WIRELESS NETWORK INFRASTRUCTURE FOR ISPSC-STA.MARIA

MARK ANTHONY M. CASTELO
CHARLES PAUL T. FELICITAS
ROBEL CHRISTIAN D. DURO
MARK KEVIN C. ESCOBAR
RODELYN A. CABALLES
JEREMY F. AGPALO

A CAPSTONE PROJECT PRESENTED TO THE FACULTY OF
ILOCOS SUR POLYTECHNIC STATE COLLEGE
INSTITUTE OF COMPUTING STUDIES
SANTA MARIA, ILOCOS SUR

IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS
FOR THE DEGREE OF

BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY
(NETWORKING)

JUNE 2018

TABLE OF CONTENTS

Chapter I

INTRODUCTION

Project Context

In the 21st century, the internet has become a powerful tool for everybody regardless of age. Its purpose varies among users. Some see it as a reliable source of getting information and making a business transaction. Others also use it as a medium to connect to different people across the globe on social networks, play online games, upload and download music and videos, etc. People can connect to the internet either through a wired or wireless network. A lot of universities prefer wireless mean of providing internet to the wired connection using wireless local area networks (WLAN). This is because it has flexibility in installation and cost. Since it uses Orthogo1nal Frequency-Division Multiplexing (OFDM), it allows users to move around within a local coverage while still connected to the network. However, wireless networks are prone to some security issues (Appenzeller *et al.*, 2000).

In the light of the above statement, necessary measures must be taken to ensure security. Therefore, it is very important to deploy secured methods for authentication and encryption so that the network can only be used by those individuals and devices that are authorized. In a WLAN, communication and data transfer use radio transmission, which is open to all users (Soewito, 2014). This attracts people to use WLAN without

permission. The reasons behind are to get free internet access, steal data, spy on other users' activities or even damage the system. As a result, Wired Equivalent Privacy (WEP) was the 802.11 standard initially published in 1997 by the IEEE to avoid unauthorized access and encrypt data (Radvan, 2010).

WEP has been deprecated because of the vulnerabilities associated with obtaining the security keys. In response to these vulnerabilities found in WEP, Wi-Fi Protected Access (WPA) was introduced in 2001 by the WiFi Alliance (WFA) to curb the problems associated with WEP. WPA uses the Temporal Key Integrity Protocol (TKIP) which uses dynamic keys that were not backed up with WEP and RC4 for encryption. The TKIP method used with WPA was utilized until vulnerabilities were found in TKIP. These vulnerabilities centre on the fact that TKIP uses some of the same mechanisms that WEP does which allow similar attacks. In response to the vulnerabilities in WPA/TKIP, the IEEE 802.11i standard was defined and implemented in June 2004. WPA2 replaced TKIP with Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) which is based on Advanced Encryption Standard (AES) (Sean, 2011). However, some researchers have uncovered a vulnerability in the WPA2, which is the strongest for Wi-Fi encryption and authentication currently standardized and available (Mamat *et al.*, 2013). Hence, to improve the security of WLAN, a new secure mechanism called Captive Portal has been

introduced which uses a webpage to authenticate users. If a user tries to access the internet, the web browser redirects the request to a login page. As long as the login process is transported over a secure connection like TLS it will be difficult for malicious users to intercept other users' login details (Cisco, 2011).

Also, IEEE has developed advanced authentication and encryption protocol called 802.1X to solve the vulnerabilities found in WPA2. However, the 802.1X standard needs devices that work with the protocol, making it complicated than Captive Portal. Therefore, 802.1X is not widely deployed in WLAN. Another advantage of Captive Portal is that users need not install the access controller software on their mobile device. All they need to do is start a web browser to authenticate themselves. There exist quite a few numbers of Access controller, which are licensed for free or commercial use that integrates Captive Portal. Few examples are: (i) Air Marshall, software-based for Linux platform (commercial); (ii) LofiSense, Billing &OSS / Network Access Control (commercial); (iii) PacketFence, Linux-based Network Access Control Software with Captive Portal (open source); and (iv) pfSense, FreeBSD-based firewall software derived from m0n0wall (open source). pfSense is an open source firewall/router software which is based on FreeBSD operating System (Mamat *et al.*, 2013). It also supports the installation of third-party packages like free Radius or Squid through its Package Manager.

According to IEEE Society, WLAN Stands for Wireless Local Area Network, which is also known as Wi-Fi. WLAN is a Wireless version of the Ethernet network where the data is transferred between nodes through radio waves. The area covered by a single WLAN is called the Basic Service Set (BSS), which is identified by the Service Set Identifier (SSID). The standard used in WLAN is IEEE 802.11(ABG). The wireless medium of a wireless network is established through the usage of the following components: a) Basic service set (BSS): is the medium of communication and consists of all the components that construct a wireless network. The BSS can be independent and contain no access points; in this case, it is called an Ad-Hoc network. Ad-Hoc networks are equivalent to Peer to Peer wired networks. b) Access Points (AP): are the base stations and the means of communication between the clients and the rest of the network through radio frequencies. The access point may enforce data encryption using WEP and WPA to improve security. Every access point has a unique MAC address. c) Clients: are devices that use the services of the WLAN. They can include laptops, PDA's, mobile devices, and printers. In general, a station is a device that is connected to the WLAN through a wireless network interface card (WNIC). Every WNIC has a unique MAC address. d) Service Set Identifier (SSID): is the name of the BSS and consists of 32 bytes. A single access point can serve more than one BSS thus can have more than one SSID. e) Channel: is the radio frequency used by the AP to transmit the data to the clients. There are 11 different

channels ranging from 1 to 11. Having adjacent networks using the same channel can cause interference and reduce the quality and speed of communication.

As mentioned by H. Bergel, Wireless APs can be "open" or "closed" [4]. In the first case, the wireless AP broadcasts its SSID name. Wireless cards on the client's machines identify the strongest SSID signal and connect to the corresponding AP. In the second case, also known as "hidden", the AP doesn't broadcast the SSID name. The client has to manually insert the SSID name in order to establish a wireless network connection. Once the client enters the SSID name, the wireless card requests a connection through all channels; the AP receives the request and approves the connection.

There has been an enormous growth in the adoption of IEEE 802.11 wireless networks in the last few years. The ease of installation and the low infrastructure cost of 802.11 networks makes them ideal for network access in offices, malls, airports, cafes, hotels and so on. The widespread deployment of IEEE 802.11 networks means that a wireless client is often in the vicinity of multiple APs with which to affiliate. The selection of the AP that the client decides to affiliate with needs to be done carefully since it will dictate the client's eventual performance. The conventional approach to access point selection is based on received signal strength measurements from the access

points within range. However, it has been pointed out in several papers (A. Balachandran et. al, Y. Bejerano et. al and G. Judd et. Al) that affiliation based on signal strength can lead to very bad performance for the end-host, since the signal-strength metric does not convey information regarding other attributes that affect end-host performance, such as the AP load and the amount of contention on the wireless medium.

Wireless networks are one of the most growing segments of information technology. Because of the flexibility of wireless networks, businesses, educational establishments and households are adapting this technology which makes it an integral part of modern life. The introduction of new technologies always comes with a by-product, which is the abuse of the technology. For that reason, the secure usage of wireless networks has become a major field of study. War Drivingis the "art" of sniffing 802.11 wireless traffic using a network card set to monitor (RFMON) mode. The first officially recognized War Driving was performed by Peter Shipley in 1999, who presented his work to the hacker community at DEFCON 9 in July, 2001 (H. Berghel). Laptops with WLAN cards can use special software to perform War Driving. Some software, such as AirMagnet, SnifferPDA, and Fluke WaveRunner, require expert protocol users. Other software, such as Wireless Security Auditor (WSA), can be easily used by

normal users. WSA does a complete wireless network analysis and auditing. It also assists in discovering all possible security threats and vulnerabilities (IBM Corp.). Today, PDAs and mobile devices can also be used to sniff wireless data by running special purpose software.

Captive Portal can only use the LAN interface of the pfSense firewall. In setting up the portal with RADIUS authentication, the Captive Portal check box was enabled, interface selected, RADIUS authentication checked, and upload an HTML page with portal contents as described in the section called "Portal page contents" of the Captive Portal configuration page. The configuration of a local user on the Users tab of the Services Captive Portal page was then completed. The Captive Portal detail configuration options are as follows: 1) Interface – select the LAN interface Captive Portal will run on. 2) Maximum concurrent connections – This field specifies the maximum number of concurrent connections per IP address. It has a maximum limit of 50. This limit exists to prevent a single host from exhausting all resources on pfSense firewall, whether inadvertent or intentional. 3) Idle Timeout – Set the time to 15 minutes. It will disconnect idle users and users will be able to log back in immediately. 4) Hard Timeout – To forcefully log off users after a specified period. It will ensure sessions are removed if users do not log off, as most likely will not. Users will be able to log back in immediately after the hard timeout, if their credentials are still valid. 5) Logout Popup Window –

Check this box to enable a logout pop up window. Most browsers have pop blockers hence logout popup windows may not work in most browsers. 6) Concurrent User Login – Check this box. If this box is checked, only one login per user account is allowed. The most recent login is permitted and any previous logins under that username will be disconnected. 7) Authentication – Choose RADIUS authentication. Do the necessary configuration by entering the RADIUS server IP address, Port number and shared key to let Captive Portal communicate with RADIUS server. 8) Authentication Error Page Content – Upload an HTML page to be displayed on authentication errors. An authentication error occurs when a user enters a bad username or password.

This study would pave way for ISPSC to realize the need of getting connected to the Internet and other ways of communication with the use of an Access Point Receivers to the buildings at the northern area.

Problem

The transactions in the frontline services and other offices in ISPSC relies in online or the use of the internet. All of which use computer network. But even with the advancement of information systems, ISPSC still have hard time with network maintenance, troubleshooting and security. The ISPSC still encounters problems such as poor internet connectivity since all offices has their own internet subscription.

Importance

This study as perceived by the proponents is meaningful and significant to the following:

To Ilocos Sur Polytechnic State College, that they will benefit to this study in a way that it will guide them to improve their network security, with a secured data transfer and communications that rely with the internet. This study will eliminate the current problems encountered and will give way for future plans that is related to the wireless computer networking.

To ISPSC Employees, the plan helps employees to have better and way of communication in different offices.

To Network Administrators and Engineers, that they can use this as a basis for creation of wireless network infrastructure and to make upgrade and troubleshooting of network infrastructure easier.

To Future Researchers, that they will use this study as their reference for the conduct of similar studies and serves as a reference for their review of literature.

Finally, the Researchers, that this study helped them enhance their capabilities and skills of designing a wireless networ for ISPSC.

Literatures

Categorization of Clustering Protocols

Clustering protocols can be broadly categorized into cluster head-based clustering protocols and non-cluster head-based clustering

protocols. In the cluster head-based clustering protocols, the cluster head with extra control functions are chosen in each cluster, whereas in the non-cluster head-based clustering protocols, and all mobile nodes are identical with no chosen cluster head. Cluster head-based clustering protocols outperform non-cluster head-based clustering protocols in terms of traffic overhead. Based on the hop distance of the cluster members from its associated cluster head, the cluster head-based clustering can be further divided into 1-hop clustering and multi-hop clustering. In 1-hop clustering, the maximum distance between two cluster members is 2-hops, thereby maintaining one hop distance between the cluster members and its associated cluster head. In multi-hop clustering, cluster head can reach its farther member nodes by taking multiple hops through intermediate cluster members and relax its restriction of having direct connection with its associated members. Low-Maintenance clustering aims at providing stable cluster structure architecture without the excessive consumption of network resources for cluster maintenance, thereby incurring less maintenance cost. The re-affiliation and re-clustering are the two major events that influence the cost of cluster maintenance. The re-affiliation refers to the disassociation of cluster member from its cluster head and associating itself to another cluster without affecting the corresponding cluster head(s). Re-clustering is an event that completely rebuilds the cluster topology over the whole

network. These two events change the network topology more frequently with the drastic increase of clustering maintenance overheads.

Hierarchical- based routing

In a hierarchical architecture, higher energy nodes can be used to process and send the information and lower energy nodes used to sense the environment. So there is a hierarchy of low and high energy nodes. The creation of clusters and assigning special tasks to cluster heads can affect the scalability, lifetime, and energy efficiency. Hierarchical routing is two-layer routing where one layer is used to select cluster heads and the other for routing. This can be further divided into two parts dynamic hierarchical based routing scheme and static hierarchical based routing scheme. In dynamic, clusters are formed dynamically whereas in static once the clusters are formed remains same throughout the network life time. Energy Efficient Protocol with Static Clustering (EEPSC) is a static clustering-based routing algorithm. EEPSC divided the network into static clusters, temporary-cluster-heads are used to distribute the energy load among high energy sensor nodes; thus, extends the network lifetime and there is no overhead to select the clusters dynamically. The operation of EEPSC is divided into rounds, where each round contains set-up phase, responsible node selection phase and steady state phase.

Hierarchical Structure in Networks

According to the previous study of Solivenet. et al (2015), the hierarchical network clustering was conducted to create and develop a hierarchical network clustering for ISPSC Santa Maria Campus. The study was conducted during the second semester of the S.Y 2014-2015.

The study was made to provide an easier way in accessing on the internet with a well-planned hierarchy of clustered network. The proponents applied the interview method to acquire the necessary information needed in the design of a network infrastructure plan for Ilocos Sur Polytechnic State College Santa Maria Campus. As basis on the design of network infrastructure plan, the necessary requirement was gathered which is the current ICT Infrastructure of ISPSC. An existing list of the ICT profile was provided by the Office of the Executive Assistant of the President for ICT and the Director for Management and Information System of ISPSC. As the proponents reviewed and analyzed all the requirements, the design started by means of setting up a wireless network plan with the use of network devices such as: router with DHCP Server enabled, wireless access point and wireless bridge connectivity. Each building of the ISPSC Campus were set with the aforementioned devices, a load test scenario was then executed on each office using iperf as the benchmark tool to determine the reliability of the network infrastructure with the use of factors throughput and packet loss on a user-datagram protocol mode of test. It was found out by the proponents that in overall result of this study in the reliability test, the longer the distance of the offices connected to the main access point may cause packet loss although the result of the time transfer was good. A packet loss in computer networking is considered to be part of the (QoS) Quality of Service and a non-managed network means bad Quality of Service. A

good QoS designed network together with good quality devices would deliver the best service for the newly designed computer network of ISPSC.

According to Lancichinetti, Fortunato and Kertész (2009) many networks in nature, society and technology are characterized by a mesoscopic level of organization, with groups of nodes forming tightly connected units, called communities or modules that are only weakly linked to each other. Uncovering this community structure is one of the most important problems in the field of complex networks. Networks often show a hierarchical organization, with communities embedded within other communities; moreover, nodes can be shared between different communities. The study of networks as the 'scaffold of complexity' has proved very successful to understand both the structure and the function of many natural and artificial systems. A common feature of complex networks is *community structures* the existence of groups of nodes such that nodes within a group are much more connected to each other than to the rest of the network. Modules or communities reflect topological relationships between elements of the underlying system and represent functional entities. Therefore, the identification of communities is of central importance, but it has remained a formidable task. The hierarchical form of organization can be very efficient, with the modules taking care of specific functions of the system. In the presence of hierarchy, the concept of community structure

becomes richer, and demands a method that is able to detect all modular levels, not just a single one.

Network Performance Evaluation

As stated from the study of Solivenet. Al (2015), iperf was used as the network performance evaluation tool. To better understand what iperf, as mentioned from http://en.wikipedia.org/wiki/Iperf is, iperf is a commonly used network testing tool that can create Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) data streams and measure the throughput of a network that is carrying them. Iperf is a tool for network performance measurement written in C. It is a compatible reimplementation of the ttcp program that was developed by the Distributed Applications Support Team (DAST) at the National Laboratory for Applied Network Research (NLANR), a research lab that merged with the University of California, San Diego's Cooperative Association for Internet Data Analysis (CAIDA) group, but which was shut down on December 31, 2006, due to termination of funding by the United States' National Science Foundation. Iperf allows the user to set various parameters that can be used for testing a network, or alternatively for optimizing or tuning a network. Iperf has a client and server functionality, and can measure the throughput between the two ends, either unidirectional or bi-directionally. It is open-source software and runs on various platforms including Linux, Unix and Windows (either natively or inside Cygwin). Iperf has two mode of testing

environment which is: a) UDP-When used for testing UDP capacity, Iperf allows the user to specify the datagram size and provides results for the datagram throughput and the packet loss; b) TCP-When used for testing TCP capacity, Iperf measures the throughput of the payload. Iperf uses 1024 × 1024 for megabytes and 1000 × 1000 for megabits. Typical Iperf output contains a time-stamped report of the amount of data transferred and the throughput measured. *(Iperf Overview, 2015)*

ISPSC's Current Computer Network Setup

A computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users. (Technopedia, 2013)

A network consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams. (Florida Center for Instructional Technology, University of South Florida, Dr. Roy Winkelman, Director)

Networking enables employees within organizations to work with each other and with people in various locations and businesses elsewhere. It enables contact in entirely new levels, across office and

right around the world. When the business is properly networked, no one is ever very far away.

The Ilocos Sur Polytechnic State College has several computer networks which are used primarily for Internet connectivity. The computer networks of ISPSC are isolated units, located and maintained in different departments or buildings. These networks are connected to the Internet through various Internet Service Providers. With the present structure and set-up of the computer networks of ISPSC, there is difficulty in maintaining the system, computer networks do not communicate with each other.

Hierarchical Network Clustering for ISPSC (previous study)

The previous study of Soliven et. Al (2015) only focused in the reliability of the data packets (packet loss). It was concluded as the overall result the researchers concludes that the farther the bridge device connection getting connected to the main access point shows a poor Quality of Service, therefore a consideration of good quality devices should then be realized.

Objectives

To establish a wireless network at the Northern Area of ISPSC Sta. Maria campus that will provide internet access and other means of communication and data packet transmission. Specifically the study sought to answer the following objectives

1. To determine the current Internet and WIFI set-up at the northern areas of ISPSC Sta. Maria campus.
2. To design a wireless network infrastructure for northern areas of ISPSC Santa Maria.
3. To determine the performance of the designed wireless network infrastructure.

Time and Place of the Study

The study made use of 5ghz Access Point to connect AP Stations from buildings from the Northern Area of ISPSC.

This study aimed to determine the performance of the 5ghz Access Points compared to the previous study which used 2.4ghz Access Points of the Santa Maria Campus.

The proponents designed a wireless network infrastructure for ISPSC and determined the performance of the Access Points using iperf. The advantages gained through this study will serve its purpose in the deployment of a good access point that can be deployed for the wireless network infrastructure of the northern area of ISPSC.

Chapter II
METHODOLOGY

Developmental Methodology

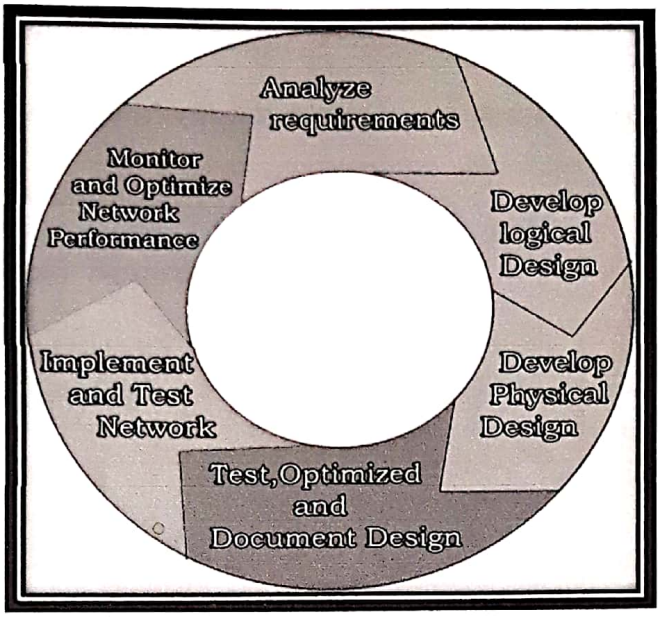

Figure 1. Top-Down Approach

The study will be conducted at Ilocos Sur Polytechnic State College Santa Maria Ilocos Sur Campus. This research will imply the use of the top-down approach. The researchers used the Top-Down Approaches their Network Life Cycle model in order to process and design an appropriate network plan based on the requirements that will be gathered which is shown in Figure 1.

A top-down approach enables a network designer to get "the big picture" first before spiraling downward into detailed technical requirements and specification.

The top-down network design is a methodology for designing networks that begins at the upper layers of the OSI reference model

before moving to the lower layers. It includes exploring organizational and group structures to find the people for whom the network will provide services and from whom the designer should get valuable information to make the design succeed. Top-down network design recognizes that the logical and the physical design can change as more information is gathered.

Table 1. The Project Schedule Gantt Chart

ACTIVITIES	JANUARY				FEBRUARY				MARCH				APRIL				MAY			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Analyze Requirements																				
Develop Logical Design																				
Develop Physical Design																				
Test, Optimize and Document Design																				
Implement and Test Network																				
Monitor and Optimize Network Performance																				

Figure 2 above shows the cycle of the methods and procedures that the proponents applied in this study. This include the following:

Analyze requirements. In this phase, the proponents interviewed the previous adviser of the study and technical personnel to gain an understanding of the study for new or enhanced plan. The task of

characterizing the existing network, including the logical and physical topology and network performance, follows. The last step in this phase is to analyze current and future network traffic, including traffic flow and load, protocol behavior, and quality of service (QoS) requirements.

Develop the logical design. This phase deals with a logical topology for the new or enhanced network, network layer addressing, naming, and switching and routing protocols. Logical design also includes security planning, network management design, and the initial investigation into which service providers can meet WAN and remote access requirements.

Develop the physical design. During the physical design phase, specific technologies and products that realize the logical design are selected. Also, the investigation into service providers, which began during the logical design phase, must be completed during this phase.

Test, optimize, and document the design. The steps in top-down network design are to write and implement a test plan, build a prototype or pilot, optimize the network design, and document your work with a network design proposal.

Implement and Test Network. To put the enhanced network plan into effect or action and to test if how reliable the plan could be.

Monitor and Optimization Network Performance. To monitor and optimize by analyzing network performance such as monitoring

network traffic and resource utilization, that affects both hardware and software.

Project Staff and Functions

Table 2. Role Requirements and Responsibility

Project Leader	Lead team, report status Review deliverables and assure quality	1	Jeremy
Documenter	Create framework content	3	Robel Rodelyn Mark Kevin
Planner and Designer	Design the project performance management tool	5	Jeremy Charles Robel Rodelyn Mark Anthony
Review Team	Build the project performance Evaluate deliverables and promote of use	6	Jeremy Charles Robel Rodelyn Mark Anthony Mark Kevin

The role requirements and responsibility of the members of the team can be seen in table 2.Table shows that each member has their different tasks and responsible of any actions assigned. The leader, who provides and give assignments to his members according to the skills they have and to help and to builds a cooperative teamwork. The leader would not only assign the team a work but must work according to the role responsibility. Members are grouped to be the project developer, documentation developer and a review team. Furthermore, each of the

staff assigned need to meet the goals and requirements needed with specific due or time.

Data Gathering Procedures

The following are the methods used in gathering data which was utilized in the conduct of this study.

Survey. The survey questionnaire was used to determine the existing ICT equipment in terms of hardware, software and peopleware of ISPSC.

Internet. This tool was very useful in providing the background and literature of this study, some needed literature can be found in the internet. Specifically, published and unpublished researches will be the basis of this study.

Network Experiment. Iperf, was used to test the experimental network under different simulated network conditions. Ubiquiti 2.4 Ghz access points and 5 Ghz access point were compared to determine which among them can perform a very well in packet of UDP and TCP transfer, bandwidth and transfer rate.

REFERENCES

Books

Appenzeller G., Roussopoulos M., Baker M., (2000), "User-Friendly Access Control for Public Network Ports" IEEE INFOCOM'99. Eighteenth Annual Joint Conference, Vol. 2, pp. 699-707.

Radvan, S. (2010), Wireless and mobile networking overview for Fedora Linux, Red Hat, Vienna, edition 1.2.

IEEE Computer Society, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications," in IEEE Standard 802.11g, 2003.

H. Berghel, "Wireless Infidelity II: Air Jacking," Communications of ACM on Digital Village, 47(12), pp. 15-21, December 2004

A. Balachandran, P. Bahl, and G. Voelker. Hot-spot congestion relief and service guarantees in public-area wireless networks. SIGCOMM Computer Communication Review, 32 (1), 2002.

Y. Bejerano, S. Han, and L. Li. Fairness and load balancing in wireless LANs using association control. In Proceedings of ACM Mobicom , Philadelphia, Oct 2004.

G. Judd and P. Steenkiste Fixing801.11 access point selection. In Poster in Proceedings of ACM Mobicon, Pittsburgh, Aug 2002.

H. Berghel, "Wireless Infidelity I: War Driving," Communications of ACM on Digital Village, 47(9), pp. 21-27, September 2004.

Webliography

IBM Corporation, "Security Research: Wireless Security Auditor (WSA)," 2007. Available: http://www.research.ibm.com/gsal/wsa.