Isolation Mechanism for Jamming Attack in MANET

Aditi[1], **Joy Karan Singh**[2]
[1]M.tech Student, Dept. of CSE,CT Institute of Technology & Research , Jalandhar,India
[2]Assistant Professor , Dept. of ECE,CT Institute of Technology & Research , Jalandhar, India
Email – sweetgagan608@gmail.com, joysachar@gmail.com

Abstract: Mobile ad-hoc networks (MANET) are more receptive to security attacks because of their distinctive features i.e. dynamic configuration and no static infrastructure etc. The necessity for a protected MANET networks is powerfully attached to the privacy and security attributes. Jamming attack is one of them. This attack influenced the network by decreasing the network performance. In this paper work we are evaluate the performance of mobile ad hoc networks with jamming attack and with a novel mechanism. The network performance is evaluated in terms of the QoS parameters i.e. packet loss, energy, PDR, retransmission attempts and throughput.

Key Words: Jamming Attack, Throughput, PDR, Energy, Retransmission attempts, Packet loss.

1. INTRODUCTION:

Mobile Ad-hoc Network (MANET) attached in a dynamic manner and it is an assembly of wireless mobile nodes. Without any fixed infrastructure nodes making a temporary network where all nodes are arbitrarily free to move. In the network nodes are act as routers, which take part in finding and maintenance of routes to other nodes [1]. Wireless connection in MANET is highly misplay and due to mobility of nodes it goes down usually. Due to highly dynamic environment coherent routing is a very difficult task in Mobile Ad-hoc Network [2].

In this paper, we esteem a particular category of DoS attacks called Jamming. In actual fact, the mobile host in mobile ad hoc networks is a part of wireless medium. Thus, the radio signals can be jammed or interfered, which make the message to be amoral or missed. If the attacker has a strong transmitter, a signal can be launched that will be strong enough to conquer the directed signals and distort communications. There are several attack schemes that a jammer can do in order to interfere with other wireless communications.

1.1 Jamming attack:

The motive of jamming attack is to fill up the communication channel with purposeless signals, due to which verified or permissible user cannot use it. Jamming slowly down the receiving and sending of messages at the destination. It is very difficult to prevent and find out the jamming attacks but still some detection algorithms are struggling to prevent the prospects of jamming attack. Another motive of Jammers is to conceal themselves from the detection algorithms so that they can begin with jamming of some particular region. [17].

- **Constant Jammer:** A constant jammer is the signal alternator that does not obey any MAC protocol and it continuously released radio signal that represents random bits.
- **Deceptive Jammer:** They dispatch semi-valid packets. This means that the payload is bootless but the packet header is sustainable.
- **Random Jammer:** Substitutes between sleeping and jamming the channel. In the first modus the jammer jams for a casual period of time (it can behaves like a constant jammer or as a deceptive jammer), and in the second modus (the sleeping mode) the jammer spins its transmitters off for a different random period of time. The energy efficiency is regulates as the ratio of the length of the jamming period upon the length of the sleeping period.
- **Reactive Jammer:** A reactive jammer attempts not to misspend resources by only jamming when it recognize that somebody is transmitting. Its object is not the sender but the receiver, taxing to input as much noise as possible in the packet to improve as many bits as possible given that only a small amount of power is required to modify sufficient bits so that when a checksum is execute over that packet at the receiver it will be categorized as not valid and therefore discarded.

2. RELATED WORK:

A numeral of previous works has been done for the detection of jamming attacks.

Wood et al. [2003] represented a novel mapping service to find out jamming attacks. JAM (Jamming Area Mapping) is a service that delivered quick and exact jamming attack reply. With the aid of this mapping service, we acquire the geographic information which informs us about the jamming area. In this technique extra particular hardware is not required which build it cost effective [2].

P. Yi et al. [2005] proposed an easy method so that flooding attacks can be averted. In this method, every node monitors and delibrates the request rate of neighborhood nodes. Now when the request appears it contrast the request rate of adjacent node with the predefined threshold. If the threshold value exceeds, then node record the ID of that node in a check-list. In future if any request appears from the node stored in the check-list, is discarded [4].

Liu et al. [2012] proposed a novel two-phase jamming detection method for sensor networks. In first phase, some signs of jamming are identified speedily. When signs are found then second phase of detection is applied. In this technique we don't requires any extra communication or hardware [19].

Babar et al. [2013] represented the game theoretic model of the jamming attack. This paper suggested a game theory based detection technique which is utilized to detect all kinds of jamming attack. This method provides better performance in words of delay, energy and throughput also [20].

S. T. et al. [2014] represented a profile based technique which is utilized to detect and suspend the flooding attack on MANET with the help Adhoc on Demand Distance Vector (AODV) routing protocol. In this technique every single node has a profile value. These profile values are put on the base of behavior of MANET. Whenever the node attempts to overreach the fixed threshold value, the attack will be identified and isolated. The key benefit of this technique is that threshold value is not defined; it is based on the average request permitted in the network which changed with the number of request in the network [22].

3. SIMULATION ENVIRONMENT:

To analyse the consequence of jamming attack AODV routing protocol is used. Our focus is to find out the attacker node that rushes the network with RREQ packets. Simulation is brings out in NS2 simulator with 22 nodes in the network. Simulation is performed to show the jamming attack and after that detection is done with the help of an efficient method. Some other parameters are shown in table 1.

Table 1. Simulation Parameters

Name	Simulation parameters
Protocol	AODV
Simulator	NS-2
Simulation area	800m×800m
Channel type	Wireless
Number of sensor nodes	22
MAC type	Mac/802_11
Attacker Node	1
Operation mode	Active
Packet size	1000 bytes
Application traffic	CBR
Data rate	1 packet at 0.05 sec
Simulation time	6.5sec

4. RESULT:

The metrics are the essential determinants which are used to find out the network performance. With the help of metrics we can assess the performance of the well organised scheme. We select five main metrics to evaluate the performance of our schemes namely energy spent, retransmission attempts, throughput, packet delivery ratio and packet loss.

4.1 Energy spent

Average energy consumed by the sensor nodes in the network is one of the essential metrics to assess the energy efficiency of routing protocol. In jamming attack, due to the existence of an attacker there is no victorious transmission. Due to that, energy consumed is the highest.

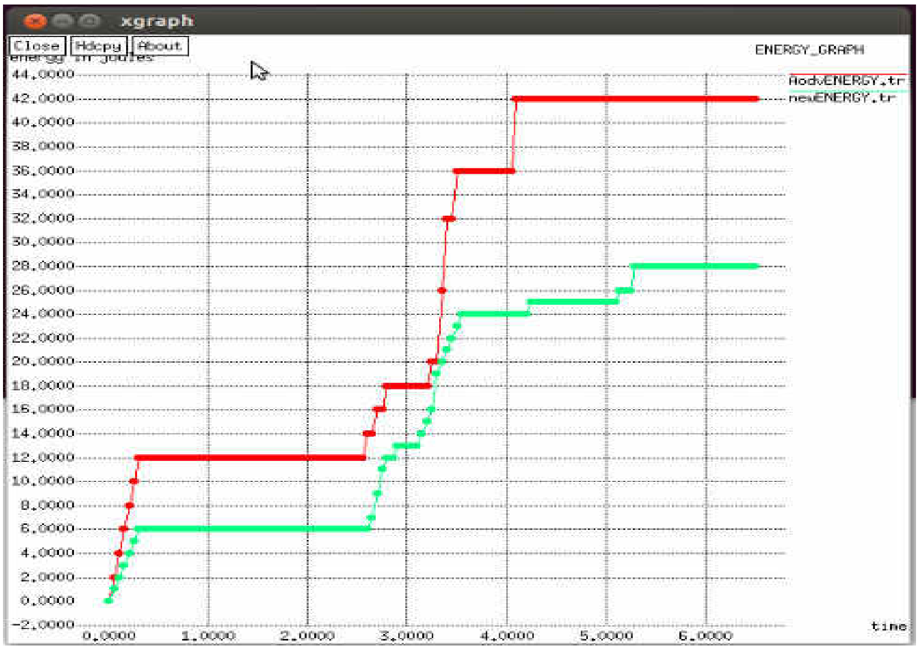

Figure 1. Energy spent graph

4.2 Throughput

The throughput represents the ratio of numbers of data packets sent by the source node to the number of data packets received by the destination.

$$\text{Throughput} = \frac{\text{No. of data packets sent}}{\text{No. of data packets received}}$$

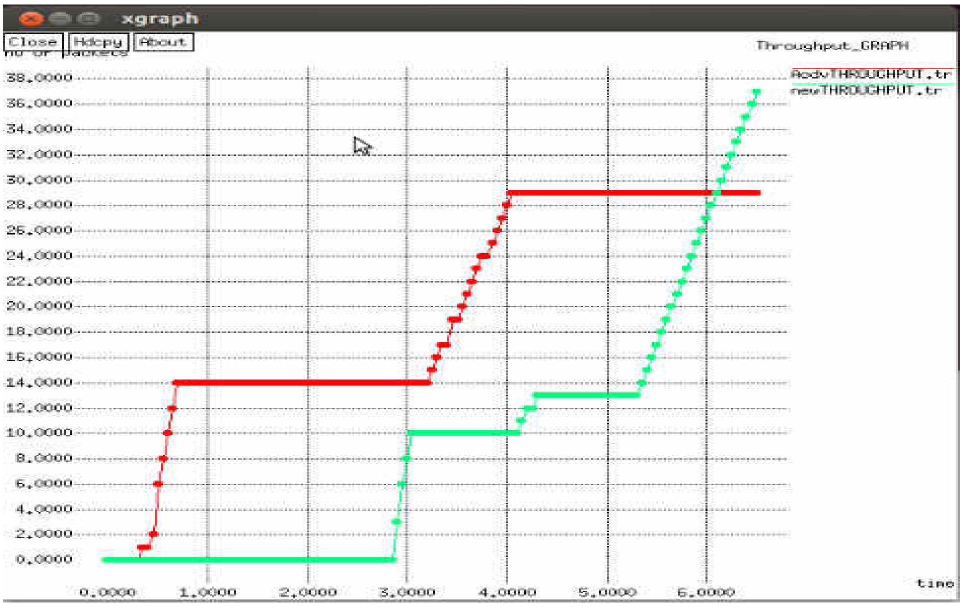

Figure 2. Throughput graph

4.3 Packet Delivery ratio

The packet delivery ratio is the ratio of total number of packets received at destination node to that of total number of packets sent by the source node.

$$\text{Packet delivery ratio} = \frac{\text{Total no. of packets receive}}{\text{Total no. of packets sent}}$$

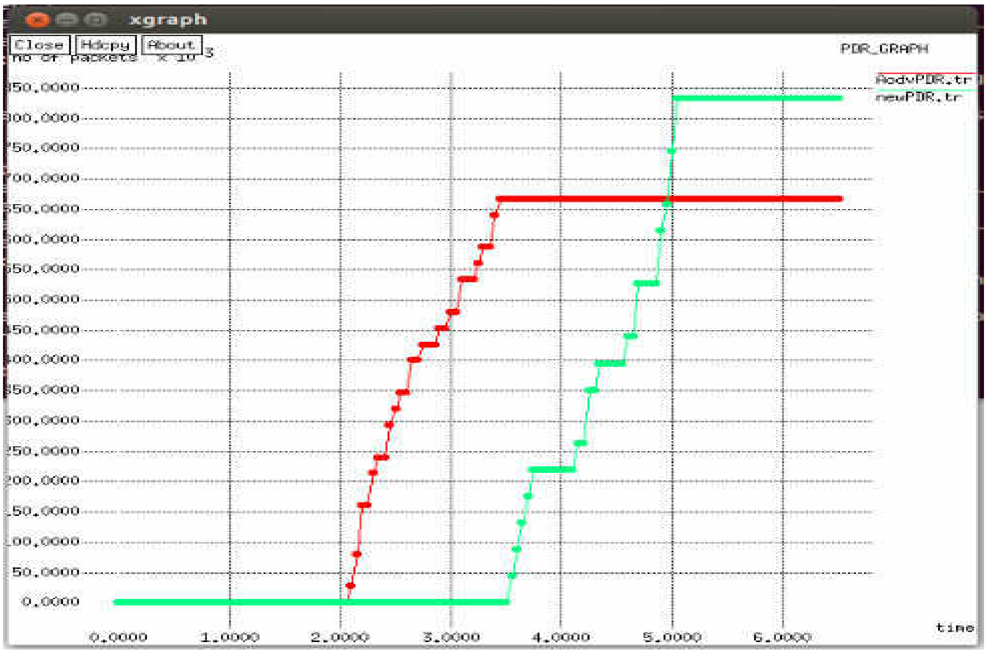

Figure 3. PDR graph

4.4 Packet loss

Packet loss is defined as total number of packets dropped in the network.
Packet loss = Total number of packet send – Total number of packet received

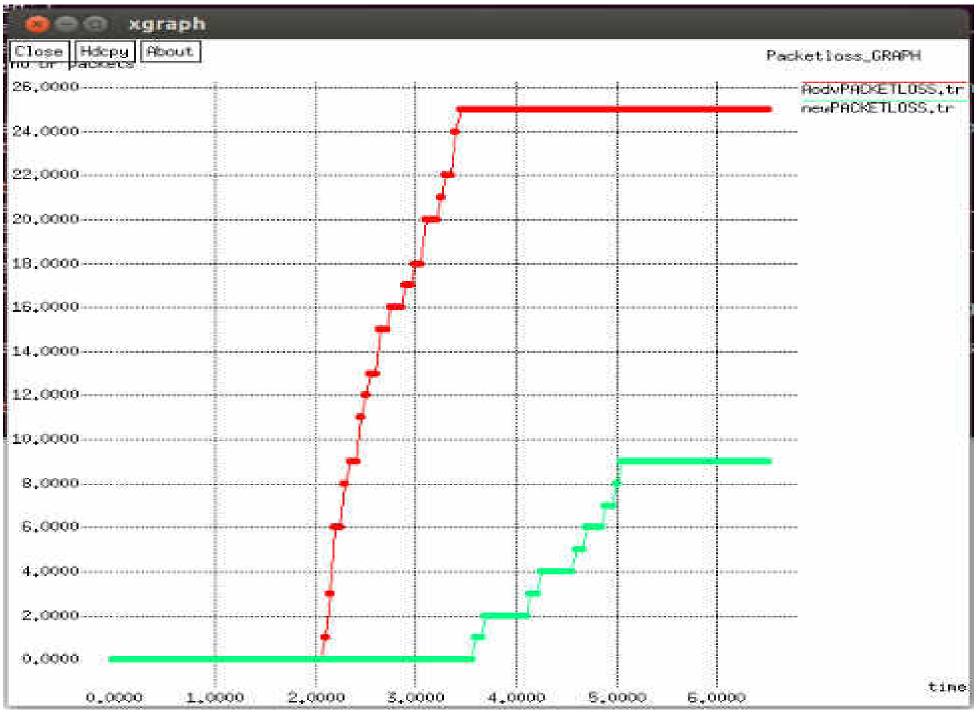

Figure 4. Packetloss graph

4.5 Retransmission Attempts

Retransmission attempts happened in network only when the delivery of packet is dropped or lost without reaching to the destination nodes.

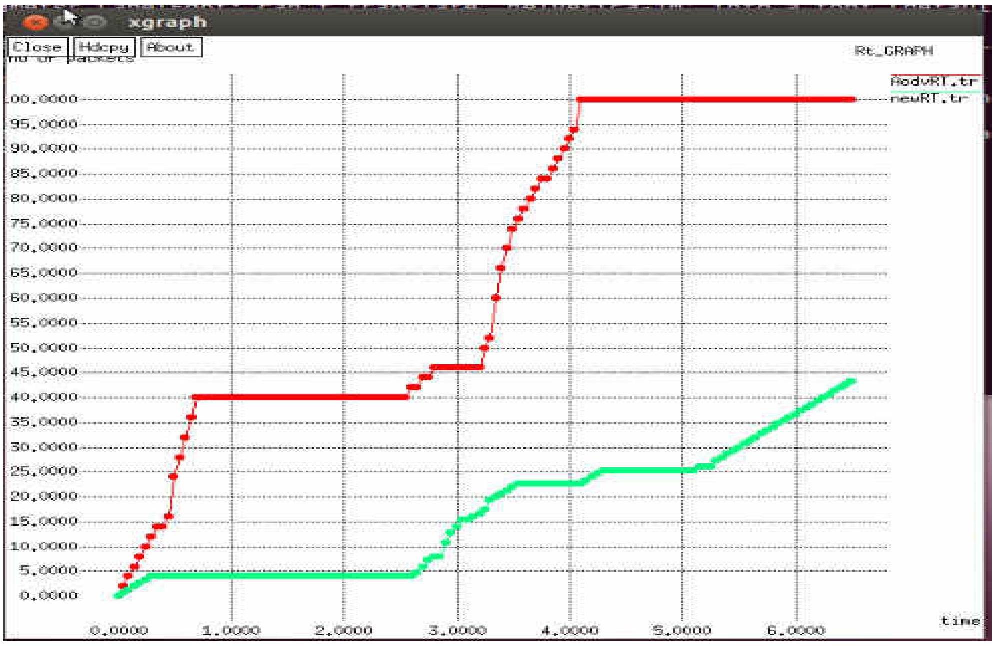

Figure 5. Retransmission attempts graph

5. CONCLUSION:

Sensor Networks are commonly used in various fields for data monitoring purposes. They are helpful in mainly industrial, civilian and scientific applications. So it is important to detect jamming attack quickly because this attack seed DDoS on WSN. This paper recommends an efficient procedure for detection of these attacks. In this procedure monitor modes are used to isolate the harmful path. To isolate the attack source deluge (flood) ICMP packets in the network. Nodes which collect ICMP packets go to the monitor mode. One node which is neighbour to the harmful node detects malicious node and send message to source node to isolate the path. Now source node isolate the path and other path will be select for the communication.

The scheme has been assessed using the simulator NS-2. The output of our implementation presents superior impact to overcome the jamming attack. This method noteworthy refines system performance and we find that the method launched is efficient because it detect jamming attack with less retransmission attempts, less energy spent, more throughput, less packet loss and more packet delivery ratio.

REFERENCES:

1. Yi S., and Kravets R., “Key Management for Heterogeneous Ad Hoc Wireless Networks” , 10th IEEE International Conference on Network Protocols (ICNP’02) 1092-1648,2002 .
2. A. D. Wood, J. A. Stankovic, and S. H. Son “JAM: A Jammed-Area Mapping Service for Sensor Networks” Proceedings of the 24th IEEE International Real-Time Systems Symposium (RTSS’03), IEEE, 2003.
3. Karthikeyan U., and Rajni ,“Security Issues Pertaining to Ad-Hoc Networks”, 2004.
4. Kyasanur P., “Selfish MAC layer Misbehavior in wireless networks”, IEEE on Mobile Computing, 2005.
5. P. Yi et al., “A New Routing Attack in Mobile Ad Hoc Networks,” Int’l. J. Info. Tech., vol. 11, no. 2, 2005.
6. Wu B., Chen J., Wu J., and Cardei M., “A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks” ,Springer ,2007.
7. Chee V., and Yau W., "Security analysis of TORA routing protocol," Computational Science and Its Applications–ICCSA. Springer Berlin Heidelberg, pp. 975-986 , 2007.
8. Tang C., and Oilver D., “An Efficient Mobile Authentication Scheme for Wireless Networks”,IEEE, 2008.
9. Hamieh A., and Othman J., “Detection of Jamming Attacks in Wireless Ad Hoc Networks using Error Distribution”, IEEE, 2009.

10. Lazos L., Liu S., and Krunz M., “Mitigating Control-Channel Jamming Attacks in Multi-channel Ad Hoc Networks” ACM, WiSec’09, March 16–18,Zurich, Switzerland, 2009.
11. Dempsey T., Sahin G., and Morton Y., "Passive and Active Analysis in DSR-Based Ad Hoc Networks," Ad Hoc Networks. Springer Berlin Heidelberg , pp. 623-638 , 2010.
12. Chen T., and Kuan W., “A Robust Mutual Authentication Protocol for Wireless Sensor Networks” ETRI Journal, Volume 32, Number 5, October 2010.
13. Cicho J., Kapelko R., Lemiesz J., and Zawada M., “On Alarm Protocol in Wireless Sensor Networks”,IEEE, 2010.
14. Şen S., Clark J., and Tapiador j., “Security Threats in Mobile Ad Hoc Networks”, IEEE, 2010.
15. Defrawy K., and Tsudik G., “ALARM: Anonymous Location-Aided Routing in Suspicious MANETs”, IEEE, Vol. 10, No. 9, September 2011.
16. Donggang L., Raymer J., and Fox A., "Efficient and timely jamming detection in wireless sensor networks." Mobile Adhoc and Sensor Systems (MASS), 2012 IEEE 9th International Conference on. IEEE, 2012.
17. A. Mummoorthy , S. S. Kumar “A Detailed Study on the Evolution of Recent Jammers in Wireless Sensor Networks” in International Journal of Engineering Research and Development Volume 4, Issue 6 (October 2012), PP. 12-15.
18. D. Liu, J. Raymer, A. Fox “Efficient and Timely Jamming Detection in Wireless Sensor Networks” in 9th International Conference on Mobile Adhoc and Sensor Systems MASS, page 335-343. IEEE Computer Society, *(*December 2012*)*
19. S. D. Babar, N. R. Prasad, R. Prasad “Game Theoretic Modelling of WSN Jamming Attack and Detection Mechanism” Published in Wireless Personal Multimedia Communications (WPMC), 2013.
20. Rajakumar P., Prasanna T., and Pitchaikkannu A. "Security attacks and detection schemes in MANET," Electronics and Communication Systems (ICECS), 2014 International Conference on. IEEE, 2014.
21. Sathish. T, Sasikala. E” Dynamic Profile Based Technique to Detect Flooding Attack in MANET” in International Journal of Innovative Research in Computer and Communication Engineering Vol.2, Special Issue 1, March 2014.
22. Kapur R., and Khatri S., "Analysis of attacks on routing protocols in MANETs," Computer Engineering and Applications (ICACEA), 2015 International Conference on Advances in. IEEE, pp. 791-798, 2015.
23. Khan M., Jadoon Q., and Khan M., "A Comparative Performance Analysis of MANET Routing Protocols under Security Attacks,” Mobile and Wireless Technology 2015. Springer Berlin Heidelberg, pp.137-145, 2015.