www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 6 June, 2013 Page No. 1766-1776

IWLAN: AN IMPLEMENTATION MODEL FOR HIGH DENSITY SMART INTRANET COMMUNICATIONS, (A CASE FOR ELDI)

***Okafor KC, Udeze CC, Nwafor CM, Abarikwu AC**

Electronics Development Institute, Awka, National Agency for Science and Engineering Infrastructure, NASENI Federal Ministry of Science and Technology, Nigeria.

ABSTRACT

The need for high performance wireless network connectivity that saves cost, time and mess of wires running across offices and in providing high speed access has continued to attract attention to individuals, private and cooperate organizations in the developing countries. This paper presents a cost effective wireless hotspot model called iWLAN for Electronics Development Institute (ELDI), Awka, Nigeria, that supports multiple user sessions simultaneously. This work present an implementation model of iWLAN as well as conduct an experimental study for an enhanced distributed channel access mechanism of Linksys 300N AP used in this work. The main focus of the study is on SMART intranet traffic engineering and QoS guarantees in the iWLAN model. With the former, we aim at distributing the bandwidth in the iWLAN according to available throughput allocation criterion. With the latter, the objective is to ensure that the performance metrics (throughput and delay) experienced by a user allows for flexible data communication within the high density zones. We present our implemented test bed with Aradial RADIUS server and Cisco Linksys wireless router that support Distributed Coordination Function (DCF) functionality and analyze the test approach for iWLAN model.

[Keywords: SMART intranet, iWLAN, DCF, Bandwidth, Cisco Linksys, Performance Metrics]

INTRODUCTION

SMART intranet traffic engineering and QoS guarantees are critical considerations in the iWLAN design initiative in this research. The iWLAN model is developed to have a fault-tolerant and fully distributed architecture, enabling users to access the internet, transfer files, to detect users' availability without server software, to send messages to offline clients, and to perform many other functions. Network Communication (decentralized access to organizational resources) and Instant Messaging constitutes routine services in ELDI. The iWLAN model presents the benefits of serverless instant smart communication over wireless local area network users with zero administration and zero configuration. While extensive technological advancements have been made in the speed and ease of implementation of Wi-Fi networks, the basic nature of radio frequency (RF) is generally unchanged. Increasing the number of users who can access the WLAN in a small physical space remains a challenge[1]. The steps and process for implementing a successful high user density iWLAN model is summarized using Cisco's Unified Wireless Network framework [1].Our implementation steps include:

i. Network Planning: Determine application and device requirements such as bandwidth, protocols, frequencies, service level agreement (SLA), etc.
ii. Network Model and Design: Determine density, cell sizing, antennas, coverage, site survey, etc.
iii. Implementation: Install, test, tune, establish baseline, etc.
iv. System Optimization: Monitor, report, adjust, review baseline for SLA.
v. Operation: Cisco Wireless Control System (WCS) monitoring, troubleshooting tools, capacity monitoring and reporting tools, etc.

The concepts underlying our high-density iWLAN design remain valid in our context, but the authors noted that the implementation strategies, content and solutions presented in this paper varies with different WLAN design scenarios. The objective of this work is to explain the implementation strategy of our iWLAN model for our high-density client environments, and through experiments validate the traffic engineering and QoS metrics for the model and consequently articulate the impact our design decisions will have on the overall system performance and stability.

RELATED WORKS

The work in [2] discussed two different access mechanisms in WLAN: the enhanced distributed channel access (EDCA) and hybrid coordination function (HCF) controlled channel access (HCCA). EDCA is a distributed scheme that extends the distributed coordination function (DCF) of 802.11, while HCCA is centralized. The focus of the work was on an experimental analysis of the EDCA mechanism with a real-life testbed to satisfy in a real environment, the requirements of two of the applications for which this protocol was designed: traffic engineering and service guarantees.

The IEEE 802.11 standard [3] defines the protocol and compatible interconnections of data communication equipment via the "air" (radio or infrared) in a local area network (LAN). It encompasses the physical (PHY) and the media access control (MAC) layers of the ISO seven-layer network model. The authors in [4] explains that within the MAC layer, Distributed Coordination Function (DCF) is used as a fundamental access method, while Point Coordination Function (PCF) is optional. DCF is also known as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol. It is an asynchronous access method based on the contention for the usage of shared channels. PCF provides a contention-free access mechanism through the RTS/CTS (Request to Send/Clear to Send) exchange. The IEEE 802.11 protocol also includes authentication, association and reassociation services, an optional encryption/decryption procedure, power management, and a point coordination function for time-bounded transfer of data.

A good introduction to the 802.11 standard, followed by a performance study of both the DCF and Point Coordination Function (PCF) is presented in [5]; this study suggests that an IEEE 802.11 network may be able to carry traffic with time-bounded requirements using the PCF. In all cases, Wireless LANs, because of their broadcast nature, require the addition of: i.) User authentication to prevent unauthorized access to network resources and ii) Data privacy to protect the integrity and privacy of transmitted data [6]. The 802.11 specification stipulates different mechanisms for authenticating wireless LAN clients: Open authentication (authentication request and authentication response) and shared key authentication, station authentication, MAC address authentication (MAC), and authentication vulnerabilities and Set Identifier (SSID authentication). The authors in [7] and website in [8] explains key WLAN modes viz: Independent BSS (IBSS), Infrastructure mode is also referred to as BSS (Basic Service Set) and Extended Service Set (ESS). Table 1 and Table 2 shows IEEE WLAN standards and WLAN Modulations.

Table 1 summarizes the IEEE WLAN standards:

	802.11a	802.11b	802.11g	802.11n
Maximum Throughput	54Mbps	11Mbps	54Mbps	300Mbps
Frequency	5GHz	2.4GHz	2.4GHz	2.4/5GHz
Modulation	OFDM	DSSS	DSSS/OFDM	OFDM
Channels(FCC/ETSI)	21/19	11/13	11/13	32/32
Ratified	1999	1999	2003	N/A

Table 2: WLAN Modulations

Scheme	Modulation	Throughput
DSSS	DBPSK	1Mbps
DSSS	DQPSK	2Mbps
DSSS	CCK	5.5/11Mbps
OFDM	BPSK	6/9Mbps
OFDM	QPSK	12/18
OFDM	16-QAM	24/36Mbps
OFDM	64-QAM	48/54Mbps

The implementation in this work achieves SMART traffic engineering and QoS guarantee for all forms of traffic in our context. In future work, through simulations ,we will present validations of our experimental results to justify stability, and convergence of the high density iWLAN based on selected QoS parameters.

iWLAN SYSTEM MODEL AND IMPLEMENTATION SPECIFICATIONS

In this work, figure 1 shows the iWLAN system model. Achieving a reliable network model with QoS guarantee after various application integrations in the model is a major consideration that calls for reliable system specifications. The following tools satisfy this basis.

i. Access Point (Cisco Linksys WRT 300N)

The test case wireless access point used in this work is the Cisco Linksys WRT300N with a data rate of over 216Mbps. It has a secure Web-based GUI (SSL) for the administrative login with four switch ports for LAN integration. The device is enabled for DHCP connectivity for users, iWLAN SSID with other administrative cluster configurable options. Wireless networking lags wired networking in terms of increasing bandwidth and throughput [9]. While as of 2010 typical wireless devices for the consumer market can reach speeds of 300 Mbit/s (megabits per second) (IEEE 802.11n) or 54 Mbit/s (IEEE 802.11g), wired hardware of

similar cost reaches 1000 Mbit/s (Gigabit Ethernet). One impediment to increasing the speed of wireless communications comes from Wi-Fi's use of a shared communications medium [9]. In the iWLAN network architecture implemented in our context, Linksys 300N was used as the access point which handles the following [9]:

i. The portions of the protocol that have real-time requirements
ii. The frame exchange handshake between a client and AP when transferring a frame over the air
iii. Buffering and transmitting frames for clients in power save operations
iv. Responding to probe request frames from clients
v. Forwarding notification of received probe requests to the controller
vi. Providing real-time signal quality information to the controller with every received frame
vii. Monitoring each of the radio channels for noise, interference, and other WLANs
viii. Monitoring for the presence of other APs and Transmitting beacon frames
ix. Encryption and decryption except in the case of VPN/IPSec clients

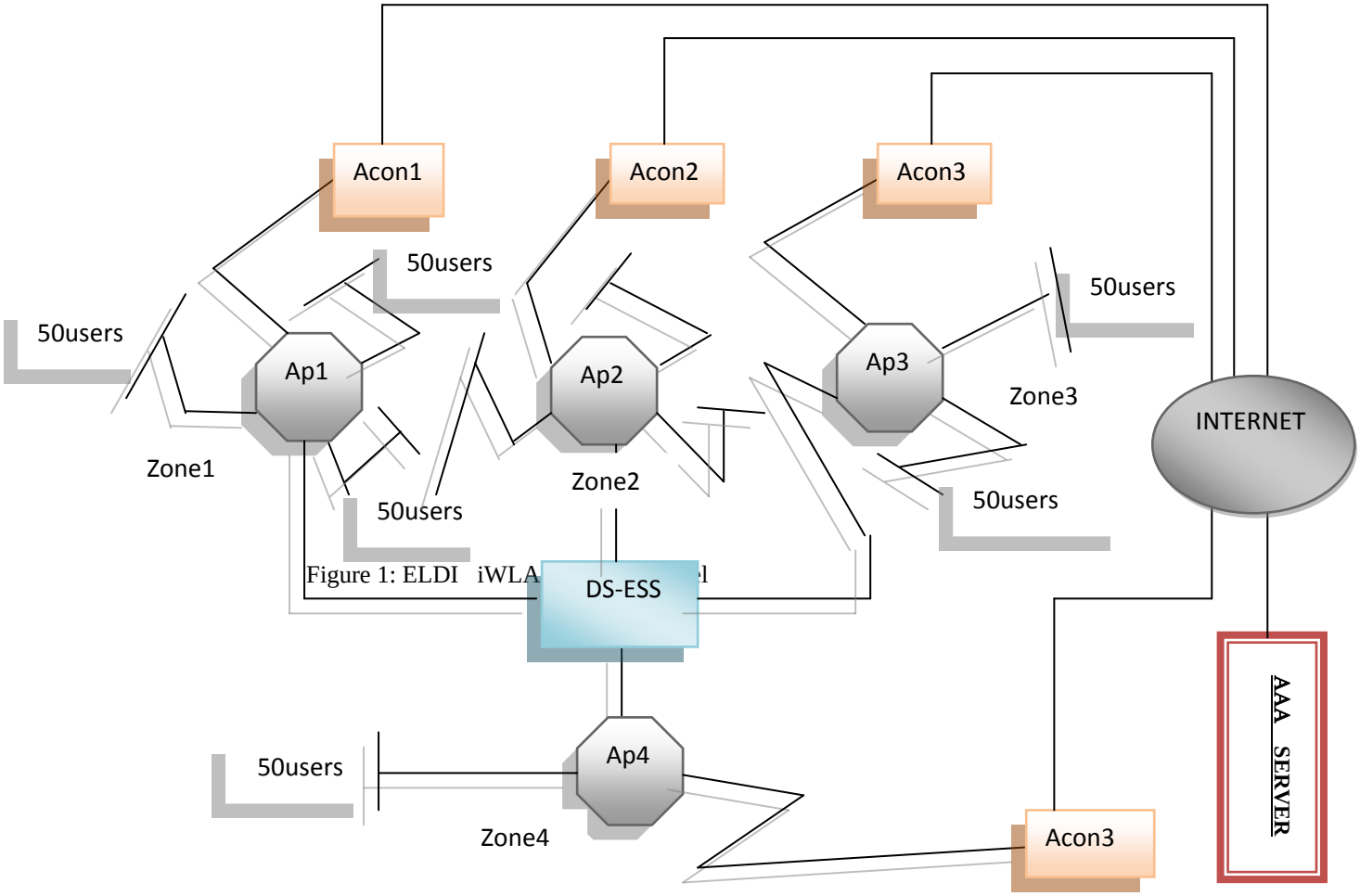

Figure 1: ELDI iWLA l

Figure 2i: Linksys 2.4GHz WRT [9]

Figure 2ii: A Linksys WRT 300N Configurations

ii. **Network Security Implementation (Access Controller Module)**

This work specifies the following security strategies in the iWLAN model viz:

- Role-based firewall with stateful inspection for all network traffic; Active firewall sessions — 100,000 per Access controller Switch and 1,200,000 per cluster which protects against IP Spoofing and ARP Cache Poisoning.
- Access Control Lists (ACLs) using wireless Intrusion Detection and Prevention systems (IDS/IPS): The implementation comprises Multi-mode rogue AP detection, Rogue AP Containment, 802.11n Rogue Detection, Ad-Hoc Network Detection, Denial of Service protection against wireless attacks, client blacklisting, excessive authentication/association; excessive probes; excessive disassociation/deauthentication; excessive decryption errors; excessive authentication failures; excessive 802.11 replay; excessive crypto IV failures (TKIP/CCMP replay); Suspicious AP, Authorized device in ad-hoc mode, unauthorized AP using authorized SSID, EAP Flood, Fake AP Flood, ID theft, ad-hoc advertising Authorized SSID.
- Anomaly Analysis on source and destination Media Access Control (MAC), Illegal frame sizes, multicast source MAC, TKIP countermeasures and all zero addresses.
- Authentication based on pre-shared keys (PSK); 802.1x/EAP—transport layer security (TLS), tunnelled transport layer security (TTLS), protected EAP (PEAP); Kerberos Integrated AAA/RADIUS Server with native support for EAP-TTLS, EAP-PEAP (includes a built in user name/password database; supports LDAP), and EAP-SIM.
- Transport Encryption based on WEP 40/128 (RC4), Key Guard, WPA—TKIP, WPA2-CCMP (AES), and WPA2-TKIP.

iii. **System Resiliency and Redundancy**

The iWLAN model implemented 1) an active, N+1 redundancy with access port in the model with load balancing support and ccritical resource monitoring.

2.) Virtual IP (DHCP): Single virtual IP (per user per zone) by an AP and controller cluster. All mobile devices or wired infrastructure can always connect to the network.

3.) SMART RF deployment for network optimization to ensure user quality of experience at all times by dynamic adjustments to channel and power (on detection of RF interference or loss of RF coverage /neighbour recovery).

The operational mechanism in figure 1 is designed to handle flexibility in communication among the nodes. Four APs connects the all the users and are carefully positioned to yeild the spatial potential, hence optimized data rate. The iWLAN architecture is built around an Extended Service Set (ESS). ESS connects the respective Aps via a distributed switche (DS). The the Acon interface links all Aps to the internet. In the architecture, the AAA server allows users into smart network. The users presents their identity using the locally supported AAA mechanisms. Based on the identity of the users, the network can decide on the user and validate the user through the AAA infrastructure. Smart applications like Skype, MSN, LANTALK and web applications are integrated on the iWLAN network in context. Application usage in our context is serverless-based while logical access is servercentric for security purposes.

ENIVRONMENTAL CHARACTERISTICS FOR iWLANs DEPLOYEMENT

In this work, SMART high-density iWLAN design refers to the complete WLAN environment where client devices will be positioned in densities greater than coverage expectations of a normal enterprise deployment with reliable traffic communication and good quality of service delivery. In our context, an indoor propagation characteristics for signal attenuation greatly depends on user density. Aggregate available bandwidth is shared among users and their connection characteristics (such as throughput, delay, radio type, signal strength, and SNR) determine the overall bandwidth available per user.

A typical ELDI office environment (Administration/Electronics), as shown in Figure 2, may have APs deployed for 2,000 to 5,000 square feet with a signal of -70 decibels in milliwatts (dBm) coverage and a maximum of 30 to 50 users per cell. That is a density

of one user every 120 square foot (sq. ft.) and yields a minimum signal of -70dBm. Figures 4i and 4ii shows the iWLAN MAP and the user density mapping.

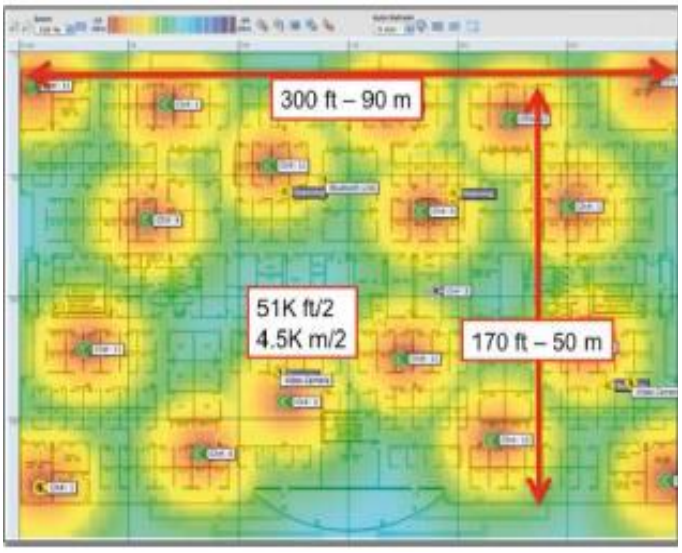

Figure 3i: ELDI iWLAN MAP (Administration/Electronics)

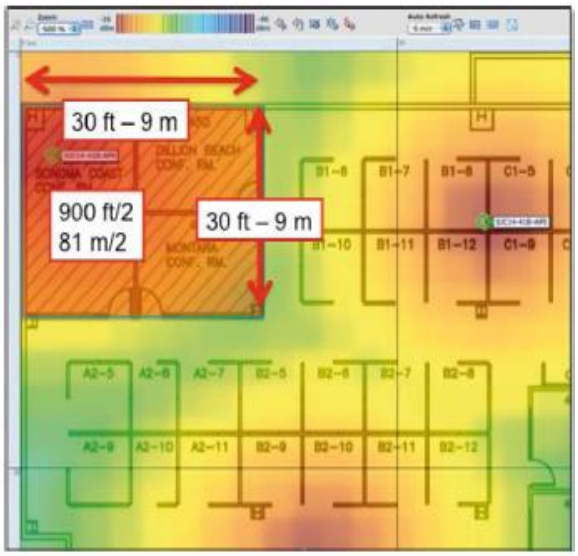

Figure 3ii: User Density Mapping

In planning and deploying our iWLAN, an AP is typically placed in an area that is expected to have a higher user density, such as in a boardroom, departments (zones) while other areas are left with less coverage. This takes care of high-density zones as shown in figure 1. High density zones are placed in clusters, for the maximum capacity and coverage. In high-density zones, the densities of users in the occupied space are anticipated to increase dramatically. User mapping is typically clustered very close together to achieve high site occupancy and coverage. The overall dimensions of the space gives an idea of the free space path loss of the AP signals. The RF dynamics of the AP are very different from those experienced at the user level. The APs are exposed in the zones with an excellent connection ratio for user devices.

BANDWITH REQUIREMENT

Table 1 shows our tested, the target application and validated bandwidth requirements. This work validated applications on a representative sample of the iWLAN platform. Linux based browsers have better efficiency than Microsoft based browsers. However, mobile devices (smart phones, tablets) have higher bandwidth requirement.
*Aggregate bandwidth = Acceptable bandwidth *No of Connections in WLAN coverage area*.
This yields the target bandwidth needed for our computations

Table1: Bandwidth Requirements per Application

Application Traffic	Nominal throughput
Web Casual	500kps-1Mbps
On-demand video Streaming	1-4Mbps
Printing	1Mbps
File Sharing &Data Transfers	1-8Mbps
Online backups	10-50Mbps

EXPERIMENTAL SETUP (MODEL DESCRIPTION)

Figure 1 shows our modelled Testbed used for measuring the media system performance in the ELDI boardrom. Figures 5i to figure 6i shows the iWLAN experimental setups. Although the 802.11n supports MIMO router with 100 Mbit/s switches standard, there are already some commercial wireless cards that partially support EDCA[2]. Our implementation was conducted with 802.11n Linksys WRT300N series form Linksys providing a maximum speed of 270 Mbit/s over the wireless network (2*2 spatial stream MIMO) and provides full support for other wireless adapter platforms. The DCF mechanism of the 802.11n standard above placed a restriction on the possible *CWmin* and *CWmax* values.
To perform our experiments, we built a testbed comprising of four iWLAN zones with 50 users per zone. iWLAN access controller establishes a link to the internet. A Radius AAA server provides authorization,authentication and accounting for the rest of the zones. Unless otherwise stated, the experiments were performed with initial 50 WLAN clients in zone1 at a distance

ranging from 20 to 100 m from each other. Traffic was generated with Etheral wireshack tool sending (TCP or UDP) 1500-byte packets. The experimental results will generated with OMNET++ tool for traffic engineering and QoS analysis in our future work.

Figure 4i: 2800 series Router in iWLAN

Figure 4ii: Boardroom system integration &Configurations

Figure 5i: SMART iWLAN server room devices

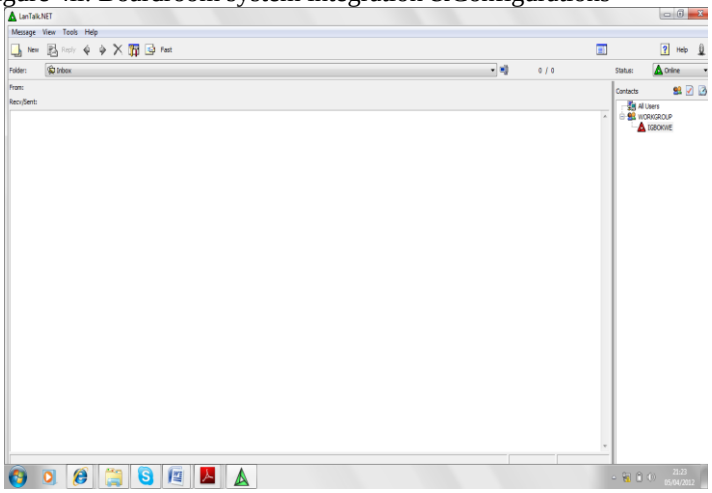

Figure 5ii: SMART instant messaging (LANTALK)

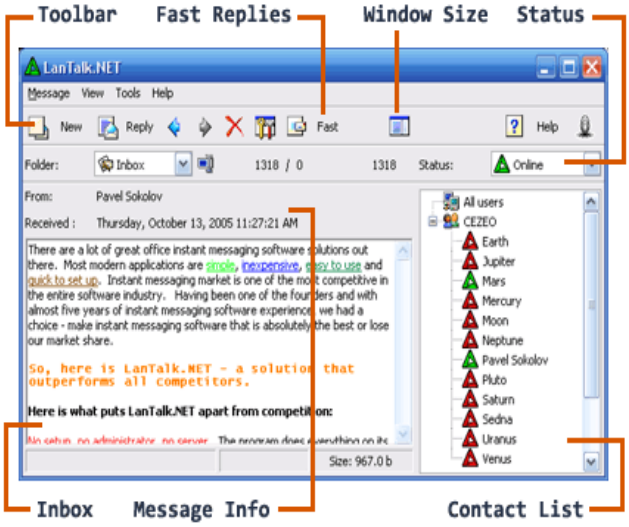

Figure 6i: SMART instant messaging interface

Figure 6ii: A Linksys WRT 300N internal architecture

SMART APPLICATION INTEGRATION with Linksys WRT 300N

The WLAN access point (Figure 2i and Figure 6ii) is a wireless LAN based router with an Ethernet interface. It is used as a router in wireless networks and it connects the wireless network to wired networks. In this context, the AP was used for WLAN clients' nodes only. The Linksys WRT 300N also uses a Linux kernel with more tools and libraries such as: iproute2, openssl, pppd, pptp-client, rp-pppoe, rp-l2tp, udhcpd (which are all popular Linux tools) and even a small sized HTTP daemon. LANTALK application which is an instant messaging tool was integrated into iWLAN model for SMART communication for paperless transfers.The Access points interfaces with the controllers and RADIUS server for internet access.

The wireless access point and RADIUS server fill the roles of the 802.11 authenticator and authentication server. The RADIUS protocol creates a layer of security where the authentication server is connected by an IP network and is separate from the authenticator. Originally designed to authenticate remote clients (iWLAN nodes) and store authentication credentials in a centralized server, in a hotspot, the RADIUS server provides iWLAN client and AP authentication. Consequently, LANTALK application,Sykpe,MSN and other web applications were enabled in the iWLAN nodes. Figure 5i and 5ii shows the SMART instant messaging interface running on the implemented iWLAN model. The future work will focus on the experimental simulation analysis with OMNET++ to validate system stability and performance at large.

SYSTEM TESTING (iWLAN NETWORK MODEL) AND DISCUSSION

In this section, we describe the tests carried out on the iWLAN implementation for ascertain connectivity efficiency. As a result of RF interferance that negatively degrades the performance of networks leading packet drops,limited bandwidth,unreliability and end user dissatisfaction, iWLAN testing becomes very expedient and since it is difficult to predict radio wave propagation, we observe that for optimal reliabilty and high throughput index in iWLAN deployment, a Wifi connection analyzer will assist this work to verify RF discovery and other wireless characteristics. At the time of this work, it was difficult to procure a reliable 20-40Ghz vector signal anaylsis bundle for our our analysis, but several ping ICMP connectivity tests were ran at various locations in ELDI. We observe also, that RF interference, router brands, congested wireless locations, mix mode B-G clients, all affect iWLAN performance.

Also the data rates depend upon AP configuration. To reach a data rate greater than 300 Mbps requires a 4x4 MIMO (multiple-input multiple-output), a double-wide 40 MHz channel. Figure 7 shows a typical vector signal analysis bundle. Performance characterization of the iWLAN model will be disscussed in our future work.

Figure 7: Agilent 89650S 26.5 GHz vector signal analysis bundle [12]

Table 2 shows the relationships between the variables that allow for the maximum data rate [13]

Table 2: WLAN Data Rates Variables

MCS index	Spatial streams	Modulation type	Coding rate	Data rate (Mbit/s)			
				20 MHz channel		40 MHz channel	
				800 ns GI	400 ns GI	800 ns GI	400 ns GI
0	1	BPSK	1/2	6.50	7.20	13.50	15.00
1	1	QPSK	1/2	13.00	14.40	27.00	30.00
2	1	QPSK	3/4	19.50	21.70	40.50	45.00
3	1	16-QAM	1/2	26.00	28.90	54.00	60.00
4	1	16-QAM	3/4	39.00	43.30	81.00	90.00
5	1	64-QAM	2/3	52.00	57.80	108.00	120.00
6	1	64-QAM	3/4	58.50	65.00	121.50	135.00
7	1	64-QAM	5/6	65.00	72.20	135.00	150.00
8	2	BPSK	1/2	13.00	14.40	27.00	30.00
9	2	QPSK	1/2	26.00	28.90	54.00	60.00
10	2	QPSK	3/4	39.00	43.30	81.00	90.00
11	2	16-QAM	1/2	52.00	57.80	108.00	120.00
12	2	16-QAM	3/4	78.00	86.70	162.00	180.00
13	2	64-QAM	2/3	104.00	115.60	216.00	240.00
14	2	64-QAM	3/4	117.00	130.00	243.00	270.00
15	2	64-QAM	5/6	130.00	144.40	270.00	300.00
16	3	BPSK	1/2	19.50	21.70	40.50	45.00
17	3	QPSK	1/2	39.00	43.30	81.00	90.00
18	3	QPSK	3/4	58.50	65.00	121.50	135.00
19	3	16-QAM	1/2	78.00	86.70	162.00	180.00
20	3	16-QAM	3/4	117.00	130.70	243.00	270.00
21	3	64-QAM	2/3	156.00	173.30	324.00	360.00
22	3	64-QAM	3/4	175.50	195.00	364.50	405.00
23	3	64-QAM	5/6	195.00	216.70	405.00	450.00
24	4	BPSK	1/2	26.00	28.80	54.00	60.00
25	4	QPSK	1/2	52.00	57.60	108.00	120.00
26	4	QPSK	3/4	78.00	86.80	162.00	180.00
27	4	16-QAM	1/2	104.00	115.60	216.00	240.00
28	4	16-QAM	3/4	156.00	173.20	324.00	360.00
29	4	64-QAM	2/3	208.00	231.20	432.00	480.00
30	4	64-QAM	3/4	234.00	260.00	486.00	540.00
31	4	64-QAM	5/6	260.00	288.80	540.00	600.00

The AP in the iWLAN allows for 20MHz wide channels but can also combine two 20MHz channels to form a 40MHz channel for increased bandwidth its MIMO (Multiple Input/Multiple Output) thrughput is increased with enhanced signal coverage and increased data rates. The number of MIMO Spatial streams that an AP router and client adapter supports will affect their maximum rate and result in different rates for transmitting and receiving. In our implementation, Ping ICMP utility was used to test the reachability of various hosts on an Internet Protocol (IP) network (via Aps in iWLAN) and to measure the round-trip time for messages sent from the test node to the destination nodes. Using Ipconfig/all command on the AP nodes, the staistics of the nodes were ascertained. On the iWLAN, with a Ping test at google.com and ELDI website (www.eldiawka.org) from the command prompt, we have test results thus:

C:>Ping www.example.com (192.0.43.10) 56(84) bytes of data.
64 bytes from 43-10.any.icann.org (192.0.43.10): icmp_seq=1 ttl=250 time=80.5 ms
64 bytes from 43-10.any.icann.org (192.0.43.10): icmp_seq=2 ttl=250 time=80.4 ms

64 bytes from 43-10.any.icann.org (192.0.43.10): icmp_seq=3 ttl=250 time=80.3 ms
64 bytes from 43-10.any.icann.org (192.0.43.10): icmp_seq=4 ttl=250 time=80.3 ms
64 bytes from 43-10.any.icann.org (192.0.43.10): icmp_seq=5 ttl=250 time=80.4 ms

--- www.eldiawka.org ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 80.393/80.444/80.521/0.187 ms

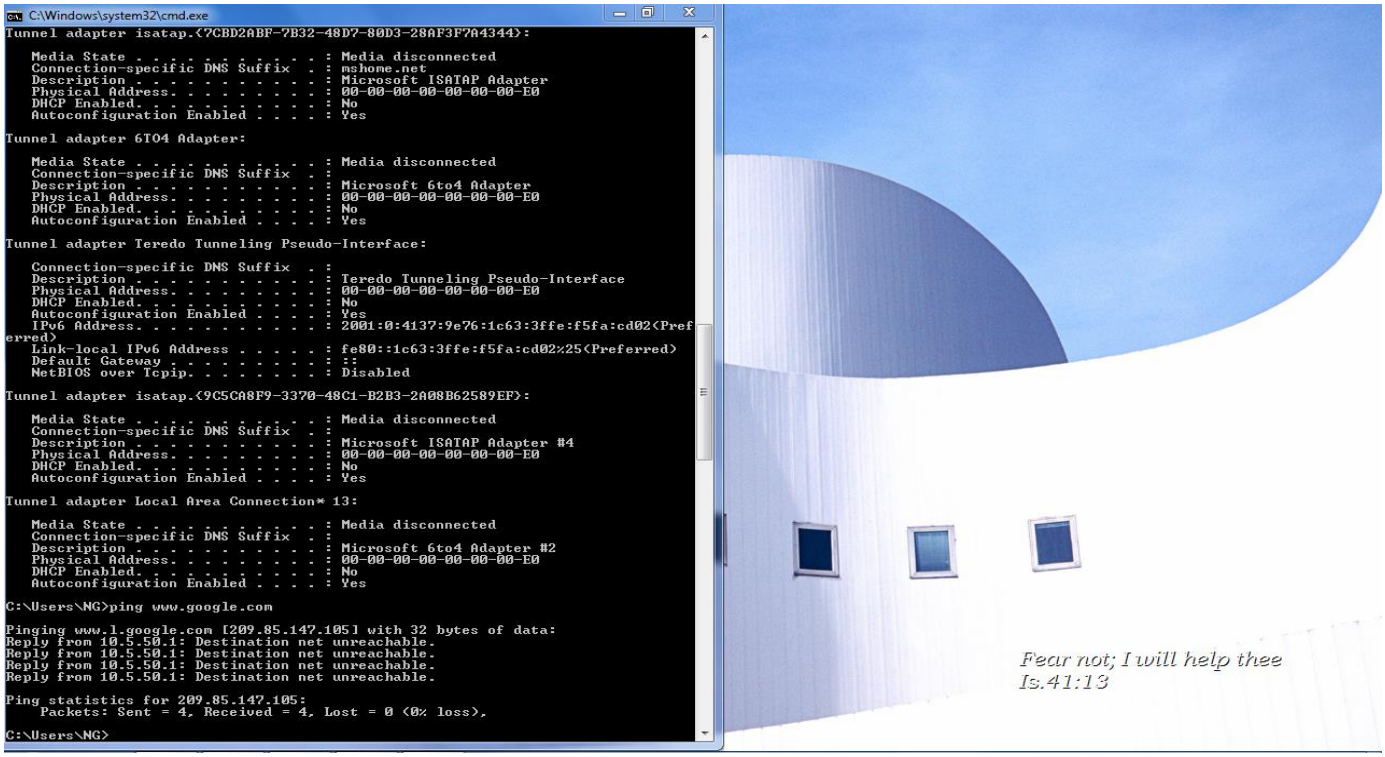

Figure 8: Ping ICMP Test

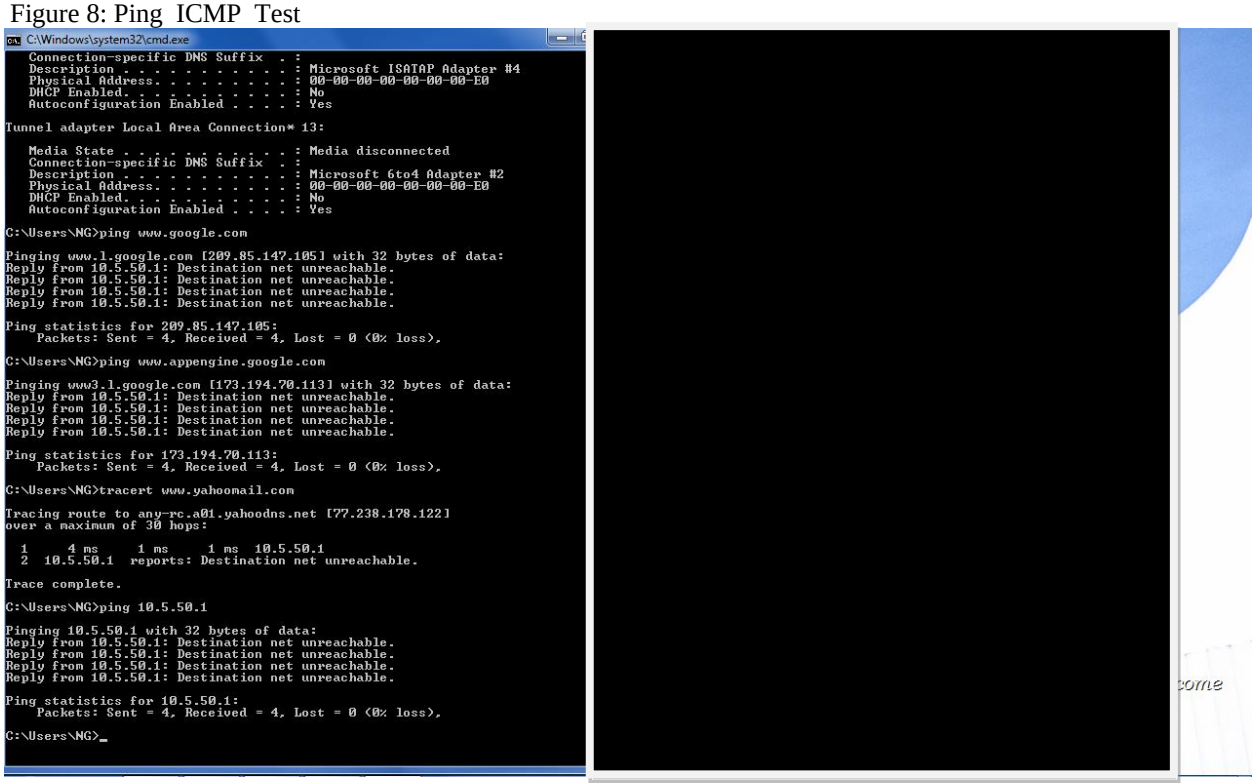

Figure 8: ICMP Ping Test

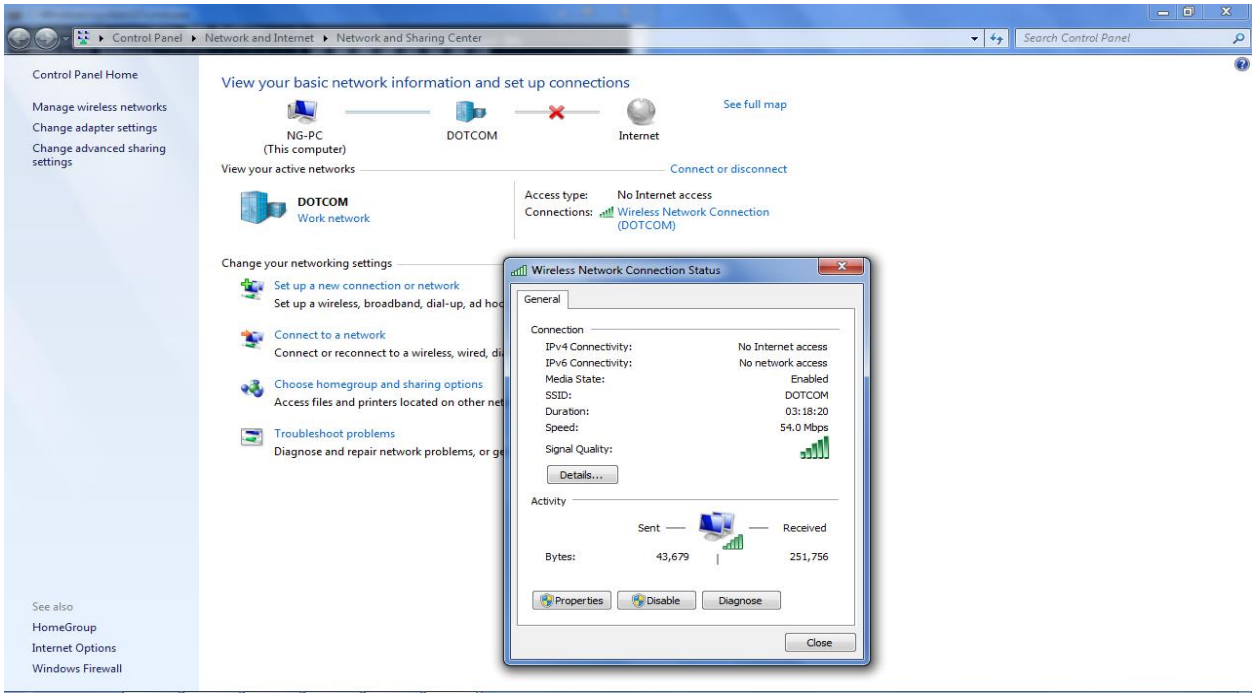

Figure 9: Ping ICMP Test for network connectivity

CONCLUSION

This paper has presented iWLAN model implementation for ELDI. The architecture and implementation model was presented in this paper. Also, the network satifies user friendliness, scalability, flexibility, compatibility, speed and robustness upon usage. The Aps assigns bandwidth to users at all instances. Future work will detail the performance characterization of the model via simulations with OMNet ++ Utility which demonstrates efficient performance metrics for our deployment . We envison that the experimental results will guarantee stability, and show the iWLAN model to be efficient for traffic engineering purposes.

ACKNOWLEDGMENT

The authors are grateful to Electronics Developement Institute (ELDI), Awka- National Agency for Science and Engineering Infrastructure, Federal Ministry of Science and Technology (NIGERIA) for making the boardroom availaible for testing our connectivity.

REFERENECES

1. Jim Florwick, Jim Whitaker, Alan Cuellar Amrod, Jake Woodhams, "Wireless LAN Design Guide for High Density Client Environments in Higher Education" Design Guide, November, 2011
2. Albert Banchs, eArturo Azcorra, Carlos García, and Rubén Cuevas, " *Applications and Challenges of the 802.11e EDCA Mechanism:An Experimental Study"* IEEE Network • July/August 2005
3. L. Bononi, M. Conti, and L. Donatiello, "Design and performance evaluation of a distributed contention control (DCC) mechanism for IEEE 802.11 wireless local area networks," in *Proceedings of First ACM International Workshop on Wireless Mobile Multimedia*, Oct. 1998, pp. 59-67.
4. Jiaqing Song and Ljiljana Trajkovic, "Enhancements and Performance Evaluation of Wireless Local Area Networks"
5. B. P. Crow, I.Widjaja, J. G. Kim, and P. T. Sakai. IEEE 802.11 wireless local area networks. *IEEE Communications Magazine*, September 1997.
6. Paul Tan, "Providing Secured Public Wireless-LAN Internet Access"
7. E.E.J. Vonk, "Design and implementation of a hotspot network independent of Wi-Fi service providers" 2005
8. http://www.packetlife.net
9. http://www.wikipedia/linksys

10. András Varga, " The Omnet++ Discrete Event Simulation System"(Unpublished).
11. OMNeT++ Discrete Event Simulation System Version 3.0 preview1, User Manual
12. Agilent WLAN Test Tools for R&D: www.home.agilent.com/agilent/redirector.jspx?...AGILENT
13. http://www.airmagnet.com/assets/whitepaper/WP-802.11nPrimer.pdf