Performance Evaluation of Wi-Fi Physical Layer Based QoS Systems on Fiber using OPNET Modeler

Adnan Hussein Ali

Abstract- Wireless Fidelity (WiFi) network is based on the IEEE 802.11 standard. WiFi units are used to provide a connection of local devices within homes or businesses. In this paper, OPNET Modeler is used to module and simulate a WiFi networks in fixed local area networks to estimate their performance based on End to End Delay and WiFi voice-packet delay for both WiFi base line and WiFi base fiber. Simulation results indicate that base line has delay larger than base fiber.

Keywords: Wireless LAN, Wi-Fi, End to End delay, OPNET.

I. INTRODUCTION

IEEE 802.11, Wireless Local Area Network (WLAN), was inserted in the beginning of 1990s. The goal was to present best-effort package access network without the use of wires. WLAN uses an unlicensed band, therefore any user can purchase a WLAN product and easily used it without any permission. This fact has allowed WLAN to quickly expand into the consumer market and be embedded in many portable devices. In late 1990s, the WLAN has been the most popular choice of communication amongst users and several companies formed Wireless Fidelity (WiFi) Alliance to create a single standard for high-speed WLAN which would be accepted worldwide [1]. This standard relies on IEEE 802.11. WiFi distributes high-speed Internet access from cables within wireless hotspots which has radically increased convenience and productivity for users. Today, millions of homes, offices, hotels, restaurants, airports and other public locations have WiFi high-speed WLAN connectivity. WiFi offers mobility and flexibility with a relatively low cost to users and usage popularity has increased by more than 4 times from year the 2004 to 2012 in every market around the world [2]. In addition, wireless technology is providing easier internet access to areas that are too difficult and expensive to reach with traditional wired infrastructure. In 1997, the primary model of the 802.11 protocol was submitted [3]. Since then, various adjusted protocols added. The IEEE 802.11 standard, with particular modifications, was designed to address wireless local area coverage. The reason was the claim for higher data rates, improved Quality of Service (QoS), different modulations and frequency transmissions, enhanced security and authentication mechanisms. These problems were directed to Wireless Fidelity Alliance. WiFi Alliance have been implemented a test suite to verify interoperability for the adopted 802.11b products which is an amendment of the initial 802.11, its operate in the band of ISM give data rates up to 11Mbps, both in infrastructure mode and in ad - hoc mode for client-to-client (C2C) connections [4].

After, the IEEE 802.11g has been familiarized and then certified as a continuity and extension to the protocol 802.11b. 802.11g works in the similar frequency range but with data rates up to 54 Mbps [5], and providing compatibility with 802.11b devices. The higher data rates attained with the usage of a larger group of modulation selections. Another significant modification was the IEEE 802.11i protocol [6], in which, newer and stronger security and authentication mechanisms were added in order to address security deficiencies that were obtainable in WiFi.

External revisions to the standard through hardware and software permit Wi-Fi products to become a metro-access distribution option. These two main revisions address two dissimilar usage models:

- Fixed-access or last-mile usage—802.11 with high gain antennas
- Portable-access or hot-zone usage—802.11 mesh networks

Wi-Fi products associated with the metro-access distribution option use these dissimilar radio frequencies:

- The 802.11a standard uses 5 GHz in an AP-to-AP interlink.
- The 802.11b and 802.11g standards use 2.4 GHz.

The frequency bands used typically for wireless networks and specially equipment for Wi-Fi are the 2.4 and 5 GHz, which are classified as shared common use. The characterization as common usage permits numerous operators or users can use these frequencies at once, according with standards established by regulation to relieve the potential for interference between emissions. In 2005, IEEE advanced a new extension of 802 standards famous as 802.11e to standardize QoS improvement efforts. This was done to tackle the QoS provisioning difficult made by the MAC methods like Point Coordination Function (PCF) and Distributed Coordinated Function (DCF) in the previous extensions [7]. The MAC techniques in the IEEE 802.11e significantly improve QoS support for Wi-Fi.

II. WiFi MODIFICATIONS

A group of specifications advanced by the Institute of Electrical and Electronics Engineers (IEEE) for wireless local area networks (WLANs) with a longtime contributor Intel to the IEEE 802.11 standard. Much of the present work on IEEE 802.11 motivations on increasing transmission speeds and range, improving Quality of Service (QoS), and adding new capabilities. Now that IEEE 802.11n, the latest version of IEEE 802.11, is shipping in volume, the motivation is on even faster results, specifically IEEE 802.11ac and IEEE 802.11ad. These improvements aim to offer gigabit speed WLAN.

Revised Version Manuscript Received on June 10, 2015.
Dr. Adnan Hussein Ali, Institute of Technology, Middle Technical University, Baghdad.

The difference is their frequencies. IEEE 802.11ac will deliver its throughput over the 5 GHz band, affording easy migration from IEEE 802.11n, which also uses 5 GHz band (as well as the 2.4 band). IEEE 802.11ad, targeting shorter range transmissions, will use the unlicensed 60 GHz band (see table 1). Through range enhancements and faster wireless transmissions, IEEE 802.11ac and ad will:

* Advance the performance of high meaning TV (HDTV) and digital video streams in the home and progressive applications in enterprise networks
* Help businesses decrease capital expenditures by freeing them from the cost of laying and maintaining Ethernet cabling
* Increase the reach and performance of hotspots
* Permit connections to handle further clients
* Advance overall user experience where and whenever people are connected

Table 1: Wireless LAN Throughput by IEEE Standard

IEEE WLAN Standard	Over-the-Air (OTA) Estimates	Media Access Control Layer, Service Access Point (MAC SAP) Estimates
IEEE 802.11b	11 Mbps	5 Mbps
IEEE 802.11g	54 Mbps	25 Mbps (when .11b is not present)
IEEE 802.11n	Up to 600 Mbps	Up to 400 Mbps
IEEE 802.11ac	Up to 867 Mbps with 2 antennas and 80 MHz; Up to 1.3 Gbps with 3 antennas and 80 MHz	Up to 600 Mbps with 2 antennas and 80 MHz; Up to 900 Mbps with 3 antennas and 80 MHz
IEEE 802.11ad	At least 1.1 Gbps (up to 4.6 Gbps in some first generation products)	Up to 700 Mbps for 1.1 Gbps OTA (up to 3 Gbps for 4.6 Gbps OTA)

WiFi is based on IEEE third modulation standard. It operates in 2.4 GHz frequency band and offers data transfer at maximum rate of 54 Mbps. The orthogonal frequency division modulation system is used at data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps. It comes back to complementary code keying (CCK) for 5.5 Mbps and 11 Mbps and direct-sequence spread spectrum (DSSS) for 1 Mbps and 2 Mbps [8]. The access to WiFi is made easy by integration of WiFi into electronic devices, Smart phones and laptops are WiFi integrated. WiFi has two kinds of components: a wireless client station and an access point (AP). Wireless client station is any user device such as computer or laptop that has a wireless network card. AP acts as a bridge between fixed and wireless networks. It connects to the cable modem or Digital Subscriber Line (DSL) modem, offers Internet services to wireless and wired Ethernet clients, organizes and grants access from multiple wireless stations to the fixed network [9].

Figure 1: WiFi client/station connection [9].

III. WiFi SECURITY MECHANISMS

One of the prime concerns in wireless networking is security. Every safety mechanism for wireless transmission is working to offer three simple functions:(i) Authentication to confirm the individuality of the authorized communicating client stations; (ii) confidentiality (Privacy) to secure that the wirelessly transferred information will remain private and protected; (iii) integrity to secure that the transmitted several MAC-level protocol data units (MPDU) from a source will reach at its destination intact, without being improved. Authentication activates at the Link Level between WiFi stations. Confidentiality and Integrity is employed in the MAC security sub layer, just a level higher from the PHY layer. As WLANs operate over the shared medium, ***eavesdropping*** by unauthorized people and critical information may be accessed with the use of ***malicious*** technologies. The early standard (Wired Equivalent Piracy) WEP had security flaws which lead the Wi-Fi forum to implement another encryption system Wi-Fi protection Access (WPA) and later WPA2. Though WPA and WPA2 are much further secure and offers good protection still it is not secure sufficient to be contend with. Further complex encryption procedures need to be employed without reducing the MAC layer throughput.

IV. TECHNOLOGICAL LIMITATIONS OF THE 802.11 FAMILY

Regardless of the frequency bands in which they operate, all standards 802.11 subfamily share some restrictions that must be familiar before making a decision on coverage , scope or speed that can be achieve.

These restrictions are five:

• Scope (range): Although commercial speech is usually a range of up 100m, this data depends on two factors, initially, the location and the presence of obstacles in the path between the access point (AP) and the terminal, and secondly, weather situations and interference, thus, open space, with good weather and outdoor antennas terminals, this range may be considerably higher.

• Bandwidth: the dissimilar standards can be attained in air channel, however, because of the effect the necessary protocols to transport user information on the air channel, the service speed is much lower. Moreover, based on environmental situations and, therefore, the quality of each communication between a terminal and the access point (AP), the width of this communication adjusting. That's why sometimes we find a connection with the Access Point 11Mbps, 5Mbps others, on 2 Mbps or even in 1Mbps. Quality of service (QoS): Not all traffic is equally significant from the scene of each user, so that a call of VoIP should take priority over a file transfer. Wi-Fi Protocols are further extensive and not comprise any mechanism to prioritize one type of traffic over one another, which is very harmful when traffic flows are mixed with very different necessities, as voice and data.

• Security: Wi-Fi did not have mechanisms sophisticated security because the emphasis was on how to transmit data in air. With the success of this technology, though, and the publication of the weaknesses of the mechanisms original security, it became essential to make developments in this area. Also, the 802.11i solves most of the original weaknesses to the point of making them comparable in safety in fixed networks.

• Mobility: Commonly considered that wireless networks are mobile, and not to connect a fixed location to access services it offers, and Internet browsing or reading email whereas, Indeed, it is difficult to use a Wi- Fi network from a vehicle moving at normal speed, for reasons related physical speed because of the restricted scope of coverage of a point access, we have to rapidly connect to additional point access, one which implies "jump" from one another. Here again the standard has shortage which might cause us to lose briefly.

V. WiFi SIMULATION SETUP

We used OPNET Modeler 14.5 to simulate WiFi scenarios [10].WiFi scenarios are used the parameters shown in Table 2.

Table 2: WiFi parameters

WiFi 802.11g		
	AP (Access Point)	Mobile Node
Tx Power	0.1W	0.1W
Data Rate	11Mbps	11Mbps
Receiver Power Threshold	-95dBm	-95dBm
Buffer Size	1024000 bits	256000 bits
Short Retry Limit	7	7
Long Retry Limit	4	9
Large Packet Processing	Fragment	Fragment
Access Point Functionality	Enabled	Disabled

We produced three OPNET models for WiFi and fixed local area networks to estimate their performance. OPNET results sample communications devices, protocols, technologies, and constructions, and simulate their performance in a dynamic virtual network environment. A connection of three subnets are employed through the work, subnet in reign one, BC that has a server, for streaming video and voice, connected to the Internet cloud. There is another subnet in reign two, which receives the video and voice data and distributes the data content from a Base Station to various subscriber station (SS) subnets around it. The SS subnets are all WiFi enabled and receive the data through their WiFi routers and distribute the data content over WiFi link to dissimilar computers.

5.1 Baseline WiFi Scenario

The Baseline Scenario of 802.11g model was formed using a diversity of the WLAN scenario deployed with OPNET standard models. The manner of a single infrastructure 802.11g WLAN has been examined to get a shape of an actual network within the framework of an employed WAN. An Internet Protocol IP cloud considered as a backbone Internet, is done with a T1 Point-to-Point (1.544Mbps) serial link. The three subnets are situated on the three sides of this IP cloud through an IP gateway linked by Point-to-Point Protocol PPP T1 link and two servers connected through a central switch using 100 BaseT, as displayed in Fig. 2.

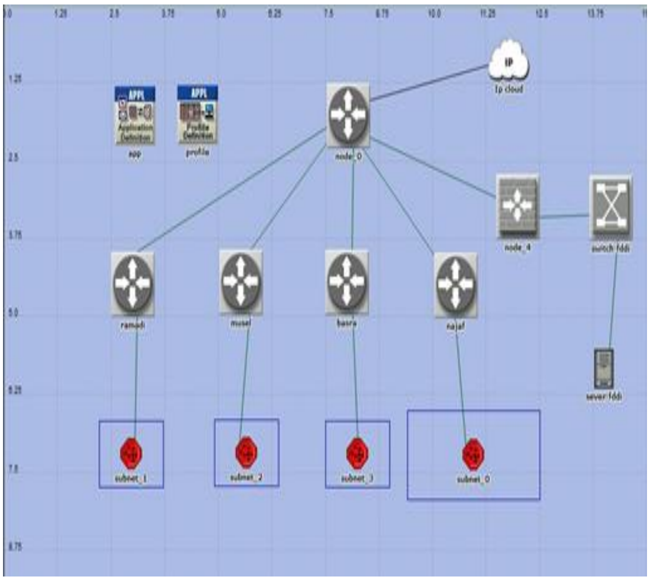

Figure 2: Simulated Wire Server with four subnets

A network's traffic server are connected by 100BaseT Ethernet on the one side of the Internet Protocol (IP) cloud, the server connected to the firewall using 100BaseT Ethernet wiring and used as the source and destination of all services: video conferencing, voice applications in the 802.11g WLAN during the simulation. The base line WiFi application shape is displayed in Figure 3 where the light, and heavy video, and PCM voice were used in the scenario.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

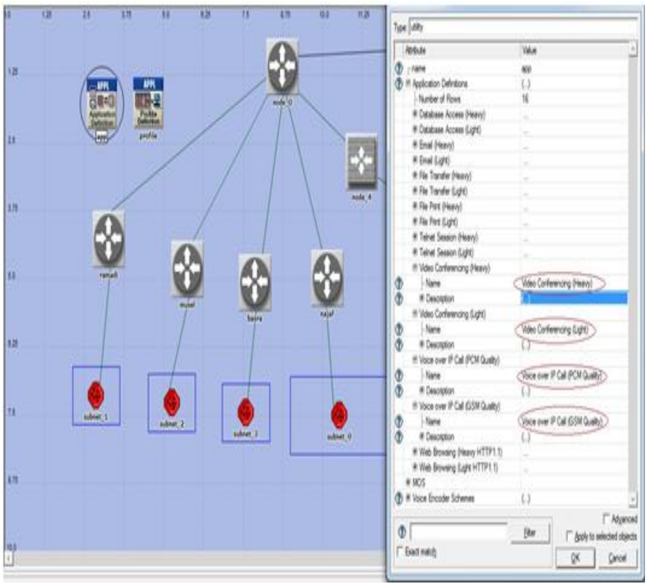

Figure 3: The base line WiFi application configuration

The base line WiFi outline shape is shown Figure 4 where assessed the applications of data transmission in the scenario.

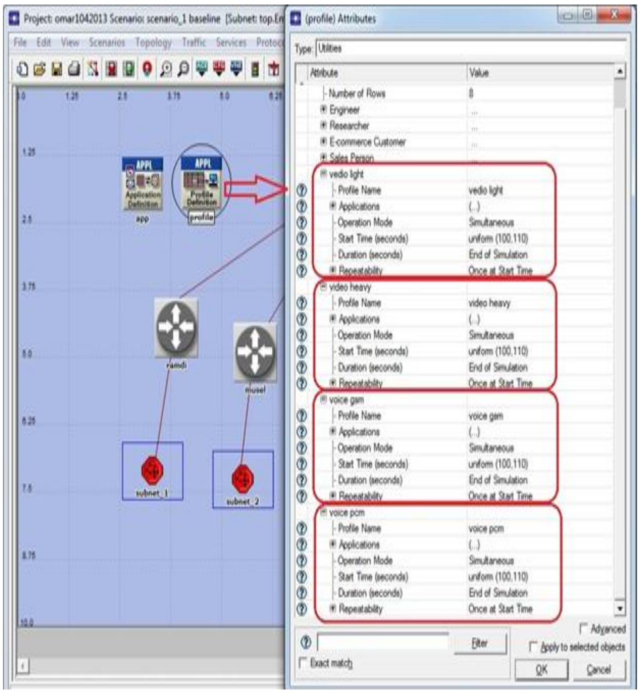

Figure 4: The base line WiFi profile configuration

The subnet one represents the remote branch office consisting an office-LAN having workstations connected by a 100BaseT link. Office LAN connected through a central switch using 100 Base T Ethernet wiring emulating a real life office situation with a standard Fast Ethernet LAN. An IP gateway connects the LAN to an IP cloud. The gateway connects to the office LAN using 100BaseT Ethernet wiring while the connection between the gateway and the IP cloud is done with a Point-to-Point T1 (1.544Mbps) serial link, as shown in Figure 5.

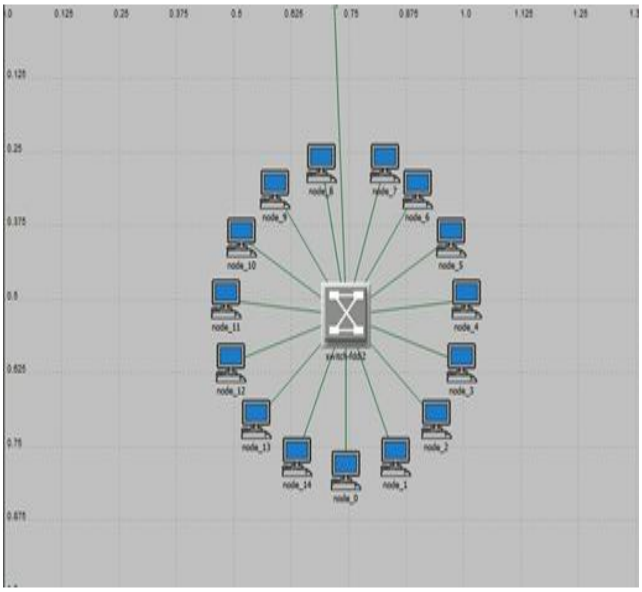

Figure 5: Subnet (1) 802.11g LAN

The subnet two situated on the additional side of the Internet Protocol cloud, the WLAN is connected via its access point to an office LAN through a central switch using Ethernet wiring with a standard Fast Ethernet LAN having a WLAN extension to an area of cabling difficulty or requiring aesthetics e.g. a conference or media room. An Internet Protocol gateway connects the LAN to an Internet Protocol IP cloud using 100BaseT Ethernet wiring whereas the connection between the IP gateway and the IP cloud is done with a Point-to-Point T1 (1.544Mbps) serial link, as displayed in Figure 6.

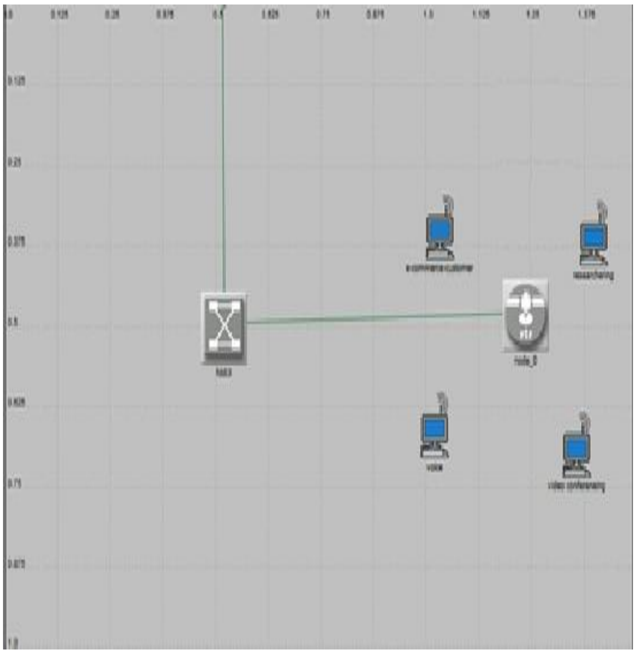

Figure 6: Subnet 2 802.11g WLAN

Subnet three represent the combination of both subnet one and subnet two with the similar parameters shapes as displayed in Figure 7.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

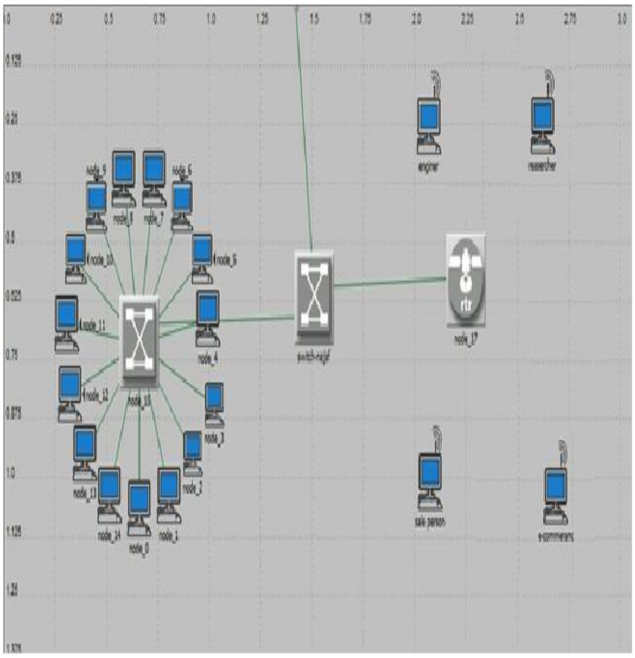

Figure 7: Subnet 3 Offices WLAN

5.2 Base Fiber Optic WiFi Scenario

In this scenario, we replaced all the Ethernet component with fddi and all the 100baseT link are replaced by fddi link

- Ethernet gateway replaced by fddi gateway
- Ethernet firewall replaced by fddi2 firewall
- Ethernet _switch16 replaced by fddi16_switch
- 100baseT link replaced by fddi link
- Ethernet server replaced by fddi server

And the fiber networks became as displayed in figures 8, 9, 10, and 11.

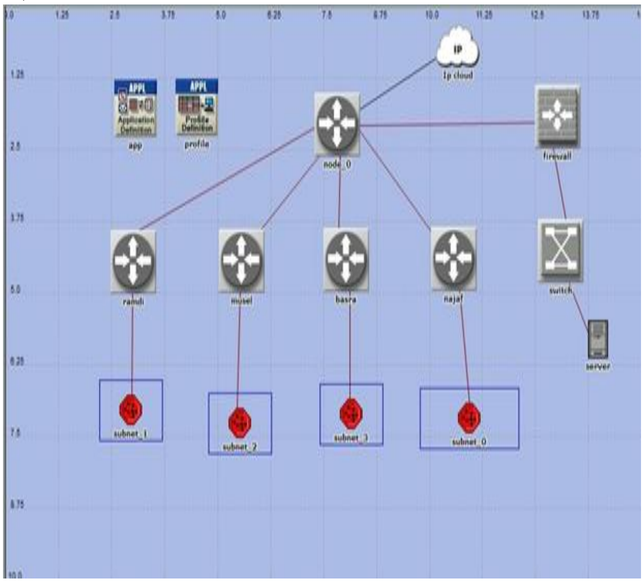

Figure 8: Simulated fiber Server with many subnets

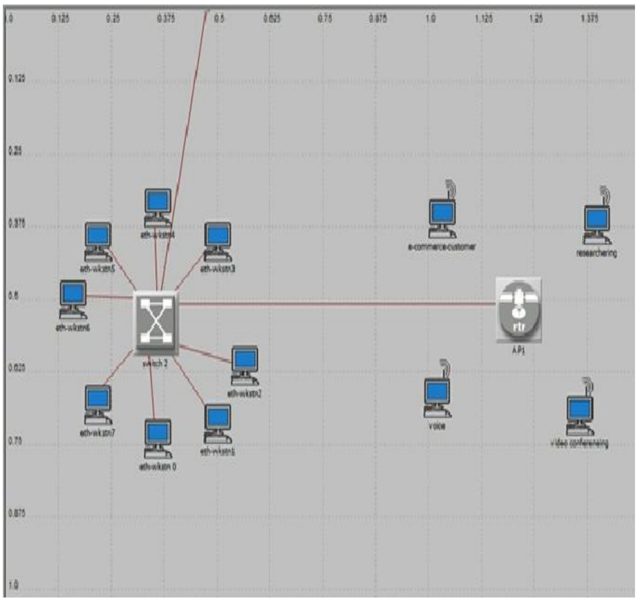

Figure 9: WiFi base fiber Subnet 1

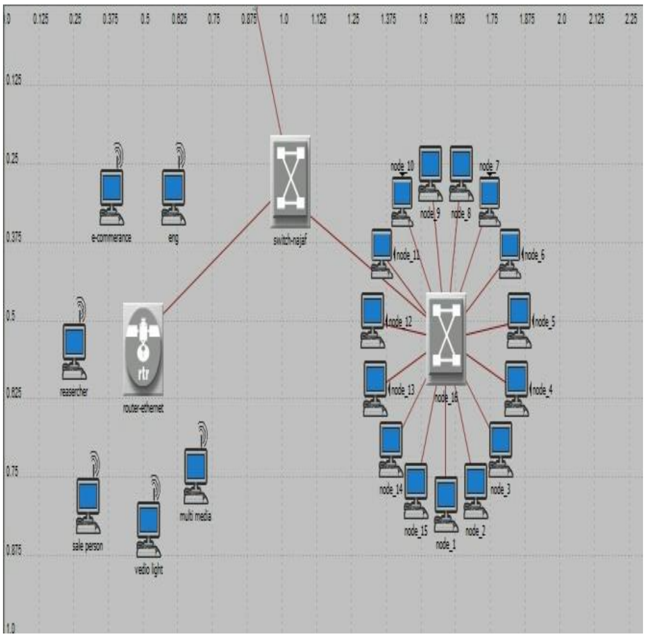

Figure 10: WiFi base fiber Subnet 2

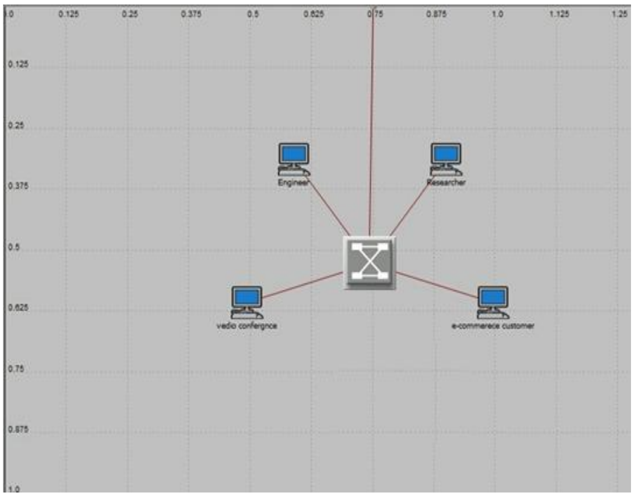

Figure 11: WiFi base fiber Subnet 3

VI. OPNET SIMULATION RESULTS & CONCLUSION

OPNET offers high-resolution modeling, simulation, and investigation of WLAN networks such as interference or overlap, transmitter/receiver, and all protocols, counting MAC, routing, higher layer protocols, and applications. It has also the ability to integrate node mobility and correlate wire line transport networks [11]. Two applications are used in two scenarios to compare the network load and queuing delay will be explained depended on time delay measurement for both WiFi base line and WiFi base fiber and measure the voice-packet end to end delay for both WiFi base line and WiFi base fiber. The period of the simulation for all situations was 350 seconds.

5.1 WiFi Delay

The measurements of the average queuing delay are taken from the moment when a packet arrives into the queue until the time when the last bit of the packet is transmitted.

5.1.1 End to End Delay: which is calculated as the average difference between the time each data packet is transmitted by a source entity and the time is received by a receiver entity, and then averaged over the total number of receiver entities. The end-to-end delay measured in the simulation of the WiFi base line connection displayed in Figure 12. From the simulation results there are no connection until 100 s where the connection network established, and the communication system reach the steady state with maximum delay 0.048 second at the second 200.

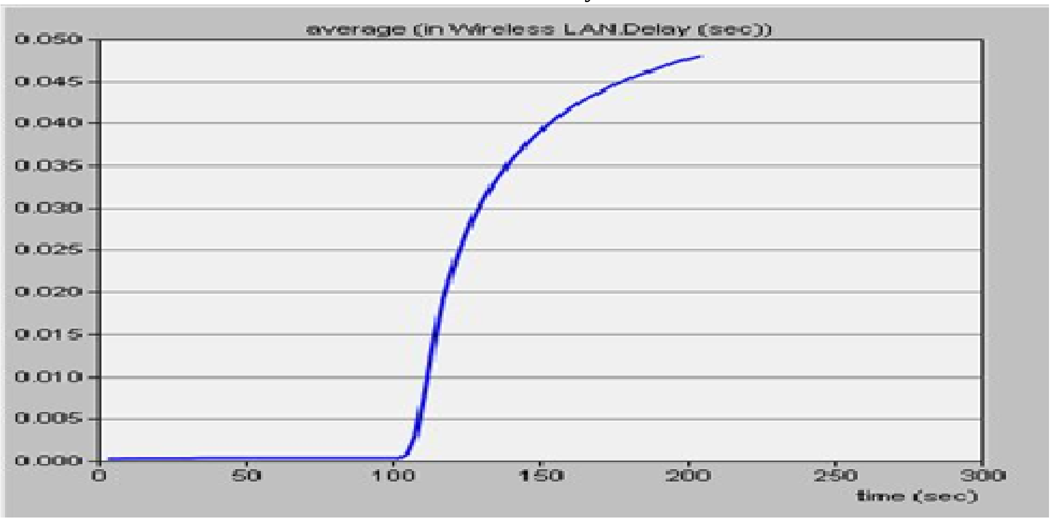

Figure 12: wireless-delay based line connection

The delay simulation results of the WiFi based fiber optic connection displayed in Figure 13. Here, after 100 s there is a connection network establishment, and the communication system reach the steady state with maximum delay 0.042 second at the second 300.

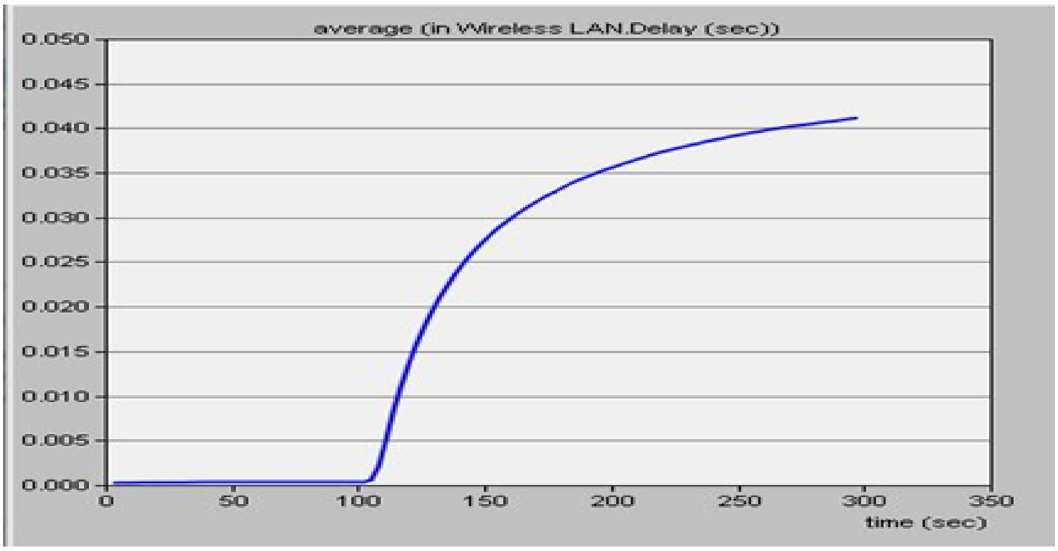

Figure 13: wireless-delay based fiber connection

A comparison between wireless-delay based line connection and wireless-delay based fiber connection can be shown in Figure 14. From the simulation results it's found that at a time of 200 s the base line WiFi has a delay of 0.048 s and the WiFi base fiber has a delay of 0.035 s, then the base line WiFi has delay larger than delay WiFi base fiber.

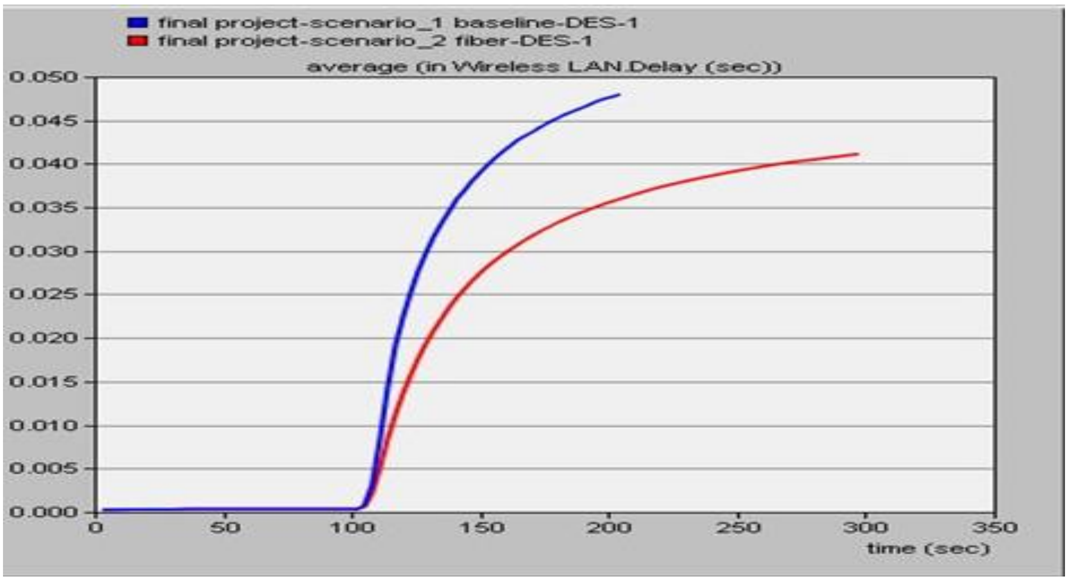

Figure 14: Delay comparing between WiFi base fiber and WiFi base line

5.1.2 WiFi voice-packet delay

The voice-packet end to end delay WiFi base line can be displayed in fig. 15. There is no link until 110 s where the connection network established, and the communication system reach the steady state with maximum delay of 1 packet at the 200 second.

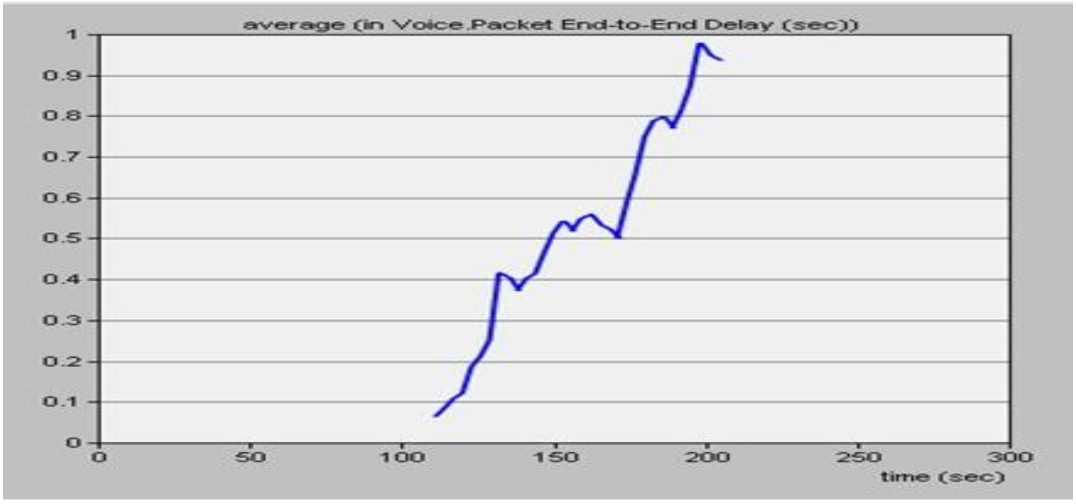

Figure 15: voice-packet end to end delay WiFi base line

For WiFi base fiber optic, it can be displayed from the simulation results of the voice-packet end to end delay, there is no connection until 110 second where the network connection will be established, and the network framework reach the steady state with maximum delay of 10 packet at the 300 second, as displayed in Figure 16.

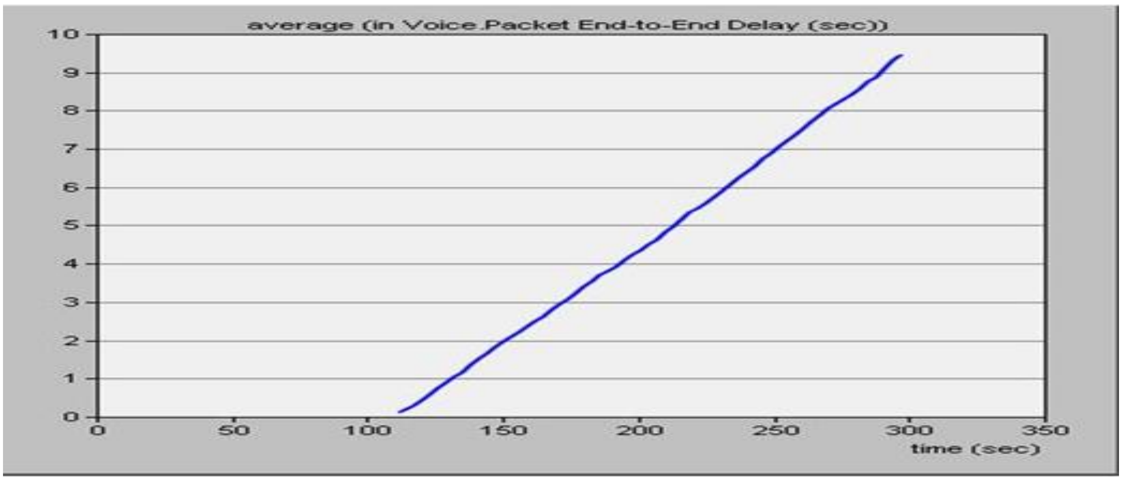

Figure 16: voice-packet end to end delay WiFi base fiber

A comparison between voice-packet end to end delay based line connection and voice-packet end to end delay based fiber connection can be shown in Figure 17. From the simulation results, at the time of 200 second the base line WiFi has one voice-packet delay and the WiFi base fiber has four voice-packet delay, it deduced that the base fiber WiFi has voice-packet delay larger than delay WiFi base line.

Figure 17: voice delay comparing between WiFi base fiber and WiFi base line

Figures (14, 17) show OPNET comparison results for the previous scenarios. They show the ratio of average End to End Delay and voice- packet Delay as a function of simulation run time that used in our experiments, the base line WiFi has delay larger than WiFi delay base fiber. The base fiber WiFi has voice-packet delay larger than delay WiFi base line.

REFERENCES

1. Zainab T. Alisa, "Evaluating the Performance of Wireless Network using OPNET Modeler", International Journal of Computer Applications, Volume 62– No.13, January 2013.
2. P.Trimintzios1 and G. Georgiou, "WiFi and WiMAX Secure Deployments" Journal of Computer Systems, Networks, and Communications Volume 2010, Article ID 423281.
3. L.M.S.C. of the IEEE Computer Society, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical ayer Extension in the 2.4 GHz Band," ANSI/IEEE Standard 802.11-1999TM.
4. Kritika, N., Namarta. "Performance Evaluation of 802.11 WLAN Scenarios in OPNET Modeler" International Journal of Computer Applications, May 2011.
5. H. Zhu, M. Li, I. Chlamtac, B. Prabhakaran, "A survey of quality of service in IEEE 802.11 networks", IEEE Wireless Communications, 2004.
6. Garima Malik *, Ajit Singh, "Performance Evaluation of WiFi and WiMax Using Opnet ", International Journal of Advanced Research in Computer Science and Software, Volume 3, Issue 6, June 2013.
7. L. Das Dhomeja, Shazia Abbasi, Asad Ali Shaikh1, Y. A. Malkani, "PERFORMANCE ANALYSIS OF WLAN STANDARDS FOR VIDEO CONFERENCING APPLICATIONS", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 6, December 2011
8. S. Banerji, R. Singha Chowdhury, "On IEEE 802.11: Wireless LAN Technology "International *Journal of Mobile Network Communications & Telematics (IJMNCT) Vol. 3, Issue. 4, 2013.*
9. Eldad Perahia, Michelle X. Gong, "Gigabit Wireless LANs: an overview of IEEE 802.11ac and 802.11ad ", Intel Corporation
10. OPNET Technologies, OPNET WORK 2007 proceedings (online). Available: http://www.opnet.com/opnetwork2007.

AUTHOR'S PROFILE

The Author is a Lecturer in the Computer Engineering Department at Institute of Technology, Baghdad, IRAQ. He has been awarded a Doctor of Philosophy in Laser and Opto-Electronics Engineering from University of Technology, Baghdad, in 2007. He has studied Master of Science in Electronics Engineering, Cupper Vapor Laser's Power supply at University of Technology, Baghdad in 2000. He has gained Bachelor in Electrical and Electronic Engineering from University of Technology, Baghdad, in 1987. Currently he is lecturer at Institute of Technology, Baghdad, IRAQ. His research interests are Radio over Fiber, Wireless Network, Laser's Power supply and OPNET.