Experimental Analysis of Jamming on Various Parameters Associated with Mobile Ad-hoc Networks (MANETs)

Henna Khosla, Rupinder Kaur

***Abstract*— MANETs are the networks having array of nodes such that the functionality of each node is independent of the infrastructure and are still a part of the whole network. Need of security is growing with the advancements of MANETs because MANETs may interact with hostile environment. Due to this interaction there may be some DoS attacks on the data sent by us. Jamming comes under DoS attacks. In these attacks, the desired data is banned from being received at the receiver such that various effects on the desired communication are obtained that are undesirable for smooth communication. So we need to secure our data from such attacks. But this security of MANETs is difficult due to various computing constraints and inherent resources. So we have shown the effects of jamming on parameters (Energy, Routing overhead, No. of hops travelled, throughput and packet loss) associated with MANETs**

***Index Terms*— MANETs, DoS, Jamming attacks, Routing overhead.**

I. INTRODUCTION

Wireless technologies have become popular among our personal as well as public lives. This technology has enabled one or more devices to communicate without cables [1]. Due to wireless nature the cost required for caballing purpose has become null but threats to security have arisen too [2]. Wireless sensor networks (WSNs) are applied in many different areas, for instance, the voltage monitoring in electric power companies, temperature and humidity remote controlling in museums and human health tracking systems. Security is the combination of processes, procedures, and systems used to have confidentiality, authentication, integrity, availability and access control. Confidentiality is required, so that the information is not read by the intruders

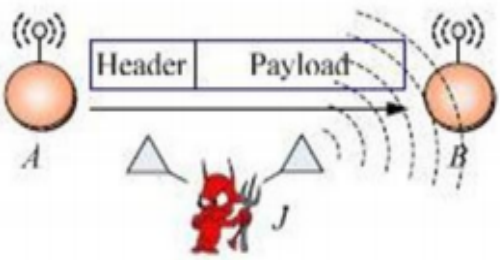

Fig.1 Jamming Attack By Intruder [1]

Manuscript received June 11, 2015

Henna Khosla, Deptt. of Electronics and Communication Engineering, Punjabi university, Patiala, India

Rupinder Kaur, Deptt. of Electronics and Communication Engineering, Punjabi University, Patiala, India

Who are unintentional [3]. Normally, the client needs to have authentication from the system called as server [4]. MANETs are part of wireless networks and are collection of nodes that do not depend on infrastructure to keep the network connected and are being used in many applications like health monitoring, military purposes, and home automation [5], [6]. Wireless networks are vulnerable to attacks because of their broadcast nature. Attacks may affect confidentiality and integrity of wireless network [6]. Unintentional attacks such as jamming can occur in wireless networks such as MANETs in which noise or interfering signal has to be sent to override the original signal in order to seize it from being received at the receiver [5], [10]. Attacker in this can send fake data on the same frequency as is used by the sender to send the original data such that they become undistinguishable [7], [8]. A protocol named as ALARM standing for Anonymous Location-Aided Routing in MANETS (ALARM) demonstrating on the feasibility of simultaneously obtaining, strong privacy, and security properties, with reasonable efficiency [9]. Due to such type of attacks no. of packets received decreases at the receiver resulting in loss of data. Throughput of the system is also affected.

Jamming is done by a device called as Jammer. Jammer can further be of four types: Constant Jammer, Deceptive jammer, Random Jammer, Reactive Jammer and Random reactive jammer.

In constant jammer, unwanted signal is sent continuously. So the legitimate user will not be able to acquire the channel used to send the data [1], [7].

In Deceptive jammer, a set of fabricated messages is present and is sent repeatedly. There is no gap between the sending of subsequent packets. So legitimate user may think fake packets are the original ones [1], [7].

In Random jammer, there is a period defined in which fake data is to be sent and remain inactive other times. There is sleeping time defined in this jammer. For certain time (which is predefined) jammer sends fake data or jamming signal and then go to sleeping mode doing no operation [1], [10].

In Reactive Jammer, Jamming is done only when some data is found to be sent by original transmitter. This type of jammer does not send any data when find the channel idle. However, this is the type of the jammer that is very hard to be detected by the legitimate user [1], [10].

Another type of jammer is random reactive jammer in which advantages of random as well as reactive are present. In this type, sleeping time is there and also it is very hard to be detected by the legitimate user [11].

II. PROBLEM FORMULATION

In MANET inside and outside attacks are possible, which degrade the performance of the network. In Inside attacks a node within the network acts as malicious node and creates

problem for original data. In outside attacks a malicious node is outside the original network and becomes the member of the network to launch attack. A passive outsider aims to compromise privacy.. Jamming packet is the partial denial of service attacks which is triggered by the malicious nodes or multiple malicious nodes in the network. Jamming has its effects on energy of the packets, routing overhead of the network, no. of hops travelled and packet loss. So our motive is to find out the effect of jamming on the above said four parameters i.e. energy of the packets, routing overhead of the network, no. of hops travelled and packet loss.

III. IMPLEMENTATION OF PROBLEM

Implementation is done on the ns-2 software. It contains "NAM" files through which animation is run. Following steps are done on animator to obtain the effects of jamming.

1. Firstly deployment of network is done, so that all the nodes are mobile.

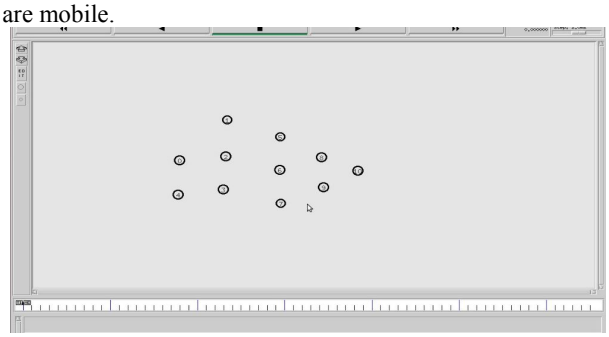

Fig.2 Deployment of nodes

2. Transmitting node sends route request to other nodes in the whole network.

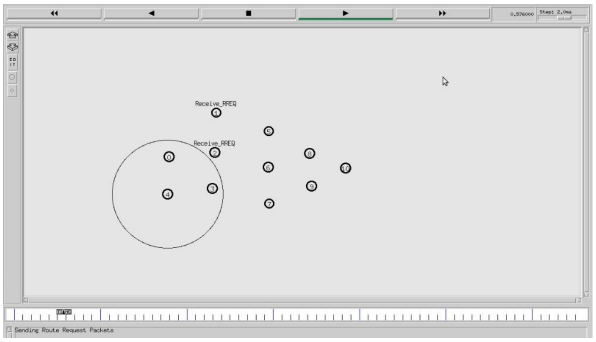

Fig.3.Route request from transmitter

3. Nodes Send Route Request packets to all other nodes and establish route from source to destination.

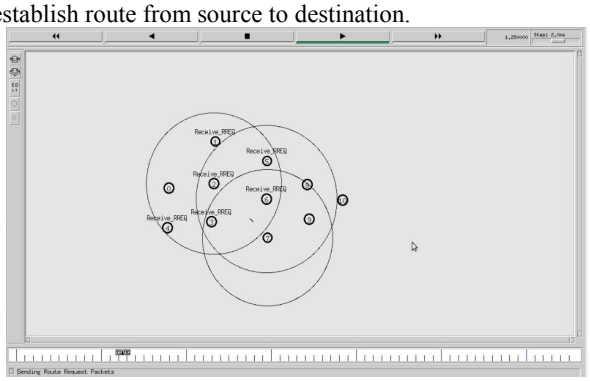

Fig.4.Establishment from source to destination

4. Source sends route packets and all the nodes receive the route reply packets from source to destination.

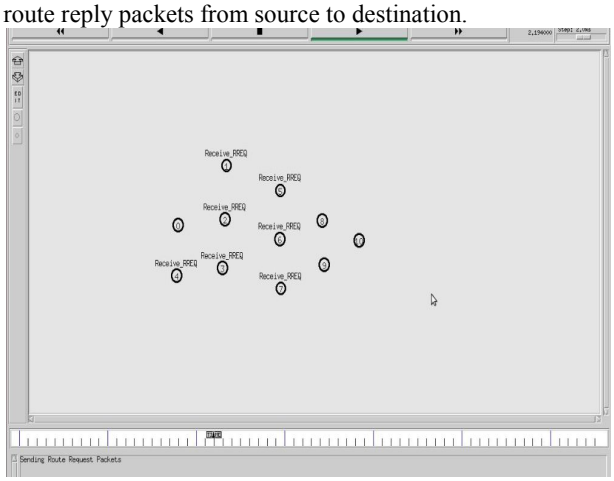

Fig.5. Route requests to establish Path

5. All the nodes in the network receive RREP message and establish path from source to destination for transferring of packets.

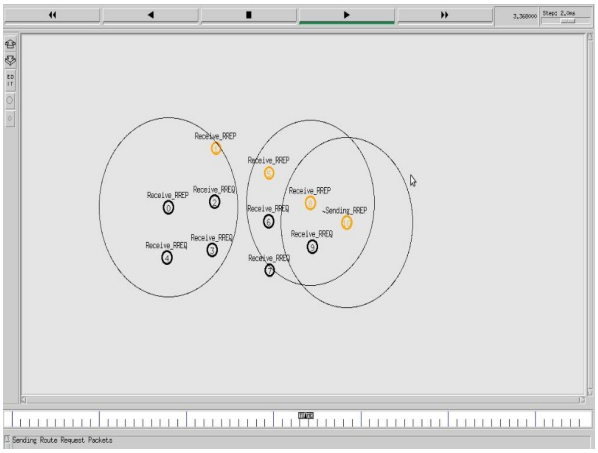

Fig.6. Establishment of path and transferring of data

6. When all the nodes receive RREQ message then they send RREP message to source to confirm that they have received the route establishment packet. When source receives RREP messsage from all the nodes then select final route for communication.

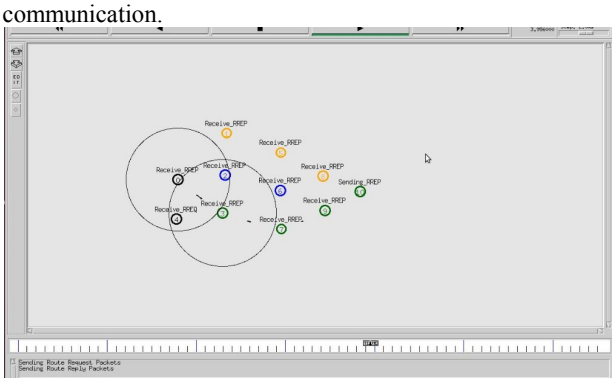

Fig.7. Final route establishment from source to destination

7. When source sends packets on its route then selfish node triggers and redirects its path and packets are dropped which degrades the security of the system. So the communication from the transmitter to the receiver is seized. No data will now

be received at the receiver due to the working of this selfish node.

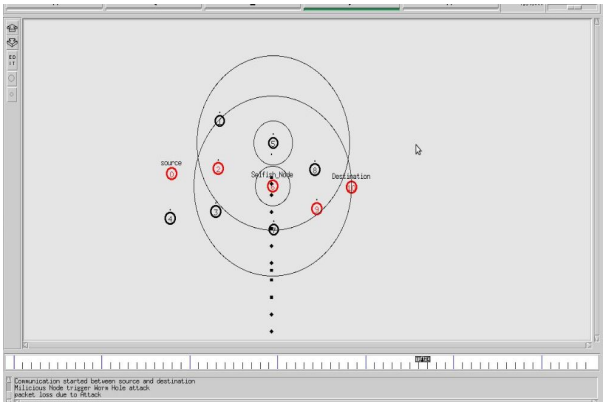

Fig.8. Packet loss due to selfish node triggering

IV. RESULTS

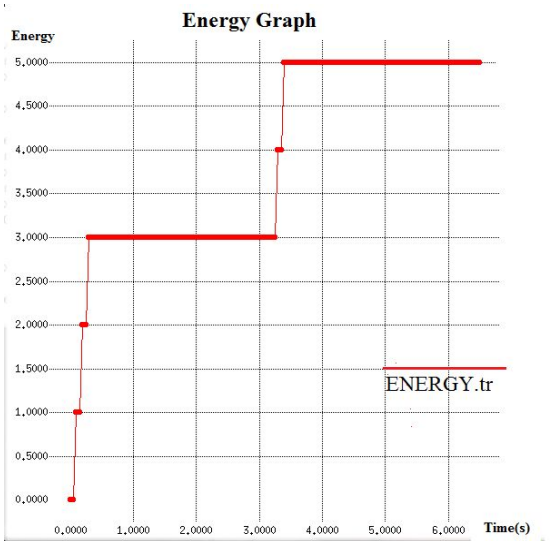

Fig.9.Energy required by packets in jammed network

In above fig. it is shown that how energy of the packets varies when a network associated with it is jammed.

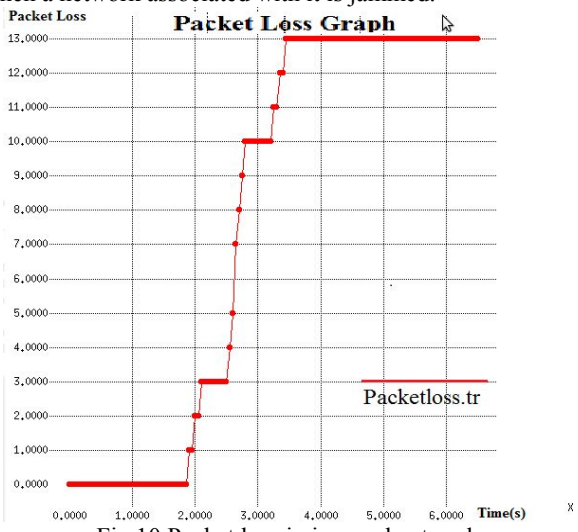

Fig.10.Packet loss in jammed network

In above fig. effects of jamming on packet loss is shown. It is found that the number of packets at the receiving end will be much lesser than that are being sent by the transmitter.

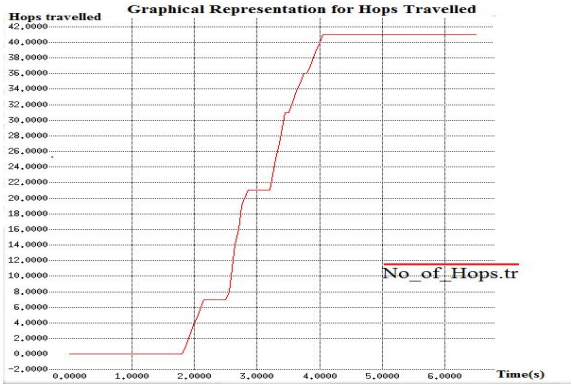

Fig.11.Hops travelled in jammed network

Above fig. represents how the no, of hops required to reach the destination from source changes as a malicious node enters in the network and tries to jam the network.

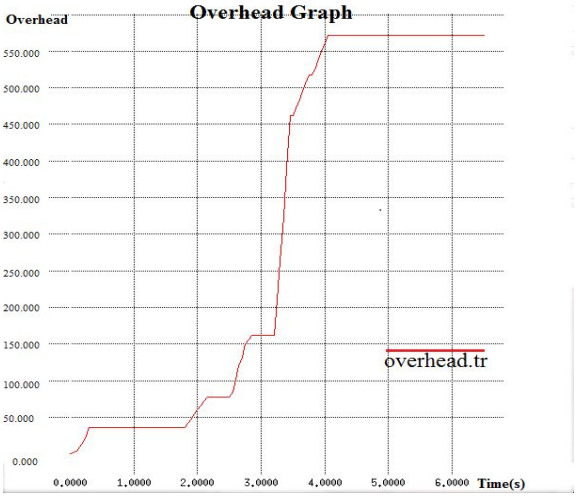

Fig.12.Overhead in jammed network

Above fig. shows how the routing overhead of the system increases when the packets are jammed by the malicious node to reach at the receiver.

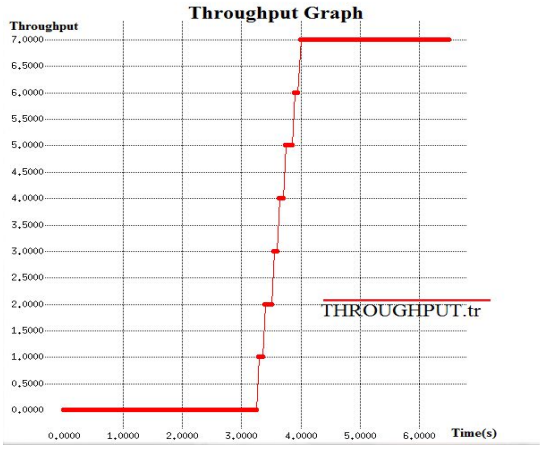

Fig.13 Throughput in the network

Above fig. shows the effects on the throughput of the system when the jamming effect has occurred in the system.

CONCLUSION AND FUTURE SCOPE

We have studied the effects of jamming attack in MANETs. We have studied about the manner in which these jamming attacks can occur in the network. In our simulation, we have found that energy of the packets sent differ if jamming attack occurs. It is seen that routing overhead and no. of hops travelled by the packets increase. It is also found that packet loss increases as the total no. of packets that are delivered at the receiving end are decreased. Throughput of the system is also varied when jamming is occurring.

We can find out the ways to combat these jamming attacks. So to find out ways to countermeasure against these attacks comes under the latest research topics.

REFERENCES

[1] G. Jayanthi Lakshmi, S. Babu, B Lakshmana Rao, P Mohan and B Sunil Kumar, "Jamming Attacks Prevention in Wireless Sensor Networks Using Secure Packet Hiding Method'', International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 9, September 2013

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

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

[4] Tien-Ho Chen and Wei-Kuan, Shih, "A Robust Mutual Authentication Protocol for Wireless Sensor Networks" ETRI Journal, Volume 32, Number 5, October 2010

[5] Baljinder Singh and Dinesh Kumar, " Jamming attack in MANET: A Selected Review", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 4, April 2015.

[6] Mr. Pushphas Chaturvedi and Mr. Kunal Gupta , "Detection and Prevention of various types of Jamming Attacks in Wireless Networks", IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.3, No2, April 2013

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

[8] A.D. Wood and J.A.Stankovic, "Denial of Service in Sensor networks",computer, vol.35, no.10, pp. 54-62,2002.

[9] Karim El Defrawy, and Gene Tsudik , "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs", IEEE TRANSACTIONS ON MOBILE COMPUTING, Vol. 10, No. 9, September 2011

[10] Abderrahim Benslimane, El Yakoubi and Mohammed Bouhorma "Analysis of Jamming effects on IEEE 802.11 Wireless Networks'', IEEE, 2011.

[11] Deepali Arora, Eamon Millman and Stephen W. Neville "Jamming Strategies on the Behavior of DYMO-based MANETs: Assessing Detectability and Operational Impacts'', International Conference on Broadband and Wireless Computing, Communication and Applications, 2012.

[12] M.K.Simon, J.K.Omura, R.A.Scholtz, and B.K.Levitt, "Spread Spectrum Communications Handbook," McGraw-Hill, 2001

Henna Khosla She is a student of M.Tech (ECE) at Department of Electronics and Communication Engineering, Punjabi university Patiala. She has done her B.Tech from PTU, Kapurthla. Her area of interest is wireless communication. Specifically she is working on wireless sensor networks.

Rupinder Kaur She is presently working as Assistant Professor in Department of Electronics and Communication Engineering, Punjabi university Patiala. She has done her M.Tech from GNDU, Amritsar. Her area of interest is wireless communication and has 4 publications in her specialized field.