INTERNATIONAL JOURNAL OF NATURAL AND APPLIED SCIENCES (IJNAS), VOL. 4, NOS.1& 2 (2009); P. 101 – 107, 1 TABLE, 4 FIGS.

Interference monitoring and control of wireless local area network (WLAN)

E. E. Williams[*1], I. O. Akpan [2] and D. E. Asuquo[3]

ABSTRACT

More and more enterprises today are discovering the benefits of mobility through wireless networking. Accessing the network wirelessly from nearly any convenient location within the enterprise provides users with better flexibility and productivity. As a result, Information Technology (IT) decision makers have moved away from the implementation of location-specific wireless access to delivering comprehensive mobility through enterprise-wide wireless implementation. The proliferation of WLANs (Wireless Local Area Networks) has coincided with the evolution of wireless networking standards, which have progressed significantly since the Institute of Electrical and Electronics Engineers (IEEE) introduced the original 802.11b standard in the late 1990s. The frequencies used by IEEE 802.11b are open to the public for use in many different devices. The common consumer wireless LAN frequencies fall around 2.4 GHz which is the same frequency used by newer cordless phones, Bluetooth devices, microwave ovens, and other wireless gears. Interferences occur when other sources of Radio Frequency (RF) are using the same frequencies as the wireless router and this occur primarily in two ways: Adjacent Channel Interference and Co-channel Interference. This research examines WLANs at specific locations in Uyo City of Akwa Ibom State of Nigeria, using *CommView for Wi-Fi* network monitoring tool. It was discovered that interference resulted primarily from channel overlap (i.e. Channel Interference). To this effect, control measures such as channel surfing, reconfiguration of network layout and upgrade to 802.11a standard are proposed with the use of channel blanket technology.

INTRODUCTION

IEEE 802.11b also known by the brand name, Wi-Fi, denotes a Wireless LAN standard developed by Working Group 11 of the IEEE (Institute of Electrical and Electronics Engineers) LAN/MAN Standards Committee (http://en.wikipedia.org/wiki/IEEE_802.11). A wireless LAN (WLAN) is a data transmission system designed to provide location-independent network access between computing devices by using radio waves rather than a cable infrastructure (http://en.wkipedia.org/wiki/Wireless_LAN). In the corporate enterprise, wireless LANs are usually implemented as the final link between the existing wired networks and a group of client computers, giving users wireless access to the full resources and services of the corporate network (Akin and Planet 3, 2002).

Wireless transmission is achieved through the use of the electromagnetic spectrum, and a greater portion of its different layers have been reserved for particular use, such that a license is required for the use of any particular frequency. These reserved portions are known as licensed frequencies. The non-reserved portion is free for use and it is known as license-free or unlicensed frequency. The 2.4GHz frequency being part of the ISM (Industrial, Scientific and Medical) Band is unlicensed and free for use. As a result, it enjoys extensive patronage from users (mostly commercial) because of its cost-free acquisition. This patronage when uncontrolled adversely affects signal propagation.

The 2.4GHz radio frequency operates in conformity to the 802.11b standard for wireless networking. IEEE 802.11b emerged in 1997 and is the most popular wireless networking standard. Operating on the 2.4GHz radio frequency of the ISM band, the 802.11b is also the current mainstay of the 802.11 family of wireless networking standards established by the IEEE (http://en.wikipedia.org/wiki/IEEE_802.11)

Since 802.11b operates on the license-free ISM band, communication or data transfer within the band coexists with other devices transmitting on this band. As a result, interfering signals affect quality transmission of signal within the band. Since there are no standard procedure for the use of bandwidth power output on the ISM band, there is no direct control over what different users do, hence interference is bound to occur. Despite these factors, investors still invest considerably in deploying and providing services using this standard. This scenario, though global, is widespread and bears heavily on the technologically developing countries, including Nigeria. This without doubt, is fueled by the prevailing harsh economic situation of these nations (Udoh, 2006).

[*]Corresponding author. Email: edemwilliam@yahoo.com

Manuscript received by the Editor June 3, 2008; revised manuscript accepted November. 24, 2008.
[1]Dept of Mathematics/Statistics & Computer Science. University of Calabar, Calabar, Nigeria.
[2]Department of Computer Science ,Akwa Ibom State College of Education, Afaha Nsit, Nigeria.
[3]Department of Mathematics/Statistics and Computer Science, University of Uyo, Uyo, Nigeria

Using Uyo city as a case study, this work examines the interference level therein, essentially from coexisting 802.11b wireless networks.

ARCHITECTURE OF 802.11B NETWORKS

The 802.11 architecture can best be described as a series of interconnected cells, and consists of the following: the wireless device or station, the access point (AP), the wireless medium, the distribution system (DS), the basic service set (BSS), the extended service set (ESS), and station and distribution services (Wheat *et al*, 2001). All of these working together providing a seamless mesh give wireless devices the ability to roam around the WLAN looking for all intents and purposes like a wired device.

The basic service set (BSS) is the core of IEEE 802.11 standard. It is made up of one or more wireless devices communicating with a single Access Point (AP) in a single radio cell. If there are no connections back to a wired network, it is called an *independent basic service set*. If there is no access point in the wireless network, it is referred to as an *ad-hoc network*. This means that all wireless communications is transmitted directly between the members of the ad-hoc network. When the BSS has a connection to the wired network via an AP, it is called an *infrastructure BSS*. In this model, the AP bridges the gap between the wireless device and the wired network. This research considered infrastructure BSS. Since multiple Access Points exist in this model, the wireless devices no longer communicate in a peer-to-peer fashion. Instead, all traffic from one device destined for another device is relayed through the AP. This doubles the amount of traffic on the WLAN.

The compelling force behind WLAN deployment is the fact that with 802.11, users are free to move about without having to worry about switching network connections manually. If we were operating with a single infrastructure BSS, this moving about would be limited to the signal range of our one AP. Through the extended service set (ESS), the IEEE 802.11 architecture allows users to move between multiple infrastructure BSSs. In an ESS, the APs talk amongst themselves forwarding traffic from one BSS to another, as well as switch the roaming devices from one BSS to another. They do this using a medium called the distribution system (DS).The distribution system forms the spine of the WLAN, making the decisions whether to forward traffic from one BSS to the wired network or back out to another AP or BSS.

What makes the WLAN so unique, though, are the invisible interactions between the various parts of the extended service set. Pieces of equipment on the wired network have no idea they are communicating with a mobile WLAN device, nor do they see the switching that occurs when the wireless device changes from one AP to another. To the wired network, all it sees is a consistent MAC address to talk to, just as if the MAC was another node on the wire.

There are nine different services that provide behind-the-scenes support to the 802.11 architecture. Of these nine, four belong to the *station services* group and the remaining five to the *distribution services* group. The four station services (*authentication*, *de-authentication*, *data delivery*, and *privacy*) provide functionality equal to what standard 802.3 wired networks would have. Between the Logical Link Control (LLC) sublayer and the MAC, five distribution services make the decisions as to where the 802.11 data frames should be sent. These distribution services make the roaming handoffs when the wireless device is in motion. The five services are *association*, *reassociation*, *disassociation*, *integration*, and *distribution.*

WLAN interference, monitoring and control

For 2.4GHz WLANs, there are several sources of interfering signals, including microwave ovens, wireless phones, Bluetooth enabled devices, and other wireless LANs (Geier, 2006). In a collaborative research carried out by Patil *et al*, 2006 to study the influence of 802.11b devices on other 802.11b devices, it was observed that when a single 802.11b device was used, no interference was present, and the signal strength stays stable during the experiment. When a single pair of 802.11b devices was introduced in the same network, there was interference between the two, causing signal fluctuation. With two pairs, the interference greatly increased. The interference factor increases when more devices operating over the same channel were added. Thus, it can be deduced that as the number of devices increases in the same network, the effective bandwidth for a particular link drops. In the experiment, an iPAQ system with D-Link card and a laptop with Orinoco card were configured to ping each other over the same channel (Channel 6 with 2.437GHz). The activities of a particular link were monitored and logged by the Orinoco Client Manager software.

In a related work conducted by Udoh (2006) to examine the level of WLAN interferences in Ibadan metropolis, it was observed that interferences occurred primarily as a result of Channel Interference and Transmit Power Level. The research was conducted in three locations in Ibadan, Nigeria, using the *Netstumbler* network detection software. As a remedy, a heuristic algorithm developed by Kin K. Leung and Byoung-Jo J. Kim in their work *"*Frequency assignment for Multi-cell IEEE 802.11 Wireless Networks*"* was proposed for implementation. It is on the strength of Udoh's findings that this research was further conducted, but in a different location (Uyo city) in Nigeria with a view to proposing simpler control measures to this problem of interference.

Choice of interference monitoring software

The *Netstumbler* software has been successfully used for a similar work (Udoh, 2006). However, having studied carefully the *CommView for Wi-Fi* tool (another WLAN monitoring tool); the decision to use it lieu of Netstumbler was informed. Following is a table comparing the Netstumbler and the CommView for Wi-Fi tool. The essence is primarily to show the advantages of *CommView for Wi-Fi* over *Netstumbler* and, by extension, the limitations of the later over the former.

Table 1. Comparison of the *netstumbler* and *CommView for Wi-Fi* tools

S/N		Netstumbler	CommView For Wi-Fi
1.	Uses	1.WLAN Auditing 2.WLAN Coverage verification 3.Site Surveying 4.Wardriving 5.Antenna Positioning 6.Detecting causes of wireless interference	1.Events notification (suspicious packets, high bandwidth utilization, or unknown addresses) 2. Site surveying 3. Analysis of packets/protocols 4. Interference detection 5. Traffic monitoring 6. Wardriving 7. WLAN detection and auditing 8. Antenna positioning
2.	Supported Platforms: (a) Protocols	Not stated	ARP, BCAST, BGP, BMP, CDP, DAYTIME, DDNS, DHCP, DIAG, DNS, EIGRP, FTP, G.723, GRE, H.225, H.261, H.263, H.323, HTTP, HTTPS, ICMP, ICQ, IGMP, IGRP, IMAP, IPsec, IPv4, IPv6, IPX, HSRP, LDAP, MS SQL, NCP, NDS, NetBIOS, NFS, NLSP, NNTP, NTP, OSPF, POP3, PPP, RARP, RADIUS, RDP, RIP, RIPX, RMCP, RPC, RSVP, RTP, RTCP, RTSP, SAP, SER, SIP, SMB, SMTP, SNA, SNMP, SNTP, SOCKS, SPX, SSH, TCP, TELNET, TFTP, TIME, TLS, UDP, VTP, WAP, WDOG, YMSG, 802.1X.
	(b)Adapters	The Proxim models, Dell TrueMobile, Compaq, Avaya Wireless 802.11b PC Card, Intersil Prism/Prism2, Atheros, Atmel, Broadcom, Cisco and Centrino chip sets.	3Com OfficeConnect, Cisco Aironet, D-Link AirPlus Xtreme, D-Link AirPremier, D-Link AirXpert DWL-AG650, D-Link Rangebooster G, Intel PRO, LinkSys WPC55AG Dualband, NETGEAR Dualband, NETGEAR RangeMax™, Proxim ORiNOCO, TRENDnet, Actiontec, Belkin, BENQ, Compaq, Corega, Dell Trumobile, DemarcTech Reliaware, Ericsson, Fujitsu, Lucent ORiNOCO, Microsoft MN-520, Nortel Networks e-mobility, Planet WL-3550, Repotec, Siemens I-Gate, SparkLAN, TrendWare, US Robotics, Xircom,.

It can be deduced from Table 1 that CommView for Wi-Fi has additional advantages of traffic monitoring and events notification (in terms of usage) over Netstumbler. It supports a wider range of **adapters** and **protocols** than Netstumbler. CommView for Wi-Fi as well as the following advantages over Netstumbler:

- clarity of the graphical interface;
- ease of comprehension of the generated report .

Hence, Netstumbler has obvious limitations in terms of functionality, number of supported adapters and protocols and its inability to generate a comprehensive report on request. However, for CommView for Wi-Fi, its major limitation is in putting ones adapter in a passive, promiscuous monitoring mode when it is running.

CommView for Wi-Fi is specially designed for capturing and analyzing network packets on wireless 802.11a/b/g networks. With CommView for Wi-Fi, one can see the list of network connections and vital Internet Protocol (IP) statistics and examine individual packets. Packets can be decrypted utilizing user-defined Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WAP) keys. Captured packets can be saved to log files for future analysis. A flexible system of filters makes it possible to drop unnecessary packets or capture the essential packets. Configurable alarms can notify the user about important events, such as suspicious packets, high bandwidth utilization, or unknown addresses.

RESULTS FROM SITE EVALUATION

At the different locations evaluated, the onsite analysis shows a significant level of interference caused primarily by channel congestion. This congestion results from the co-existence of multiple

Access Points. Most of these APs have a high Signal-to-Noise Ratio (SNR) in order to ensure their clients get good signal connection. In doing this, they also increase their transmit power level. The result is that different clients suffer a high noise level generated by signals from neighbouring APs/networks. From the evaluation, it can be deduced that a high level of interference is experienced. This is so because from the analysis, it was observed that the cell regions of the APs overlap, hence interference. In the following sections, the causes and effects of interference will be discussed, and a solution proposed to meet the peculiar needs of the evaluated environment.

Causes of co-existence problem identified during sites evaluation

During the field evaluation, cases of interference and their causes were identified. The following are some of the ways in which co-existing WLANs interfered with each other:

- Channel interference
- Edge-user problems
- Client bunching phenomena

Channel Interference: WLANs can affect each other as a result of Channel interference. This occurs in two ways:

(a) Adjacent channel Interference: This occurs as a result of adjacent channels overlapping one another. That is when two or more APs using overlapping channels are located near enough to each other such that their coverage cells physically overlap, thus causing throughput degradation.

(b) Co-channel Interference: This occurs when several APs' coverage cells on the same channel overlap. When two APs operating on the same channel attempt to transmit at the same time, they interfere with each other and must wait for retransmission, which substantially reduces capacity. Co-channel interference is especially prevalent in 802.11b wireless networks where only three non-overlapping channels are available.

Edge-user problems: In a shared medium like wireless, a collision domain is a group of clients competing for network access where only one client can transmit at a time. An edge user is a client that is too far away from the AP to connect at the highest possible data rate. When a single edge user connects to the AP at a slower speed, it reduces the connection speed for all other clients within the collision domain - even those who are located close to the AP.

Client bunching phenomena: In a cell-based wireless LAN, roaming clients make the decision to associate with another AP when the signal becomes too weak. As a client roams away from an AP, it associates with that AP until the very last moment. This occurs even if the client has moved close to another AP that can offer a much stronger connection rate. The result is an inconsistent connection rate for roaming clients, as well as reduced performance for other users in the domain as they wait for the roaming client to switch APs.

Proposed techniques to control specific interference problems

Interference on wireless networks will likely get worse before it gets better. Interference can slow connections or shut them down completely. The following are a few steps we propose for one to take in making a flaky wireless network more reliable:

Channel Surf: The 802.11b specification defines 11 channels for public use. Its frequency ranges only about 30 MHz and each channel covers 5 MHz of that range, so there's a lot of overlap between adjacent channels. This leaves one with only channels 1, 6, and 11 that are completely isolated from each other. If you have multiple routers or access points, set each of them to one of these channels. Some access points do this automatically (Lemos, 2007).

Reconfigure your network layout: Since the location of one of the wireless devices operating on the same 2.4GHz frequency band can affect the performance of the other, one may consider moving the wireless router to a different location in the house or possibly consider adding a second wireless Access Point or router to spread the LAN coverage around (Dennis, 2006).

Upgrade to 802.11a: The 802.11a specification has an advantage over standard 802.11b because it applies a new strategy for handling multi-path propagation (MPP). MPP happens when radio frequencies bounce off surfaces like metal furniture or other structural elements. This resembles an echo and can confuse standard 802.11b network devices. The 802.11a specification is better able to handle this type of problem and features more than 8 non-overlapping channels, thus allowing more devices to interact on the network without degrading their overall performance. Changing from 802.11b to 802.11a means switching to a less used part of the wireless spectrum (Dennis, 2006).

New system design to solve the interference problems

In traditional cell-based wireless LANs, each user connects to an AP, and each AP serves a cell. APs are assigned a specific channel and distributed to minimize interference between APs operating on the same channel (Fig. 1). The following is an alternative design that will tackle these limitations.

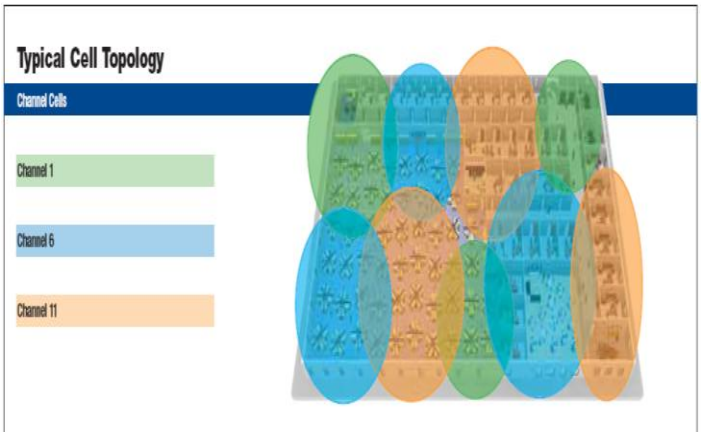

Fig. 1. A cell-based topology

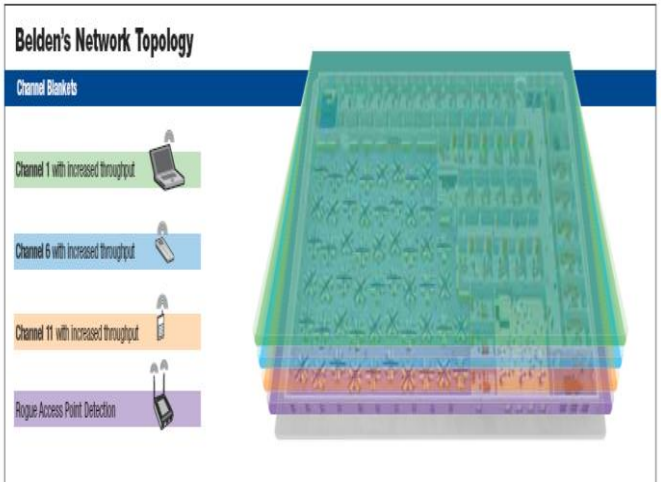

Fig. 2 . Belden's unique channel blanket topology (Belden 2007)

The channel blanket solution: Channel Blanket technology is an innovative wireless solution that solves common wireless networking challenges by eliminating the use of cells and allowing APs to be placed close together for better capacity (Meurell, 2007). In a Channel Blanket system, APs have no capabilities of their own – no IP or MAC address, software, or processing functions. Instead, each AP only acts as a gateway to a centralized switch that controls all packet routing decisions. With the switch making all the transmission decisions for each AP, users experience an extremely reliable connection similar to that of the wired network. In addition, because all security and configuration of APs is performed centrally at the switch, individual APs cannot be compromised in a security breach. In a Channel Blanket WLAN, the use of a centralized switch allows each AP to operate on the same channel and aggregate to create blankets of coverage. These blankets of coverage provide seamless mobility by eliminating co-channel interference, edge user problems, the client bunching phenomena that lead to decreased capacity, limited coverage, and poor performance. Not all Channel Blanket systems are the same. Following are key features and benefits found in the most advanced Channel Blanket systems:

(i) Overlapping blankets: Some Channel Blanket systems are single channel systems, while the more advanced systems permit all three non-overlapping 2.4GHz channels to be used on separate blanket layers. Using all three channels provide better enterprise-wide coverage, essentially multiplying capacity by as much as 300% (Fig. 2.). This feature also provides the ability to devote a specific Channel Blanket to a specific application such as VoIP (Voice over IP) or other real-time business applications. More advanced systems also offer additional Channel Blankets that can be used for security applications such as rogue access point detection.

(ii) Core vs edge (layer-2) architecture: Like traditional cell-based systems, some Channel Blanket systems also use a traditional Core Architecture design, which connects APs to the wireless switch via the core network. Unfortunately, the use of a Core Architecture interferes with the entire enterprise LAN, causing the network to become overloaded and creating the potential for performance bottlenecks, quality of service issues, and complex scalability. In contrast, a Layer-2 Edge Architecture extends the intelligence to edge switches that take over the processing of the wireless communications (Fig. 3). This makes the network core more efficient by allowing it to focus on the single function of moving packets. Set up and configuration is also easier in an Edge Architecture since APs connect directly to the wireless switch, do not require MAC or IP addresses, and can be powered directly from the switch using built-in Power over Ethernet (PoE) instead of midspan power supplies or power edge switches.

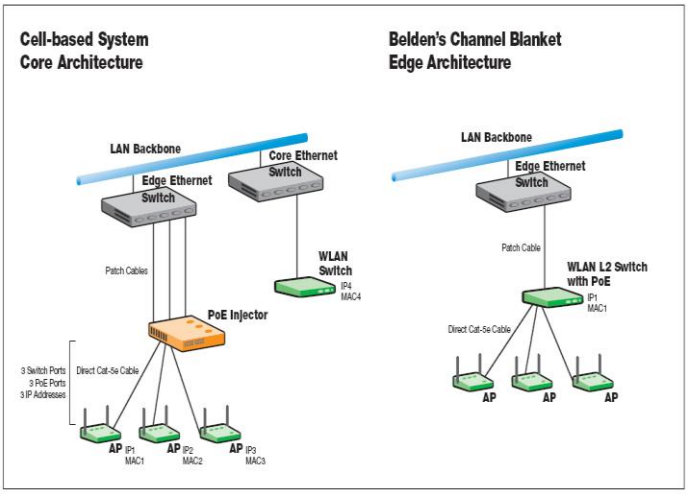

Fig. 3. Cell-based core architecture vs Belden's Channel Blanket Edge (Layer-2) Architecture.

(iii) Spectrum re-use technology: Traditional cell-based systems rely on natural spectrum re-use whenever more than three channels are required. However, the 802.11 Clear Channel Assessment (CCA) "listen before talk" that measures energy to ensure that a frequency is available for transmission often results in false positives or negatives that cause co-channel interference. Advanced Channel Blanket systems use a real-time, dynamic form of Spectrum Re-Use. The fundamental concept of Channel Blanket technology allows Spectrum Re-Use to increase capacity without causing interference. The intelligent wireless switch looks at the time differentials between all users and all APs on a packet-by-packet basis to determine if there's an opportunity to re-use a channel without causing co-channel interference. If there is, the Channel Blanket is dynamically subdivided to provide multiple, simultaneous links on the same channel. This provides increased capacity up to a tripling of aggregate packet throughput (see Fig. 4.).

Fig. 4. Spectrum re-use technology: effectively triples the throughput capacity of each channel blanket.

Management and control techniques for co-located wireless networks

The following scenarios are real-life situations that commonly occur in cell-based wireless LANs. Each scenario provides better insight into how Channel blanket technology solves these wireless networking challenges.

Scenario 1: Co-channel interference

Problem: Two 802.11b APs operating on the same channel in a cell-based system have been placed close together. Client A is attempting to download a large file from the network and is located within range of both APs. The two APs interfere with each other as they both attempt to transmit at the same time and must wait for retransmission. This ultimately causes Client A to downstream the file at a reduced rate.

Solution: In a Channel Blanket wireless LAN, the switch makes all transmission decisions for each AP operating on the same channel. This prevents APs from attempting to transmit simultaneously and interfering with each other. With no co-channel interference, APs can be spaced as close together as required to provide the maximum data, or connection, rate range for all clients in a given area.

Scenario 2: Edge-user, client bunching and latency Issues

Problem: Two 802.11b clients operating at 11 Mbps are located in close proximity to an AP in a cell-based wireless LAN. With a total shared throughput of 7.2 Mbps, both clients are downloading files from the network at 3.6 Mbps. Client A remains in one location while Client B roams to the edge of the network cell and falls back to a data rate of 1 Mbps. When down streaming traffic, an AP alternates packet transmission between Client A and Client B. Because Client B is now operating at only 1 Mbps, the time that Client A must wait for Client B to receive a data packet is increased. The total shared throughput therefore drops to just 1.6 Mbps, requiring each client to download at just 800 Kbps. As Client B roams further, it continues to associate with the AP until the very last moment when the signal is too weak. Client A is forced to experience a significantly reduced rate until Client B roams out of range and associates with another AP. At the same time, Client B is required to wait for connection, authentication, and encryption credentials to be handed off to the new AP, resulting in dropped data packets.

Solution: Because channel blanket technology enables APs to be placed close together, everyone can be close to an AP – there are no range limitations. This eliminates edge users and the possibility that one client will decrease capacity for everyone else. With the switch making all the decisions about how APs provide service, a roaming client can no longer decide to hold onto an AP until the signal is too weak but instead is instantaneously serviced by another AP at a high data rate.

CONCLUSION

This work has shown that the 802.11b networks have been plagued by its inherent problems of interference resulting from its implementation on the unlicensed frequency. But the same factors are the driving force behind the much research and development accorded this technology. The proliferation of the Wi-Fi technology has seen companies striving to implement enterprise-wide WLANs that offer comprehensive mobility with better performance while simultaneously lowering total cost of ownership.

Traditional cell-based wireless systems inherently give rise to several performance limitations that ultimately restrict capacity and coverage and result in reduced mobility and productivity. We have also shown Channel Blanket technology deployed in an Edge Architecture provides true seamless mobility by eliminating the problems associated with traditional cell-based systems. By eliminating co-channel interference, increasing capacity by as much as 300%, and providing zero roaming latency, our Channel Blanket WLANs technique enables all users to experience maximum wireless performance regardless of where they are located or what type of equipment they are using. IT decision makers would be wise to choose an Edge Architecture solution with advanced features and benefits like overlapping channels and Spectrum Re-use technology for increased capacity.

While the proposed control techniques will certainly benefit users of the 802.11b networks, it is wise and futuristic to consider a gradual migration to or adoption of the WiMax Technology, 802.11a, and 802.11n technologies for existing and intending wireless networks users.

REFERENCES

Akin, D. and Planet E. (2002). CWNA Certified network associate: official study guide.

Belden, D.(2007). Voice over WLAN. Belden Inc., USA.

Dennis, M. (2006). Solving wireless router interference problems. DIY Home Theatre, USA.

Geier, J.(2006). *Wireless LANs (2nd Edition).* CISCO Press, Indianapolis, USA.

Geier, J. (2006). Online guide to Wireless Networking. Available at: http://www.wireless_nets.com/guide.htm

IEEE 802.11 – Wikipedia, the free encyclopedia, (2007). IEEE 802.11. Available at: http://en.wkipedia.org/wiki/IEEE_802.11

IEEE 802.11 LAN/MAN Wireless LANS. Available from: http://www.ieee802.org/

Lemos, R. (2007). Got interference? Data-crowding problems looms for Wi-Fi. MetroFi, California.

Meurell, E .(2007). Solving the wireless networking challenges**.** Belden Inc., USA.

Othman, F. and K. Reoder, (2003).Wi-Fi Handbook: Building 802.11b Networks. Indianapolis, U.S.A.

Netstumbler 0.4.0 Installer (2004). Available from: http://www.netstumbler.com/downloads/

Patil, A. P., Kim, D. J. and Ni, L. M. (2006). A Study of frequency interference and indoor location sensing with 802.11b and Bluetooth technologies. *International Journal of Mobile Communications,* 4(6):621–644.

Udoh, E. S. (2006). Interference management and control in 802.11b networks within Ibadan Metropolis. MSc Research Project,(Unpublished), University of Ibadan, Ibadan, Nigeria.

Wheat, J., Hiser, R.,Tucker, J. and Neely, A. (2001).Designing a wireless network, Syngress Publishing Inc., Rockland, MA, 162pp.

Wikipedia, the free encyclopedia.(2006), Wireless LAN. Available at: http://en.wkipedia.org/wiki/Wireless_LAN

Wikipedia, the free encyclopedia.(2006).Spread Spectrum, Available at: http://www.wikipedia.org/wiki/spread_spectrum

WiMAX Broadband Technology Access .(2005). What is WiMAX? Availablefrom :http://www.intel.com./netcomms/technologies/wimax/