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 result 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.
Table-3 New wireless Trace Format

<table>
<thead>
<tr>
<th></th>
<th>1.000000</th>
<th>1.000000</th>
<th>1.000000</th>
<th>1.000000</th>
<th>1.000000</th>
<th>1.000000</th>
<th>1.000000</th>
<th>1.000000</th>
<th>1.000000</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>1.000000</td>
<td>1.000000</td>
<td>1.000000</td>
<td>1.000000</td>
<td>1.000000</td>
<td>1.000000</td>
<td>1.000000</td>
<td>1.000000</td>
<td>1.000000</td>
</tr>
</tbody>
</table>

Test Bed

A test bed is also created for knowing the security issues of WLAN where we have access points with stationary 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 result in unnecessary delay and have to wait for an unnecessarily long period of time.

Timing Relation [56]

-- SIFSTime and SlotTime are fixed per PHY.
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, Hamdipur, Delhi, PDM College of Engineering, M.D. University, 3A, Sarai Aurangabad, Bahadurgarh, Haryana and Mewar University, NH-79, Gangrar Chittorgarh Rajastan who supported the most in preparing this document.

7. REFERENCES


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


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


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

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


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


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


