Wireless LAN Technologies: A Model for Planning, Designing, and Implementing in a Global Manufacturing Enterprise

by

Ronald G. Wolak

A preliminary dissertation proposal submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy

The Graduate School of Computer and Information Sciences
Nova Southeastern University

May 2002

An Abstract of a Preliminary Dissertation Proposal Submitted to Nova Southeastern University in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

Wireless LAN Technologies: A Model for Planning, Designing, and Implementing in a Global Manufacturing Enterprise

by
Ronald G. Wolak

May 2002

The preliminary dissertation proposal that follows was submitted to partially fulfill the requirements for the degree of Doctor of Philosophy. Wireless local area networks have the potential to improve the flexibility, productivity, and the quality of work life of an enterprise. While WLAN technologies offer the benefits of mobility, reduced installation time, and decreased cost, many challenges must be met by companies deploying them. These issues are related to security, speed, interoperability, equipment selection, ease of use, reliability, signal interference, installation, and health risks. The proposed research addressed a problem confronting many large manufacturing companies in the present-day (i.e. how to best plan, design, and implement WLAN technologies). The goal of the research was to provide large manufacturing enterprises a model for deploying secure WLAN technologies in their offices, manufacturing facilities, and employee residences. The model was to be developed from a case study of WLAN projects to be implemented at American Axle and Manufacturing. Four WLAN initiatives were to be the subject of the case study: Worldwide Wireless Connectivity in Executive Conference Rooms, AAMatHome, Enhanced WLAN Security, and Wireless Connectivity on the Plant-floor.

Table of Contents

Introduction

Wireless local area networks (WLANs) have the potential to improve the flexibility, productivity, and the quality of work life of an enterprise (Sage Research Staff, 2001). American Axle and Manufacturing (AAM) is typical of a large manufacturing company. AAM is a tier one supplier of automotive driveline systems headquartered in Detroit, Michigan (AAM, 2001). AAM specializes in the design, engineering, validation, and manufacture of driveline systems, chassis systems, and forged products for trucks, buses, sport utility vehicles, and passenger cars. The company is a global enterprise with 12,000 employees and seven million square feet of manufacturing space in 17 manufacturing facilities located in the United States, Brazil, Mexico, and the United Kingdom.

AAM's existing network infrastructure is wireline. Employees at AAM locations worldwide connect to the AAM network using wired ports connected to a fiber optic backbone. Remotes users access the network through a dial-up modem pool. AAM's wireline network model severely limits the accessibility and effectiveness of the AAM network. For example, employees in AAM facilities are unable to access the network easily from meetings, the cafeteria, or anywhere other then their offices. In addition, the effectiveness of remote users is limited by the slow speed of present-day dial-up modem connections.

The following sections describe the problem to be investigated and the goal to be achieved. Next, the research questions to be explored are briefly stated. Also provided is an analysis of the relevance and significance of the research and a discussion of barriers

and issues related to achieving the goal. In addition, the approach, milestones, and resources to be used in accomplishing the goal are discussed. Finally, a brief summary is provided along with an annotated bibliography of the literature.

Problem Statement and Goal

The proposed research will address a problem confronting many large manufacturing companies in the present-day (i.e. how to best plan, design, and implement WLAN technologies). While WLAN technologies offer the benefits of mobility, reduced installation time, and decreased cost, many challenges must be met by companies deploying them (Geier, 2001). These issues are related to security, speed, interoperability, equipment selection, ease of use, reliability, signal interference, installation, and health risks.

For example, rapidly emerging WLAN standards are making it difficult for business organizations to choose the right technology when deploying WLAN technologies (Railsback, 2001). This is further complicated for manufacturing enterprises where plant-floor environments are combined with office and residential settings. WLAN technologies must, by design, interface with many areas of a company's network infrastructure. This makes interoperability a necessity.

In addressing the problem, the proposed research will use the case study method to examine the plan, design, and implementation of WLAN technologies at AAM. At present, the wireline local area network (LAN) technologies employed by AAM include 10/100BaseT Ethernet at each desktop. Ethernet ports at the desktop are switch connected to an Asynchronous Transfer Mode (ATM) fiber optic backbone. AAM's remote

facilities connect to the network using switched Frame Relay services along with Internet Virtual Private Network (VPN) connections.

These technologies are of limited effectiveness in connecting employees while at work and at home to the AAM network. AAM's wireline infrastructure does not allow employees on the move to leverage the time they spend at meetings, in the cafeteria, and other locations to catch up on e-mail, retrieve information, or perform other work related activities (Sage Research Staff, 2001). For example, the way Microsoft employees interact at work was dramatically affected by the company's installation of Institute for Electrical and Electronic Engineers (IEEE) 802.11b WLANs (Orenstein, 2001). Microsoft employees no longer attend virtual meetings using desktop videoconferencing. Instead, they go to real meetings and bring their offices with them (i.e. laptops with WLAN connectivity).

In addition, the cost and time required to install and operate wireline networks in large manufacturing facilities to support industrial automation is often excessive. For example, the total cost of ownership (TCO) for a WLAN in the typical small office is 15 percent lower than the TCO for a wired LAN (Blackwell, 2001). The spread between wired and wireless LAN TCO is likely to be greater for LANs installed in large manufacturing facilities. These plant-floor LANs are common in AAM's facilities and are comprised of thousands of feet of cable. This cabling connects a variety of industrial automation controllers together and facilitates system control and data acquisition (SCADA) along with control program uploads and downloads. Wireless LAN technologies would seem to be more appropriate in this environment since plant-floor

LAN cabling is frequently removed or relocated in reaction to changing manufacturing process requirements.

The limitations of wireline networks also extend into AAM employee residences. Remote users connect to the AAM network using dial-up connections with a maximum data rate of 56 kilobits per second (Kbps) downstream and 33.6 Kbps upstream. This remote access solution does not provide telecommuters and other less frequent work-at-home users the benefits of untethered high speed access to corporate applications from small home/home office (SOHO) venues.

The goal of this research is to provide large manufacturing enterprises a model for deploying secure WLAN technologies in their offices, manufacturing facilities, and employee residences. The model will be developed from a case study of WLAN projects to be implemented at AAM. While companies such as Intel were quick to embrace WLAN technologies and applied a strategic rather than a tactical approach to their deployments (Staff, 2001). Many other companies including Allina Health System reconsidered planned wireless initiatives in light of security inadequacies, changing standards, and equipment interoperability issues. Allina originally planned a full-scale implementation of WLAN technologies throughout its medical facilities. However, security issues forced the company to reconsider the plan. WLAN suppliers now emphasize that the implementation of wireless technologies must be part of an overall wireless strategy (MSI Editors, 2001). The WLAN implementation model that will be developed will benefit large-sized manufacturing companies.

In addition to the model, this research will provide a template of a comprehensive wireless security policy for use by manufacturers. This policy will address the proper use

of corporate wireless networks in addition to the existence of user configured wireless networks.

Research Questions

One of the most important steps in conducting a research case study is the definition of research questions (Yin, 1994). The research project will seek to answer a number of questions related to the problem of how to best plan, design, and implement WLAN technologies in a large manufacturing enterprise. These include:

- What are the benefits of WLANs?
- What WLAN standards and technologies are currently available for deployment?
- What are the limitations of WLAN technologies?
- What solutions are available to secure WLANs?
- Which existing and future WLAN technologies are most appropriate for deployment?
- What applications are most appropriate for the WLAN?
- Which WLAN tactics and strategies should be employed?
- How are WLAN technologies best implemented?
- What positive or negative impact does the implementation of WLANs have?
- Will WWANs eventually replace WLANs?
- How should WLAN technologies be integrated with WWAN technologies and services?

Relevance and Significance

WLANs are beginning to replace traditional wired LANs as the preferred approach to the "last ten feet" of enterprise network environments (Hannon, 2001). In fact, more than 50 percent of companies have plans to purchase and install WLAN systems. The release of high data rate and Ethernet-equivalent WLAN technologies is primarily responsible for this trend (Intel Staff, 2001). Low cost, high speed, interoperable products provide companies the flexibility to wirelessly transfer large data files, access the Internet, support wireless videoconferencing, and rapidly reconfigure sites.

Existing WLAN technologies include infrared, ultra high frequency (UHF) narrowband, and spread-spectrum (Garg, 2001). Most WLAN systems use spread-spectrum, which is a wideband radio frequency (RF) technique that uses the entire allotted spectrum in a shared manner as opposed to dividing it into discrete pieces as with UHF narrowband (Garg, 2001). The Institute of Electrical and Electronic Engineers (IEEE) 802.11 family of standards, which are based on Ethernet technology, employ spread-spectrum solutions.

The four IEEE 802.11 standards that exist at present are 802.11, 802.11a, 802.11b, and the recently approved 802.11g (Krazit, 2001). IEEE 802.11 provides 1 or 2 megabits per second (Mbps) transmission in the 2.4 Gigahertz (GHz) band using either a frequency-hopping spread-spectrum modulation (FHSS) technique or direct-sequence spread-spectrum (DSSS). IEEE 802.11b defines an 11 Mbps data rate in the 2.4 GHz band, IEEE 802.11a defines a 24 Mbps data rate in the 5 GHz band, and 802.11g defines a data rate of 54 Mbps in the 2.4 GHz band.

In addition, Bluetooth, a short-range wireless standard, provides up to 720 Kbps data transfer in 2.4 GHz band. Companies deploying these high rate WLAN technologies must be aware of possible interference between IEEE 802.11, Bluetooth, and other 2.4 GHz devices sharing the same bandwidth (Brewin, 2001). WLANs that employ the 802.11b standard are the most prevalent. Examples include networks at hospitals and university campuses along with retail stores and warehouses (Wheat, Hiser, Tucker, Neely, & McCullough, 2001).

WLAN technologies offer large manufacturing companies the ability to enable wireless mobility throughout a facility. WLANs also facilitate the addition or relocation of workstations and the connection of users in areas where the installation of a wireline network is difficult (Intel Staff, 2001). However, as widespread deployment of WLAN technologies continues, companies must ensure that their wireless networks integrate with their wireline infrastructure to form a seamless entity.

This model for the deployment of WLAN technologies, which is the goal of the research, is valuable because it will benefit large manufacturing companies as they continue the installation of WLANs. Network design engineers have struggled for years to streamline the design and implementation process (Wheat et al., 2001). WLAN technologies have further complicated this process. This research will contribute to the body of knowledge and improve professional practice by providing a modern life cycle model to plan, analyze, design, implement, and support enterprise wireless initiatives based upon real life lessons learned from a case study of AAM's WLAN projects (Whitten, Bentley, & Dittman, 2000).

The planning phase of the model will seek to identify and prioritize wireless technologies and applications that will provide the greatest return on investment to a large manufacturing company (Whitten, Bentley, & Dittman, 2000). Activities performed in this phase include specifying the business mission, defining an information architecture, and evaluating business areas. The second or analysis phase of the model will study current company networks and define the user requirements and priorities for the WLAN. This phase is made up of three basic activities: surveying project feasibility, analyzing current infrastructures, and defining and prioritizing user requirements.

The systems design or third phase of the process will be an evaluation of alternative solutions and the specification of a detailed WLAN solution (Whitten, Bentley, & Dittman, 2000). This will be followed by the implementation phase, which entails the construction of the wireless network and the delivery of a working system into day-to-day operation. The final phase of this SDLC process will be the systems support or ongoing maintenance of the WLAN. This includes both maintenance and improvements.

Brief Review of Literature

The literature review that follows is provided to establish the background of the investigation. The review begins with an historical overview of the research literature and follows with a discussion of literature specific to the subject of planning, designing, and implementing wireless local area networks in a global manufacturing enterprise. The detailed literature review will be organized into seven subject areas: WLAN technologies and standards, WLAN security, WLAN hardware, WLAN deployments, wireless service

providers, wireless tactics and strategy, and the case study method. Literature related to WLAN technologies and standards is reviewed in this preliminary dissertation proposal. The remaining six subject areas will be covered in detail in the formal dissertation proposal.

Historical Overview

Radio frequency (RF) and network technologies first complemented one another in 1971 with a project called ALOHANET (Geier, 2001). ALOHANET, a University of Hawaii research project and the first wireless wide area network (WWAN), connected computers at the university's seven campuses on four neighboring islands with a mainframe computer on the island of Oahu. All stations in the network transmitted their packets to the "master" station on Oahu without regard for other network traffic (Armyros, 1992). The result of these random transmissions and lack of central control resulted in high collision rates and a maximum channel efficiency of 18.4 percent. Although this first system was inefficient, it was successful in replacing costly and unreliable telephone lines.

Later, the American Radio Relay League (ARRL) and the Canadian Radio Relay League (CRLL) began promoting the use of wireless connectivity in the 1980s (Geier, 1999). These amateur radio hobbyists connected their personal computers to one another using terminal node controllers (TNCs) and very high frequency/ultra high frequency (VHF/UHF) radio transceivers. The TNCs converted digital signals from the personal computers to analog signals. These signals were then broadcasted using a packet switching technique. Next, the Federal Communications Commission (FCC) assisted the

development of wireless network technologies by authorizing the public use of the Industrial, Scientific, and Medical (ISM) bands (902 MHz – 5.85 GHz) in 1985 (Geier, 1999). This action spurred the development of WLAN components. Following the creation of the ISM bands, the IEEE 802 Working Group began development of WLAN standards in the late 1980s. The effort culminated with the publication of the IEEE 802.11 standard in June of 1997.

Wireless local area networks have been in use since 1990 (Prasad & Prasad, 2001b). These networks are primarily based upon spread spectrum technologies developed by the U.S. military during World War II. Spread spectrum technologies transmit voice and data over a range of frequencies using either the frequency hopping spread spectrum (FSSS) or the direct sequence spread spectrum (DSSS) modulation techniques. Newer systems, operating in the 5 GHz frequency band, achieve higher data rates using orthogonal frequency division multiplexing (OFDM). In addition to spread spectrum WLANs, systems employing infrared and UHF narrowband technologies are also in limited use.

WLAN Technologies and Standards

Literature related to WLAN technologies and standards is reviewed in the following sections. These technologies and standards include UHF narrowband, spread spectrum, ultrawideband, IEEE 802.11, HIPERLAN, MMAC, HomeRF, and IrDA,

UHF Narrowband

UHF narrowband technology was originally developed by amateur radio operators (Prasad & Prasad, 2001b). The term narrowband refers to the narrow band of RF spectrum, 12.5 KHz to 25 KHz, used to transmit data. Existing narrowband systems transmit on both licensed and unlicensed frequencies and operate at higher power levels than spread spectrum systems. The result is that UHF narrowband systems are able to transmit the greatest distance (35 to 50 kilometers) of all WLAN technologies.

However, UHF narrowband has a number of disadvantages (Jensen, 1999). These include regulatory barriers when operating at data rates above 56 Kbps and the instability of frequencies at which the technology operates (i.e. interference and propagation anomalies). In addition, UHF narrowband packet radio systems require considerable knowledge and effort to install. Commercially packaged solutions are not available and systems must be custom built. Elements involved in a typical system installation include assembling equipment, configuring antennas, verifying radio link performance, and installing network software.

Spread Spectrum

Spread spectrum radio transmission techniques continuously change signal patterns and frequencies (Freedman, 2002). Spread spectrum systems in contrast to narrowband systems use more bandwidth than is needed for transmission. In addition, spread spectrum transmissions are more secure (i.e. difficult to detect, intercept, and decode) than narrowband transmissions (Perez-Jimenez, Riera, & Lopez-Hernandez, 2001). However, spread spectrum systems are more complex and were only adopted by commercial systems after integrated digital signal processors (DSPs) became available at

low cost and high quantity. Both narrowband and spread spectrum transmission systems are able to use the same frequency band with little interference with one another.

Two types of spread spectrum systems are most frequently used: direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS) (Perez-Jimenez, Riera, & Lopez-Hernandez, 2001). DSSS, which is employed in code division multiple access (CDMA), multiplies data by a pseudo-random bit pattern (PN sequence). This spreads the data over a coded stream that uses the full bandwidth of the radio channel. The primary reason to select the DSSS transmission method is its ability to share spectrum with other techniques.

The FHSSS transmission method uses conventional modulation techniques, but continuously changes the center carrier frequency multiple times per second in a sequence (Freedman, 2002). This sequence is the code that makes FHSSS transmissions secure and extremely difficult to monitor (Perez-Jimenez, Riera, & Lopez-Hernandez, 2001). The FHSSS receiver must know the code or it is not be able to follow the frequency hops. When the hopping rate is faster than the bit rate, the system is fast frequency hopping (FFH). Slow frequency hopping (SFH) occurs when the hopping rate is slower than the bit rate.

Another type of spread spectrum transmission is orthogonal frequency division multiplexing (OFDM) (Freedman, 2002). OFDM distributes the transmitted data over a large number of carriers, which are separated at predetermined frequencies. This spacing prevents receivers from seeing signals other than their own. A variation of this technique, coded OFDM (COFDM), incorporates forward error correction.

UWB

Ultrawideband (UWB) technology is a short range, low power wireless technology (Leeper, 2001). UWB radio systems are defined as those that have a bandwidth of greater than 1.5 GHz or more than 25 percent of its center frequency. In addition, UWB systems emit very narrow pulses over a wide spectrum of frequencies. The technology, which was first developed in the 1980s, is primarily used for radar and is often used to pinpoint objects hidden underground or behind barriers.

The FCC's recent approval to use UWB technology in commercial applications along with advances in low cost, low power switching technology make it feasible to use the technology in consumer-grade communication devices (Paulson, 2002). The technology is most appropriate for small devices with limited power capacities such as smart cellular phones and personal digital assistant. In addition to the benefits of UWB's low power consumption, the technology's use of time hopping makes it extremely secure.

IEEE 802.11

IEEE 802.11 is the first international standard for WLANs (O'Hara & Petrick, 1999). The standard was first adopted by the IEEE in 1997 and was subsequently revised in 1999. IEEE 802.11 is officially titled the IEEE Standard for Wireless LAN Medium Access (MAC) and Physical Layer (PHY) Specifications (Prasad, Kamerman, & Moelard, 2001). IEEE 802.11's purpose is to provide wireless connectivity to mobile equipment and machinery within a local area. Similar to other IEEE 802 standards such as IEEE 802.3 and IEEE 802.5, IEEE 802.11's primary purpose is to deliver MAC service data units (MSDUs) between peer logical links (LLCs).

The IEEE 802.11 standard also takes into account factors specific to wireless networking (Prasad, Kamerman, & Moelard, 2001). These include power management, bandwidth, security, and addressing. In addition, the standard supports two topologies for wireless device interaction. These are independent basic service set (IBSS) and extended service set (ESS) networks. Each access point and its wireless devices is defined as a basic service set (BSS) (Freedman, 2002). ESS networks are comprised of two or more BSSs in the same subnet. In contrast, IBSS networks are made up of wireless devices communicating in peer-to-peer mode without the use of an access point.

IEEE 802.11 also defines two authentication service subtypes: open system and shared key (Prasad, Kamerman, & Moelard, 2001). Open system authentication is a null authentication algorithm. Any wireless station that requests authentication with this algorithm is authenticated. In contrast, shared key authentication requires wireless stations to possess a shared secret key. Transmission of the shared key is encrypted using the Wired Equivalent Privacy (WEP) algorithm.

When IEEE 802.11 was enacted in 1997, FHSS and DSSS devices in the 2.4 GHz band went into widespread production. Data rate capabilities of these units were 1 Mbps and 2 Mbps (Rappaport, 2002). In 1999, the IEEE 802.11b physical layer extension (also called the High Rate standard) was approved. This standard provided for DSSS transmissions with data rate capabilities of 11 Mbps, 5.5 Mbps, 2 Mbps, and 1Mbps. In addition, the IEEE 802.11b standard was named “Wi-Fi” by the Wireless Ethernet compatibility Alliance (WECA).

In addition to the DSSS and FHSS physical layers, IEEE 802.11 supports the IR PHY (O'Hara & Petrick, 1999). Unlike DSSS and FHSS, the IR PHY uses near-visible

light as the transmission media. IR communications are dependent on light energy that is transmitted by reflection off objects or by direct line-of-sight. Data transmissions are supervised using the IR physical medium dependent (PMD) sublayer. In addition, the IR physical layer convergence procedure (PLCP) sublayer directs the IR PMD.

Another physical layer extension to IEEE 802.11 is IEEE 802.11a (Rappaport, 2002). The IEEE 802.11a standard provides up to 54 Mbps throughput in the 5 GHz radio frequency band. Also providing high data rates is the new IEEE 802.11g extension. IEEE 802.11g provides up to 54 Mbps throughput in the 2.4 GHz band. Unlike IEEE 802.11b, which uses the DSSS modulation technique, the IEEE 802.11a and IEEE 802.11g standards employ OFDM to achieve their higher data rates. In addition, IEEE 802.11g is backward compatible with IEEE 802.11b since it is also able to transmit using the DSSS modulation technique in the 2.4 GHz band.

HIPERLAN

The HIPERLAN standard was developed in the mid 1990s to provide functionality similar to IEEE 802.11 (Rappaport, 2002). The European standard provides asynchronous data rates up to 20 Mbps. In addition, HIPERLAN was designed to operate at a distance of 50 meters and in vehicles moving at speeds up to 35 kilometer per hour. The HIPERLAN and HIPERLAN/2 standards were created by the European Telecommunications Standards Institute (ETSI) and operate in the 5 GHz frequency band (Bates, 2001).

HIPERLAN/2 and IEEE 802.11a technologies have similar physical layers and a connectionless protocol (Geier, 2001). However, HIPERLAN/2, which grew from the

ATM development effort, more closely resembles ATM than Ethernet. The technology provides quality of service (QOS) support for video, voice, and images. In addition to HIPERLAN and HIPERLAN/2, HIPERACCESS and HIPERLINK were defined by the ETSI (Prasad & Prasad, 2001a). HIPERACCESS operates in various frequency bands and provides fixed wireless broadband point-to-point communications, while HIPERLINK operates in the 17 GHz frequency band and is used for wireless broadband interconnections.

MMAC

The Ministry of Post and Telecom (MPT) in Japan created the Multimedia Mobile Access Communication (MMAC) committee to study next generation broadband mobile communication systems in 1995 (Prasad & Prasad, 2001a). MMAC systems are designed to transmit ultrahigh speed, high-quality multimedia content to mobile users. Four system types are defined: High-speed Wireless Access, Ultrahigh Speed WLAN, 5 GHz Band Mobile Access, and Wireless Home-Link. MMAC High-Speed Wireless Access Systems transmit data at rates up to 30 Mbps using frequencies from 3 to 60 GHz. This technology is appropriate for mobile video telephone conversations. MMAC Ultrahigh Speed WLAN systems, able to transmit at data rates up to 156 Mbps in the 30 to 300 GHz band, are suitable for indoor video conferences. Prototype MMAC WLAN systems operating in the 60 GHz band have demonstrated the feasibility of ATM and Ethernet interfaces with data rates up to 155 Mbps (Ohmori, Yamao, & Nakajima, 2000).

The MMAC 5 GHz Mobile Access standard defines both ATM and Ethernet wireless systems operating in the 5 GHz band (Prasad & Prasad, 2001a). These systems

are capable of transmitting multimedia information at date rates up to 20 to 25 Mbps. ATM type systems are similar to those using the European HIPERLAN/2 standard. Minor differences exist in the protocol for intercellular synchronization. Ethernet type systems are compatible with the IEEE 802.11a standard. The fourth type of MMAC system is Wireless Home-Link. These systems are designed for indoor use and are able to transmit data rates up to 100 Mbps using frequencies from 3 to 60 GHz. The primary use for this system type is the transmission of multimedia content between personal computers and audiovisual equipment.

HomeRF

The HomeRF working group is made up of approximately 100 computer, communications, and microelectronics manufacturers (Riera & Perez-Jimenez, 2001). The HomeRF specification was prepared to provide wireless voice and data networking in the home. The physical layer specification for the technology is based on IEEE 802.11 Frequency Hopping (FH) mode and includes data rates from .8 to 1.6 Mbps with hop times of 300 microseconds. The frame, or hop time, consists of two subframes: time division multiple access with time division duplex (TDMA/TDD) and carrier sense multiple access with collision avoidance (CSMA/CA). TDMA/TDD is used for isochronous voice communications and CSMA/CA is used for peer-to-peer asynchronous data communications.

The newer HomeRF 2.0 standard employs wideband frequency hopping (WBFH) and is able to transfer data at rates up to 10 Mbps with a range of 50 meters (Prasad & Prasad, 2001a). Devices using this technology are in direct competition with those

employing the IEEE 802.11b Wi-Fi standard (Caswell, 2001). Proponents of the HomeRF standard cite benefits that include toll-quality voice services, lower power consumption, higher reliability, and support for high-network-density environments such as hotels and apartment buildings. In addition, HomeRF's use of frequency hopping makes it more secure and less susceptible to interference than IEEE 802.11b. However, WiFi's market penetration currently offsets any disadvantages the technology possesses (Batista, 2000).

IrDA

Infrared technology is primarily used for in-room WLAN communications (Prasad & Prasad, 2001b). Since information is transmitted by invisible beams of light, applications are restricted to line of sight (LOS) connections between transmitters and receivers. The deployment of infrared WLANs has been limited as a result. Standards groups governing the development and manufacture of infrared WLAN components include the IEEE and the Infrared Data Association (IrDA). The IrDA standard is discussed in the next section.

The IrDA standard specifies point-to-point infrared transmission rates of 115.2 Kbps between computer, printers, and fax machines (Geier, 1999). The Fast Infrared (FIR) high-speed extension (up to 4 Mbps) has also been defined. IrDA is comprised of the IrDA Serial IR physical layer (IrDA-SIR) and the Infrared Link Access Protocol (IrLAP) data link protocol. In addition, the IrDA Management Protocol (IrLMP) provides the mechanism to multiplex and handshake two or more simultaneous data streams. The typical IrDA subsystem is composed of four elements: an IR controller, an IR transceiver,

an IrDA enabling application, and an IrDA software protocol stack (Santamaria, Vento-Alvarez, Rabadan, & Perez-Jimenez, 2001). The interfaces between the elements are not defined in the IrDA standard.

The standard also includes LAN access extensions for link management protocol: IrLAN (Santamaria et al., 2001). In general, the IrLAN protocol is a passive protocol that defines a bi-channel interface between a protocol server and a protocol client. The IrLAN protocol enables an IrDA enabled computer to connect to a LAN through an access point or to communicate with another computer as though they were attached to a LAN. In addition, it allows and IrDA enabled computer to attach to the LAN through a second LAN attached computer.

Summary

The brief review of literature provided above began with an historical overview of the research literature and followed with a discussion of literature specific to the subject of planning, designing, and implementing wireless local area networks in a global manufacturing enterprise. The detailed literature review will be organized into seven subject areas: WLAN technologies and standards, WLAN security, WLAN hardware, WLAN deployments, wireless service providers, wireless tactics and strategy, and the case study method. Literature related to WLAN technologies and standards was reviewed above. The remaining six subject areas will be covered in detail in the formal dissertation proposal.

Barriers and Issues

The goal of this research is difficult and has not already been met for a number of reasons. One explanation is the complexity of planning, designing, and implementing WLAN technologies in a large manufacturing company. Underlying issues include limited access to worldwide facilities, information technology resources, and network infrastructure, along with the security weaknesses inherent in the existing Wired Equivalent Privacy (WEP) algorithm (Fluhrer, Mantin, & Shamir, 2001). An additional issue is the need to integrate properly new WLAN technologies with existing wireline infrastructures. The resultant mixed-mode wireless and wired configuration should operate more efficiently than the previous single-mode environment.

Another issue is the emergence of competitive IEEE WLAN standards: 802.11b, 802.11a, and 802.11g (Curl, 2001). In addition, different countries and organizations are promoting their own WLAN protocols such as High Performance Radio Local Area Network (HIPERLAN) and HIPERLAN/2 (Bourin, 2001). Enterprises considering WLAN technologies must determine which available or emerging technology is the best fit based upon project timing, equipment compatibility, equipment availability, and their existing network topology (MSI Editors, 2001). Companies must be careful to implement wireless applications as part of an overall wireless strategy and not just as isolated solutions.

Approach

The Modern System Development Lifecycle (MSDLC) method consists of five phases: planning, analysis, design, implementation, and support (Whitten, Bentley, & Dittman, 2000). This method will be employed to implement four WLAN initiatives at

AAM. These wireless projects will serve as the subject of the case study, which is a key element of this research. Case studies are most appropriate when "how" and "why" research questions need to be answered (Yin, 1994). The AAM WLAN projects are briefly described as follows:

Wireless Connectivity in Executive Conference Rooms - Worldwide

The scope of this project will include the evaluation, selection, and implementation of 25 IEEE 802.11b wireless access points at 12 locations worldwide with 70 wireless users. These locations will be Detroit Corporate Headquarters, Detroit Gear and Axle Plant, Detroit Forge Plant, Three Rivers Driveline Plant, MSP Industries, Tech Center, Global Procurement Center, Colfor Manufacturing, Buffalo Gear and Axle Plant, Tonawanda Forge Plant, AAM de Mexico, and Albion Automotive. Once installed, WLAN access at these locations will provide the AAM executive staff with the ability to access seamlessly key management applications while they are out of the office reviewing remote plant operations. These applications will include e-mail, calendar, Factory Information System (FIS), and Enterprise Resource Planning (ERP).

AAMatHome

The scope of AAMatHome will include the evaluation, selection, and implementation of a wireless solution to be used by AAM executives and remote users to access corporate applications while wirelessly connected at home to high speed broadband Internet connections. Integral to the project will be the installation of broadband cable Internet connections along with WLANs in the homes of ten users. Six

of these users will be Information Technology Department managers and four will be AAM vice presidents. In addition, a VPN (Virtual Private Network) server and Terminal Services (TS) server will be installed on the AAM wireline network to allow users fast, secure access from the Internet to commonly used AAM applications. These applications will include Microsoft Office Pro, Microsoft Project, Microsoft Outlook, Microsoft Publisher, Microsoft Visio, Oracle Enterprise Resource Planning (ERP), and the AAM Portal.

Enhanced Wireless LAN Security

The scope of this project will include the evaluation, selection, and implementation of an enhanced wireless security solution for the AAM enterprise. This additional layer of security will offset recently discovered weaknesses in the IEEE 802.11b WEP security protocol (Borisov, Goldberg, & Wagner, 2001). The use of the WEP algorithm is not considered an adequate long term WLAN security solution for large enterprises such as AAM (Reynolds, 2001). Solutions that will be evaluated during the implementation of this project include a combination of VLAN (Virtual Local Area Network) and VPN technologies, ReefEdge Mobile VLAN, WEP Plus, IEEE 802.1x and other proprietary solutions from a host of wireless equipment manufacturers. In addition, the project will evaluate, select, and implement a tool to detect unauthorized (rogue) wireless access points that are illegally attached to the AAM network. The threat from unauthorized access points has increased significantly since the release of the wireless "hacker" tools (e.g. AirSnort) (Delio, 2001).

Wireless Connectivity on the Plant-Floor

This project will include the installation of six IEEE 802.11b wireless access points in the AAM Detroit Forge plant. The plant-floor fixed wireless LAN will connect 19 machining center CNCs (Computerized Numeric Controllers) and six PLCs (Programmable Logic Controllers). The network will be installed as a substitute for a proprietary wired Data Highway network and a wired serial RS-232 network. The intent of the project is to demonstrate that the time and cost to install wireless plant-floor LANs are significantly less than wired LANs.

The projects described above were granted full approval and funding by the Chief Information Officer (CIO) of AAM on December 12, 2001. The researcher, who is employed by AAM as Senior Technology Manager for the Information Technology Department, will serve as project manager for the projects. In addition, the projects will be implemented simultaneously using the modern SDLC method. The implementation model, which is the goal of this research, will be developed from a case study of the WLAN projects just described. The model will also be structured using the modern SDLC method.

Milestones

The major steps to accomplish the goal of this research are as follows:

1. Submitted dissertation idea paper — December 21, 2001
2. Completed project planning phase — January 18, 2002
3. Completed systems analysis phase — February 1, 2002
4. Completed systems design phase — March 1, 2002

5.	Submitted preliminary proposal	May 18, 2002
6.	Form Dissertation Committee	June 10, 2002
7.	Obtain IRB Approval	June 10, 2002
8.	Complete systems implementation phase	July 31, 2002
9.	Complete systems support phase	August 31, 2002
10.	Submit dissertation formal proposal	September 15, 2002
11.	Submit final dissertation report	March 9, 2003

Resources

The resources required to conduct this research include the following:

- Approval by AAM to conduct the case study in AAM facilities worldwide
- Funding by AAM to purchase all required hardware and software
- Assignment of select members of the AAM Information Technology staff to implement the WLAN projects discussed above
- Assignment of this researcher, AAM Senior Technology Manager, to act as project manager for the WLAN projects

The Executive Director of Information Technology/Chief Information Officer (CIO) of AAM has approved all of the above.

Summary

Companies purchasing wireless LAN technologies during 2001 surpassed analysts' expectations (Bassuener, 2001). In fact, the WLAN market is expected to grow from 3.3 million units in 2000 to 23.6 million in 2005. WLAN technologies provide

companies with many competitive advantages when properly leveraged. In the above sections, this paper described the problem to be investigated and the goal to be achieved. The problem was how large manufacturing enterprises are best able to plan, design, and implement WLAN technologies. The goal was to provide a model for those companies to deploy WLAN technologies in their offices, manufacturing facilities, and employee residences. Next, the research questions to be explored were briefly stated. Also provided was an analysis of the relevance and significance of the research along with a discussion of barriers and issues related to achieving the goal. In addition, the approach and resources to be used in accomplishing the goal were discussed. Finally, a brief summary was provided along with an annotated bibliography of the literature.

Annotated Bibliography

Andersson, C. (2001). *GPRS and 3G Wireless Applications.* New York: Wiley Computer Publishing.

The author, Manager of Special Projects and Applications at Ericsson, provided a guide through the technical issues behind the development of software applications and content for wireless devices and networks. The book was intended as an aid to software developers in optimizing their applications for wireless networks. Topics included ways of coping with intermittent radio conditions, accessing network features such as Quality of Service (QOS), and adding location dependence to an application. The text was written in three sections. The first section explained how wireless networks function and complement each other. The second section gave examples for optimizing applications for wireless networks and devices, and the third section examined the interaction between applications and other component technologies.

The text illuminated the research project with an examination of current and future wireless devices. Wireless applications are highly dependent on the devices that are available. Mobile Internet devices can be classified in two groups: integrated and divided. The integrated device concept combines the modem with the application. This is an all-in-one device that provides for most of a user's wireless needs. The divided device concept separates the modem from the application. One example is the pairing of a Bluetooth enabled cellular phone with a Bluetooth enabled personal digital assistant. Advantages of the divided concept included high flexibility and smaller device size.

Aspatore Books Staff (Ed.). (2001). *The Wireless Industry: Industry Leaders Share Their Knowledge on the Future of the Wireless Revolution*. Bedford, MA: Aspatore Books.

The authors, CEOs of companies that lead the wireless industry, shared their insights concerning the future of wireless technology. Topics covered were the future of the wireless industry, wireless devices, 3G, wireless applications, international markets, government issues, and industries most suited for wireless implementation.

The book contributed to the research project by detailing the importance of WWAN services in an enterprise wireless strategy. It is predicted that the 160 million worldwide Internet users will soon be supplemented by a second wave of wireless users. As 3G technologies are implemented worldwide, millions of existing cellular voice users will become new Internet users.

Barnes, C., Bautts, T., Lloyd, D., Ouellet, E., Posluns, J., Zendzain, D., & O;Farrell, N. (2002). *Hack Proofing Your Wireless Network*. Rockland, MA: Syngress Publishing.

The authors, IT professionals specializing in wireless networking and computer security, provided a comprehensive look at WLAN system security. The text began with an overview of current and future wireless technologies. These included IEEE 802.11, HomeRF, cellular-based wireless data, and PAN. Security concerns related to each of these were also reviewed. The text continued with an examination of common security standards and their implications for WLAN technologies. One chapter focused on wireless network architecture and design specific to fixed wireless, WLANs, PANs, and mobile wireless. Subsequent chapters discussed design methodologies, common attacks and vulnerabilities, wireless security countermeasures, intrusion detection, and auditing.

The book illuminated the research project in a number of ways. The section that discussed the creation of a wireless design methodology outlined the most critical steps in any implementation. These included creating a network plan, gathering requirements, baselining the existing network, analyzing competitive practices, initiating operations planning, and performing a gap analysis. The need for layered wireless security measures was demonstrated with real-life examples of wireless security attacks. These included WEP weaknesses, interception, spoofing, hijacking, denial of service, and malware. Finally, the text provided a number of case scenarios to aid in securing a wireless network. Fundamental to each of these was the development of a wireless security checklist.

Bates, R. (2001). *Wireless Broadband Handbook*. NY: McGraw-Hill.

The author, President of TC International Consulting, examined wireless broadband communications from a business perspective. The text was written for the CEO, CFO, or CIO and sought to answer three questions. What is it? What will it do? What is it going to cost? After a brief history of wireless, the book reported on satellite systems, microwave systems, cellular communications, Personal Communications Services (PCS), Global Services for Mobile (GSM) and data over wireless. In addition, WLANs, WWANs, 3G wireless, and wireless applications were covered. Regulatory and standards developments were also discussed.

The book illuminated the research project by exposing key business factors that enter into the formation of an enterprise wireless strategy. In addition, WLAN technology considerations were explored. These included distance from the cell, interference from other devices, power output capabilities of the mobile set, and the overall distance/speed ratio for the mobile device. One important benefit of WLAN technology was the ability to provide up to 1,000 times the data transmission rate of a WWAN network with no usage fees. Other advantages included mobility and reduced installation time, cost, and complexity.

Coyle, F. (2001). *Wireless Web: A Manager's Guide*. Boston: Addison Wesley.

The author, director of the Executive Software Engineering program at Southern Methodist University, detailed how the growth of wireless services affects the business environment. CEOs, CIOs, CTOs, and consultants were the intended

audience of the text. The book provided a brief summary of the wireless web and its benefits along with an introduction to wireless technologies, devices, and emerging standards. Wireless security frameworks that included PKI, digital certificates, and VPNs were also discussed. The author predicted a time when the term "wireless" would be replaced by "the web," one entity with wired access for high-bandwidth multimedia deliver and wireless connectivity for convenience and personalized services.

The book contributed to the research project with a discussion of the relationship between wireless and XML. XML, a data representation technology, facilitates content delivery to mobile devices and platforms. Examples of XML-based wireless initiatives are SyncML, WML, and XHTML. WAP and i-mode support for these technologies increases the importance of XML as a wireless enabler. Finally, the text presented a number of useful Internet-based wireless resource links.

Flickenger, R. (2002). *Building Wireless Community Networks* (First ed.). Sebastopol, CA: O'Reilly & Associates.

The author, a network administrator for O'Reilly & Associates, described solutions to the problem of building a wireless network for public use. The book was written for the technical user who is interested deploying IEEE 802.11b networks throughout an entire community. The text begins with a brief history of the state of public wireless networks in the United States. Examples of existing wireless community networks (e.g. neighborhoods, schools, and businesses) are given along with demonstrations of techniques and equipment necessary to interconnect wireless and wired networks. One section covered the characteristics and placement of antennas. Antenna types included omnidirectional, sector, yagi, and parabolic dish.

The book illuminated the research project with a discussion of wide area network saturation. Specifically, the text described how to extend a network's range using a variety of software and hardware tools. These included topographic mapping software to evaluate long distance links, methods of calculating the effective range of wireless equipment, and the use of specialized antennas, cables, and connectors. Particularly interesting was the section that explored the complexity and variability of point-to-point connections. A detailed list of techniques to increase link reliability was reported.

Garg, V. (2001). *Wireless Network Evolution: 2G to 3G*. Upper Saddle River, NJ: Prentice Hall.

The author, a Distinguished Member of Technical Staff at Lucent Technologies Bell Laboratories, investigated key 3G wireless standards and technical issues associated with the planning, management, and optimization of 3G systems. Specifically, the text covered 3G standards activities, 3G European and North American systems, Wireless Application Protocol and 3G systems, RF optimization techniques, and 3G data services for UTRA/W-CDMA, cdma2000,

GPRS, and EDGE networks. The intended audience of the book was telecommunications engineers and wireless system planners and decision makers. In addition, a detailed review of fundamental 2G system principles was provided along with guidance on migrating from 2G to 3G.

The book contributed to the research paper by providing a basis from which to evaluate the role of 3G systems in an enterprise wireless strategy. In addition, one chapter examined Wireless Application Protocol (WAP), Bluetooth, and WLANs. WAP, for example, specifies a microbrowser that employs the new Wireless Markup Language standard which is optimized for mobile handhelds. The broad industry acceptance and interoperability of these technologies promotes the use of affordable, high-speed wireless solutions in the home, small business, and enterprise markets. IEEE 802.11b is an excellent example of this.

Geier, J. (1999). *Wireless LANs: Implementing Interoperable Networks.* USA: Macmillan Technical Publishing.

The author, an electrical engineer specializing in computer networking, provided information on how to plan, configure, and implement wireless networks. The book was written for network engineers, designers, and architects. Subject areas included migrating from proprietary to IEEE 802.11 solutions, interoperability between new and existing wired and wireless infrastructures, common network problems, wireless data collection systems, and the reduced cost of wireless deployments. In addition, the text detailed the primary WLAN applications, the features and functionality of the IEEE 802.11 standard, the selection of a spread spectrum type, and the migration to 2.4 GHz networks.

The text contributed to the research paper with a detailed discussion of WLAN deployment. This included wireless system integration, planning, and implementation. In addition, wireless case studies were reported throughout the text to further understanding. These included the use of a wireless system for disaster recovery, the installation of a wireless bar code system, the development of the project scope for a warehousing system, and the implementation of higher-capacity WLANs. Also reported were studies that showed the problems with mixed standards and how to increase efficiency and reduce paperwork with a wireless network.

Geier, J. (2001). *Wireless LANs: Implementing High Performance IEEE 802.11 Networks* (Second ed.). Indianapolis, Indiana: Sams Publishing.

The author, an independent consultant specializing in the development of wireless network products and the integration of wireless networks, provided an overview of wireless network technologies. Emphasis was placed on WLANs employing IEEE 802.11 standards. The book's intended audience included engineers developing WLAN solutions, managers planning and executing wireless projects, and information systems staff. The text began by explaining the concepts, benefits, and issues related to wireless networking. Next, the IEEE 802.11 medium access control and physical layers were detailed. The book continued by

reporting on the deployment of WLANs. This included wireless system integration, and WLAN planning and implementation.

The book contributed to the research project with an in depth discussion of wireless project planning and implementation. Topic areas included requirements and feasibility analysis, network design and installation, and operational support of the network. Also included were relevant case studies of wireless deployments. They illustrated the process of designing a WLAN system, developing a wireless system, and preparing for WLAN operational support in a variety of enterprises.

Lin, Y., & Chlamtac, I. (2001). *Wireless and Mobile Network Architectures*. New York: Wiley Computer Publishing.

The authors, professors at the University of Taiwan and the University of Texas, approached the topic of wireless and mobile network architectures from the perspective of networks, systems, and services. Network engineers and managers were the intended audience of the text. The book began with brief summary of radio technology, which was followed by a detailed discussion of ANSI 41 mobile network protocols, GSM Mobile Application Part (MAP), SS7, ISDN, and AIN. The text also described mobile services that included mobile database overflow, failure restoration, number portability, prepaid service, international roaming, and wireless application protocol. Advanced industrial developments in PCS technology were reported.

The text illuminated the research project with a discussion of wireless handheld operating systems. These operating systems are needed to support the functionality required by 3G handsets and include Windows CE, EPOS, PalmOS, and Linux. Unlike the personal computer, it is unlikely that a single wireless operating system will become the standard in the near future. Key operating system and handset design criteria include capability, portability, battery life, cost, and performance. Finally, handheld operating systems must be able to support advance user interfaces (e.g. voice and handwriting recognition technologies).

Nichols, R., & Lekkas, P. (2002). *Wireless Security: Models, Threats, and Solutions*. New York: McGraw Hill.

The authors, CTOs of prominent security technology firms, provided a comprehensive view of wireless security technologies, techniques, and methodologies. The intended audience of the text included managers, policy makers, and IT professionals responsible to protect wireless information assets. The book covered four topic areas: wireless threats, cryptographic countermeasures, application solutions, and hardware solutions. Wireless threats to air-to-ground interfaces and telephone and satellite system vulnerabilities are also examined. In addition, advanced encryption technologies that included stream ciphers, elliptic curve cryptography, Rijndael, and the advanced encryption standard were discussed relative to their ability to protect wireless communications.

The book contributed to the research paper with a discussion of the security principles and flaws of WLANs, WAP, TLS, Bluetooth, and VOIP. Two schools of thought relating to the implementation of wireless device security were examined. One was based on hardware and the other on software. While software techniques were considered legitimate and convenient, they were shown to be insecure in many cases and to offer poor performance in streaming bit traffic. However, hardware-based solutions consistently delivered the performance needed to authenticate and encrypt wireless connections in real-time.

O'Hara, B., & Petrick, A. (1999). *IEEE 802.11 Handbook: A Designer's Companion*. NY: IEEE Press.

The authors used their experience, gained from many years of contributing to the IEEE 802.11 standard, to assist readers in navigating through the standard's complexity and to focus on core issues. The intended audience of the text included individuals developing IEEE 802.11 products and those simply wishing to gain a better understanding of the standard. The standard (400 pages when originally published in 1997) was the first international standard for WLANs. Topics covered in the text included Medium Access Control (MAC) functionality, management, and attributes. In addition, subject areas related to IEEE 802.11 physical layer functionality and modulation methods were covered in detail. Physical layer extensions such as IEEE 802.11a were also discussed.

The book contributed most to the research project with a chapter that focused on IEEE 802.11 system design considerations. One issue affecting the implementation of an interoperable WLAN system is the RF communication media. The media employed for home, enterprise, and manufacturing WLANs is often quite different. Diverse multipath and path loss properties must be considered when designing for these three environments. Finally, the difference between data rate and aggregate throughput in wireless environments was discussed along with the concept of antenna diversity and the site survey.

Rappaport, T. (2002). *Wireless Communications: Principles and Practice* (Second ed.). Upper Saddle River, NJ: Prentice Hall.

The author, a professor of Electrical and Computer Engineering at Virginia Polytechnic Institute, covered issues basic to all wireless networks. The book began with an informative history of wireless communications in the United States and the rest of the world. Also, included in the text were a comprehensive set of reviews of current wireless standards and technology. Wireless local area networks and 3G systems were covered in detail along with the fundamentals of voice, data, cordless, paging, fixed broadband, and mobile broadband wireless technologies. In addition, the book discussed such design fundamentals as trunking efficiency, channel assignment, capacity planning, and large-scale fading. Modulation, diversity, and coding technologies were also enumerated.

The text contributed to the research by providing in-depth explanations of project related wireless technologies. These included IEEE 802.11a/g, HIPERLAN,

BRAN, Bluetooth, fixed wireless, and Local Multipoint Distribution Service (LMDS). The chapter on wireless networking was particularly relevant with its coverage of first, second, and third generation wireless networks along with the new 3G interface standards: cdma2000, EDGE, GPRS, UMTS, and W-CDMA.

Santamaria, A., & Lopez-Hernandez, F. (Eds.). (2001). *Wireless LAN Standards and Applications*. Norwood, MA: Artech House.

The authors, professors of engineering at the University of Madrid, provided a review of existing WLAN standards. These included IEEE 802.11, IrDA, and HIPERLAN. In addition, the roles of wireless technologies in transportation, personal communications, the office, and the home were examined. The book began with a detailed description of the IrDA standard. Topics included exploring the physical layer, serial infrared link access protocol, and IrDA link management protocol. The text then proceeded to discuss the specifics of the IEEE 802.11 standard. Included were the physical layers of IEEE 802.11 radio and infrared systems. Next, the European HIPERLAN standard was explained. HIPERLAN is a high performance WLAN in which all nodes use a single shared communications channel. The standard operates in the 5 GHz band and has bit rates of 23 Mbps.

The text illuminated the research project with a description of different wireless application scenarios. These included installations in schools, hospitals, courtrooms, train stations, airports, businesses, homes, and industrial facilities. This was followed with a review of organizations involved in the development and commercialization of wireless devices. These included WLANA, WECA, Bluetooth SIG, WLIF, Home RF, and BWIF. Finally, the book looked into the future of HIPERLAN, IEEE 802.11, DECT, Bluetooth, WATM, and HomeRF.

Sbihli, S. (2002). *Developing a Successful Wireless Enterprise Strategy*. New York: Wiley Computer Publishing.

The author, cofounder and Chief Technical Officer of Mobile Design Technologies, provided a comprehensive strategy for the deployment of wireless applications, security, middleware, handhelds, and networks. The book was written for a number of audiences. Discussions on wireless strategy, process, and deployment were most appropriate for Chief Information Officers (CIOs) and IT directors while the sections that covered architecture and technology tools were directed at IT project managers. The text began by describing the business drivers for wireless solutions. This was followed by a discussion of the impact of wireless technologies on a company's business processes and the return on investment of wireless projects. The basic architecture of all wireless solutions was also covered. Included were devices, networks, wireline synchronization, synchronization servers, databases, and security.

The text contributed to the research project with a chapter that detailed the costs associated with wireless and handheld computing. These included project, wireless data, consulting services, and middleware expenditures. Two chapters

were dedicated to wireless case studies. The first explored a large-scale wireless implementation of a business-to-business dot-com. The second reported on a healthcare application for capturing the medical costs at the time and location they occurred. Finally, the text presented short- and long-term forecasts for the wireless industry. Some of the technologies evaluated were device convergence, XML, MPEG-4, biometrics, Bluetooth, voice recognition, and third generation wireless.

Skoudis, E. (2001). *Counter Hack*. Upper Saddle River, NJ: Prentice Hall.

The author, Vice President of a leading independent infrastructure consulting firm, illustrated how computer network attacks are conducted and methods to defend against them. The intended audience of the text included system administrators, security personnel, and network administrators. The book began by focusing on the different categories of tools commonly used by computer attackers. In addition, end-to-end attack sequences were presented. This highlighted the phased approach of many attacks. Typical phases included reconnaissance, scanning, gaining and maintaining access, and removing traces of the attack. The book also described how sophisticated attackers combine attack tools to create new and complex assaults. Analogies are used throughout the text to highlight how the technologies work.

The text contributed to the research project by illustrating the importance of security when implementing WLANs. Attackers are able to expose fundamental weaknesses in a network's architecture using sniffers, spoofers, and session hijackers. These tools are powerful and able to undermine Transport, Network, and Data Link layer capabilities. Finally, the text recommended a number of Web sites that monitor advances in the tools and techniques used to attack computer networks. These included Security Focus, Security Portal, and Bugtraq.

Wang, J. (2001). *Broadband Wireless Communications: 3G, 4G, and Wireless LAN*. Boston: Kluwer Academic Publishers.

The author, an Associate Professor at the University of Hong Kong, presented a research and development perspective of wireless broadband communications. Individuals with a thorough understanding of digital communications and spread spectrum/CDMA were the intended audience. The text described recent research developments in the field and identified areas that required further research. These included 3G mobile communications, wideband CDMA, multicode CDMA, advanced loop tracking, CDMA overlay, and adaptive filtering. Open loop power control, closed loop power control, wireless frequency hopping, and 4G mobile communications were also discussed.

The book contributed to the research project with a chapter that explored 4G mobile communications. 3G mobile systems are currently being deployed worldwide. They will be able to provide multimedia services with data rates up to 2 Mbps. 4G systems are forecasted to deliver 20 Mbps by the year 2020. However, extensive international research and development and standardization

will be required to make this a reality. For example, the cell radius of 4G cellular systems must be small (i.e. 20 to 30 meters). Therefore, multiple access techniques will be required to provide capacity and high data rates. A combination of OFDM and CDMA technologies is one possible technique.

Webb, W. (2001). *The Future of Wireless Communications*. Norwood, MA: Artech House.

The author, Director of Strategy at Motorola, forecasted the changes in mobile communications over the next 20 years. Professionals responsible to develop wireless strategies were the intended audience of the book. The book identified key technical constraints. These included bandwidth scarcity, battery power scarcity, Shannon's law, limited capacity per cell, cell management complexity, and the high probability of a capacity increase of three times per cell over the next 20 years. In addition, the effect of standards, regulatory issues, spectrum, and internal funding were projected.

The text illuminated the research project by predicting the integration of home and office wireless networks with the mobile communications device. In addition, it is expected for WLAN coverage in hotels and public buildings not to become ubiquitous until 2015 - 2020. WLANs will not be widely deployed in dense urban areas until sometime after 2005. Finally, data rate requirements will increase from 10 Mbps to 60 Mps by 2020.

Wheat, J., Hiser, R., Tucker, J., Neely, A., & McCullough, A. (2001). *Designing a Wireless Network*. Rockland, MA: Syngress Publishing.

The authors, wireless technology professionals at Lucent Technologies, discussed a number of wireless communication topics. These included a history of wireless communications, the physics behind the technology, the components of a wireless network, the Open Systems Interconnection Reference Model, available wireless technologies, and methodologies used to design and implement a wireless network. Four functional wireless areas were identified: fixed wireless, mobile wireless, wireless LANs and PANs, and optical technologies. In addition, the text's emphasis was on WLANs and their widespread use at work and in the home.

The book illuminated the research project by enumerating the design methodologies employed by the Lucent Technologies Professional Services Division. These included exploring the design process, identifying the design methodology, developing a network architecture, formalizing the detailed design phase, and understanding wireless network attributes. Finally, the last four chapters of the text detailed case studies of fictional wireless projects based upon the authors' experience. The case studies discussed wireless design projects in industrial, hospital, college, and home environments.

Yin, R. (1994). *Case Study Research: Design and Methods* (Second ed.). Thousand Oaks, California: Sage Publications.

The author, President of COSMOS Corporation - a research technology company specializing in social policy problems, detailed the distinctive characteristics of the case study strategy in comparison to other types of research. The object of the book was to guide anyone trying to employ case studies as a rigorous method of research. After introducing case studies, the text provided a general approach for designing and conducting case studies. This included criteria for judging the quality of research designs and the case study protocol. In addition, strategies for analyzing case study evidence and for composing a case study report were discussed.

The text illuminated the dissertation topic by providing recommendations and examples for designing, conducting, analyzing, and reporting a case study. For example, research questions that focus on "how" and "why" are most appropriate for case studies. Also, defining the research questions is probably the most important step in conducting a research study. Valid research questions must have both substance and form. Finally, exemplary case studies have five basic characteristics. They must be significant, complete, consider alternative perspectives, display sufficient evidence, and be composed in an engaging manner.

Appendix A

Dissertation Topic Approval Letter from American Axle and Manufacturing

From: Wolak, Ronald

Sent: Wednesday, December 12, 2001 8:47 AM

To: Shanti, Abdallah

Subject: Ph.D. Dissertation Topic Approval

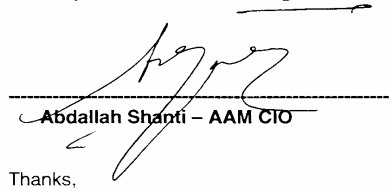
Importance: High

Hi Abdallah:

I am back from University training. While there, I met with my Ph.D. dissertation advisor, Dr. Marlyn Littman, and she recommended (per Nova Southeastern University guidelines) that I obtain your written permission to conduct the case study which is integral to my dissertation paper. My dissertation is titled "Wireless LAN Technologies: A Model for Planning, Designing, and Implementing in a Global Manufacturing Enterprise." The paper will use the case study method and will describe the implementation of wireless LAN technologies at American Axle and Manufacturing (AAM). The case study will consist of the following four approved and funded project components for which I am project manager:

1. **Enterprise-wide Wireless Connectivity in Executive Conference Rooms**
   Project scope includes the installation of 25 IEEE 802.11b wireless access points at 10 locations worldwide with 70 WLAN users.
2. **AAM@Home Elite**
   Project scope includes the evaluation, selection, and implementation of a wireless solution to be used by AAM executives and remote users to access corporate applications while wirelessly connected at home to high speed broadband Internet connections. Integral to the project is the installation of a wireless network in each home in addition to a VPN server and Terminal Services server on the AAM network to allow users fast, secure access to commonly used applications. These applications will include Microsoft Office Pro, Microsoft Project, Microsoft Outlook e-mail, Microsoft Visio, Oracle Enterprise Resource Planning (ERP), and the AAM Portal.
3. **Enhanced Wireless LAN Security**
   Project scope includes the evaluation, selection, and implementation of an enhanced wireless security solution for the AAM enterprise. Weaknesses in the existing IEEE 802.11b WEP security standard have driven the need for an added layer of security for a large enterprise such as AAM. Solutions under consideration include a combination of VLAN and VPN technologies, ReefEdge Mobile VLAN, WEPPlus, and other proprietary solutions from a host of wireless equipment manufacturers. In addition, the project will evaluate, select, and implement a method for AAM to detect non-approved (rogue) wireless access point illegally attached to the AAM network.
4. **Wireless Connectivity on the Plant Floor**
   Project scope includes the installation of 6 IEEE 802.11b wireless access points in the AAM Detroit Forge plant. The plant floor wireless network will connect 19 machining center CNCs (Computerized Numeric Controllers and 6 PLCs (Programmable Logic Controllers) – substituting for a proprietary wired Data Highway network and a wired serial RS232C network.

Please print this e-mail and sign below indicating your approval:



Abdallah Shanti – AAM CIO

12/12/2001

Date

Thanks,
Ron

Reference List

AAM. (2001). AAM: Company Profile. *American Axle and Manufacturing*. Retrieved December 9, 2001, from the World Wide Web: http://www.aam.com/about/about_profile.html.

Armyros, S. (1992). On the behavior of Ethernet: Are existing analytic models adequate? *Journal of the Computer Systems Research Institute, CSRI-259*, 1-107.

Bassuener, K. (2001). Market For Business Wireless LAN Exceeds Expectations. *Wireless Week*. Retrieved December 18, 2001, from the World Wide Web: http://www.wirelessweek.com/index.asp?layout=print_page&doc_id=59318.

Bates, R. (2001). *Wireless Broadband Handbook*. NY: McGraw-Hill.

Batista, E. (2000). FCC: HomeRF gets up to speed. *Wired News.* Retrieved May 9, 2002, from the World Wide Web: www.wired.com/news/technology/0,1282,38564,00.html.

Blackwell, G. (2001). Assessing Total Cost of Ownership. *802.11 Planet*. Retrieved December 17, 2001, from the World Wide Web: http://www.80211-planet.com/columns/article/0,4000,1781_917751,00.html.

Borisov, N., Goldberg, I., & Wagner, D. (2001). Security of the WEP Algorithm. *University of California - Berkeley*. Retrieved December 19, 2001, from the World Wide Web: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html.

Bourin, B. (2001). High Performance Radio Mobility in LANs. *ETSI*. Retrieved December 20, 2001, from the World Wide Web: http://www.etsi.org/literature/aa_oldtokeep/stateart/bourin.htm.

Brewin, B. (2001). New Wireless LAN Standard Receives IEEE Approval. *Computerworld*. Retrieved December 21, 2001, from the World Wide Web: http://www.computerworld.com/itresources/rcstory/0,4167,STO66052_KEY68,00.html.

Caswell, W. (2001). Which standard is better for teleworkers: Wi-Fi or HomeRF? *Network World*. Retrieved May 9, 2002, from the World Wide Web: www.nwfusion.com/forum/2001/0409faceoffhomerf.html.

Curl, D. (2001). Finding The Way Forward In Wireless Technologies. *GlobalTechnoScan.com*. Retrieved December 20, 2001, from the World Wide Web: http://www.globaltechnoscan.com/21stFeb-27thFeb01/wireless.htm.

Delio, M. (2001). Wireless Networks in Big Trouble. *Wired News.* Retrieved December 19, 2001, from the World Wide Web: http://www.wired.com/news/print/0,1294,46187,00.html.

Fluhrer, S., Mantin, I., & Shamir, A. (2001). *Weaknesses in the key scheduling algorithm of RC4.* Paper presented at the Selected Areas in Cryptography Conference (SAC 2001), Toronto.

Freedman, A. (2002). *Computer Desktop Encyclopedia* (Vol. 15.2). Point Pleasant, PA: The Computer Language Company.

Garg, V. (2001). *Wireless Network Evolution: 2G to 3G*. Upper Saddle River, NJ: Prentice Hall.

Geier, J. (1999). *Wireless LANs: Implementing Interoperable Networks.* USA: Macmillan Technical Publishing.

Geier, J. (2001). *Wireless LANs: Implementing High Performance IEEE 802.11 Networks* (Second ed.). Indianapolis, Indiana: Sams Publishing.

Hannon, J. (2001). *Comprehensive solutions for securing and managing the wireless LAN*. Fort Lee, NJ: ReefEdge.

Intel Staff. (2001). IEEE 802.11b High Rate Wireless Local Area Networks. *Intel*. Retrieved December 21, 2001, from the World Wide Web: http://www.intel.com/network/documents/pdf/wireless_lan.pdf.

Jensen, M. (1999). A guide to using low-cost radio communication systems for telecommunication in developing countires - An African perspective. *International Research Development Centre*. Retrieved May 9, 2002, from the World Wide Web: www.idrc.ca/acacia/03866/wireless.

Krazit, T. (2001). Study: Wireless Networking Unchained in 2001. *Computerworld*. Retrieved December 21, 2001, from the World Wide Web: http://www.computerworld.com/itresources/rcstory/0,4167,STO66413_KEY68,00.html.

Leeper, D. (2001, June, 2001). A long-term view of short-range wireless. *IEEE Computer, 34*, 39-44.

MSI Editors. (2001). The Wireless Wave. *MSI*. Retrieved December 17, 2001, from the World Wide Web: http://www.manufacturingsystems.com/archives/2001/apr/ms0401f7.asp.

O'Hara, B., & Petrick, A. (1999). *IEEE 802.11 Handbook: A Designer's Companion*. NY: IEEE Press.

Ohmori, S., Yamao, Y., & Nakajima, N. (2000). The future generations of mobile communications based on broadband access technologies. *IEEE Communications*.

Orenstein. (2001). Microsoft's Wireless Road Ahead. *Business 2.0*. Retrieved December 17, 2001, from the World Wide Web: http://www.business2.com/articles/web/print/0,1650,36308,FF.html.

Paulson, L. D. (2002, May, 2002). US approves new uses for wireless technology. *IEEE Computer, 35*, 27.

Perez-Jimenez, R., Riera, J., & Lopez-Hernandez, F. (2001). The IEEE 802.11 Standard. In A. Santamaria & F. Lopez-Hernandez (Eds.), *Wireless LAN Standards and Applications* (pp. 45-107). Norwood, MA: Artech House.

Prasad, A., Kamerman, A., & Moelard, H. (2001). IEEE 802.11 Standard. In N. Prasad & A. Prasad (Eds.), *WLAN Systems and Wireless IP for Next Generation Communications* (pp. 77-126). Boston, MA: Artech House.

Prasad, N., & Prasad, A. (2001a). Wireless Networking and Internet Access Standards. In N. Prasad & A. Prasad (Eds.), *WLAN Systems and Wireless IP for Next Generation Communications* (pp. 25-75). Boston, MA: Artech House.

Prasad, N., & Prasad, A. (2001b). WLAN Systems - Introduction. In N. Prasad & A. Prasad (Eds.), *WLAN Systems and Wireless IP for Next Generation Communications* (pp. 1-24). Boston, MA: Artech House.

Railsback, K. (2001). Strategy: Building a wireless infrastructure. *InfoWorld*. Retrieved May 18, 2002, from the World Wide Web: http://www.infoworld.com/articles/tc/xml/01/05/07/010507tctcap.xml.

Rappaport, T. (2002). *Wireless Communications: Principles and Practice* (Second ed.). Upper Saddle River, NJ: Prentice Hall.

Reynolds, M. (2001). What's up with WEP? *Gartner.com, HARD-WW-DP-0093*.

Riera, J., & Perez-Jimenez, R. (2001). Upcoming Standards and Future Trends. In A. Santamaria & F. Lopez-Hernandez (Eds.), *Wireless LAN Standards and Applications* (pp. 9-44). Norwood, MA: Artech House.

Sage Research Staff. (2001). Wireless LANs: Improving Productivity and Quality of Life. *Sage Research*. Retrieved December 1, 2001, from the World Wide Web: http://newsroom.cisco.com/dlls/sage_report.pdf.

Santamaria, A., Vento-Alvarez, J., Rabadan, J., & Perez-Jimenez, R. (2001). The IrDA Standard. In A. Santamaria & F. Lopez-Hernandez (Eds.), *Wireless LAN Standards and Applications* (pp. 9-44). Norwood, MA: Artech House.

Staff, I. R. (2001). Wireless 802.11 Security in a Corporate Environment. *Intel Corporation*. Retrieved December 1, 2001, from the World Wide Web: http://www.intel.com/ebusiness/products/related_mobile/wp012602.htm.

Wheat, J., Hiser, R., Tucker, J., Neely, A., & McCullough, A. (2001). *Designing a Wireless Network*. Rockland, MA: Syngress Publishing.

Whitten, J., Bentley, L., & Dittman, K. (2000). *Systems Analysis and Design* (Fifth ed.). NY: McGraw-Hill Higher Education.

Yin, R. (1994). *Case Study Research: Design and Methods* (Second ed.). Thousand Oaks, California: Sage Publications.