Jamming Attack Detection and Isolation to Increase Efficiency of the Network in Mobile Ad-hoc Network

[1]**Henna Khosla,** *Student, Department of Electronics and Communication Engineering, Punjabi University, Patiala, Punjab, India*

[2]**Rupinder Kaur,** *Assistant Professor, Department of Electronics and Communication Engineering, Patiala, Punjab, India*

Abstract*-MANET is a mobile Adhoc network. It is self-configuring network which is infrastructure less in nature. In MANET different nodes are connected through wireless links. Each node is free to move i.e. no central controller is available. There are several types of attacks in MANETs like jamming, selective packet drop attack etc. In this paper we will discuss about jamming attack. A novel technique will be proposed to detect and isolate jamming attack. Experimental results show that proposed technique is more efficient than the existing one.*

Keywords: MANET, security, ICMP packets and topologies.

1. INTRODUCTION

Ad-hoc networking is a concept in computer communications, which means that users are waiting to communicate with each other form a temporary network without any form of centralized administration. Each node participating in the network acts both as a host as well as a router and must therefore is willing to forward packets for other nodes. For this purpose a routing protocol is needed. MANET is a mobile Adhoc network. It is self-configuring network which is infrastructure less in nature. In MANET different mobiles are connected through wireless links. Each node is free to move i.e. no central controller available [1]. Nodes are randomly connected with each other and forming arbitrary topology. They have self configuring ability making 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 topologies are used [2]. There are many security issues in MANETS like attacks, sniffing, spoofing etc. Many types of attacks can be done on MANETs. Some of the attacks are discussed below:

1.1 Denial of Service Attack

The aims of attack are to hit the accessibility of a node and all the nodes in the entire network. The services will not be accessible if the attack is successful. The attacker generally uses battery exhaustion method and radio signal jamming. It has further sub categories:

1. Smurf Attack
2. Distributed denial of services
3. SYN flood attack

1.2 Byzantine Attack

In this attack, a intermediate compromised node carries out attacks such as creating collision forwarding packets on non-optimal paths, routing loops, and dropping packets selectively which result in interruption or dreadful conditions of the routing services [3].

1.3 Jamming

In this attack, attacker keeps monitoring wireless medium initially in order to verify frequency at which destination node is getting signal from sender. Signal is transmitted on that frequency to hinder error free receptor [4].

1.4 Man in the Middle Attack

In this attack, attacker sits between the

sender and receiver and any information being sent between two nodes is sniffed by him. In some cases, attacker may masquerade as the sender to communicate with receiver or masquerade as the receiver for replying the sender. It starts when first attacker sniffs and eavesdrops the packets [5].

In section 2nd we will study background of jamming attack, in section 3rd we will discuss about jamming attack in detail. After that proposed methodology, experimental results and conclusion respectively will be discussed in detail.

2. BACKGROUND

In this paper [6], **A. Hamieh et. al** have proposed a new model based on the measure of correlation among the error and the correct reception times in order to detect the presence of jamming attack in ad hoc networks. The correlation is defined here as a measure of the association between two random variables. Main purpose is to detect specific type of jamming, in which the jammer transmits only when valid radio activity is signaled from its radio hardware, which it represents the major case of such attack. The simulation results of the model are quite promising. In fact, we have been able to detect the presence of jamming with very high degree of confidence. Our objective in the future is to use our approach to detect other DoS attacks and to find an effective reaction mechanism to cope up with jamming.

In this paper [7], **L. Lazos et.al** addressed the problem of control-channel jamming in multi-channel ad hoc networks, under node compromise. We proposed a randomized distributed channel establishment scheme that allows nodes to select a new control channel using frequency hopping. Our method differs from classical frequency hopping in that the communicating nodes are not synchronized to the same hopping sequence. Instead, each node follows a unique hopping sequence. They showed that their scheme can uniquely identify compromised nodes through their unique sequence and exclude them from the network. They evaluated the performance of their scheme based on the newly proposed metrics of evasion entropy, evasion delay, and evasion ratio. The proposed scheme can be utilized as a temporary solution for the control channel re-establishment until the jammer and the compromised nodes are removed from the network.

In this paper [8], **S. Yi et.al,** discussed various mutual authentication schemes of mobile ad hoc network. They had discussed the symmetric key and asymmetric key distribution schemes. They had also discussed PKI (Public Key Infrastructure) scheme which is based on the symmetric key distribution scheme. In this paper authors proposed a new authentication scheme named as MOCA (Multimedia Over Coax Alliance) which is hybrid type of scheme and uses both PKI and asymmetric schemes for mutual authentication.

In this paper [9], **Karthikeyan et. al,** introduced about the study threats faced by the ad hoc network environment and provide an arrangement for various security mechanisms. The strengths and vulnerabilities of the existing routing protocols are analyzed and have suggested a broad and comprehensive framework that can provide a tangible solution.

3. JAMMING ATTACK

A jammer is an entity whose main aim is trying to get in the way with the physical transmission and reception of wireless communications. A jammer always constantly emits RF signals to fill a wireless channel so that legal traffic will be completely blocked. The common characteristics for all the jamming attacks are that their interactions are not amenable with MAC protocols [7]. The ratio of packets that are effectively sent out by a justifiable traffic source compared to the number of packets it intends to send out at the MAC layer. In this attack number of source are formed instead of single source which sends rough packets to the transmission channels and jammed the channel. Due to this jamming, packet loss starts. It decreases the efficiency and reliability of the system. Due to this attack many problems arise like channel becomes busy, delay in transmission, new packets being dropped etc [12].

3.1 Physical Jamming (Physical Layer) Physical or Radio jamming in a wireless medium is a simple but disruptive form of DoS attack. These attacks are launched by either continuous emission of radio signals or by sending random bits onto the channel. The jammers causing these attacks can deny complete access to the channel by monopolizing the wireless medium. So communication has an unusually large carrier sensing time waiting for the channel to become idle. This has an adverse propagating effect as the nodes enter into large exponential back-off periods [13].

3.2 Virtual Jamming (MAC Layer) In IEEE 802.11 based MAC protocols, virtual carrier sensing is used at the MAC layer to determine the availability of the wireless medium. Jamming can be launched at the MAC layer through attacks on the RTS/CTS frames or DATA frames. A significant advantage of MAC layer jamming is that the adversary node consumes less power in targeting these attacks as compared to the physical radio jamming. Here, we focus on DoS attacks at the MAC layer resulting in collision of RTS/CTS control frames or the DATA frames [14].

4. PROPOSED METHODOLOGY

Jamming packet is the partial denial of service attacks which is triggered by the malicious nodes or multiple malicious nodes in the network. In the previous times, many techniques have been proposed to isolate jamming attacks from the network. When jamming attack is triggered in the network, throughput of the network is reduced and delay is increased as steady rate. In our work, we work on to detect and isolate jamming attack in AODV Protocol [10]. The route is established between source and destination on the basis of hop counts and sequence numbers. The malicious node exists in the route which acts as source or multiple sources. The malicious node will be responsible for triggering the jamming attack. The proposed methodology will detect the malicious node and isolate it from the network. The methodology is based on the throughput of the network. When the throughput of the network will degrade to certain threshold value, nodes in the network will go to monitor mode and detect the malicious node. In our proposed work we overcome the problem of dropped packet by detecting them and redirect to the source with the help of monitoring nodes. ICMP packets will generate from source side and flooded in the network. Then these packets will act as monitor nodes. Monitoring nodes detect malicious node which further does not send it to the destination. So the nodes which detect the malicious node reply to a source node expect route node so that source isolates the path and stop forwarding more packets.

5. EXPERIMENTAL RESULTS

In Fig.1 Energy graph is represented. Red line shows new energy and green line shows previous energy. New proposed system takes less energy as compared to the existing system. So, new technique is more efficient.

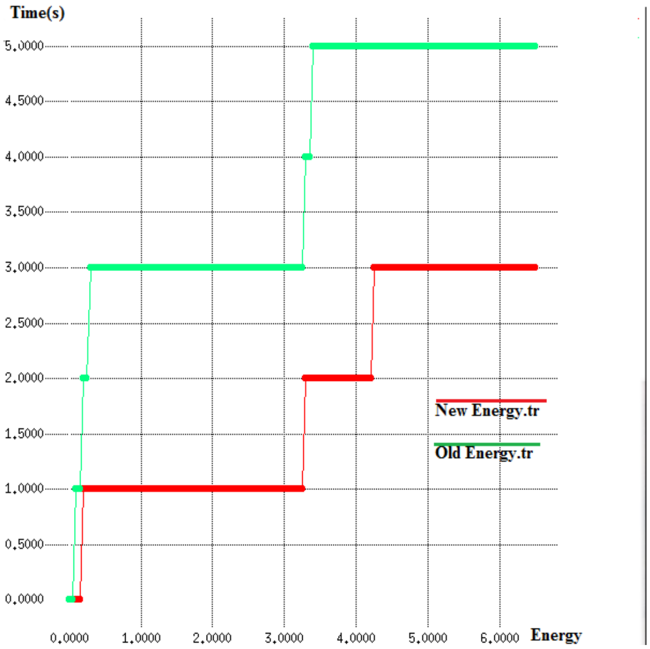

Fig. 1 Energy graph

In Fig. 2, packet loss is represented. Packet-loss is lesser in new proposed than the existing system. Red line shows lesser packet loss of new system and Green line shows more packet loss in existing system.

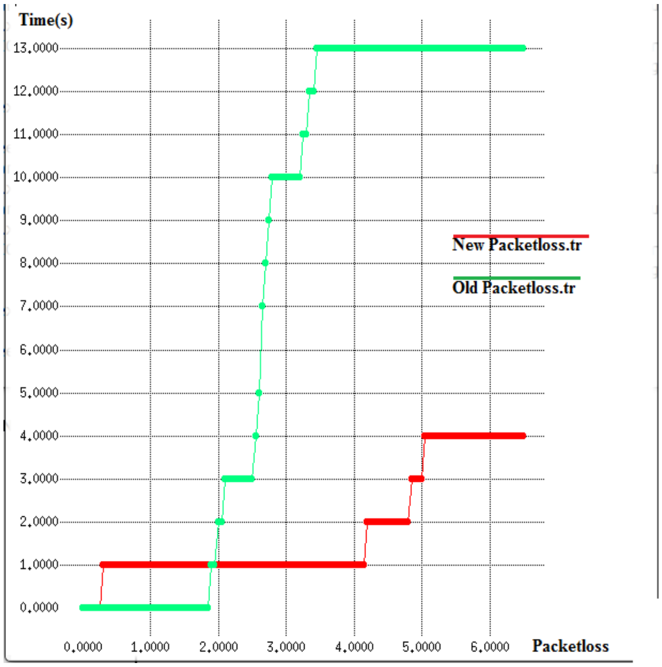

Fig. 2 Packet loss graph

6. CONCLUSION

In this paper, we conclude that monitoring nodes are required to prevent various inside and outside attacks. We review the ICMP protocol for authentication. In our work, we propose new technique to isolate attack between the mobile nodes. We implement new proposed technique and compare the results with the previous techniques. Experimental Result shows that proposed technique is better than existing technique.

REFERENCES

[1] Bing Wu, Jianmin Chen, Jie Wu and Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks" ,Springer ,2006

[2] Wenjia Li and Anupam Joshi , "Security Issues in Mobile Ad Hoc Networks- A Survey", Networking Conference Special Sessions , Las Vegas, Nevada, 2006

[3] Sevil Şen, John A. Clark and Juan E. Tapiador, "Security Threats in Mobile Ad Hoc Networks", IEEE, 2010

[4] Vinit Garg, Manoj Kr.Shukla, Tanupriya Choudhury and Charu Gupta, "Advance Survey of Mobile Ad-Hoc Network," IJCST Vol. 2, Iss ue 4, Oct . - Dec. 2011

[5] Humayun Bakht, " Survey of Routing Protocols for Mobile Ad-hoc Network" , Volume 1 No. 6, October 2011 ISSN-2223-4985 International Journal of Information and Communication Technology Research

[6] Ali Hamieh and Jalel Ben-Othman, "Detection of Jamming Attacks in Wireless Ad Hoc Networks using Error Distribution", IEEE, 2009

[7] Loukas Lazos, Sisi Liu, and Marwan Krunz, "Mitigating Control-Channel Jamming Attacks in Multi-channel Ad Hoc Networks" ACM, WiSec'09, March 16–18, 2009, Zurich, Switzerland, 2009

[8] Seung Yi and Robin Kravets, "Key Management for Heterogeneous Ad Hoc Wireless Networks" , 10th IEEE International Conference on Network Protocols (ICNP'02) 1092-1648, n.d.

[9] Karthikeyan U and Rajni ,"Security Issues Pertaining to Ad-Hoc Networks", International

Journal for Research in Applied Science & Engineering Technology Volume 2 Issue XI, November 2014 ISSN: 2321-9653.

[10] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, "An Overview of Mobile Ad Hoc Networks: Applications and Challenges", IJSER, 2005

[11] Rusha Nandy, "Study of Various Attacks in MANET and Elaborative Discussion Of Rushing Attack on DSR with clustering scheme" Int. J. Advanced Networking and Applications Volume: 03, Issue: 01, Pages:1035-1043 (2011)

[12]Pranita Chaudhar, C. RamaKrishna and Sasmita Behera, "A Review on Packet-Hiding Methods to Hamper Selective Jamming Attacks in wireless networks", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 8 August, 2013 Page No. 2377-2387

[13] Nischay Bahl, Ajay K. Sharma and Harsh K. Verma "Impact of Physical Layer Jamming on Wireless Sensor Networks with Shadowing and Multicasting" I. J. Computer Network and Information Security, 2012.

[14] K. Arisha, M. Youssef, and M. Younis, "Energy-aware TDMA based MAC for sensor networks. In IEEE Workshop on Integrated Management of Power Aware Communications" Computing and Networking (IMPACCT 2002), May 2002