changing network topology causes link breakage and invalidation of end-to-end route. There is highly dynamic nature of wireless network imposes severe restrictions on routing protocols [5].

II. Literature Review

***Wadbude and Richariya* [4],** discussed about an ad-hoc network is a multi-hop wireless network where all nodes cooperatively maintain network connectivity without a centralized infrastructure. As the network is wireless, security becomes the major issue in MANETs. Some of the attacks such as modification, fabrication, impersonation and denial of service attacks are due to misbehaviour of malicious nodes, which disrupts the transmission. Here proposed an efficient secure AODV routing protocol. Simulation results show that proposed routing algorithm provides a better level of security and performance than existing works.

***Desai and Ramanuj* [6],** proposed a mechanism based on the mobile agent in which each mobile agent has two parameters, one is expiry time and other is RTT time. In a fixed time interval mobile agent is generated from source node and move to the network. In a fixed time period, it should calculate the overhear rate of its next hop and compare it with the threshold value. In this algorithm, mobile agent does not visit each neighbour node but only observes the next node in current route. This algorithm detects the gray hole and minimizes the packet drop and congestion.

***Bakshi et. al* [11],** implemented different approaches to initially detect whether there is single grey hole node in the network or multiple grey hole nodes. By applying different approaches it is simplified that whether there is single or multiple grey hole nodes acts as malicious nodes to grab the packets.

***Yi and Kravets* [12],** discussed various mutual authentication schemes of MANET. In this symmetric key and asymmetric key distribution schemes. In this also discuss PKI (public key distribution) scheme which based on the symmetric key distribution scheme. In new authentication scheme had been proposed named as MOCA, in which hybrid type of scheme, both PKI and asymmetric schemes used for mutual authentication.

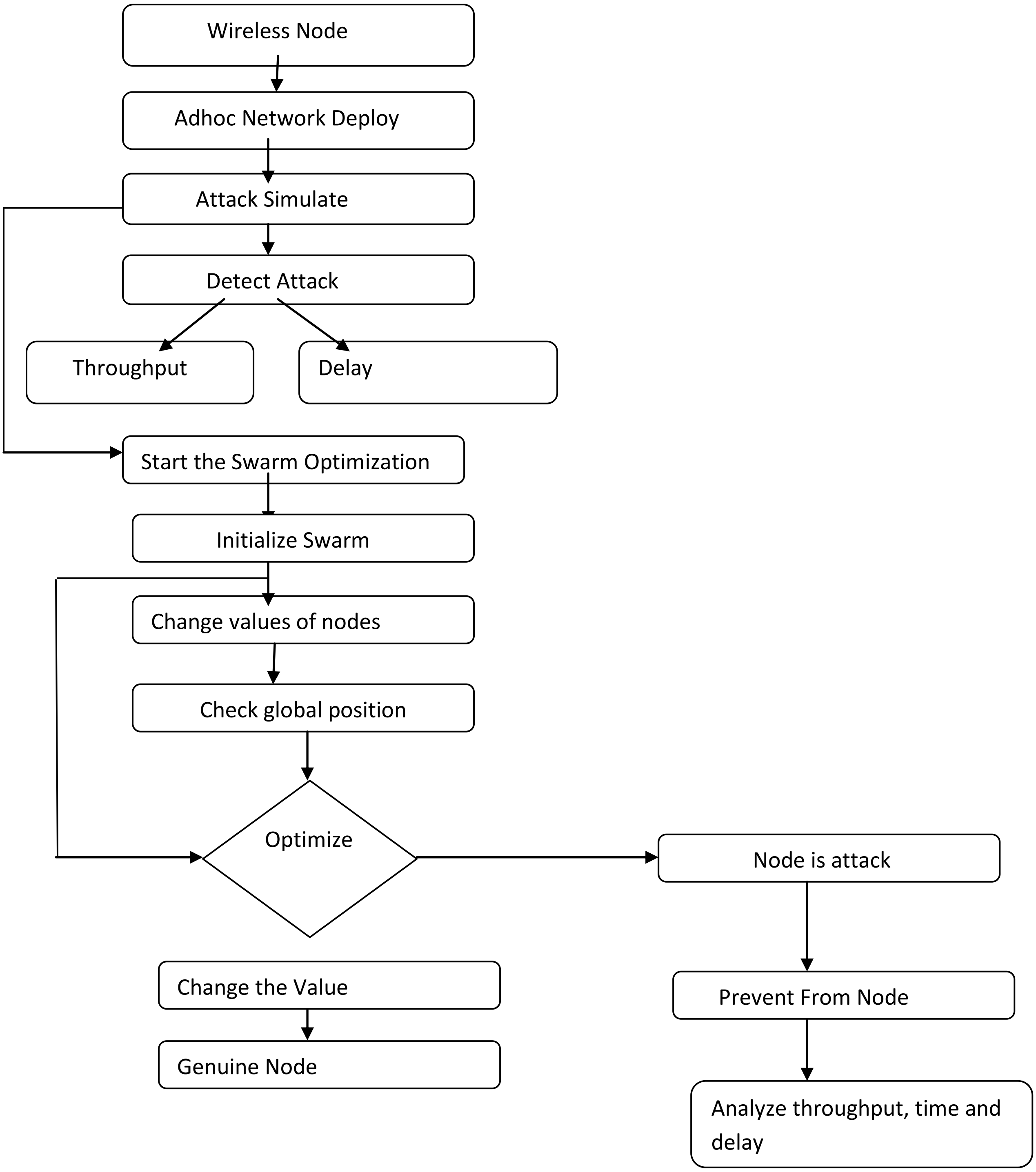
***Chandure and Gaikwad* [19],** proposed an algorithm that is based on security based technique which is used to recognize and eradicate the problem of gray hole attack. It works in two phases, firstly it develops a method which is used to handle the malicious node in the network and then routing protocol is used to recognize the gray hole attack.

***Chandure et. al* [21],** presented a method which is used to detects and prevents the gray hole attack and also detects the behavior of malicious node. This algorithm increases the packet delivery ratio and end to end delay. The performance of the network also increases by using SAODV in the algorithm.

III. Problem Formulation

In this method i.e. RTMAODV (Real Time Monitoring AODV), neighbor node detects and prevents grey hole attack using real time monitoring. The concept of broadcasting is being used in the method. Node which replies to Route Request (RREQ) by source is being monitored in promiscuous mode. Detection of malicious node is actually done by neighbor node of Route Reply (RREP) sender node i.e. suspected node. Two counters as fvalue and rvalue are used for performing a check on malicious node by counting number of forwarded packets and number of received packets respectively. fvalue reaches a threshold value and rvalue is 0 then node is considered to be malicious and is discarded from the network by broadcasting INTNOT Packet. It also used two performance matrices such are packet delivery ratio and average end-to-end delay for analyzing the work. Here the work is done to detect and mitigate single grey hole attack in the network. So the algorithm will be modified to detect and mitigate the cooperative grey hole attack in the network. Also the performance will be analyzed and compared on the basis of parameters such as PDR, End-to-End Delay, Throughput and Routing Overhead.

IV. Methodology



Step 1: deploy the wireless node in one-thousand X one-thousand.

Step 2: Step the mobility of the nodes and set the packet distribution parameter with FCFS method.
Step 3: Stimulate the attack on more than one node and analyze the throughput, time delay and drop packet.
Step 4: Initialization of preventation of attack by Particle Swarm Optimization and initialize the swarm which depend on number of nodes.
Step 5: Optimize the shortest path value of every node if it will change then, it's a genuine node, otherwise attacker node.
Step 6: After identifying the attacker node, set the shortest path value of these nodes infinite.

Step 7: Analyze the throughput, time delay in different set of nodes.

V. Results and Discussions

Table 5.1: Comparison of Delay (PSO) and Delay (Existing) method on different number of nodes

Number of Nodes	Delay PSO	Delay (Existing)
20	**38.60241**	**40.23**
30	**45.39759**	**46.23**
40	**52.62651**	**55.23**
50	**62.26506**	**63.56**

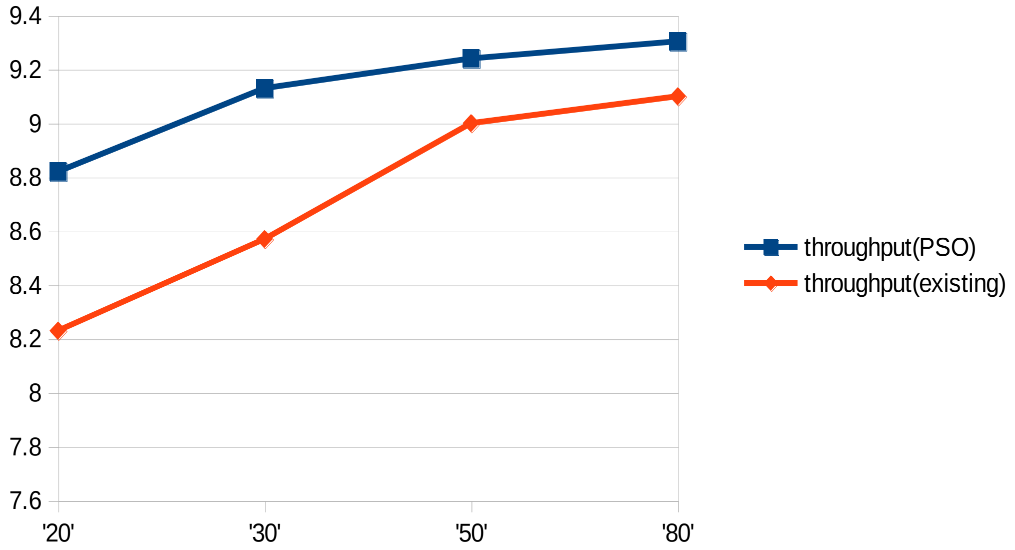
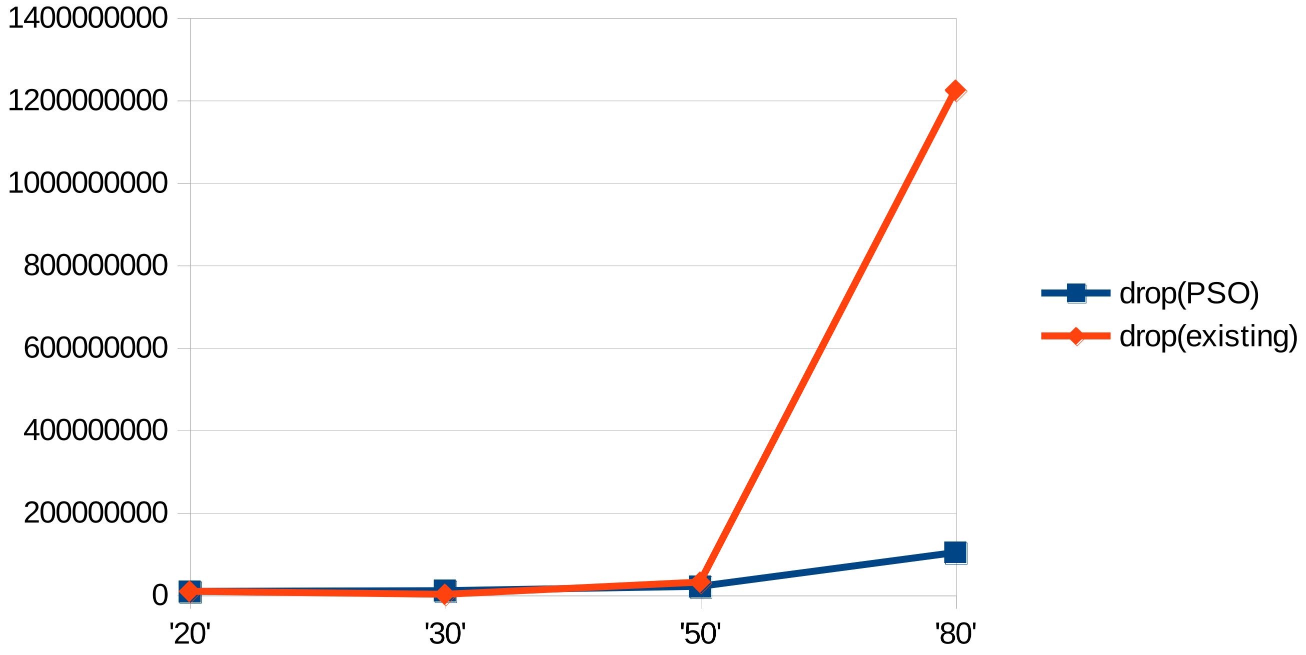


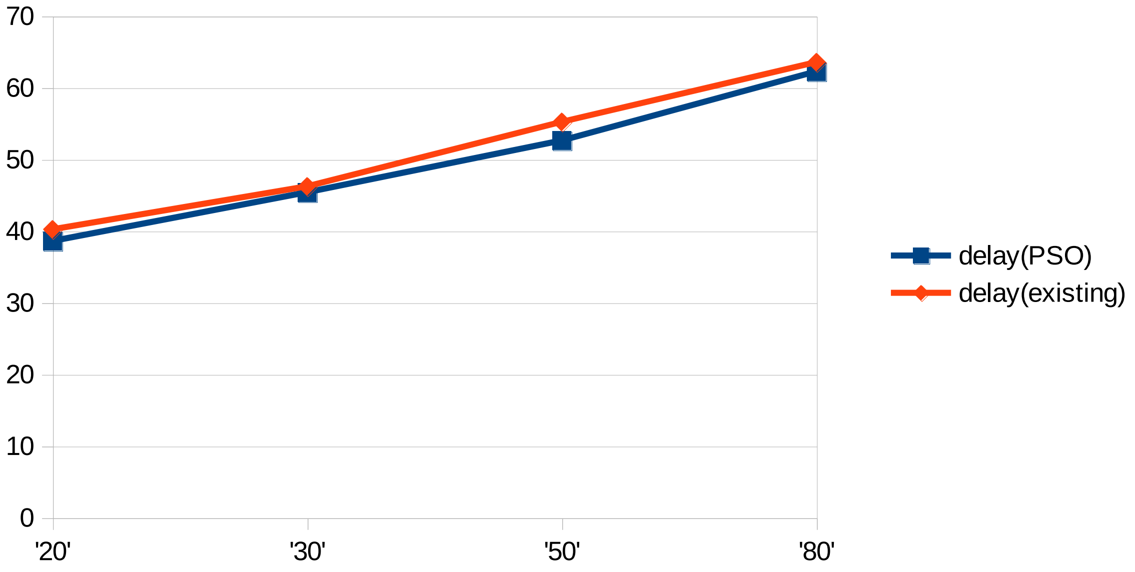
Table 5.2: Comparison of Drop (PSO) and Drop (Existing) method on different number of nodes

Number of Nodes	Drop (PSO)	Drop (Existing)
20	7938014	8234123
30	9720795.2	1023452
50	20236048	30345234
80	102331663	1223316631



Number of Nodes	Delay (PSO)	Delay (Existing)
20	38.60241	40.23
30	45.39759	46.23
50	52.62651	55.23
80	62.26506	63.56

CONCLUSIONS AND FUTURE WORK



Mobile Ad Hoc Networks has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. With the importance of MANET comparative to its vast potential it has still many challenges left in order to overcome. Security of MANET is one of the important features for its deployment. In our thesis we have analyzed the behavior and challenges of security threats in mobile ad hoc networks with solution finding technique. Although many solutions has been proposed but still these solutions are not perfect in terms of effectiveness and efficiency. If any solution works well in the presence of single malicious node, it cannot be applicable in case of multiple malicious nodes. After studying all the approaches our conclusion is that the approach offered suit well in our scenario. The intermediate reply messages if disabled leads to the delivery of message from destination node will not only improve the performance of network rather it will secure the network from attack.

References

[1] Sukla Banerjee, "Detection/Removal of Cooperative Grey and Gray hole Attack in Mobile Ad-Hoc Networks.", In the Proceedings of the World Congress on Engineering and Computer Science, pp.1-6, 2008.

[2] Sevil Şen, John A. Clark and Juan E. Tapiador, "Security Threats in Mobile Ad Hoc Networks Auerbach Publications", pp. 1-20, 2011.

[3] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, "An Overview of Mobile Ad Hoc Networks: Applications and Challenges", Journal-Communications Network, Vol. 3(3), pp. 60-66, 2004.

[4] Durgesh Wadbude and Vineet Richariya, "An Efficient Secure AODV Routing Protocol in MANET", International Journal of Engineering and Innovative Technology, Vol. 1(4), pp. 274-279, 2012.

[5] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", Springer Journal of Wireless Mobile Network Security , pp. 103-135, 2006.

[6] Ashok Desai and Prof. Purvi Ramanuj, "Agent Based Mechanism for Gray Hole Detection in MANET", International Journal of Innovative Research & Studies, Vol. 2(5), pp. 442-452, 2013.

[11] Aditya Bakshi, A.K.Sharma and Atul Mishra, "Significance of Mobile Ad-Hoc Networks (MANETs)", International Journal of Innovative Technology and Exploring Engineering (IJITEE), Vol.2(4), pp.1-5 , 2013.

[12] Seung Yi and Robin Kravets, "Key Management for Heterogeneous Ad-Hoc Wireless Networks", In the Proceedings of the 10th IEEE International Conference on Network Protocols, pp. 1092-1648, 2002.

[19] Onkar V. Chandure and V. T. Gaikwad, "A Mechanism for Recognition & Eradication of Gray Hole Attack using AODV Routing Protocol in MANET", International Journal of Computer Science and Information Technologies, Vol. 2(6), pp. 2607-2613, 2011.

[21] Onkar V. Chandure, Aditya P. Bakshi, Saudamini P. Tidke and Priyanka M. Lokhande, " Simulation of Secure AODV in Gray Hole Attack for Mobile Ad-hoc Network" , International Journal of Advances in Engineering & Technology, Vol. 5(1), pp. 67-76 , 2012.