Elimination of Jamming Attack in Ad Hoc Environment

Mohit Sharma[1] Renu Singla[2]

M-Tech Student[1], Assit. Prof.[2] & Department of CSE & Shri Ram College of Engg. & Mgmt
Palwal, Haryana, India

***Abstract*— MANETs have unique features i.e. dynamic configuration, wireless radio medium, restricted resources and lack of centralized management; as a result, they are susceptible to various kinds of attacks in many layers of protocol stack. Every node in a MANET is able of functioning as a router. The requirement for a protected MANET networks is powerfully connected to the privacy and security characteristics. This Jamming attacks are one of them. These happen by transmitting continuous radio waves to inhibit the transmission between receiver and sender. These attacks influence the network by reducing the network performance. Formerly there had been significant research in the field of enhancing the network performance by employing routing protocols.**

In our paper work we are enhancing the performance of mobile ad hoc networks under jamming attack by utilizing a CTS/RTS integrated method. The suggested work involves a network with high mobility, utilizing IEEE Along a standard with enhanced AODV (Ad hoc On Demand Distance Vector) routing protocol parameters. Video conferencing and FTP with large data rate are being created in the network. The network performance is evaluated in terms of the QoS parameters i.e. delay and throughput. OPNET (Optimized Network Engineering Tool) Simulator 16.0 is employed for simulation. The results of simulation establish that the total network performance with jamming attack has been enhanced by utilizing the integrated method.

Keywords: MANETs, Jamming Attack, Throughput, OPNET.

I. INTRODUCTION

The growing demand of wireless devices and wireless communication have tends to research on self-healing, self-configuring, networks without the disturbance of any pre-established or centralized infrastructure/authority. The networks with the absence of any centralized or pre-established management are called Ad hoc networks. Ad hoc Networks are the part of wireless networks that utilizes multi hop radio relay. Mobile Ad-hoc Network (MANET) is a set of wireless mobile nodes and associated in dynamic way. Nodes making a temporary/short-lived network without any static infrastructure where all nodes are free to move about randomly.

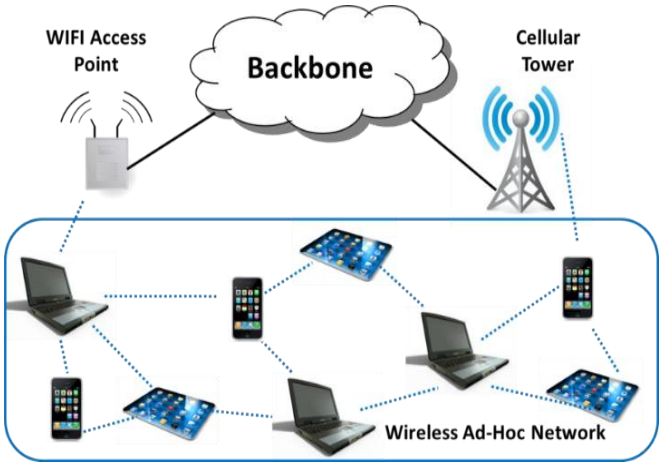

Figure 1 Mobile Ad Hoc Networks

Nodes must act as routers, take part in finding and maintenance of paths to another nodes in the network [1] Wireless links in MANET are greatly error prone and can go down quickly because of mobility of nodes. Stable routing is a very vital task because of highly dynamic infrastructure in Mobile Ad-hoc Network [2]. So mobile ad-hoc network (MANET) is a self-organizing network of mobile routers (and associated hosts) linked by wireless links - the union of which make a random configuration. The routers are free to move arbitrarily and configure themselves at random. This type of network may operate in a standalone manner, or may be associated to the larger Internet. Minimal topology and frequent deployment build ad hoc networks appropriate for emergency conditions i.e. military conflicts, natural or human induced dissters, and emergency medical situations. [3]

II. RELATED WORK

Sisi Liu et al. (2012) here authors discuss the problem of removing Denial of service (DoS) attacks available in the form of jamming. They took an advanced adversary who has knowledge of the cryptographic quantities and of the protocol particulars used to secure network operations. This type of adversary cannot be stopped by anti jamming methods that believe on spread spectrum. They proposed a new security metrics to evaluate the ability of the adversary to deny access to the control channel, and got a randomized distributed

ISSN: 2278 – 7798

system that allows nodes to establish and keep the control channel in the availability of the jammer. The proposed method is related to networks with statically or dynamic distributed spectrum. Furthermore, two algorithms for unique identification of the set of decided nodes were proposed, one for independently acting nodes and other for colluding nodes[19].

Dorus.R et al. (2013) presents a process for preventing jamming attacks on wireless networks, examine the perception efficiency of communication overhead and jamming attack of the wireless network by utilizing proactive and reactive protocols. RSA algorithm is used and analyzed for providing data packets integrity information in wireless transmission. After performance examine and simulation, the conducted prevention mechanism and the integrity preservation provides higher packet delivery ratio in proactive routing protocol (OLSR) in comparison of reactive routing protocol (AODV).

Nadeem Sufyan et al. (2013) see into a multi-modal system that simulates several jamming attacks by discovering the relation among three parameters: packet delivery ratio, signal strength variation and pulse width of the obtained signal.

III. Methodology Used

This section explains the simulation tool employed along with the suggested method.

Simulation tool used:

OPNET Simulator (16.0) is broad and a very powerful simulation software with large variety of possibilities. The whole heterogeneous networks with several routing protocols can be modeled utilizing OPNET. High level of user interface is employed in OPNET which is made from C and C++ source code blocks.

Simulation Setup:

The simulation concentrates on enhancing of MANETs performance under jamming attack. Thus an Integrated method is utilized to enhance the network performance under jamming attack. This method involves:

- Network with high mobility
- High data rate of 54mbps by utilizing IEEE 802.11g standard
- Enhanced parameter of AODV routing protocol
- Generation of high resolution FTP traffic and video conferencing.

IV. Simulation Model and Experiment Design

The tool employed for the simulation study is OPNET 14.5 Simulator. OPNET is a application and network based software utilized for network analysis and management [9-10]. OPNET simulates communication devices, architecture of different networks and technologies, various protocols and offers simulation of their performances in the virtual environment. OPNET offers several research and development solutions which supports in the research of analysis and enhancement of wireless technologies i.e. Wi-Fi, WIMAX, UMTS, examining and designing of MANET protocols, enhancing core network technology, offering power management solutions in wireless sensor networks. In our case we employ OPNET for simulating of network nodes, choosing its statistics and then running its simulation to obtain the result for analysis. In this simulation experiment, 3 various scenarios are generated and illustrated by the OPNET simulation package.

Table I: MANET Simulation Parameters

Examined Protocols Cases	AODV without Jamming Attack
Number of Nodes	100 and 200
Types of Nodes	Mobile
Simulation Area	60*60 km
Simulation Time	3600 seconds
Mobility	Uniform(10-100) m/s
Pause Time	200 seconds
Performance Parameters	Throughput, Delay, Net.load
Trajectory	VECTOR
Long Retry Limit	4
Max Receive Lifetime	0.5 seconds
Buffer Size(bits)	25600
Mobility model used	Random waypoint
Data Type	Constant Bit Rate (CBR)
Packet Size	512 bytes
Traffic type	FTP, Http
Active Route Timeout	4 sec.
Hello interval(sec)	1,2
Hello Loss	3
Timeout Buffer	2
Physical Characteristics	IEEE 802.11g (OFDM)
Data Rates(bps)	54 Mbps
Transmit Power	0.005

ISSN: 2278 – 7798

RTS Threshold	1024
Packet-Reception Threshold	-95

V. RESULTS

After introducing the basic results of all simulations conducting in both scenarios, we examine and talk about all these results. The performance metrics gathered and introduced in our results are either depends on the object statistics or global statistics of the MANET model i.e. the whole network. We examine and compare within every scenario and also both scenarios based on their end-to-end delay and throughput.

5.1: Throughput:

Throughput can be defined as the ratio of the overall amount of data arrive a destination node from the source node. The time it considers by the destination node to obtain the last message is known as throughput. It can represent as bytes or bits per seconds (byte/sec or bit/sec). There are many factors that influence the throughput i.e. changes in configuration, availability of restricted bandwidth, unreliable communication between nodes and restricted energy. A high throughput is absolute selection in each network. In figure the graph displays the throughput in bits/seconds. The x-axis represents the simulation time in minutes and the y-axis represents throughput in bits per seconds.

Scenario 1 shows the scenario with no harmful event and general network state,

Scenario 2 shows the network that is under the jamming attack

Scenario 3 shows the mobile jammers and implementation of the suggested method.

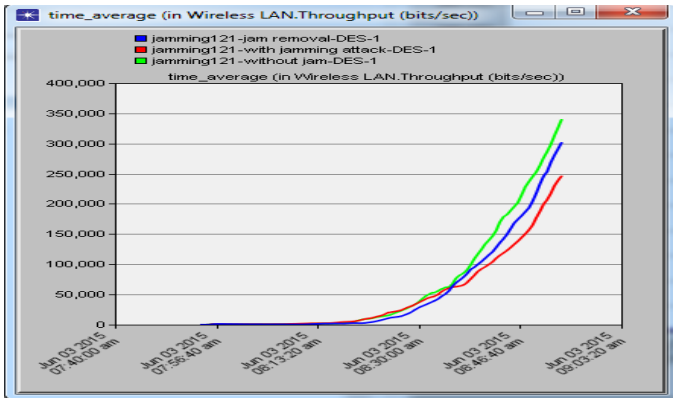

Figure: 2 Throughput of all three scenarios at 100 nodes

Table: 5.1 Throughput of all three scenarios at 100 nodes

No. of Nodes	Without Jamming	With Jamming	Jam Removal
100	350064	300435	310054
200	14563478	10435675	14206537

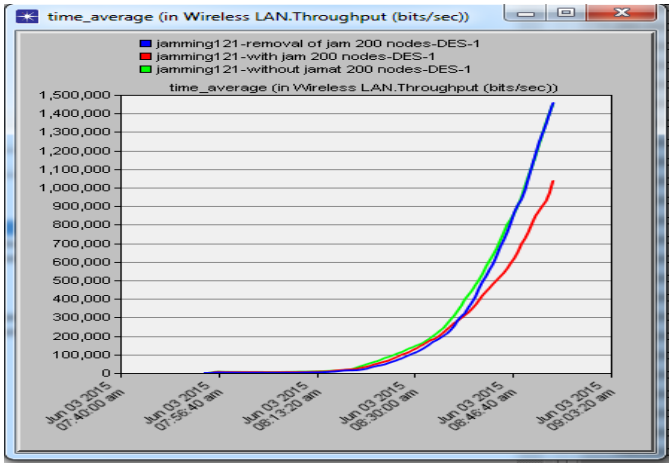

Figure: 3 Throughput of all three scenarios at 200 nodes

This loss of packets in form of throughput is because of the jamming effect. The recovery of the throughput takes place with suggested method by removing of the jamming attack as throughput comes to same to the normal scenario.

5.2 End to End Delay:

The packet end to end delay is the mean time that packets consider to travel in the network. This is the time from the creation of the packet by the sender node up to their reception at the destination node and is measured in seconds. Thus all the delays in the network are known as packet end-to-end delay. It involves all the delays in the network i.e. processing delay (PD,) propagation delay (PD), queuing delay (QD), transmission delay (TD).

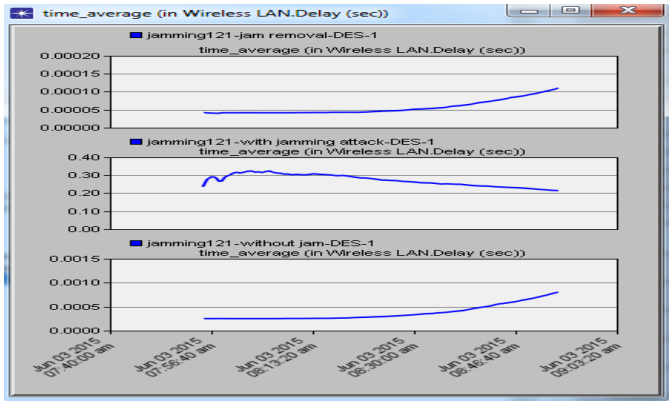

Figure: 4 Delay of all three scenarios at 100 nodes

Table 5.2 Delay of all three scenarios at 100 and 200 nodes

No. of Nodes	Without Jamming	With Jamming	Jam Removal
100	0.0010	0.35	0.0007
200	0.0020	0.30	0.0021

ISSN: 2278 – 7798

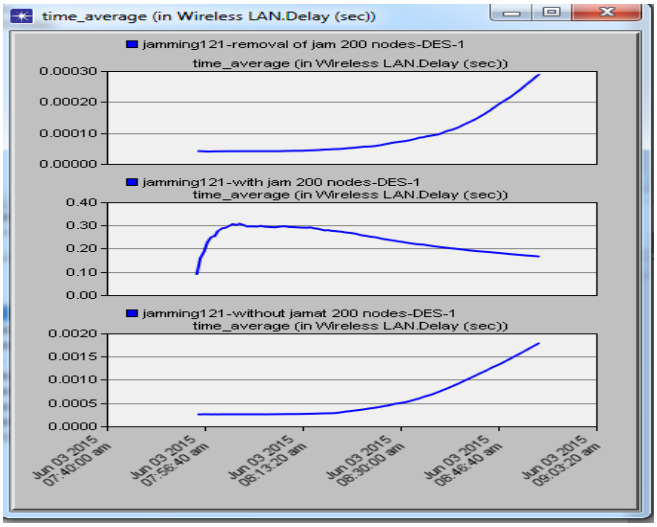

Figure: 5 Delay of all three scenarios at 200 nodes

The recovery of the end to end delay reduces with our suggested method by elimination of the jamming attack as end to end delay comes to same to the value 0.000256 seconds. Thus our suggested mechanism removes jamming attack in network

CONCLUSION

Jammers attacks will have an impact on performance of network as a result of the jammers disrupts with the conventional operation of the network. The impact of attackers studied was by data dropped traffic obtained and sent, increasing delay, and reducing packer loss ratio of the network. The network performance under jamming attack is examining by employing integrated method. The objective of this simulation research study was to realize the effect of a combination of security methods against jamming attacks. The unified mechanism is implemented on the chosen nodes on the network and deployed in the particular region. The discoveries of the research clearly describes that, the implementation of these unified mechanisms have a important effect on the total network throughput positively. On the other side, the implementation of these mechanisms does not only mitigate the jamming attack impacts, it also improves the total performance above the normal state of the network. The unified mechanism that consist a combination of PCF and RTS/CTS displays sufficient performance in MANET. Since 2 mobile jammers utilized in this simulation experiment, the suggested security mechanism sufficiently mitigated the impacts of the jamming attack on the network and improved the total performance of the network while increasing data drop rate. The data dropped rate reduces successfully. Since the jamming attack causes packet drop rate and low throughput effect on the network, the rate of delay seems satisfactory on the network. Future studies can be conducted to change the current model to reduce a total delay on the network.

FUTURE WORK

We assume future research works concentrated on utilizing real time attacks which is required to determine greater degree of detection of particular susceptibilities in both Mobile and ad hoc Sensor networks. Depending on the attack classifications in many levels specified in this work, it becomes imperative to identify a representative set of attacks that can sequentially be utilized in raw attack generations to measure IDS is a more systematic way. However depending on our simulations and for more accurate representation of data set, there is requirements to further incorporate error correction algorithms utilized to examine the degree of anomalies and implement this into Riverbed Simulator. Also we intend to explore more possibilities for determination of sophisticated attacks by incorporating a cryptographic security strategy utilizing trust certificates and expand the results as well to other wireless protocols. This would support as a baseline action for further research problems in Intrusion detection systems (IDS).

REFERENCES

[1] Fatima Ameza, Nassima Assam and Rachid Beghdad, “Defending AODV Routing Protocol Against the Black Hole Attack”, International Journal of Computer Science and Information Security, Vol. 8, No.2, 2010, pp.112-117.

[2] Nital Mistry, Devesh C. Jinwala and Mukesh Zaveri, “Improving AODV Protocol against Blackhole Attacks”, International Multiconference of Engineers and Computer Scientists 2010, vol. 2, March 2010.

[3] Payal N. Raj and Prashant B. Swadas,”DPRAODV: A dynamic learning system against black hole attack in AODV based Manet”, International Journal of Computer Science Issues, Vol. 2, Issue 3, 2010, pp: 54-59.

[4] Hoang Lan Nguyen and Uyen Trang Nguyen, ”Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks”, International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, April 2006, pp. 149-149

[5] Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar and Bhavin I. Shah, “MANET Routing Protocols and Wormhole Attack against AODV”, International Journal of Computer Science and Network Security, vol. 10 No. 4, April 2010, pp. 12-18.

[6] N. Shanthi, Dr. Lganesan and Dr.K.Ramar, “Study of Different Attacks on Multicast Mobile Ad hoc Network”,

ISSN: 2278 – 7798

Journal of Theoretical and Applied Information Technology, December 2009, pp. 45-51.

[7] Abhay Kumar Rai, Rajiv Ranjan Tewari and Saurabh Kant Upadhyay , "Different Types of Attacks on Integrated MANET-Internet Communication", International Journal of Computer Science and Security, vol. 4 issue 3, July 2010, pp. 265-274.

[8] Jakob Eriksson, Srikanth V. Krishnamurthy, Michalis Faloutsos, "TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks", 14th IEEE International Conference on Network Protocols, November 2006, pp.75-84.

[9] Mahdi Taheri, Dr. majid naderi, Mohammad Bagher Barekatain, "New Approach for Detection and defending the Wormhole Attacks in Wireless Ad Hoc Networks", 18th Iranian Conference on Electrical Engineering,, May 2010, pp. 331-335.

[10] Dang Quan Nguyen and Louise Lamont, "A Simple and Efficient Detection of Wormhole Attacks", New Technologies, Mobility and Security, November 2008, pp. 1-5.

[11] Viren Mahajan, Maitreya Natu, and Adarshpal Sethi, "Analysis of Wormhole Intrusion Attacks in MANETs", Military Communications Conference, November 2008, pp.1-7.

[12] Maria A. Gorlatova, Peter C. Mason, Maoyu Wang, Louise Lamont, Ramiro Liscano, "Detecting Wormhole Attacks in Mobile Ad HocNetworks through Protocol Breaking and Packet Timing Analysis", Military Communications Conference, October 2006, pp. 1-7.

[13] Mani Arora, Rama Krishna Challa and Divya Bansal, "Performance Evaluation of Routing Protocols Based on Wormhole Attack in Wireless Mesh Networks", Second International Conference on Computer and Network Technology, 2010, pp. 102-104.

[14] Yih-Chun Hu, Adrian Perrig,and David B. Johnson, "Wormhole Attacks in Wireless Networks", IEEE Journal on Selected Areas in Communications, vol. 24 no. 2, February 2006, pp. 370-380.

[15] W. Weichao,B. Bharat, Y. Lu and X. Wu, "Defending against Wormhole Attacks in Mobile Ad Hoc Networks", Wiley Interscience, Wireless Communication and Mobile Computing, January 2006.

[16] L. Qian, N. Song, and X. Li, "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks Through Statistical Analysis of Multipath," IEEE Wireless Commuunication. and Networking Conference, 2005.

[17] I. Khalil, S. Bagchi, N. B. Shroff," A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks", International Conference on Dependable Systems and Networks, 2005.

[18] L. Lazos, R. Poovendram, C. Meadows, P. Syverson, L.W. Chang, "Preventing Wormhole Attacks on Wireless Ad Hoc Networks: a Graph Theoretical Approach", IEEE Communication Society, WCNC 2005.

[19] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks", 11th Network and Distributed System Security Symposium, pp.131-141, 2003.

[20] L.Lazos, R. Poovendran, "Serloc: Secure Range-Independent Localization for Wireless Sensor Networks",ACM Workshop on Wireless Security, pp. 21-30, October 2004.

ISSN: 2278 – 7798