A Novel Design of Contradiction Based on Grey Hole Attack Minimization for MANET

T. Manjula
PG and Research Department of Computer Science
Government Arts College (Autonomous)
Salem, India
manjulat.1994@gmail.com

M. Malathi
PG and Research Department of Computer Science
Government Arts College (Autonomous)
Salem, India
malamani2009@gmail.com

***Abstract*- Mobile Ad-Hoc Network (MANET) is a self-configuring network of mobile nodes simultaneous by wireless topology with randomly (*Md. Sameeruddin Khan, Md. Yusuf Mulge (2017)*) .The nodes do not depend upon other nodes. The main purpose of MANET network is to communicate each other and act upon wireless network and wireless devices such as mobile, laptop and some hardware communication devices. MANET is dynamic topology, each node has not inhibited mobility, connectivity and changes its link within a fraction of seconds to move frequently. Routing in MANET is done together between nodes. Each node works as router that forwards packets for other nodes (*Hosny M. Ibrahim, Nagwa M. Omar, Ebram K. William (2015)*). In this paper, our aim to describe the minimization of grey hole attack in MANET network using network simulator tool to address the detection and prevention of malicious node of grey hole attack in mobile ad-hoc network.**

Keywords: MANET, AODV, Grey hole attack, Simulation results.

1. INTRODUCTION

Mobile Ad-hoc Network MANET) is a independent network to communicate between one device or network to two or more devices or networks. MANET is a self classify network and finding router path. Each device in MANET is free to move separately in any direction, and alter its link to other device frequently. Every node act as a router (Shani Makwana, Krunal Vaghela (2015)). In this paper is introduced a technique of AODV (Ad Hoc On Demand Distance Vector). AODV is a routing protocol and uses for find well-organized route path, it helps to detect and destroy the grey hole attack in the MANET network. In this paper, we are using Network Simulator (NS-2) for calculate the performance of parameters. The result of simulations is End-to-End Delay, Packet Delivery ratio, energy ratio and throughput parameter.

2. RELATED WORK

Defence Model for grey hole attacks in MANET. This Defence model provides addresses for all the data attacks and produces reliable data transmission in the network. It can develop a robust solution to the grey hole attack (S.V.Vasantha, Dr.A. Damodaram (2014)). Detection and prevention of grey hole attack in MANET using ADOV routing protocol. A MANET is a multi-hop wireless network to protect the network and detect malicious nodes of activities (Onkar V. Chandure, V. T. Gaikwad (2012)). The detection and elimination of malicious node on the network using Overhearing Misbehaviour Detection [OMD]. This detection detects the duplicate node and also evaluate their forwarding behavior (T.Sasilatha, S.Vidhya and P.Sures Mohan Kumar (2017)).

3. AODV

Ad Hoc On Demand Distance Vector (AODV) is an algorithm for detecting the malicious node in the network. AODV is the suitable technique for MANET to discard the duplicate nodes. AODV is a very simple, efficient and effective routing protocol, it works on MANET and do not fixed infrastructure network topology, it includes limited bandwidth are minimal space complexity, maximum exploitation of the bandwidth, most effective routing information, loop free routes, highly scalable etc., AODV is reactive routing protocol, can handle highly dynamic behaviour and used for both unicasts and multicasts using the join multicast flag in the packets (Krishna Gorantala (2006)).

4. GREY HOLE ATTACK

Grey hole attack is one of the attacks in network layer which comes under security active attacks in MANET. Grey hole attack is the attack in the Ad-hoc networks. The grey hole attack in which the nodes will drop packets selectively (V.Shanmuganathan, Mr. T.Anand M.E. (2012)). In previously, the attack node drops all the generated packets in the network. Grey hole nodes in MANET are very effective and every node maintains a routing table that stores the next hop node information for a route, a packet to destination node. When source node needs to route a packet to the destination node, it uses specific route if such route is available in its routing table. Grey hole attacks act as a misbehaviour node in the network. When malicious node occurs, it will drop the packet with take tiny period to discard the nodes in the network.

5. EXISTING SYSTEM

In previous work to detect the grey hole attack with DSDV (Dynamic Destination Sequenced Distance Vector) Routing protocol. DSDV is a proactive routing protocol. It creates smaller number of nodes. When the malicious node occurs in the network, it drops the entire data packet in the network and do not forward them on the same route. It recovers the sequence number again and update the routing table. DSDV is not appropriate for high forceful networks.

6. PROPOSED SYSTEM

A mechanism is proposed with the AODV (Ad Hoc On Demand Distance Vector) technique for detecting the malevolent attacks on the network. AODV is the advanced technique to detect, eliminate and prevent the malicious nodes in which the data packets on the network. When the malicious node occurs in the network, it drops the packet in the network with selective manner. And also, to be forwarded on the same route from source to destination. AODV performs to calculate the shortest path to transfer the data with safe mode. It uses some parameters to evaluate the results through Network Simulator (NS2). This technique is suitable for all high dynamic networks.

7. SIMULATION RESULTS

7.1 Performance Parameters

There are four parameters are used for evaluation of grey hole attack. They are,

7.1.1 Throughput

No. of bytes received above transmitted per second is called as throughput.

$$\text{Average throughput} = \frac{\text{No.of bytes received x 8}}{\text{Simulation time x 1000}}$$

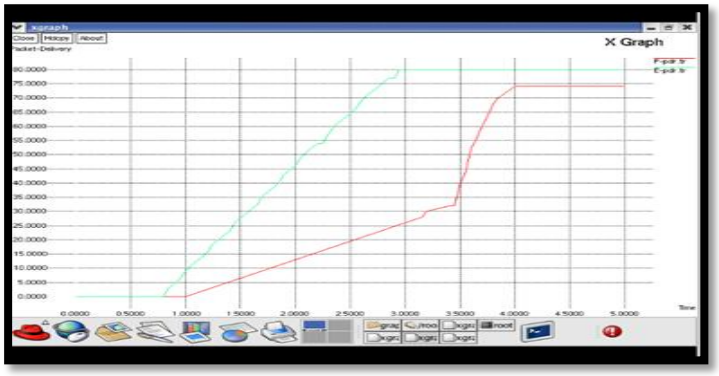

Figure 7.1.1. Throughput

7.1.2 Packet Delivery Ratio

Level of delivery data to destination with the speed of network. NS2 calculates the percentage of PDR using the equation 1 as in the figure 1.

$$\text{PDR (\%)} = \frac{\text{Total no.of packets received}}{\text{Total no.of packets send}} \text{ x } 100 \quad (1)$$

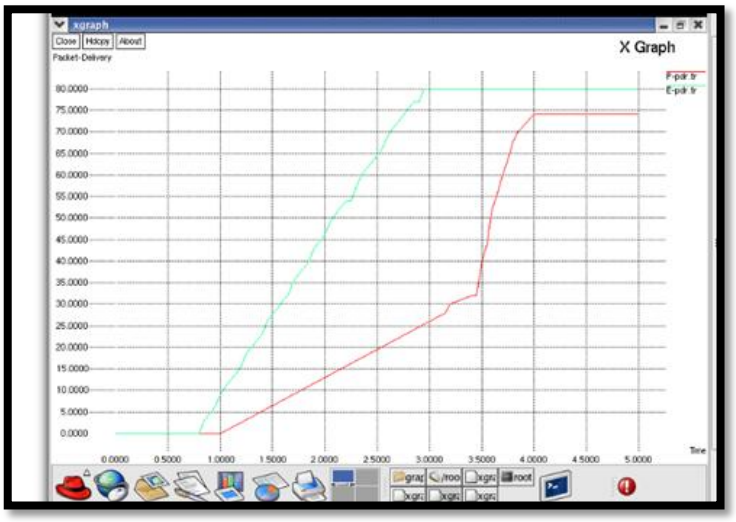

Figure 1. Packet Delivery Ratio

7.1.3 Energy Consumption

Every node has energy level utilization while sending and receiving the data during transmission on the network.

Figure 2. Energy Consumption

7.1.4 End-to-End Delay

Transmit the data packet by time taken for each node from source to destination in the network is shown in the figure 3.

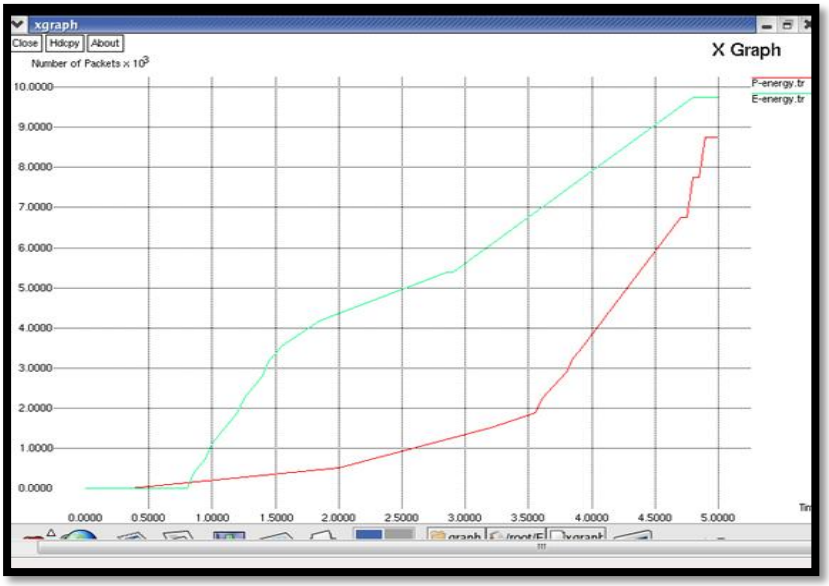

Figure 3. End-to-End Delay

8. RESULTS AND DISCUSSION

8.1 Node Creation

The number of nodes is created in the network is shown in the figure 4.

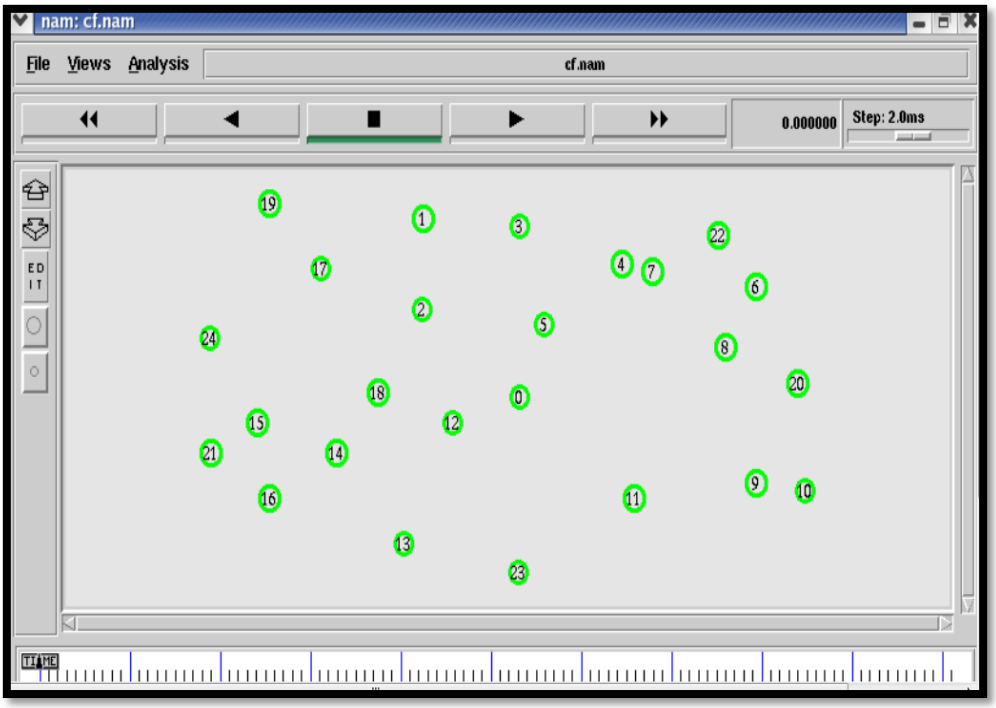

Figure 4. Node Creation in Network

8.2 Malicious Node Detection

The malicious node detected and represent circles in the below figure 5.

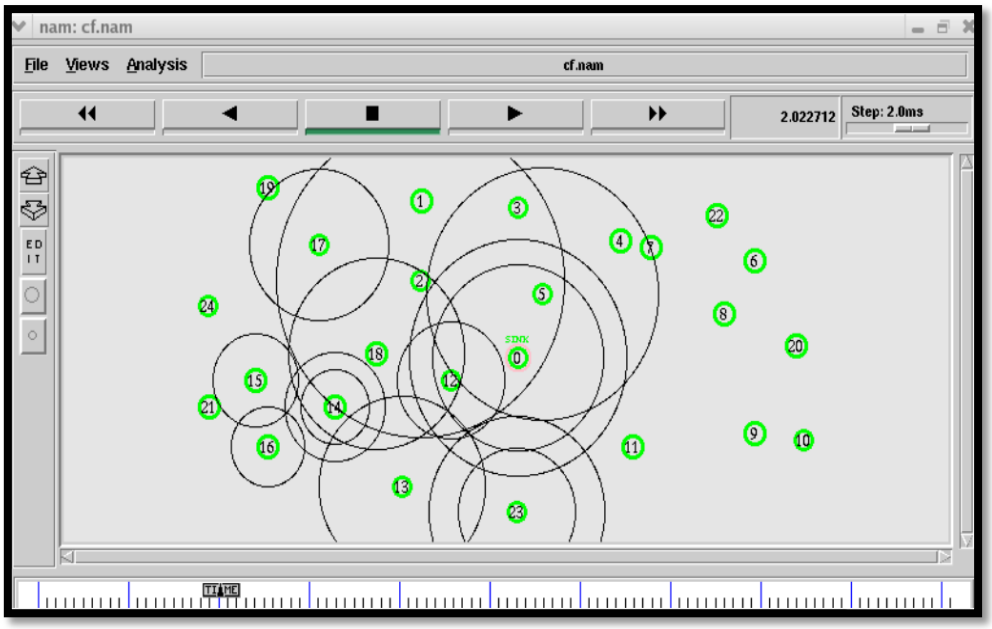

Figure 5. Malicious Node Detection

8.3. Grey Hole Attack Detection

To exhibit grey hole attack new source and destination node is selected 7-10-19 and Grey Hole is detected in the node 11 & 18 as shown in the below figure 6.

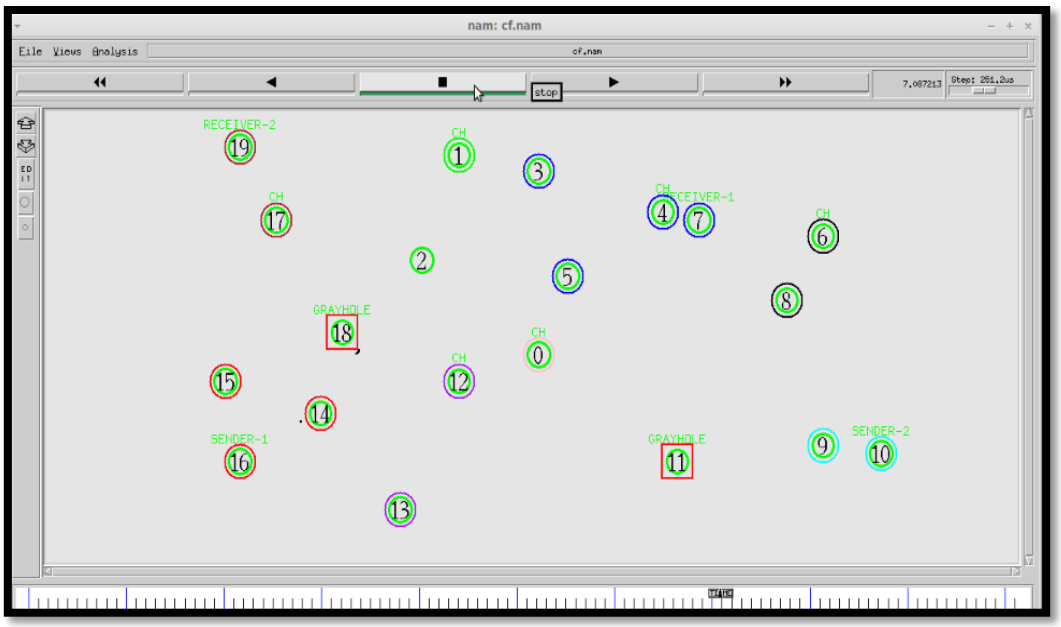

Figure 6. Grey Hole Detection

9. CONCLUSION

In this paper, we have implemented AODV technique to detect the malicious node in the network. using Network Simulator tool, to give graphical results with sequence manner. AODV is suitable technique to detect grey hole attack. The simulation results are represented some parameters are Throughput, Packet Delivery ratio, Energy level Consumption and End-to-End delay using graphical interface with X and Y axis respectively.

RFERENCES

Md. Sameeruddin Khan, Md. Yusuf Mulge (2017), Efficient and Secure Data Transmission in MANET's against Malicious Attack using AODV Routing and PSO Clustering with AES Cryptography, International Journal of Pure and Applied Mathematics, 117(21)

Hosny M. Ibrahim, Nagwa M. Omar, Ebram K. William (2015), Detection and Removal of Gray, Black and Cooperative Black Hole Attacks in AODV Technique, (IJACSA) International Journal of Advanced Computer Science and applications, 6(5).

Shani Makwana, Krunal Vaghela (2015), Detection and Elimination of Gray Hole Attack using Dynamic Credit based Technique in MANET, International Journal of Computer Applications, 125(4).

S.V.Vasantha, A. Damodaram (2014), A Defense Model for Black hole and Grey hole attacks in MANET, IJCSMC, 3(11).

Onkar V. Chandure, V. T. Gaikwad (2012), Detection and Prevention of Grey hole attack in MANET using AODV Routing Protocol, International Journal of Computer Applications, 41 (5).

T.Sasilatha, S.Vidhya and P.Sures Mohan Kumar (2017), Detection and Elimination of Black Hole and Grey hole attack on MANET, International Journal of Pure and Applied Mathematics, 16 (24).

Krishna Gorantala (2006), Routing Protocols in Mobile Ad-hoc Networks, UMEA University, Department of Computer Science, SE-901 87 UMEA, SWEDEN.

V.Shanmuganathan, Mr. T.Anand M.E. (2012), A Survey on Gray Hole Attack in MANET", International Journal of Computer Networks And Wireless Communication (IJCNWC), 2.