Proposing of Collisions Free and Secure Network for IEEE 802.11 WLAN

Mohd. Izhar
HMR Inst. of Tech. & Mgt, GGSIP University, Delhi,
Ph.D. Scholar of Mewar University, NH-79,
Gangrar, Chittorgarh, Rajsthan India

V.R.Singh, Ph.D
Ph.D. Supervisor of Mewar University, NH-79,
Gangrar, Chittorgarh, Rajsthan India

ABSTRACT
IEEE 802.11 wireless network contains various problems such as packets delay and drop because of collision due to the heavy traffic. Packets are dropped either by the buffer overflow or by the MAC layer contentions. Such packet losses decrease throughput. Packet delay is also 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. SAODV, SEAR and SEED protocols are used for solutions. But when some security measures are taken it may results in decreasing the throughput. Even network security in infrastructure mode for Wi-Fi point is of great concern where pre-RSNA as well as RSNA methods fail to provide proper security. This paper simulates such problems in NS2 and proposes the model of securing and increasing the throughput with least delay. .

General Terms
Throughput, Delay, Security, Routing Protocol .and Simulation

Keywords
ad hoc network, LAN, mobility, radio frequency, wired, wireless Network and IEEE 802.11, AODV, SAODV.

1. INTRODUCTION
Security issues and higher throughput with least delay are the main concern for IEEE 802.11 WLAN Network. Old legacy MAC protocol IEEE 802.3 is surely secure and provides collision free environment with better throughput when it is compared with the 802.11 but if area includes hilly region or such where laying of fiber optic cable is altogether unrealistic, WLAN is of great importance at that time. So, proper measures are required to solve the difficulties of 802.11 in order to provide Security, increased throughput and least delay. This Paper that is why pays attention to these problems and proposes collisions free and secure model for IEEE802.11 WLAN.

2. RELATED WORK
Many Papers have been published relating to such kind of problem inwhich Security issues and higher throughput are taken care of. Some of these Papers compare the result with different routing protocols in order to know which protocol provides the best throughput but not concerned with Security issues. While certain papers talks about security measures but ignores the necessity of throughput and fair delay. While security, throughput and end to end delay are important parameters and required to be considered at the same time.

3. TOOLS METHOD AND SERVICE

3.1 Simulation and Testbed
NS2 is used to simulate the model in order to know the way of increasing the throughput and reduce the delay time where different nodes at different slot time is tested. The statistics appears in trace file format. The Different Trace results formats used in NS2 are as follows :

Table-1 Old legacy Trace-file

1. Event	2. Time	3. From Node	4. To Node	5. Pkt Type	6. Pkt Size	7. Flags	8. Flg Id	9. Src Addr	10. Dst Addr	11. Seq. No.	12. Pkt id
+	0.2	0	1	Tcp	40	-	1	0.0	1.0	0	0
-	0.2	0	1	Tcp	40	-	1	0.0	1.0	0	0
r	0.210032	0	1	Tcp	40	-	1	0.0	1.0	0	0
+	0.210032	1	0	Ack	40	-	1	1.0	0.0	0	1
-	0.210032	1	0	Ack	40	-	1	1.0	0.0	0	1
r	0.220064	1	0	Ack	40	-	1	1.0	0.0	0	1
+	0.220064	0	1	Tcp	1040	-	1	0.0	1.0	1	2
-	0.220064	0	1	Tcp	1040	-	1	0.0	1.0	1	2
+	0.220064	0	1	Tcp	1040	-	1	0.0	1.0	2	3
-	0.220896	0	1	Tcp	1040	-	1	0.0	1.0	2	3
r	0.230896	0	1	Tcp	1040	-	1	0.0	1.0	1	2

Ns2 provides two types of trace format for wireless Network, old wireless trace format and new trace file format. One can use any of the layouts as per their requirement and parameters used in simulation.

Table-2 Old Wireless Trace-format

1	s	R	send, receive, drop, forwarding - s / r / D / f
2	0.2	0.2	timestamp
3	_0_	_0_	node ID for this node
4	AGT	RTR	name of object type tracing or trace level (AGent Trace, Router Trace, MAC, and so on)
5	---	---	reason for tracing
6	1	1	packet identifier
7	tcp	Tcp	packet type
8	40	40	packet size
9	[13a 1 0 800]	[13a 1 0 800]	**13a :** expected time to send data in hexa **1 :** MAC destination address **0 :** MAC source address **800 :** type – ARP (0x806) / IP (0x800)
1	-------	-------	
1	[0:0 1:0 32 1]	[0:0 1:0 32 1]	**0 :** source IP address **0 :** source port number **1 :** destination IP address in decimal (8.8.8 format – 36 implies 0.1.0) **0 :** destination port number **32 :** TTL **1 :** next hop address
1	[00]	[00]	TCP sequence number 0 TCP ack number 0
1	0	0	?
1	0	0	?

Table-3 New wireless Trace Format

```
s -t 2.556838879 -Hs 1 -Hd -2 -Ni 1 -Nx 426.02 -Ny 9.49 -Nz 0.00 -Ne
-1.000000 -Nl AGT -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 1.0 -Id 2.0 -
It cbr -Il 512 -If 0 -Ii 0 -Iv 32 -Pn cbr -Pi 0 -Pf 0 -Po 2
SFESTs 2.709814214 _1_ 0 [1 -> 2] 1(1) to 98 [1 |98 2 ]
r -t 2.731668849 -Hs 2 -Hd 2 -Ni 2 -Nx 40.50 -Ny 47.72 -Nz 0.00 -Ne
-1.000000 -Nl AGT -Nw --- -Ma 13a -Md 2 -Ms 62 -Mt 800 -Is 1.0 -Id
2.0 -It cbr -Il 512 -If 0 -Ii 0 -Iv 31 -Pn cbr -Pi 0 -Pf 2 -Po 2
d -t 2.866032021 -Hs 80 -Hd 1 -Ni 80 -Nx 242.86 -Ny 37.23 -Nz 0.00 -
Ne -1.000000 -Nl IFQ -Nw ARP -Ma 13a -Md 50 -Ms 50 -Mt 800 -Is 2.255
-Id 1.255 -It DSR -Il 60 -If 0 -Ii 20 -Iv 252 -P dsr -Ph 4 -Pq 0 -Ps
2 -Pp 1 -Pn 2 -Pl 4 -Pe 1->2 -Pw 0 -Pm 0 -Pc 0 -Pb 0->0
```

Test Bed

A test bed is also created for knowing the security issues of WLAN where we have access points with stationery and mobile nodes. Typical Scenario includes a leased line that is wired internet at the back connected to the server through router with built in firewall. Various access points are connected through different switches. These access points are points where WLAN users log-on to connect the nets.

3.2 Tools

IP scanners are the tools used for scanning the whole network that provides the information of each and every node such as ip and mac address. Angry Ip Scanner has been used in this paper for the purpose of scanning whole network. The list are as follows : Advanced IP Scanner 2.2.224, Colasoft MAC Scanner Pro 2.2, Angry IP Scanner 2.x, IPScan-II.The tool which has been used for scanning the network is free open source Angry IP scanner[38].

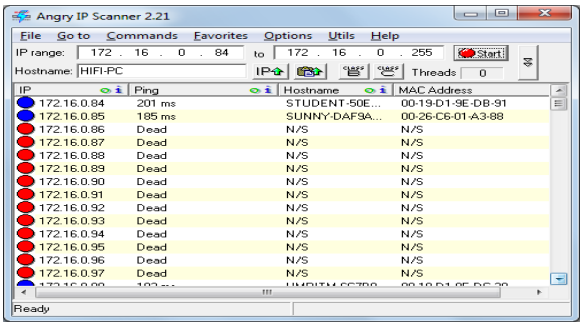

Figure 1.: Result of the Ip Scanner

3.3 CSMA/CA

A station willing to transmit senses the medium, if the medium is busy then it defers. If the medium is free for a specified time (called DIFS, Distributed Inter Frame Space, in the standard) then the station is allowed to transmit, the receiving station will check the CRC of the received packet and send an acknowledgment packet (ACK). Receipt of the acknowledgment will indicate the transmitter that no collision occurred. If the sender does not receive the acknowledgment then it will retransmit the fragment until it gets acknowledged or thrown away after a given number of retransmissions. [55]

Setting the slot time to an optimum value is important. If slot time is having less value it would result in collision and if it is big value it would results in unnecessary delay and have to wait for an unnecessarily long period of time.

Timing Relation [56]

-- SIFSTime and SlotTime are fixed per PHY.

SIFS=RxRFDelay+ RxPLCPDelay + MACProcessingDelay + RxTxTurnaroundTime.

Slot Time is = CCATime + RxTxTurnaroundTime + AirPropagationTime + MACProcessingDelay.

-- The PIFS and DIFS are derived by the following equations

PIFS = SIFS Time + Slot Time

DIFS = SIFS Time + 2 * Slot Time

4. RESULT AND DISCUSSION

4.1 Simulation

The following table shows the combined result of throughput and average delay with varied slot time.

Table-4 throughput and average delay

Slot time Micro sec	Average (delay)	average (throughput)	Result Per 1000 (Throughput)
20	1094	5693.093721	5203.924791
15	1099.2	5733.795312	5216.334891
12	1402.6	5548.114837	3955.593068
10	1062.8	5672.135207	5336.973285

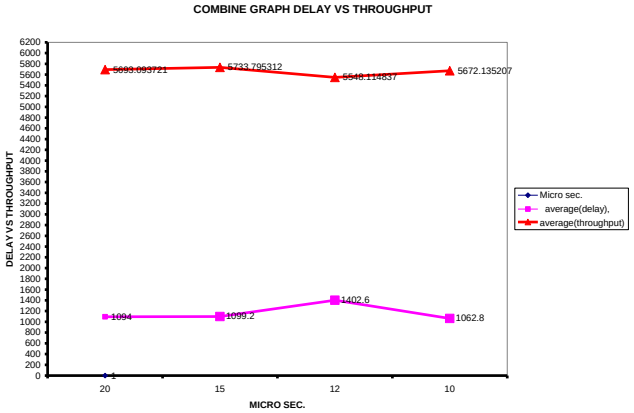

Figure 2: Throughputs vs. end to end delays

The result shows optimum point is 10 micro sec. as per our model. Nos. of nodes are reduced from 100 to 50 and then 25 and table and graph shows the same result.

Table-5 delay after reducing nos. of nodes

Slot time Micro sec	Average (Delay) 100 nodes	Average (delay) 50 nodes
20	1094	1051
15	1099.2	1122
12	1402.6	1123
10	1062.8	1043

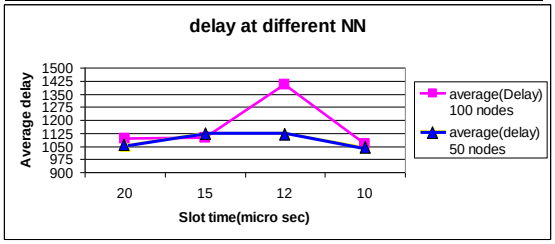

Figure 3: delay after reducing nos. of nodes

Table-6 Throughput Vs. Delay at varied nodes

Slot time Micro sec	Throughput VS. Delay 100 nodes	Throughput VS. Delay 50 nodes	Throughput VS. Delay 25 nodes
20	5203.924791	5065.680304	4848.838599
15	5216.334891	4945.641711	4433.870968
12	3955.593068	4848.174533	4969.019784
10	5336.973285	5244.534995	4892.237197

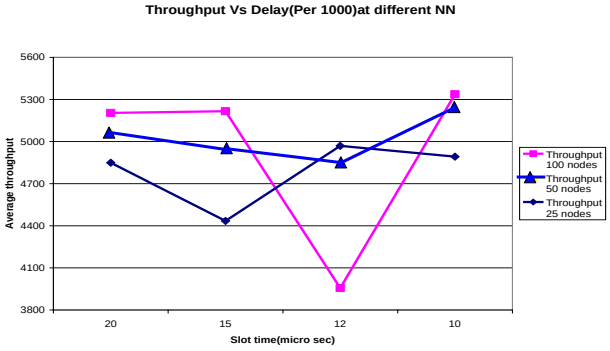

Figure 4 : Throughput Vs. Delay at varied nodes

On the basis of this graph one can conclude that the throughput at more nodes is best at slot time of 10 ms while the throughput of lesser nodes of best slot time is 12 m/s.

4.2 Practical Approach

This paper builds various practical scenarios for examining the several security issues and shows that how easily the security is breached and/or bypassed. First and upper most is MAC filtering which allows only some MAC address to be part of wireless network but there are various ways by which one can easily change the MAC address as desired[25]. Typically following 3 ways are common[53]:

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.

3. The MAC address can be changed through the MAC address Changer such as TMAC and SMAC soft wares.

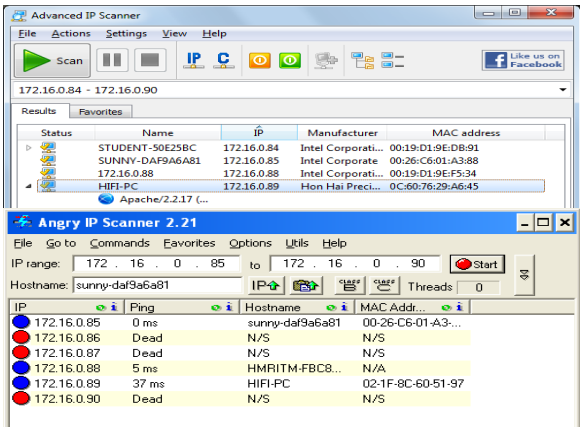

Figure 5. Orignial and Spoofed MAC Address

Second is WEP Key and its Cracking[51-56], The procedure for wep key cracking is very simple and one need only a Bootable DVD of Backtrack which contains various utilities used for cracking. WPA encryption is understood stronger than wep and it was designed specifically to replace wep. The Problem by using WPA2 is that the entire device on network must use WPA2 or compatible. 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. D-link offers DAP-1360 wireless N access points as shown in figure.

The Phishing attack can be minimized by using the latest browser capabilities such as SmartScreen Filter from Microsoft. Internet Explorer 9 allows to use ActiveX Filtering to block ActiveX controls, the 3rd party software which are not trustworthy one and are used for web rich experiences such as audio video players plug in. InPrivate filtering prevents websites from collecting information of a user who uses the browser as InPrivate filtering, cookies and temporary internet files are kept in memory and cleared as the browser is closed. Even temporary information is encrypted and stored to show web pages correctly. It is secured to an extent but it can not prevent hackers from seeing and recording which websites you visited.

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.

5. CONCLUSION AND FUTURE WORK

Higher throughput, least delay and Network Security are prime concern for researchers. This paper through simulation and practical approaches takes care of each one and concluded that one can use different slot time for different nodes for better throughput and least delay, it also provides in developing the collision free environment. While Security is concerned, shortcomings of each and every method are highlighted and proper measures are discussed in result and discussion. As far as routing protocol is concerned, the problem of them are solved by using secure routing algorithms such SAODV, SEAD and SEAR but it may affect the throughput, delay and other parameters. The present work can be extended to get all the answers in near future.

6. 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 document.

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

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

[26] 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.

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

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

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

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

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

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

[33] Website :http:// milesweb.com , MAY 2014

[34] Website : http://www.technitium.com, MAY 2014

[35] Website : http://www.klcconsulting.net/smac.

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

[37] Website : http://ip-scan.qarchive.org/, MAY 2014

[38] Website: ww.radmin.com/products/ipscanner,MAY 2014

[39] Website : http://www.angryip.org/w/Home, MAY 2014

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

[41] Website : http://www.wikipedia.org. MAY 2014.

[42] Website : http://www.aircrack-ng.org. MAY 2014

[43] Website : http://www.makeuseof.com

[44] website : http://Microsoft.com/india, MAY 2014

[45] Website :http:/ Cisco.com MAY 2014

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

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

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

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

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

[51] 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

[52] 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.

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

[54] 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

[55] 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.

[56] 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