RESEARCH ARTICLE OPEN ACCESS

Impact of Jamming Attack in Performance of Mobile Ad hoc Networks

Jagat Singh [1], Sachin Gupta [2]
Department of Computer science and Engineering
Assistant Professor [2]
MVN University
Palwal - India

ABSTRACT
MANETs have unique characteristics like dynamic topology, wireless radio medium, limited resources and lack of centralized administration; as a result, they are vulnerable to different types of attacks in different layers of protocol stack. Each node in a MANET is capable of acting as a router. The necessity for a secure MANET networks is powerfully tied to the security and privacy features. This Jamming attacks are one of them. These occur by transmitting continuous radio ways to inhibit the transmission among sender and receiver. These attacks affect the network by decreasing the network performance. Previously there had been considerable research in the field of increasing the performance of network by using routing protocols. In this paper we are analyzing the performance of Vehicular ad hoc networks under jamming attack. This work includes a network with high mobility, using IEEE Along g standard with improved AODV (Ad hoc On Demand Distance Vector) routing protocol parameters. Video conferencing and FTP with high data rate are being generated in the network. For the Simulation purpose we employed OPNET (Optimized Network Engineering Tool) MODELER 14.5 is used for simulation. The performance of network is measured with respect to the QoS parameters like, network load, retransmission attempts, media access delay and. Throughput

Keywords:- AODV,FTP,MANET,OPNET.

I . INTRODUCTION

Ad-Hoc networks have no infrastructure where the nodes are free to join and left the network. The nodes are connected with each other through a wireless link. A node can serve as a router to forward the data to the neighbors' nodes. Therefore this kind of network is also known as infrastructure less networks. These networks have no centralized administration. Ad-Hoc networks have the capabilities to handle any malfunctioning in the nodes or any changes that its experience due to topology changes. Whenever a node in the network is down or leaves the network that causes the link between other nodes is broken. The affected nodes in the network simply request for new routes and new links are established Ad-Hoc network can be categorized in to static Ad-Hoc network (SANET) and Mobile Ad-Hoc network (MANET). In our research work we are improving the performance of mobile ad hoc networks under jamming attack by using an integrated approach. The proposed work includes a network with high mobility, using IEEE Along g standard with improved AODV (Ad hoc On Demand Distance Vector) routing protocol parameters. FTP and Video conferencing with high data rate are being generated in the network.

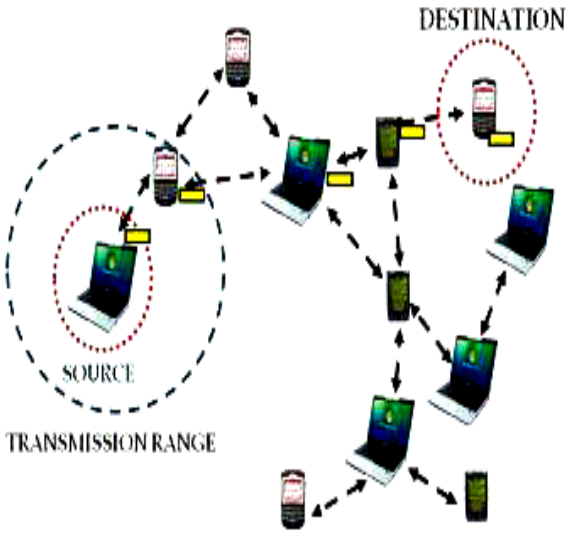

Figure1. Mobile Ad hoc Network

II . JAMMING ATTACK

Jamming attack deliberately transmits of radio signals to disrupt the whole communications by decreasing the signal-to-noise ratio. The term jamming is used to differentiate it from unintentional jamming which called interference. In MANET Jamming is a serious threat to its security. Jammers constantly send.

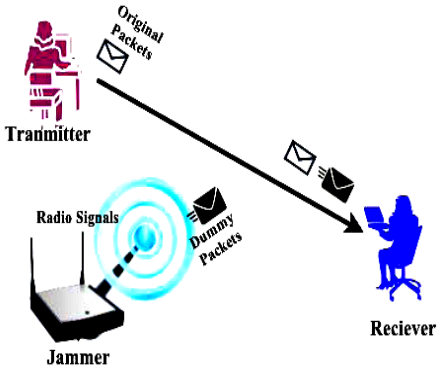

FIGURE 2: JAMMING ATTACK

II. LITERATURE REVIEW

Sisi Liu et al. (2012) addresses the problem of mitigating DoSattacks manifested in the form of jamming. The author considered a sophisticated adversary who has knowledge of the protocol specifics and of the cryptographic quantities used to secure network operations. This type of adversary cannot be prevented by anti jamming techniques that rely spread spectrum. The author proposed a new security metrics to quantify the ability of the adversary to deny access to the control channel, and introduced a randomized distributed scheme that allows nodes to establish and maintain the control channel in the presence of the jammer. The proposed method is applicable to networks with static or dynamically allocated spectrum. Furthermore, two algorithms for unique identification of the set of compromised nodes were proposed, one for independently acting nodes and one for colluding nodes[19]. Dorus.R et al. (2013) proposes a mechanism for preventing jamming attacks on wireless networks, examine the detection efficiency of jamming attack and communication overhead of the wireless network using proactive and reactive protocols. RSA algorithm is used and analyzed for providing data packets integrity information during wireless transmission. Through simulation and performance analysis, the implemented prevention mechanism and the integrity preservation provides higher packet delivery ratio in proactive routing protocol (OLSR) than reactive routing protocol (AODV). Nadeem Sufyan et al. (2013) investigates a multi-modal scheme that models different jamming attacks by discovering the correlation between three parameters: packet delivery ratio, signal strength variation, and pulse width of the received signal

III. METHODOLOGY

A. Simulatoin Tool used:

This section describes the simulation tool used along with the proposed method.

OPNET modeler v14.5 is extensive and a very powerful simulation tool with wide variety of possibilities. The entire heterogeneous networks with various routing protocols can be simulated using OPNET. High level of user interface is use in OPNET which is constructed from C and C++ source code blocks.

B. Simulatoin Setup:

The simulation work focuses on analysing the performance of MANET under jamming attack. Therefore an Integrated approach is used to analyse the network performance under jamming attack. This approach includes:

• High data rate of 54mbps by using IEEE 802.11g standard [9]

• Network with high mobility [2]

• Improved parameter of AODV routing protocol

• Generation of high resolution video conferencing and FTP traffic.

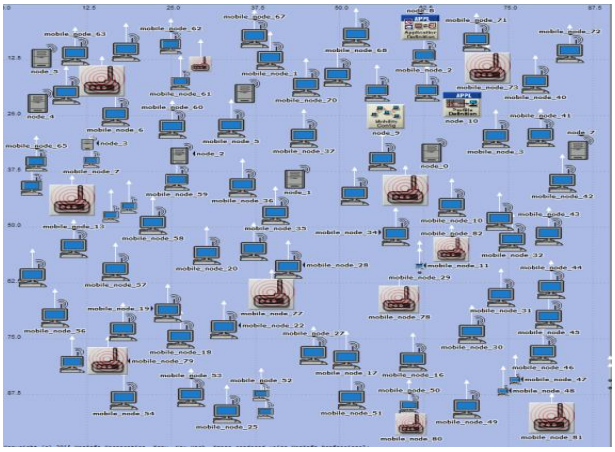

Figure 3: Jamming attacks scenario in MANET

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

Table: 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.

Table II: MANET Simulation Parameters for Jammer

Examined Protocols Cases	**AODV without Jamming Attack**
Number of Nodes	100 and 200
Types of Nodes	Mobile
Simulation Area	50*50 km
Simulation Time	3600 seconds
Mobility	Uniform(10-100) m/s
Pause Time	200 seconds
Performance Parameters	Throughput, Delay, Network load
No. of Jammers	10
Jammer Bandwidth	100,000
Jammer band base frequency	2,402
Jammer Transmitter Power	0.001
Trajectory	VECTOR
Data Type	Constant Bit Rate (CBR)

Packet Size	512 bytes
Traffic type	FTP, Http
Active Route Timeout(sec)	4
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
Performance Parameters	Throughput, Delay, Network load
Trajectory	VECTOR
Long Retry Limit	4
Max Receive Lifetime (seconds)	0.5
Buffer Size(bits)	25600

IV. RESULT

A. ***Delay***: Represents the end to end delay of all the packets received by the wireless LAN MACs of all MANET nodes in the network and forwarded to the higher layer. Jammers would affect the performance of system by increasing the delay as shown in the Fig.4 and 5.

B. ***Data dropped*****:** Total higher layer data traffic (in bits/sec) dropped by the all the WLAN MACs in the network as a result of consistently failing retransmissions. Jammers could affect the network by increasing Data dropped of network as shown in Fig. 6 and 7.

C. ***Network Load:*** Figure 8 and 9 shows that the network load of the normal network is noted as 22,340 bits/sec and with the jamming nodes in the network it is noted as 25840 bits/sec. The jamming attacker nodes drop the packets and not forwarding the packets for the other nodes.

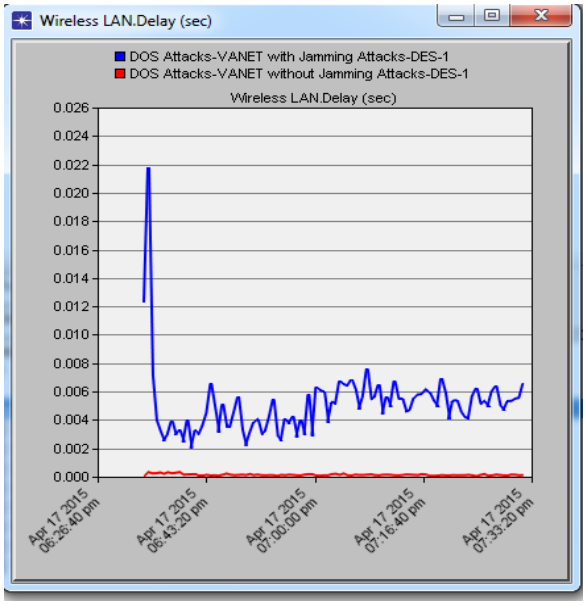

Figure 4: Average Delay of 100 Nodes

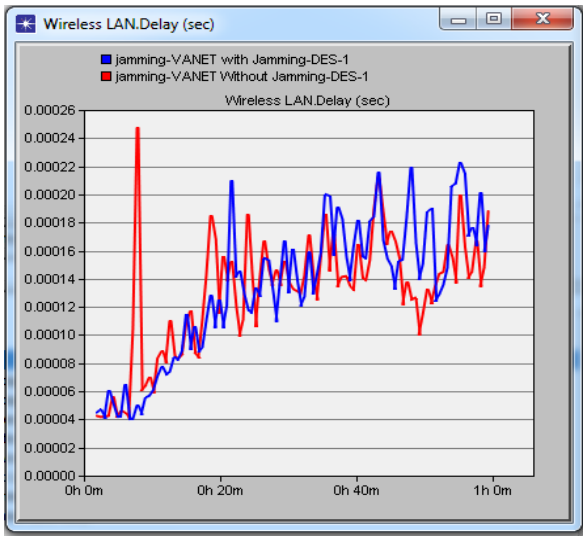

Figure 5: Average Delay of 200 Nodes

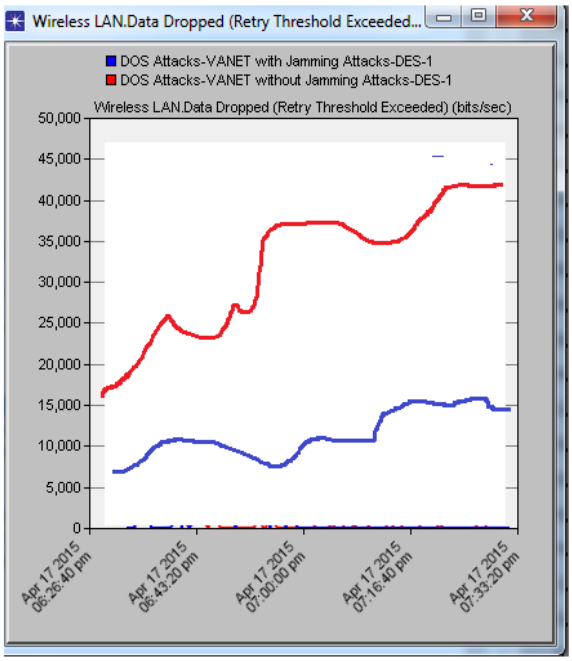

Figure 6: Average Data dropped of 100 Nodes

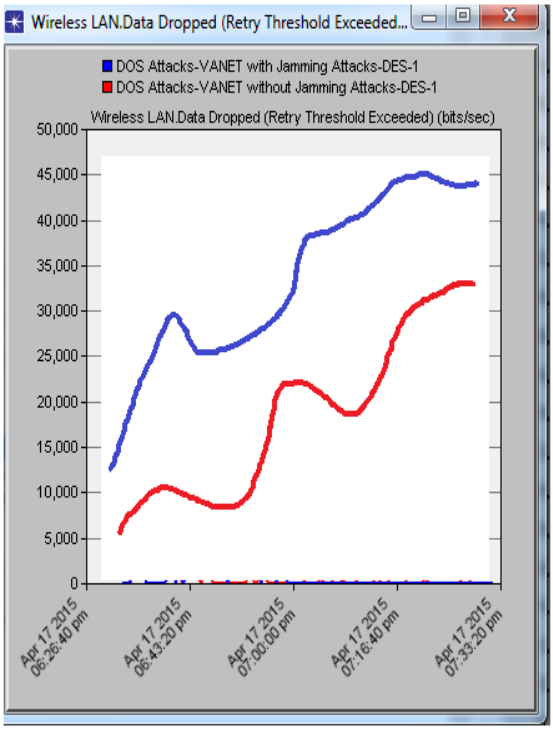

Figure 7: Average Data dropped of 200 Nodes

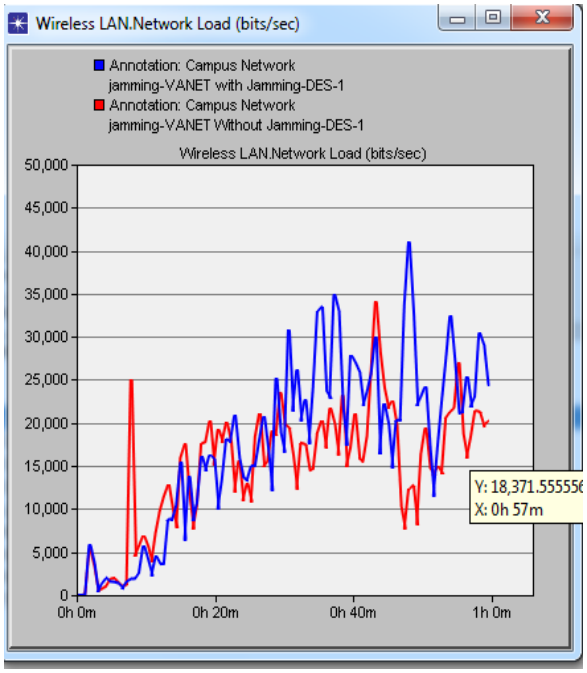

Figure 8: Average Network load of 100 Nodes

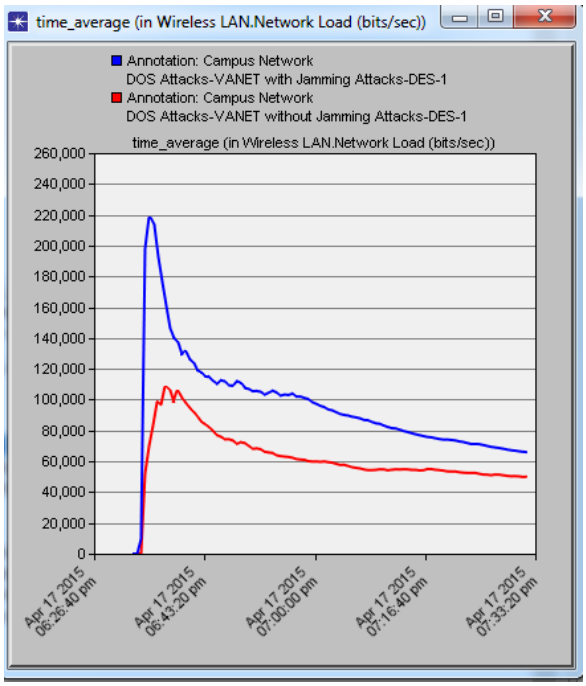

Figure 9: Average Network load of 200 Nodes

V. CONCLUSION

Because of the wireless nature of mobile ad hoc networks,.variouse attacks are performed degrade the

network performance. Jamming attack is one of them therefore e routing protocols are used to increase the net work throughtput . In this research work, Impact of Jamm ing Attack in Performance of Mobile Ad hoc Networks. Jammers attacks will have an effect on network's performance as a result of the jammers interferes with the traditional operation of the network. The effect of attackers studied in this paper was by increasing delay, data dropped traffic received and sent and decreasing packer drop ratio of the network. In this research work, the network performance under jamming attack is analyzing by applying integrated approach. This approach includes a network with high mobility, IEEE 802.11g standard with max data rate, heavy traffic like FTP and video conferencing, improved AODV parameters and increased buffer size. In our paper, it was shown that jamming attack reduces the network throughput, retransmission attempts and increases the media access delay

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", 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.

[21] W. Wang, B. Bhargava, "Visualization of Wormholes in sensor networks", ACM workshop on Wireless Security, pp. 51-60, 2004.

[22] Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks", ACMSE, April 2004, pp.96- 97.

[23] Anu Bala, Munish Bansal and Jagpreet Singh, "Performance Analysis of MANET under Blackhole Attack", First International Conference on Networks & Communications, 2009, pp. 141-145.

[24] Latha Tamilselvan and Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 2007, pp. 21-26.

[25] Geng Peng and Zou Chuanyun,"Routing Attacks and Solutions in Mobile Ad hoc Networks", International Conference on Communication Technology, November 2006, pp. 1-4.

[26] S. Lee, B. Han, and M. Shin, "Robust Routing in Wireless Ad Hoc Networks", International Conference on Parallel Processing Wowrkshops, August 2002.

[27] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato1, Abbas Jamalipour, and Yoshiaki Nemoto1," Detecting Blackhole Attack on AODV-based

Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, vol..5 no..3, Nov. 2007, pp.338–346.

[28] Nadia Qasim, Fatin Said, and Hamid Aghvami, "Performance Evaluation of Mobile Ad Hoc Networking Protocols", Chapter 19, pp. 219-229.

[29] G.S. Mamatha and S.C. Sharma, "A Robust Approach to Detect and Prevent Network Layer Attacks in MANETS", International Journal of Computer Science and Security, vol. 4, issue 3, Aug 2010, pp. 275-284.

[30] Preetam Suman, Dhananjay Bisen, Poonam Tomar, Vikas Sejwar and Rajesh Shukla, "Comparative study of Routing Protocols for Mobile Ad- Hoc Networks", International Journal of IT & Knowledge Management, 2010.