ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 5, May 2016

Effect of Jamming Attack in Mobile Ad Hoc Environment

Pawani Popli[1], Paru Raj[2]

M-Tech Student[1], Assit. Prof.[2] & Department of CSE & Prannath Parnami Institute of Management & Technology Hisar, Haryana, India

***Abstract*—**
Mobile ad-hoc networks (MANET) are more susceptible to security attacks because of their special features i.e. dynamic configuration, no static infrastructure, and multi hop scenario and resource limitations. 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 evaluate the performance of mobile ad hoc networks with and without jamming attack. The suggested work involves a network with high mobility, utilizing IEEE Along a standard with AODV (Ad hoc On Demand Distance Vector) routing protocol parameters. Voice 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. end to end dealay delay and throughput. OPNET (Optimized Network Engineering Tool) Simulator v14.5 is employed for simulation purpose.

Keywords: ***MANETs, Jamming Attack, Throughput, Delay, OPNET.***

I. INTRODUCTION

Mobile Ad-hoc Network (MANET) connected in dynamic manner and it is a collection of wireless mobile nodes. Without any fixed infrastructure nodes making a temporary/short-lived network where all nodes are arbitrarily free to move. Nodes must act as routers, take part in discovery and maintenance of routes to other nodes in the network [1] Wireless connection in MANET are highly error prone and due to mobility of nodes it go down frequently. Due to highly dynamic environment stable routing is a very critical task in Mobile Ad-hoc Network [2].

In this paper, we consider a particular category of DoS attacks called Jamming. In fact, the mobile hosts in mobile ad hoc networks part a wireless medium. Thus, a radio signal can be jammed or interfered, which make the message to be corrupted or missed. If the attacker has a powerful transmitter, a signal can be generated that will be strong enough to overcome the directed signals and disrupt communications. There are lot of different attack scheme that a jammer can do in order to interfere with other wireless communications. Some possible strategies are exposed below [6]:

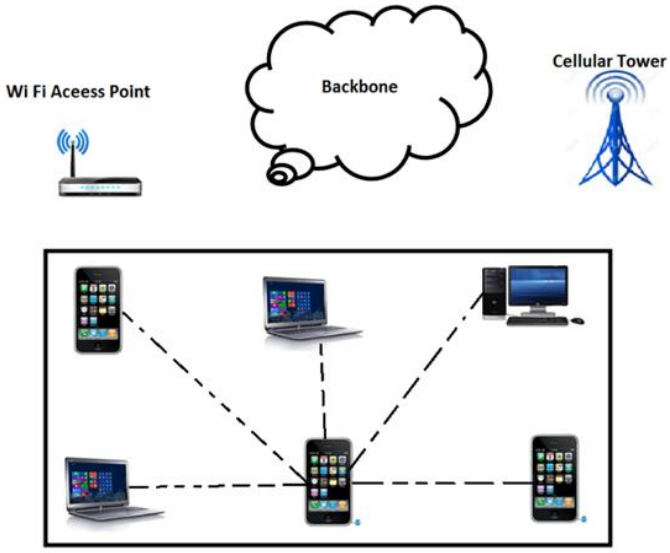


Figure 1: Mobile Ad Hoc Networks

• Constant Jammer: A constant jammer is the signal generator that does not follow any MAC protocol and it continuously emits a radio signal that represents random bits.
• Deceptive Jammer: They transmit semi-valid packets. This means that the payload is useless but the packet header is valid.
• Random Jammer: Alternates between sleeping and jamming the channel. In the first mode the jammer jams for a random period of time (it can behave either like a constant jammer or a deceptive jammer), and in the second mode (the sleeping mode) the jammer turns its transmitters off for another random period of time. The energy efficiency is determined as the ratio of the length of the jamming period over the length of the sleeping period.
• Reactive Jammer: A reactive jammer tries not to waste resources by only jamming when it senses that somebody is transmitting. Its target is not the sender but the receiver, trying to input as much noise as possible in the packet to modify as many bits as possible given that only a minimum amount of

power is required to modify enough bits so that when a checksum is performed over that packet at the receiver it will be classified as not valid and therefore discarded.

1.1 JAMMING ATTACK

IEEE 802.11 one of the most popular attack is jamming attack. Ad-Hoc networks are very prone to security threats. One of the type of Denial Of Service (DoS) is Jamming attack . Interferences are caused by jamming attack. The radio signals are continuously sending in between the transmission which injects the dummy packets and thus causing interferences. Since the radio frequency is an open medium, therefore jamming is big problem for wireless networks. By effecting their throughput, network load, end to end delays etc. Jamming decreases the overall performance of network.

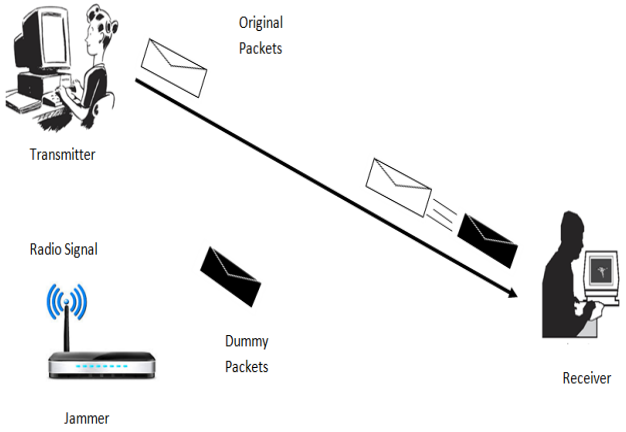


Figure 2: Jamming Attack

In 1997 the IETF established the Mobile Ad hoc Networking Working Group [14] and since then substantial effort has been put in by the research community for standardization on this emerging paradigm. The purpose of this working group is to standardize the routing protocol by considering their suitable functionality in MANETs environment. They developed two standard track routing protocol specifications as reactive MANET protocols and proactive MANET protocols. One of the main considerations for the standardization of routing protocols is their performance issues such as loop freedom, demand based operations, distributed operation and proactive operations [15]. Taking into consideration the configuration issues of MANETs, IETF recently formed another working group called Ad Hoc Networks Auto configuration (auto conf) [16]. The main aim of this working group is to describe the issues in addressing model for ad hoc networks that is how the nodes in ad hoc network configure their address both locally and globally when they connect to other networks. The auto conf working group has contributed in a form of internet draft [17], where they propose and describe a model for configuring IP addresses in ad hoc networks. The research community perspective on this multi hop ad hoc networking technology has changed as the technology has developed in the last two decades. In [18] they defined the term *pure MANETs* referring to an ad hoc network with no infrastructure support as compared to one with limited infrastructure support.

II. RELATED WORK

Geethapriya Thamilarasu et al. [1]: Here, In this paper author's Improve Reliability of Jamming Attack Detection in Ad Hoc Network using the GLoMoSim network simulator and CBR application simulation framework. For performance evaluation they used several Jammer metrics such as Jamming Rate, Malicious Node Ratio and Channel Congestion Rate. For simulation purpose authors had taken few metrics like Detection Rate, False Positive Rate. Effects of Jamming at Physical and MAC layers in a wireless ad hoc network and presented a detection algorithm to reliably detect jamming attacks are not different from collision due to hidden terminal and network congestion. For improving Detection accuracy utilized the channel utilization metric for evaluating network congestion state and performed tests to find out collision is due to jamming or network traffic conditions. After the simulation result authors conclude the effectiveness of scheme and also demonstrated that it can be used to detect attack with enhanced reliability and accuracy.

S. Raja Ratna et al. [2]: Here, In this paper author's describe various Denial of Service Attacks mitigating techniques in wireless network. To prevent the cyberspace from DOS attack this paper propose a survey on three types of DOS attack such as selective forwarding attack, pollution attack, jamming attack and its detection techniques. For Selective forwarding attack they use Channel Aware Detection (CAD) algorithm, for Pollution Attack use Digital Signature to identify pollution attack and for Jamming Attack using honey nodes for defending against jamming attack. This paper also concludes that we do not protect against jamming in all the available ways. Anti-jamming technologies should not only design and deployed but also deployed and used.

Sabbar Insaif Jasim et al. [3]: Here In this paper author's work on jamming attacks impact on the performance of mobile ad-hoc network and improvement using MANET routing protocols. For the performance evaluation author's had taken OPNET Modeler (v 14.5). In their work author's used different performance parameters for HTTP application such as Delay, Throughput, Data dropped, Traffic received and sent. The main work of this paper is studied the effect of attackers by increasing delay, data dropped traffic and decreasing throughput of the network. Four protocols were taken DSR, OLSR, TORA & GRP in order to show which of them can improve the performance of the network in terms of parameters affected by attackers. HTTP traffic received & sent at the expense of increasing throughput and decreasing data dropped. OLSR protocol was more successful in increasing throughput and decreasing data dropped but it caused larger delay. So, some security works can be done to reduce the effect of attackers.

Ajana J. et al. [4]: Here, In this paper author's mitigate inside jammers in MANET using Localized Detection Scheme. For performance evaluation author's had taken NS2 Simulation tool for simulation purpose with taking various parameters such as 200 by 200 meters grid size, 10 nodes, simulation time 200 sec. , antenna Omni-directional with unity gain, No fading radio model with range of 376 meters, routing protocol

AODV. For evaluation of performance metrics parameters such as throughput and delay. In this paper author's proposed a method that acts as a LDS for identifying inside Jammers in MANET and also compare the performance of LDS and a cluster organized network. After the simulation results authors conclude by using the algorithm delivery ratio & signal strength is less efficient in clustered algorithm and it also managing the reputation values that create a little overhead. By mitigating jamming attacks, bandwidth utilization can be improved & hence improve the overall network efficiency. It also shows that LDS is better than the clustered approach.

III. Methodology Used

This section explains the simulation tool employed along with the several simulation parameters.

Simulation tool used: OPNET Simulator (14.5) is broad and 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 evaluate of MANETs performance with and without jamming attack. Thus an Integrated method is utilized to analysis he network performance under jamming attack. This method involves:

- Network with high mobility
- High data rate of 48 mbps by utilizing OFDM
- Enhanced parameter of AODV routing protocol
- Generation of high resolution FTP traffic and Voice with IP Telephony.

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, two different scenarios are generated and illustrated by the OPNET simulation package and flow of the two scenarios that shown in figure 3 and 4.

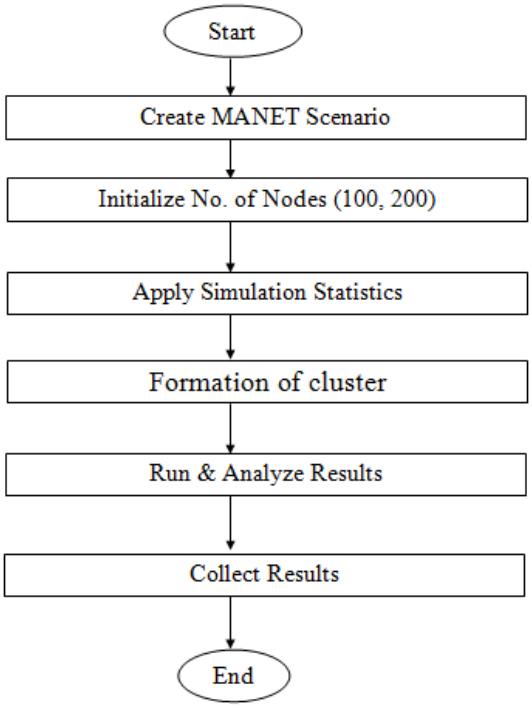


Figure 3: Normal Flow of MANET

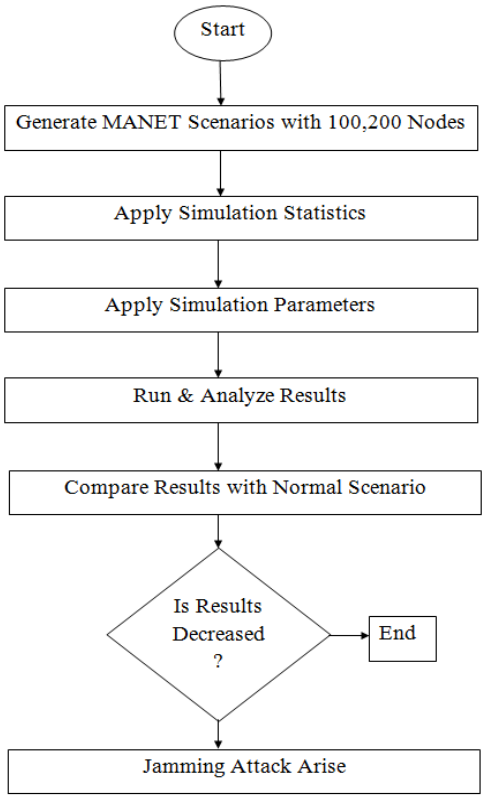


Figure 4: Jamming Flow in MANET

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
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
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.

Table 2: At 100 Nodes Throughput

Time	Without Jamming	With Jamming
10 min.	2000	2100
20 min.	2000	2100
30 min.	10000	11000
40 min.	51000	58000
50 min.	100000	120000
60 min.	245000	340000

Table 3: At 200 Nodes Throughput

Time	With Jamming	Without Jamming
10 min.	4218	5036.6
20 min.	7722.10	10052.1
30 min.	56130.3	71383.2
40 min.	206479.2	231431.2
50 min.	522294.6	717171.4
60 min.	1041538	1455733

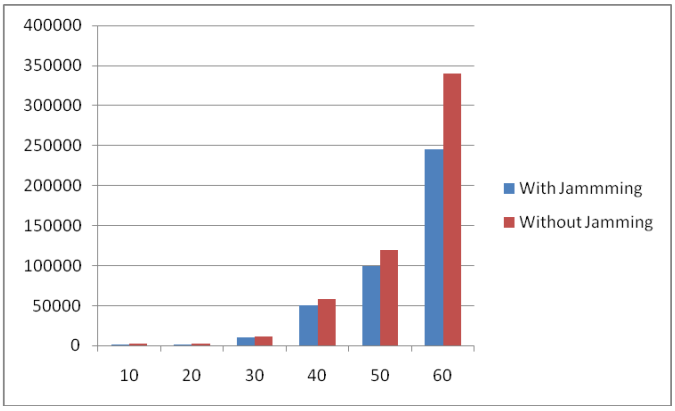


Figure: 6 Throughput of all scenarios at 100 nodes

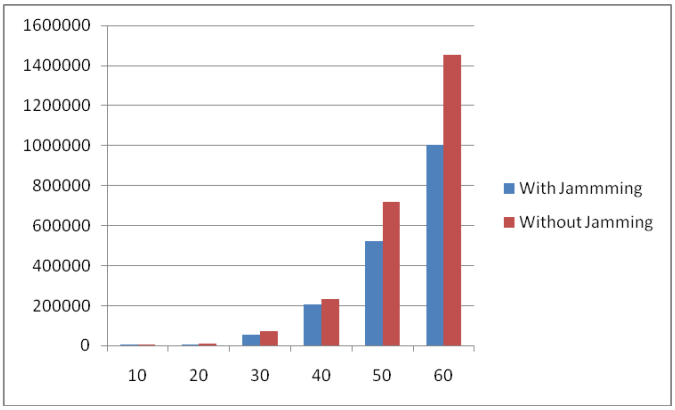


Figure: 7 Throughput of all three scenarios at 200 nodes

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 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. After the simulation results we get jamming attack decreased throughput in 100 and 200 nodes about 2 times.

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). After the simulation results we get jamming attack increases end to end delay around 30 times at 100 and 200 nodes.

Table 2: At 100 Nodes Delay

Time	With Jamming	Without Jamming
10 min.	0.334	0.00025
20 min.	0.249	0.000254
30 min.	0.1534	0.000414
40 min.	0.119	0.000634
50 min.	0.169	0.001261
60 min.	0.145	0.0025

Table 4: At 200 Nodes Delay

Time	With Jamming	Without Jamming
10 min.	0.2958	0.000257
20 min.	0.2912	0.000269
30 min.	0.2545	0.000375
40 min.	0.2151	0.000653
50 min.	0.186071	0.001203
60 min.	0.1661	0.001791

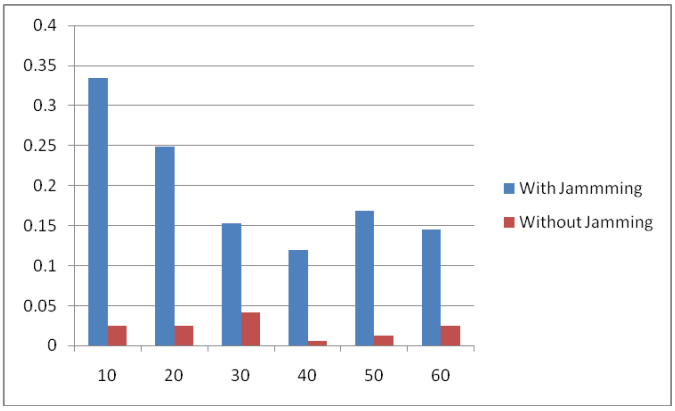
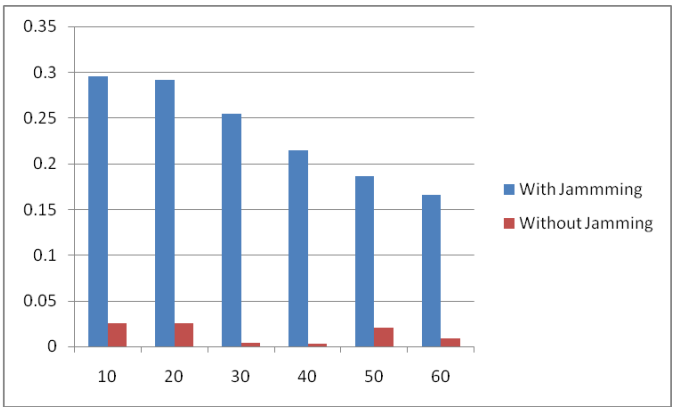


Figure: 8 Delay of all three scenarios at 100 nodes



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.

REFERENCES

[1] Geethapriya Thamilarasu, Sumita Mishra and Ramalingam Sridhar," Improving Reliability of Jamming Attack Detection in Ad-Hoc Networks", International Journal of Communication Networks and Information Security (IJCNIS) , Vol. 3, No.1, April 2011, pp. 57-66.

[2] S. Raja Ratna, R. Ravi and Dr. Beulah Shekhar," Mitigating Denial of Service Attacks in Wireless Networks", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 2, No.5, May 2013, pp. 1716-1719.

[3] Sabbar Insaif Jasim," Jamming Attacks Impact On the performance of Mobile Ad-Hoc Network and Improvement Using MANET Routing protocols," International Journal of Engineering and Advanced Technology(IJEAT), Volume 3, Issue 2, Dec. 2013, pp. 325-330.

[4] Ajana J., Helen K.J, "Mitigating Inside Jammers in MANET Using Localized Detection Scheme", International Journal of Engineering Science Invention, Volume 2, Issue 7, July 2013, pp. 13-19.

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