Network Security Vulnerabilities: Malicious Nodes attack

MOHD IZHAR* & DR. V.R.SINGH**

* HMR Inst. of Tech. & Mgt. & Ph.D. Scholar of Mewar University
** Recognised Supervisor of Mewar University

Abstract- Network Security is always foremost and big issue in wired and wireless network. Wireless network, whether it is infrastructure mode or mobile adhoc mode, breaks the barriers of wired network and are easily accessible to everyone but everything is at a cost, the cost is in the form of increased susceptibilities and vulnerabilities of network. Packet delay is a result of poor utilization of network capacity when it is integrated with routing algorithms. Routing protocol contains very serious security issues in adhoc network. The code of AODV and DSDV are having such issues and new protocol are extended in the form of SEAD, SEAR and SAODV. This paper analyses the ways the security is breached by the hackers who emerge as malicious node in Infrastructure as well as in adhoc mode of network. The handiwork is prepared by way of Developing experimental Testbed and simulation in NS2 then proper measure are proposed in order to overcome all the problems.

Index Terms- Wireless Network, MAC, Intrusion Detection Systems and malicious node.

I. INTRODUCTION

Wireless networks are convenient, but it is dangerous if they do not employ latest methods of network security because the network's signal go beyond the boundaries of home and organization. If one connects to a network which is vulnerable, it is possible that any malicious node can easily steel everything and it can do that what one do on his/her device[55]. The nodes, nearby of such network might be able to access the information stored on authorized nodes and can use Internet connection to log on the web. Malicious node can impersonate the source node by forging RREQ message and Destination node can be impersonated by forging a RREP with its address as destination address. Malicious node can become a black hole to the entire sub network.IEEE 802.11i and 802.11-2007 provides RSNA methods for security of wireless network. WECA, the alliance for Wi-Fi devices provides WPA2 modes of security. These Standards for wireless network classifies security algorithms into: RSNA and Pre-RSNA. Pre-RSNA algorithms are the algorithms used before RSNA. Pre-RSNA security comprises the algorithms; WEP and IEEE 802.11 entity authentication. RSNA security comprises the algorithms like TKIP, CCMP, RSNA establishment and termination procedures, including use of IEEE 802.1X authentication, key management procedures and providing mechanisms for protecting management frames[61].
This paper discloses the main point of vulnerability of Pre-RSNA, RSNA and WPA2 Method by developing experimental testbeds and simulation in NS2 and provide its countermeasures.

II. BACKGROUND

Primary factors for security in a wireless environment are [55-61] : 1. Theft: Unauthorized users often try stealing data. 2. Access Control : Wireless networks have all the same access control vulnerabilities as wired networks; even it can be easily targeted. 3. Authentication: Unauthorized users can also log onto them illegally. 4. Encryption: Wireless routers support medium and strong levels of encryption 5. Protection : The best protection is to become familiar with WLAN and wireless router. Routing protocol issues: Black Hole Attack is attack at network integrity where full data loss happens. Message integrity, where the destination node is able to verify that the contents of message are not altered by malicious node. Node is understood selfish when it ignores requests from other nodes in order to save its own resources, it is compromised if it is insider and behaves maliciously. The Node becomes malicious node if it is attacker and cannot be authenticated itself as a legitimate node due to the lack of valid cryptographic information. AODV is extended to secure AODV for providing security features like integrity, authentication and non-repudiation[49].
Both the IEEE and WECA provide standard for WLan in order to secure and reliable communication. WPA-2 is the Standard developed by WECA compatible with IEEE security mechanism. An Intruder has several ways to attack on a wireless network. The easiest method of attack is MAC spoofing by which malicious node can impersonate as an authorized wireless access point or as an authorized client.
Security measure MAC filtering results in vulnerability of MAC spoofing such as [63]

1. MAC spoofing can be done to get access of wireless network.
2. MAC spoofing can be result in illegitimate use of Wireless Network for any kind of crime.
3. Internet Service Provider bind their services to a specific MAC address, unauthorized node may access of the service by using MAC address of authorised user.
4. Some software licences are based on MAC address, one malicious node uses it as authentic user.

Some solutions are there to solve the problem of MAC spoofing:
1. OS can check the MAC address entries and delete it automatically if there is some change in it.
2. MAC address at ARP can be compared with that of MAC address through OS whenever packets arrive to it
3. MAC address are stored in OS and received from OS, it can be checked directly from NIC.
4. Association of MAC address with IP address can solve the problem.

5. Encryption of the communication between the wireless PC and access point can also be used as a solution to the problem.

Various papers have been published showing how to crack WEP, this is very simple procedure and one need only a Bootable DVD of Backtrack which contains various utilities used for cracking. Aircrack is the most popular tool for this purpose which is used to attack WEP and WPA encryption[57].

WPA uses TKIP for security, which stands for Temporal Key Integrity Protocol. In the TKIP mode, the encryption keys are changed at set intervals. WPA2 can also be used for wireless encryption and is known as 802.11i standard/AES. The Problem by using WPA2 is that all the device on network must use WPA2 or compatible. If any of the device on the network that only supports WPA, this device will not be able to join the network unless router supports WPA/WPA2 mixed mode. Also WPA2 and advanced encryption such as CCMP-AES is understood secure way for home and small offices but the problem is that many AP still in use are good enough for security purposes but they are lacking Wireless-N or other advanced encryption of WPA2.

III. TOOLS AND MTHODS

Testbed

A typical scenario of WLAN is developed in which different nodes are considered connecting through an access points in order to test the pre-RSNA and RSNA Methods of Security. The developed scenario has a server with internet facility, the server is connected with various access points at different wings and these access points are accessed, as and when required, by various moving / stationery nodes. The equipments used for this scenario is fully compatible with IEEE and WPA2 standards and methods.

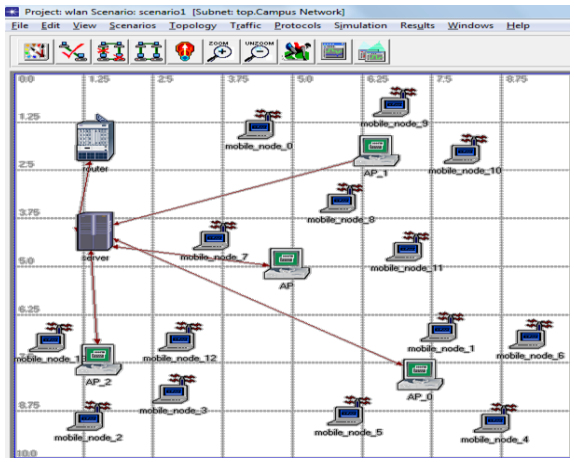

Figure1 : Typical WLAN Scenario

Tools

A free open source Angry IP scanner tool scans the WLAN network and shows dead and alive nodes with their MAC Address that means providing various information of node(s) to the malicious node(attacker) that may result in MAC address spoofing and in turn breaching the security.

Advanced ip scanner has also been used and they provide more advanced features which on the one hand are very useful for the Tester for WLAN networks but provides handy information to hackers.

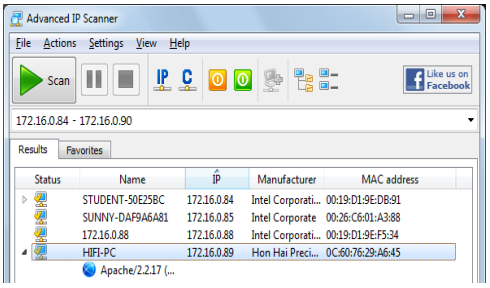

Figure2 : Advanced IP Scanner

Simulation

NS-2.35 is used for simulations which consist of the collection of network protocols to simulate many of the existing network topologies[29]. But NS-2.35 contains wireless ad-hoc routing protocols, it does not have any modules to simulate malicious node so a Black Hole patch is used to show one of serious security issue of routing Protocol. In black hole attack a malicious node waits RREQ messages[31]. When it receives an RREQ message, without checking its routing table, immediately sends a false RREP message to destination to itself, assigning a high sequence number before other nodes send a true one. So requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node. The typical scenario of simulation is as follows :

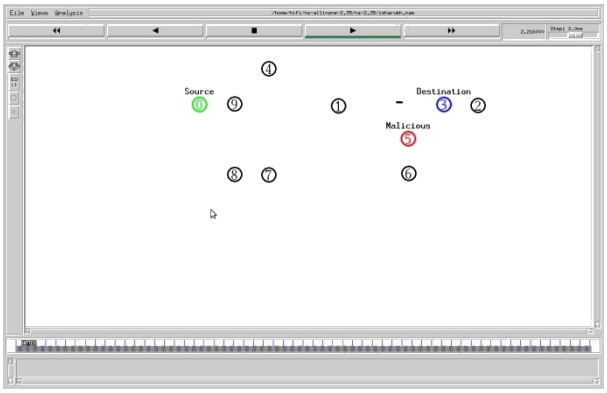

Figure 3 : Typical Scenario of NS2

Adding Patch in NS2 : NS2 provides limited functionality so patch is required for performing and simulation of suggested changes. The necessary changes or changes through patches are added through as per the following procedure:[49]

Patch –p1 –t1 <bh.patch
./configure
make clean
make
make install

IV. RESULT AND DISCUSSION

Malicious node for Infrastructure mode : The Test Result for MAC Spoofing is clear where malicous node can easily change the MAC address as desired through all the following ways :

1. One can change the MAC address through device manager of the System.
2. One can also change the MAC address through editing the Registry of the System. The Method is shown through the following picture :
3. The MAC address can be changed through the MAC address Changer such as TMAC and SMAC software. The Changed MAC address has been show through the following picture.

The Changed MAC address of malicious node is not traceable by other node or server. wireless network catches the fake address of the malicious unauthorized node as the authorized legitimate user. The following result captured through authorized node points out the same.

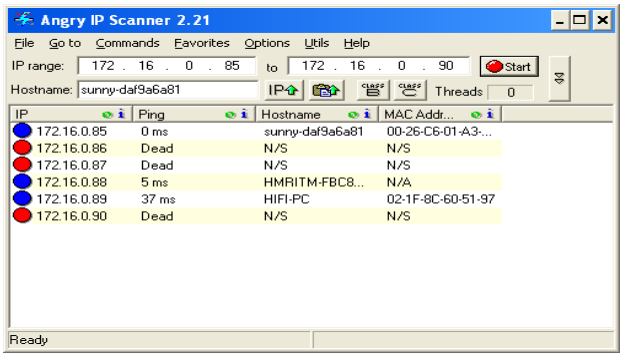

Figure 4: Malicious Node having Spoofed Address

It was implemented that Step by Step procedure with Bootable DVD of Backtrack easily find out the Wep key. Security by WPA2 needs latest software and hardware. Latest web browser capabilities and OS firewall Competence with these advanced modes of RSNA methods has also been taken into account in order to develop secure network model. It was learnt through tests that one can minimize the Phishing attack through browser capabilities. Software\Hardware Firewall is also one of the best solutions to protect the network from various attacks. A typical hardware firewall has different solution to the network security issues. But the System needs an efficient system administrator to install the same and to optimum use of its all facilities which can be affordable for mid-level organization. Small and Home Office can rely on software firewall which comes as a free utility of OS or browser.

Malicious node in the adhoc mode of Network :

When the malicious node is not in the network, data are as usual sent and received. But as malicious node join the network, it receiving the data packets to drop and data received and ratio value becomes 0. The results are as follows : cbr s:1238 r:1238, r/s Ratio:1.0000, f:2478 – without Blackhole attack
and cbr s:1238 r:0, r/s Ratio:0.0000, f:2478 – with black hole.

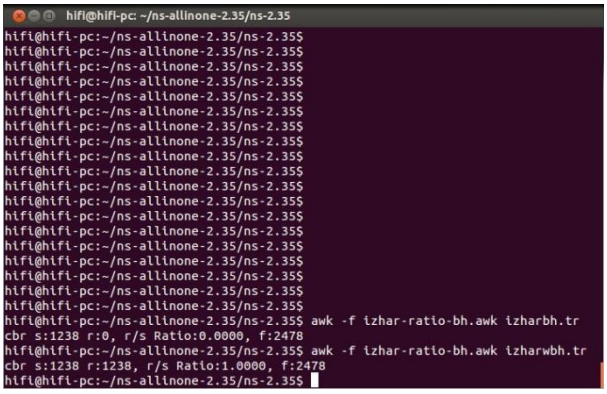

Figure 5 : Filtered Result of Trace file

The picture through NAM animator also shows the same, when malicious node is not active. Data is sent from source is received by Destination node.

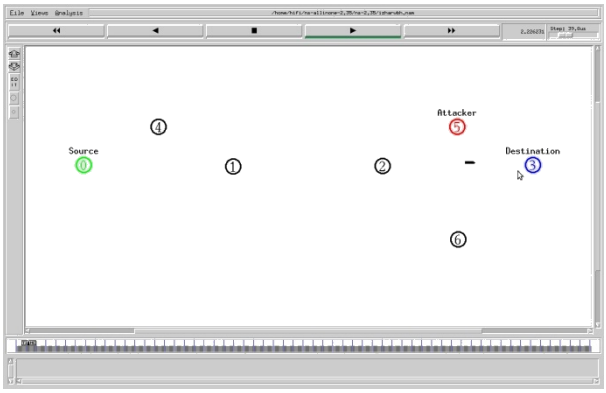

Figure 6 : Malicious node not active

But when the malicious node active, it starts receiving and dropping the data.

Figure 7 : Malicious Node absorbing all data

On examination of trace file it is seen that after a while second RREP message came to source node from the real destination node. For solution one can assume that malicious node send a first RREP message. But in some cases, the second RREP can be received at source node from an in-between node or the second RREP message may also come from the malicious node if the real destination node is nearer than the black hole node.

Table 1 : Showing RREP Message of Nodes

BH	BH	BH	WBH	WBH
s	s	r	s	r
1.007371858	1.007372152	1.012751242	1.007372152	1.012479842
_5_	_3_	_2_	_3_	_2_
RTR	RTR	RTR	RTR	RTR
---	---	---	---	---
AODV	AODV	AODV	AODV	AODV
44	44	44	44	44
[0	[0	[13a	[0	[13a
0	0	2	0	2
0	0	5	0	3
0]	0]	800]	0]	800]
-------	-------	-------	-------	-------
[5:255	[3:255	[5:255	[3:255	[3:255
0.177083333	0.177083333	0.177083333	0.177083333	0.177083333
30	30	30	30	30
2]	2]	2]	2]	2]
[0x4	[0x4	[0x4	[0x4	[0x4
1	1	1	1	1
[3	[3	[3	[3	[3
4]	4]	4]	4]	4]
10.000000]	10.000000]	10.000000]	10.000000]	10.000000]
(REPLY)	(REPLY)	(REPLY)	(REPLY)	(REPLY)

V. CONCLUSION AND FUTURE WORK

WLAN Security threats as pointed out can be addressed for Small office and Home office through economical methods such as by making OS to be dynamic, MAC address at ARP can be compared with that of MAC address taken through OS, MAC addresses can be checked directly from NIC. Association of MAC address with IP address can solve the problem and also encryption of the communication between the wireless PC and access point can also be used as a solution to the problem. Latest hardware and software can also help in achieving the better security. Hardware security modules can be used for big and military organization. Packet drop problem is sorted out by using SAODV algorithm instead of AODV protocol. Authentication and integrity in SAODV are achieved using digital signatures and message authentication codes. But all such security measure affects the speed, throughput, delay and other performance parameters and how much they affects the performance of the network, this may be known by developing performance model for performance evaluation as their future work for the researchers..

ACKNOWLEDGMENT

Our sincerely thanks to the management of HMR Institute of Technology and management, GGSIP University, Hamidpur, Delhi, PDM College of Engineering, M.D. University, 3A, Sarai Aurangabad, Bahadurgarh, Haryana and Mewar University, NH-79, Gangrar, Chittorgarh Rajasthan who supported the most in preparing this documents.

REFERENCES

[1] IEEE Std 802.11™-2007, Revision of IEEE Std 802.11-1999, IEEE 3 Park Avenue New York, NY 10016-5997, USA 12 June 2007.

[2] IEEE Std. 2009 Revision of IEEE Std 802.11™-2007, 30 Sept. 2009.

[3] Changhua He & John C Mitchell "Security Analysis and Improvements for IEEE 802.11i", Network and Distributed System Security Symposium, San Diego, California, 3-4 February 2005.

[4] Shivaputrappa Vibhuti, "IEEE 802.11 WEP (Wired Equivalent Privacy) Concepts and Vulnerability" , San Jose State University, CA, USA, CS265 Spring 2005 (26.03.2005)

[5] NETGEAR, Inc. "Wireless Networking Basics", October 2005.

[6] Lu Zhengqiu; Tian Si; Wang Ming; Ye Peisong; Chen Qingzhang; "Security analysis and recommendations for Wireless LAN 802.11b network", Consumer Electronics, Communications and Networks (CECNet), 2011 International Conference on 16-18 April 2011.

[7] Finn Michael Halvorsen & Olav Haugen "Cryptanalysis of IEEE 802.11i TKIP", Norwegian University of Science and Technology, June 2009.

[8] IEEE Std 802.11i-2004, Amendment to IEEE Std 802.11™, 1999 Edition (Reaff 2003) as amended by IEEE Stds 802.11a™-1999, 802.11b™-1999,802.11b™-1999/Cor 1-2001, 802.11d™-2001, 802.11g-2003, and 802.11h-2003] Amendment 6: Medium Access Control (MAC) Security Enhancements, 23 July 2004.

[9] Back and Tews "Practical attacks against WEP and WPA", November 8, 2008.

[10] Paul Arana, "Benefits and Vulnerabilities of Wi-Fi Protected Access 2 (WPA2)", INFS 612 – Fall 2006

[11] Behrouz A. Forouzan "Data Communication and Networking", McGraw-Hill Forouzan Networking Series, Fourth Edition Copyright © 2007.

[12] NIST Special Publication 800-97, "Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i", February 2007.

[13] Diaa Salama Abd Elminaam1, Hatem Mohamed Abdual Kader, and Mohiy Mohamed Hadhoud, "Evaluating The Performance of Symmetric Encryption Algorithms", International Journal of Network Security, Vol.10, No.3, PP.213{219, May 2010

[14] A.K.M. Nazmus Sakib et al"Security Improvement of WPA 2 (Wi-Fi Protected Access 2)" (IJEST), Vol. 3 No. 1 Jan 2011

[15] Vijay Chandramouli, "A Detailed Study on Wireless LAN Technologies", 23.10.2002

[16] "Understanding the New WPA TKIP Attack Vulnerabilities & Motorola WLAN Countermeasures", Motorola, Inc. 2008.

[17] Dajiang He, Charles. Q. Shen. "Simulation study of IEEE 802.11e EDCF" 2003

[18] Ismahnsi Binti Ismail, "Study of Enhanced DCF(EDCF) in Multimedia Application", 2005

[19] Preeti Venkateswaran, "Experiments to Develop Configurable Protocols", 2005

[20] Mark Greis, Tutorial for the Network Simulator "ns" 2008

[21] Lecture notes 2003-2004 University de Los Andes, Merida, Venezula and ESSI Sophia-Antipols, France.

[22] Guillermo Alonso Pequeño Javier Rocha Rivera, "Extension to MAC 802.11 for performance improvement in MANET", 2007

[23] Sam De Silva, Using TCP "Effectively in Mobile Ad-hoc Wireless Networks with Rate Adaptation", 2007

[24] Dheeraj babu gulluru, Performance evaluation of a secured ad-hoc routing protocol, JTNU, AP, 2002

[25] Turkan Ahamad & Manar Younis "The Enhancement of Routing Security in Mobile Ad-hoc Networks", IJCA(0975 – 888),Volume 48– No.16, June 2012.

[26] Payal Pahwa, Gaurav Tiwari, Rashmi Chhabra "Spoofing Media Access Control (MAC) and its Counter Measures", IJAEA, Jan. 2010 .

[27] Farhad Soleimanian & Zeinab Abbasi "Analysis and Evaluation of Dynamic Load Balancing in IEEE 802.11b Wireless Local Area" , IJCA(0975 – 888), Volume 47– No.22, June 2012.

[28] Joshua Wright "Detecting Wireless LAN MAC Address Spoofing", 2003.

[29] Mubashir Husain Rehmani at el, A Tutorial on the Implementation of Ad-hoc Demand Distance Vector AODV On in NS2, 2009

[30] Fanglu Guo and Tzi-cker Chiueh " Sequence Number-Based MAC Address Spoof Detection", 2005.

[31] Yuxia Lin et al, Experimental Comparisons between SAODV and AODV Routing Protocols, ACM 1-59593-183-X/05/0010, 2005

[32] Stuart Compton, SANS Institute, "802.11 Denial of Service Attacks and Mitigation", May 2007.

[33] D. Gupta, G. Tiwari,Y. K and P. Kumar "Media Access Control (MAC) MAC Spoofing and its Counter Measure", IJRTE, 2009

[34] Siemens Enterprise Communications, "WLAN Security Today: Wireless more Secure than Wired", white paper July 2008.

[35] Website :http://computer.howstuffworks.com,May- 2014

[36] Website :http:// milesweb.com , May- 2014

[37] Website : http://www.technitium.com, May- 2014

[38] Website : http://www.klcconsulting.net/smac May- 2014

[39] Website: http://www.softpedia.com/ get/ Network-Tools/ IP-Tools/ IPScan-II.shtml

[40] Website : http://ip-scan.qarchive.org/, May- 2014

[41] Website : ww.radmin.com/products/ipscanner,May- 2014

[42] Website : http://www.angryip.org/w/Home, May- 2014

[43] Website : http://www.opnet.com/itguru-academic

[44] Website : http://www.wikipedia.org. May- 2014

[45] Website : http://www.aircrack-ng.org. May- 2014

[46] Website : http://www.makeuseof.com, May- 2014

[47] website : http://Microsoft.com/india, May- 2014

[48] Website :http:/ Cisco.com May- 2014

[49] Website :http:/ mohittahiliani.blogspot.com, May 2014

[50] Preeti Venkateswaran, Experiments To Develop Configurable Protocols 2009

[51] Richa Bansal, Siddharth Tiwari, Divya Bansal "Non-cryptographic methods of MAC spoof detection in wireless LAN", ICON 2008: 1-6.

[52] Guenther Lackner, Udo Payer, and Peter Teu, " Combating Wireless LAN MAC-Layer Address Spoofing with Fingerprinting Methods", January 20, 2009.

[53] Hassene Bouhouche & Sihem Guemara, "A QoS-based Resources Reservation Mechanism for Ad Hoc Networks", IJCA (0975 – 8887), Volume 6– No.3, September 2010

[54] CERT-In Monthly Security Bulletin- February 2012, website : http://www.cert-in.org.in

[55] Mohd. Izhar, Mohd. Shahid & Dr. V.R.Singh"A Practical Approach for Evaluation of Security Methods of Wireless Network" for Vol. 4, No. 10 , October 2013 E-ISSN 2218-6301/ ISSN 2079-8407

[56] Mohd. Izhar, Mohd. Shahid & Dr. V.R.Singh, " Reliable and Secure wifi Performance model by way of cryptography and RSNA" , 6th International Conference on Quality, Reliability, Infocom Technology and Industrial Technology Management (ICQRITITM 2012) held at Delhi University, 26-28 Nov. 2012.

[57] Mohd. Izhar, Mohd. Shahid & Dr. V.R.Singh, "Network Security Vulnerabilities heading for malicious attack" IJCA Special Edition for CTNGC 2012, Nov 2012

[58] Mohd. Izhar, Mohd. Shahid & Dr. V.R.Singh, "Design & Modeling of Manet using different slot time simulated by NS-2", International Journal on Computer Science & Engineering(IJCSE), ISSN : 0975-3397, Vol. 3 No. 5 May 2011

[59] Mohd. Izhar, Mohd. Shahid & Dr. V.R.Singh "Enhanced Security Evaluation and Analysis of Wireless Network based on MAC Protocol", published for Nov. 2013 issue at International Journal of Scientific and Research Publications(IJSRP), ISSN 2250-3153.

[60] Mohd Izhar, Amit Prkash Singh & Dr. Rafat Parveen "Performance Model for Campus Area Network Based On Mac Protocol" (Paper No - P574) at "International Conference on Innovative Technologies (ICIT-09): held on June18, 19 2009 at PDM College of Engineering, Bahadurgarh Sponsored by IEEE.

[61] Mohd. Izhar, Mohd. Shahid & Dr. V.R.Singh , Proposing of collisions free and secure network for ieee 802.11 wlan, IJCA july 2014-communicated.

[62] Turkan Ahamad & Manar Younis, IJCA(0975 – 888),Volume 48– No.16, June 2012. The Enhancement of Routing Security in Mobile Ad-hoc Networks.

[63] Payal Pahwa, Gaurav Tiwari, Rashmi Chhabra, *IJAEA, Jan. 2010*. Spoofing Media Access Control (MAC) and its Counter Measures.

[64] Farhad Soleimanian & Zeinab Abbasi, IJCA(0975 – 888), Volume 47– No.22, June 2012. Analysis and Evaluation of Dynamic Load Balancing in IEEE 802.11b Wireless Local Area.

[65] Joshua Wright, 2003. Detecting Wireless LAN MAC Address Spoofing.

[66] Fanglu Guo and Tzi-cker Chiueh, 2005. Sequence Number-Based MAC Address Spoof Detection.

[67] Stuart Compton, SANS Institute, May 2007. 802.11 Denial of Service Attacks and Mitigation.

[68] D. Gupta, G. Tiwari,Y. K and P. Kumar, IJRTE 2009.Media Access Control (MAC) MAC spoofing and its countermeasures.

[69] Siemens Enterprise Communications, July 2008. WLAN Security Today: Wireless more Secure than Wired, white paper.

[70] George Ou, Jan 3, 2005. Wireless LAN security guide.

[71] Richa Bansal, Siddharth Tiwari, Divya Bansal, ICON 2008: 1-6. Non-cryptographic methods of MAC spoof detection in wireless LAN.

[72] Guenther Lackner, Udo Payer, and Peter Teu, January 20, 2009. Combating Wireless LAN MAC-Layer Address Spoofing with Fingerprinting Methods.

[73] Hassene Bouhouche & Sihem Guemara, IJCA (0975 – 8887), Volume 6– No.3, September 2010. A QoS-based Resources Reservation Mechanism for Ad Hoc Networks.

[74] IEEE Std 802.11™-2007, Revision of IEEE Std 802.11-1999, IEEE 3 Park Avenue New York, NY 10016-5997, USA 12 June 2007.

[75] IEEE Std. 2009 Revision of IEEE Std 802.11™-2007, 30 sept. 2009.

[76] IEEE Std 802.11i-2004, Amendment to IEEE Std 802.11™, 1999 Edition (Reaff 2003) as amended by IEEE Stds 802.11a™-1999, 802.11b™-1999,802.11b™-1999/Cor 1-2001, 802.11d™-2001, 802.11g-2003, and 802.11h-2003] Amendment 6: Medium Access Control (MAC) Security Enhancements, 23 July 2004.

[77] Yih-Chun Hu , David B. Johnson b, Adrian Perrig, 175–Elsevier 192, , SEAD: secure efficient distance vector routing, for mobile wireless ad hoc networks, 2003

AUTHORS

First Author MOHD. IZHAR, Associate Professor, HMR Inst. of Tech. & Mgt, GGSIP University, Delhi, Ph.D. Scholar of Mewar , University, NH-79, Gangrar, Chittorgarh (Rajasthan) India, email : mohd.izhar.delhi@gmail.com

Second Author – DR. V.R.SINGH, Recognized supervisor of Mewar University, NH-79, Gangrar, Chittorgarh (Rajasthan) India-312901, email : vrsingh@ieee.org.

Correspondence Author – MOHD. IZHAR. email : mohd.izhar.delhi@gmail.com