

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

by

Ronald G. Wolak

A formal 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

December 2002

An Abstract of a Formal 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 a WLAN Solution in a Global Manufacturing Enterprise

by
Ronald G. Wolak

December 2002

The formal dissertation proposal that follows was submitted to partially fulfill the requirements for the degree of Doctor of Philosophy. Wireless Local Area Networks (WLANs) have the potential to improve the flexibility, productivity, and work environment of employees in an enterprise. While WLAN technologies offer the benefits of mobility, reduced installation time, and decreased cost, many challenges must be met by the companies deploying them. These issues are related to security, speed, interoperability, equipment selection, ease of use, reliability, signal interference, and installation. The proposed research addresses a problem confronting many large manufacturing companies in the present-day environment. This problem is how to effectively plan, design, and implement WLAN technologies. The goal of the research is to provide large manufacturing enterprises a model for deploying secure WLAN technologies in offices, manufacturing facilities, and employee residences. The model will be developed from a case study of WLAN projects to be implemented at American Axle and Manufacturing (AAM). Four WLAN initiatives are the subject of the case study: Wireless Connectivity in Executive Conference Rooms, AAMatHome, Enhanced WLAN Security, and Wireless Connectivity on the Plant-Floor.

Table of Contents

Abstract ii

Chapters

1. Introduction 1

Problem Statement and Goal 2
Relevance and Significance 6
Barriers and Issues 9
Research Questions 10
Limitations and Delimitations 11
Definition of Terms 12
Summary 33

2. Review of Literature 34

Historical Overview 34
Wireless LAN Technologies 36
 Ultra High Frequency (UHF) Narrowband 36
 Spread Spectrum 37
 Direct Sequence Spread Spectrum (DSSS) 38
 Frequency Hopping Spread Spectrum (FHSS) 38
 Orthogonal Frequency Division Multiplexing (OFDM) 39
 Spread Spectrum Interference 39
 Ultrawideband (UWB) 40
 Infrared 41
Wireless LAN Standards and Wireless Standards Associations 42
 IEEE 802.11 42
 IEEE 802.11b 43
 IEEE 802.11a 45
 IEEE 802.11g 46
 IEEE 802.11x 46
 European Telecommunications Standards Institute (ETSI) 47
 High Performance Radio Local Area Network-Type 1 (HiperLAN-1) 48
 High Performance Radio Local Area Network-Type 2 (HiperLAN-2) 48
 HiperACCESS and HiperLINK 49
 Japan Ministry of Post and Telecom (MPT) Multimedia Mobile Access
 Communication (MMAC) Committee 50
 HomeRF Working Group 51
 HomeRF 1.0 51
 HomeRF 2.0 52
 Infrared Data Association (IrDA) 52
Wireless LAN Security 54

IEEE 802.11 Security Vulnerabilities	55
Wireless LAN Security Enhancements	59
Wireless LAN Health and Safety Considerations	61
Wireless LAN Initiatives in the Corporate Arena	63
General Motors	63
Intel	64
Office Depot	64
Corrugated Supplies Company	65
Wireless LAN Vendor Offerings	65
Wireless LAN Service Providers	67
Wireless LAN Strategy	69
Summary of Knowns and Unknowns	71
Contribution to the Field	72
Summary	72
3. Methodology	74
Research Method to Be Employed	74
Case Study	75
Modern Systems Development Life Cycle (MSDLC)	77
Audience	79
Specific Procedures to Be Employed	79
AAM Wireless LAN Initiatives	79
Wireless Connectivity in Executive Conference Rooms	80
AAMatHome	83
Enhanced Wireless LAN Security	86
Wireless Connectivity on the Plant-Floor	89
Case Study	92
Design	93
Date Gathering	95
Evidence Analysis	96
Formats for Presenting Results	97
Projected Outcomes	98
Resource Requirements	98
Reliability and Validity	98
Summary	99
4. Expectations	100
Anticipated Benefits	100
Projected Outcomes	100
Practical Applications of the Findings	100
Constraints and Limitations of the Study	101
Recommendations for Additional Studies	102
Contributions to the Field	102
Annotated Bibliography	104

Appendixes

A. Dissertation Topic Approval Letter from AAM 129

Reference List 130

Chapter 1

Introduction

Wireless Local Area Networks (WLANs) have the potential to improve the flexibility, productivity, and work environment of employees in an enterprise ("*Wireless LANs*," 2001). American Axle and Manufacturing (AAM) is typical of a large manufacturing company. Headquartered in Detroit, Michigan, AAM is a tier one supplier of automotive driveline systems (Manardo, 2001a). 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 7 million square feet of manufacturing space in 17 manufacturing facilities located in the United States, Brazil, Mexico, and the United Kingdom.

AAM's Local Area Network (LAN) is based on air-blown multimode optical fiber (Blair, 2002). Employees at AAM locations worldwide connect to the AAM network infrastructure via wired ports interlinked to the fiber optic backbone. The wireline LAN technologies employed by AAM include 10 Megabits per second (Mbps) Ethernet and 100 Mbps Fast Ethernet at each desktop. These Ethernet ports are switch connected to an Asynchronous Transfer Mode (ATM) fiber optic backbone.

Remote facilities connect to the AAM network via switched Frame Relay services along with Internet-based Virtual Private Network (VPN) links (Blair, 2002). AAM's in-place wireline network 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 than their offices. In addition, the effectiveness of remote employees is limited by the slow speed of present-day dial-up modem connections.

In the following sections, the problem to be investigated and the goal to be achieved in this dissertation study are described. Also provided are an analysis of the relevance and significance of the research and a discussion of barriers and issues related to achieving the goal. Next, the research questions to be explored are briefly stated, and definitions of key terms used throughout the paper are provided. Finally, the limitations and delimitations of the research are provided along with a short summary.

Problem Statement and Goal

The proposed research will address a problem confronting many large manufacturing companies in the present-day environment, specifically, how to effectively plan, design, and implement WLAN technologies (Dulaney, 2002; Geier, 1999; Rogak, 2001; Sbihli, 2002). While WLAN technologies offer the benefits of mobility, reduced installation time, and decreased cost, major challenges must be met by the companies deploying them (Geier, 2001). These issues are related to security, speed, interoperability, equipment selection, ease of use, reliability, signal interference, and installation.

Rapidly emerging WLAN standards are making it difficult for business organizations to choose the right technology when deploying WLAN solutions (Railsback, 2001). This is further complicated for manufacturing enterprises such as AAM where networks in plant-floor environments are combined with configurations in office and residential settings. WLAN technologies must, by design, interface with all areas of AAM's network infrastructure. This makes interoperability a necessity.

AAM's in-place wireline technologies are of limited effectiveness in connecting employees while at work and at home to the AAM network (Blair, 2002). The company'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 ("*Wireless LANs*," 2001).

By contrast, the way Microsoft employees interact at work is dramatically affected by the company's installation of Institute for Electrical and Electronic Engineers (IEEE) 802.11b WLANs (Orenstein, 2001a). Microsoft employees no longer attend virtual meetings via desktop videoconferences at the workplace. Instead, they go to a real meeting place and bring their offices with them by wirelessly connecting their laptops to corporate Information Technology (IT) resources.

Large manufacturing enterprises must also consider the cost and time required to install and operate wireline networks in office and production facilities (Blackwell, 2001). 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. 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 (Blair, 2002). 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 than a wireline installation in this environment since plant-floor LAN cabling is frequently removed or relocated in reaction to changing manufacturing process requirements.

The limitations of the AAM wireline network also affect networking activities in AAM employee residences (Blair, 2002). 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 Office/Home Office (SOHO) venues.

Alternatives include wireline and wireless broadband residential access solutions such as cable modem, Local Multipoint Distribution System (LMDS), Multichannel Multipoint Distribution System (MMDS), Very Small Aperture Terminal (VSAT), and Digital Subscriber Line (DSL) technologies (Littman, 2002). However, LMDS and MMDS services are not available in AAM residential areas. While VSAT, Digital Subscriber Line (DSL), and cable modem services are available in AAM residential areas, these services cannot be securely connected to AAM's in-place network infrastructure (Blair, 2002).

Companies such as Honeywell, General Motors, and Intel were quick to embrace WLAN technologies and applied a strategic rather than a tactical approach to company

deployments (Moozakis, 2001; "*Honeywell goes*," 2002; "*Wireless 802.11*," 2001).

Honeywell, for example, has a vision and strategy for corporate digitization based on wireless infrastructure ("*Honeywell goes*," 2002). The company is aggressively deploying WLAN technologies to increase productivity and reduce costs.

In contrast, other companies including Allina Health System, Andersen Cancer Center, and Best Buy reconsidered planned wireless initiatives in light of security inadequacies, changing standards, and equipment interoperability issues (Brewin, 2001b; Lipschultz, 2001; Smith, 2002). Allina, for example, originally planned a full-scale implementation of WLAN technologies throughout company medical facilities. However, security issues forced the company to reconsider the plan. To minimize such cancellations or delays, WLAN suppliers now emphasize that the implementation of wireless technologies must be part of an overall wireless strategy ("*The wireless wave*," 2001). An enterprise wireless strategy minimizes the existence of multiple standards, devices, and applications and allows a company to leverage investments and create tangible business value (Sbihli, 2002).

The goal of this research is to provide large manufacturing enterprises with a model for deploying secure WLAN technologies in offices, manufacturing facilities, and employee residences. The approach will be to develop the model from previous research literature, the Modern Systems Development Life Cycle (MSDLC) strategy defined by Whitten, Bentley, and Barlow (1994), and the results of a case study of AAM WLAN initiatives.

Relevance and Significance

WLANs are beginning to replace traditional wired LANs as the preferred approach to the “last ten feet” of enterprise network environments (Singhal, 2001, p. 1). 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 ("*IEEE 802.11b*," 2001). Low cost, high-speed, interoperable products provide corporate personnel the flexibility to wirelessly transfer large data files, access the Internet, videoconference, and rapidly reconfigure networked sites. WLANs also increase productivity by encouraging greater collaboration among employees (Singhal, 2001).

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 the allotted spectrum into discrete pieces as with UHF narrowband (Garg, 2001). The Institute of Electrical and Electronic Engineers (IEEE) 802.11 family of standards that are based on Ethernet technology employ spread spectrum solutions.

The IEEE 802.11 specification and extensions provide the framework for broadband Fixed Wireless Access (FWA) LAN implementations (Littman, 2002). IEEE 802.11 extensions include IEEE 802.11a, IEEE 802.11b, and the recently approved first draft of IEEE 802.11g (Krazit, 2001). IEEE 802.11-compliant WLAN systems provide 1 Mbps or 2 Mbps transmission in the 2.4 gigahertz (GHz) band using either Frequency Hopping Spread Spectrum (FHSS) or Direct Sequence Spread Spectrum (DSSS) modulation

techniques (O'Hara & Petrick, 1999). IEEE 802.11b-compliant WLAN solutions deliver data rates up to 11 Mbps. IEEE 802.11a-compliant WLAN solutions provide data rates up to 54 Mbps in the 5 GHz band, and IEEE 802.11g-compliant WLAN solutions deliver data rates up to 54 Mbps in the 2.4 GHz band.

Bluetooth is an evolving third-generation specification that provides the framework for Wireless Personal Area Network (WPAN) implementations (Littman, 2002). Bluetooth solutions employ FHSS technology to eliminate signal interference, Time-division Duplexing (TDD) for modulation, and Forward Error Correction (FEC) to limit the effects of random noise. Bluetooth WPANs are short-range, low-power, rapidly deployed, and capable of data rates up to 720 Kbps in the 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, 2001a). WLANs that conform to IEEE 802.11b standard are the most prevalent. IEEE 802.11b-compliant WLANs support network operations 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 ("*IEEE 802.11b*," 2001). 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. However, as widespread deployment of WLAN technologies continues, companies must ensure that wireless networks integrate with wireline networks to form a seamless infrastructure.

The model for the deployment of WLAN solutions based on outcomes from this inquiry will facilitate the WLAN implementation process in large manufacturing companies. This research will contribute to the body of knowledge and improve professional practice by employing a MSDLC approach (Whitten, Bentley, & Barlow, 1994). The MSDLC approach will contribute to the development of a WLAN model to plan, analyze, design, implement, and support enterprise wireless initiatives. In addition, this model will be based on previous research literature and real life lessons drawn from a case study of AAM WLAN projects (Yin, 1994).

In terms of the MSDLC, Phase 1 or the Systems Planning Phase will identify and prioritize wireless technologies and applications that can provide the greatest return on investment to a large manufacturing company such as AAM (Whitten et al., 1994). Activities performed in Phase 1 include specifying the business mission, defining an information architecture, and evaluating business areas. Phase 2 or the Systems Analysis Phase will study current company networks and define the user requirements and priorities for the WLAN. Phase 2 is made up of three basic activities: surveying project feasibility, analyzing current infrastructures, and defining and prioritizing user requirements.

Phase 3 or the Systems Design Phase of the process will include the evaluation of different wireless systems and the specification of a detailed WLAN solution (Whitten et al., 1994). The criteria for evaluating WLAN effectiveness in terms of business requirements will include performance, manageability, and cost (Molta & Laxminarayanan, 2002). In addition, factors such as interoperability, reliability, scalability, ease of deployment, ability to upgrade, industry compliance, power

consumption, and VPN compatibility will be considered (Molta, 2001). Security issues will be addressed through the assessment of both industry standard and proprietary wireless security solutions.

The Systems Design Phase or Phase 3 will be followed by Phase 4, the Systems Implementation Phase, which will involve the construction of the wireless network and the delivery of a working system into day-to-day operation (Whitten et al., 1994). The final stage of this MSDLC process will be Phase 5 or the Systems Support Phase. Phase 5 involves ongoing support and includes program maintenance and system improvement.

Barriers and Issues

The goal of this research is ambitious and has not already been met for a number of reasons. The complexity of planning, designing, and implementing WLAN technologies in a large manufacturing company such as AAM is a deterrent to WLAN deployment (Chen, 2002; Coffee, 2002; Crump, 2001b; Dulaney, 2002; Geier, 1999, 2001; Moozakis, 2001; MSI Editors, 2001; Rogak, 2001; Sbihli, 2002). Underlying issues at AAM include non-standard network configurations across the company's worldwide facilities, a shortage of IT Department resources, and security weaknesses inherent in the Wired Equivalent Privacy (WEP) algorithm (Blair, 2002; Fluhrer, Mantin, & Shamir, 2001). An additional challenge is the complexity of integrating new WLAN technologies with existing wireline infrastructures (Fluhrer et al., 2001). The resultant mixed-mode wireless and wired configuration should operate more efficiently than the previous single-mode implementation.

The emergence of competitive IEEE WLAN standards such as 802.11b, 802.11a, and 802.11g is another issue (Curl, 2001). In addition, countries in the European Union and members of the European Telecommunications Standards Institute (ETSI) promote their own WLAN standards such as High Performance Radio Local Area Network-Type 1 (HiperLAN-1) and High Performance Radio Local Area Network-Type 2 (HiperLAN-2) (Bourin, 2001). This is an issue for AAM and other global manufacturers intending to implement a common WLAN solution across all facilities.

Enterprise managers considering WLAN technologies must determine which available or emerging technology is the best fit based upon project timing, equipment compatibility, equipment availability, their existing network topology, and their available budget ("*The wireless wave*," 2001). IT managers must be careful to implement wireless applications as part of an overall wireless strategy and not just as isolated solutions.

Research Questions

One of the most important steps in conducting a research case study is the definition of research questions (Yin, 1994). Often the most difficult challenge an investigator must overcome is to design research questions that will direct the study enough but not too much (Stake, 1995). This researcher will answer the following questions:

- What are effective procedures for planning, designing, and implementing a WLAN solution in a large manufacturing enterprise?
- What are the key factors that contribute to WLAN deployment?
- What are the major benefits and limitations associated with WLAN utilization?
- What WLAN standards and technologies are currently available for deployment?

- What existing and projected WLAN technologies are most appropriate for deployment?
- What mechanisms adequately secure the integrity of WLAN transmissions?
- What WLAN strategies should be employed to ensure the most effective use of wireless technology?

Limitations and Delimitations

A number of restrictions beyond the control of the researcher will influence the study. These constraints include limitations related to corporate business objectives, resource availability, and changing WLAN standards and technologies. For example, the wireless initiatives that will serve as the subject of the case study were selected based on appropriateness to the research and ability to return immediate value to the corporation. Resource availability including monetary and IT staff will be another limiting factor. The wireless projects will be funded from a predefined departmental expense budget, and staff resources will be required to complete the projects along with their regular work activities. In addition, changing wireless standards and technologies may delay progress until the required standards-based hardware and software technologies become available.

In addition to the aforementioned limitations, several constraints will influence the scope and focus of the study. Delimitations that will restrict the wireless technologies deployed include the size of the WLAN user groups and the length of time allotted for project completion. For example, the focus of one of the projects will be on the use of WLAN technologies by users with new laptops configured with the Microsoft Windows

2000 operating system. In addition, the projects must be deployable in a 12-month period with limited resources and no negative effect on manufacturing operations.

Definition of Terms

The following are definitions of key terms used throughout this investigation:

2.5G - A term used to describe digital cellular phone technologies that are between second-generation and third-generation (Mitchell & Kay, 2001). 2.5G wireless systems provide fast data transfer, enhanced e-mail, and Internet access. For example, 2.5G deployments by AT&T Wireless and T-Mobile, based on General Packet Radio Service (GPRS) technology, provide a maximum transfer rate of 144 Kbps.

3G (Third-Generation) - A term used to describe digital cellular phone technologies designed to transmit enhanced multimedia such as voice, data, video, and remote control (Agrawal, 2002). The Universal Mobile Telecommunications System (UMTS) is a 3G system that is standardized in the European Union (Littman, 2002). Wideband-Code Division Multiple Access (Wideband-CDMA or W-CDMA) and CDMA2000, the primary 3G technologies, support both circuit-switched and packet-switched operations (Komagan, 2000). W-CDMA solutions enable transmission rates up to 2 Mbps and provide Quality of Service (QoS) assurances for multimedia applications. In addition, 3G systems facilitate advanced global roaming.

Advanced Encryption System (AES) - AES is the National Institute of Standards and Technology (NIST) standard for secret key cryptography that officially replaced the Triple DES (Data Encryption Standard) method in 2000 as the United States government standard (Smith, 2001). AES protected technologies employ the Rijndael

algorithm and are able to encrypt in a single pass instead of three passes. While Triple DES technology is designed for hardware, AES technology is efficient in a range of environments that include smart cards, programmable gate arrays, and PCs.

Advanced Mobile Security Architecture (AMSA) - A proprietary security scheme developed for use with IEEE 802.11 WLANs by Agere Systems that specifies authentication and encryption services ("*Agere Systems announces*," 2002). ASMA systems use RC4 per-user per-session encryption with Diffie-Helman key exchange (Molta, 2001). Authentication is managed by a Remote Authentication Dial-In User Service (RADIUS) server.

ALOHANET - A University of Hawaii research project and the first packet radio network, connected computers at the university's seven campuses on four neighboring islands with a mainframe computer on the island of Oahu (Geier, 2001). ALOHANET operated at 9600 bps (bits per second) and was the basis of Ethernet (Abramson, 2002).

American Radio Relay League (ARRL) - An organization of approximately 163,000 radio experimenters that promotes interest in amateur radio communications and experimentation ("*About the ARRL*," 2002). The ARRL maintains a standard of conduct for radio operators and represents United States radio amateurs with the Federal Communications Commission and other government agencies in the United States and abroad.

Asynchronous Transfer Mode (ATM) - ATM is a broadband network technology that supports voice, video, and data transmissions at rates from 1.544 Mbps to 13.21 Gbps (Littman, 2002). ATM networks employ Classes of Service (COS) to

optimize network performance. Each COS supplies a different level of service and associated Quality of Service (QoS) guarantees.

Basic Service Set (BSS) - A set of wireless stations that are logically associated with one another (Gast, 2002). The BSS is the building block of IEEE 802.11 wireless networks.

Bluetooth - A wireless networking technology that operates globally in the 2.4 GHz license-exempt band (Littman, 2002). Bluetooth technology is designed for short-range, low-power transmission of voice and data between mobile and desktop devices. Bluetooth Wireless Personal Area Networks (WPANs) are freestanding and ad hoc network configurations that function without a wireline infrastructure. Bluetooth WPANs employ FHSS technology to minimize signal interference.

Canadian Radio Relay League (CRRL) - An organization of Canadian amateur radio enthusiasts that merged with the Canadian Amateur Radio Federation in 1993 to form the Radio Amateurs of Canada (RAC) ("*What is Amateur*," 2002). The RAC is the official voice of Amateur Radio in Canada.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) - A network random access control method that was created following the deployment of the Aloha radio network (ALOHANET) (Littman, 2002). ALOHANET's Aloha protocol led to the development of CSMA/CA and CSMA/CD. IEEE 802.11-compliant wireless networks employ access control mechanisms based on the principal of CSMA/CA (Geier, 1999a). CSMA/CD is a commonly used protocol in Ethernet networks.

CDMA2000 - A third-generation (3G) cellular communications technology that employs the 1xRTT (ITU Radio Transmission Technologies) specification as an

operating foundation (Littman, 2002). CDMA2000 circuit-mode and packet-mode transmissions are able to achieve data rates reaching 2.4 Mbps.

Computerized Numerical Control (CNC) - A term used to describe automated machine tools used in manufacturing to perform tasks such as milling, punching, turning, and drilling (Martec, 2002). CNC machines are able to produce accurately machined parts at rates greater than manually machined parts. Computer Aided Manufacturing (CAM) systems generate the CNC tool path programs used to machine the required parts.

Complimentary Code Keying (CCK) - CCK is a set of 64 eight-bit code words used to encode data for IEEE 802.11b-compliant WLANs transmitting at rates of 5.5 Mbps and 11 Mbps in the 2.4 GHz band ("CCK," 2002). CCK code words have unique mathematical properties that allow them to be distinguished from one another in noisy environments. CCK works in conjunction with the DSSS technology specified in the IEEE 802.11b standard.

Customer Premises Equipment (CPE) - Communications equipment that is located on the customer's premises ("CPE," 2002).

Cyclic Redundancy Check (CRC) - A technique used to check the accuracy of digital data transmissions (Scott, 1999). A CRC performs a mathematical calculation on a block of data and returns a number or fingerprint that represents the organization and content of that data. The number that is used to identify the data is called a checksum.

Digital Signal Processor (DSP) - A specialized microprocessor designed to manipulate analog information that has been converted to digital format ("*Digital signal*," 2002).

Digital Subscriber Line (DSL) - A high bandwidth transmission service that operates over standard copper telephone lines (Flickenger, 2002). A range of transmission rates are supported depending on the DSL variant used. Asymmetric Digital Subscriber Line (ADSL), for example, supports rates ranging from 1.544 Mbps to 8 Mbps within 18,000 feet of the telephone company central office (Littman, 2002).

Direct Sequence Spread Spectrum (DSSS) - A radio transmission technique that spreads the RF signal over a wide frequency band and continuously alters the transmission pattern by constantly changing the data pattern (Gast, 2002). DSSS multiplies the data bits by a pseudo-random bit pattern. This spreads the data over a coded stream that utilizes the full bandwidth of the channel.

Dynamic Security Link - A proprietary security mechanism developed by 3Com for use in IEEE 802.11 WLANs ("*3Com unveils*," 2002). Dynamic Security Link provides authentication and 128-bit encryption. In addition, each user is given a unique key, which is changed every session.

EAP-MD5 (Extensible Authentication Protocol - Message Digest 5) - EAP-MD5 is a challenge handshake authentication protocol that enables the authentication of remote clients of Ethernet LANs ("*EAP*," 2002).

EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) - An EAP type used in certificate-based security environments ("*EAP*," 2002). EAP-TLS enables encryption method negotiation, mutual authentication, and secure private key exchange for wireless LANs.

EAP-TTLS (Extensible Authentication Protocol - Tunneled Transport Layer Security) - A proprietary protocol developed by Funk Software and Certicom (Funk,

2002b). EAP-TTLS is a strong authentication method that operates in conjunction with the IEEE 802.1x security protocol. In addition to enhancing WLAN security, EAP-TTLS reduces WLAN management tasks.

Enterprise Resource Planning (ERP) - An all-in-one integrated information system that is utilized by the manufacturing industry (Freedman, 2002). ERP systems typically include software modules for shipping, receiving, manufacturing, order entry, accounts receivable and payable, general ledger, purchasing, and human resources. ERP application companies include SAP, Oracle, PeopleSoft, Oracle, Baan, and J.D. Edwards.

Ethernet - A local area network medium access method that operates at 10 Mbps, 100 Mbps, 1 Gbps, and 10 Gbps (Littman, 2002). Ethernet is the technology of choice for LAN implementations in schools, hospitals, government agencies, libraries, and corporations.

European Telecommunications Standards Institute (ETSI) - The ETSI is a multinational body of 912 members from 54 countries with regulation and standardization authority over much of Europe ("*ETSI*," 2002). ETSI represents administrations, network operators, manufacturers, service providers, and research bodies. The Institute develops a wide range of telecommunications, broadcasting, and information technology standards and technical documentation. Examples include the Global System for Mobile Communications (GSM), HiperLAN-1 and HiperLAN-2 standards.

Extended Service Set (ESS) - A set of two or more wireless Access Points (APs) and associated wireless devices in the same network subnet (Gast, 2002). When all stations are configured to recognize each other, link layer roaming is possible.

Extended Service Set Identifier (ESSID) - The name that identifies an IEEE 802.11 wireless network ("*WiFi Alliance*," 2002). Also called Service Set Identifier (SSID), Network Name, Preferred Network, or Wireless LAN Service Area, the ESSID differentiates one WLAN from another. The ESSID is a 32-character unique identifier attached to packet headers transmitted over an IEEE 802.11-compliant WLAN. All APs and devices attempting to connect to a specific WLAN must use the same ESSID.

Extensible Authentication Protocol (EAP) - An extension of Point-to-Point Protocol (PPP), EAP enables a number of authentication protocols and is not tightly bound to the security method (Blunk & Vollbrecht, 1998). PPP enables the transport of multi-protocol packets over point-to-point links. PPP is extended by EAP, which provides negotiation of an authentication protocol for authenticating peers before allowing network layer protocols to transmit over a data link.

Frequency Hopping Spread Spectrum (FHSS) - A radio transmission technique where the data signal is modulated with a narrowband carrier signal that hops in a random but predictable sequence from frequency to frequency as a function of time over a band of frequencies ("*FHSS*," 2002). Two types of spread spectrum systems are most frequently used: FHSS and DSSS (Perez-Jimenez, Riera, & Lopez-Hernandez, 2001). The unauthorized monitoring of FHSS transmissions is extremely difficult because a fixed frequency is not used.

Gantt Chart - A floating horizontal bar chart developed as a production control tool in 1917 by Henry L. Gantt ("*Gantt chart*," 2002). Gantt charts show the progress of a project in relation to time. The horizontal axis of a Gantt chart represents the total time span of a project and a vertical axis represents the tasks that make up a project.

General Packet Radio Service (GPRS) - GPRS is an advanced second-generation cellular telephone solution capable of data rates up to 171.2 Kbps (Littman, 2002). GPRS networks are packet-switched and operate in conjunction with GPRS circuit-switched networks.

Global System for Mobile Communications (GSM) - A second-generation digital cellular phone solution popular throughout the European Union, South America, Asia, Australia, New Zealand, Africa, and the Middle East (Littman, 2002). GSM uses Time-Division Multiple Access (TDMA) and Frequency-Division Multiple Access (FDMA) technologies for base station carrier frequency assignment.

High Performance Radio Local Area Network (HiperLAN) - A wireless standard developed and endorsed by the ETSI (Littman, 2002). HiperLAN-Type 1 (HiperLAN-1) supports wireless operations and communications services in infrastructure-based and ad hoc configurations. HiperLAN-1-compliant systems operate in the 5 GHz frequency band and support data rates up to 20 Mbps ("*ETSI HIPERLAN/1*," 2002).

HiperACCESS - A wireless standard defined by the ETSI ("*ETSI approves*," 2002). HiperACCESS-compliant systems support fixed wireless point-to-point communications with data rates up to 100 Mbps.

HiperLAN-2 (HiperLAN-Type 2) - A radio LAN (RLAN) specification, developed by the ETSI, that supports wireless operations and communications services in infrastructure-based and ad hoc configurations (Littman, 2002). HiperLAN-2-compliant systems operate in the 5 GHz frequency band and support data rates up to 54 Mbps ("*ETSI HIPERLAN/2*," 2002).

HiperLINK - A wireless standard defined by the ETSI (Prasad & Prasad, 2001a). HiperLINK-compliant solutions provide interconnections between HiperLAN and HiperACCESS compliant systems. HiperLINK-compliant systems support data rates up to 155 Mbps.

HomeRF - A home wireless networking standard created by the HomeRF Working Group ("*HomeRF*," 2001). HomeRF specifies FHSS technology and the Shared Wireless Access Protocol (SWAP) to enable an open standard for short-range transmission of digital voice and data. HomeRF and Wi-Fi (Wireless Fidelity) solutions are competitors in the marketplace.

Hot Spot - A geographic area covered by a wireless Access Point (AP) that allows users to connect to the Internet ("*Hot spot*," 2002). Hot spots are typically located in airports, train stations, hotels, and convention centers.

IEEE 802.11 - A specification by the IEEE that defines WLAN operations at Layer 1 and Layer 2 of the OSI Reference Model (Littman, 2002). The IEEE 802.11 standard specifies an open architecture and interoperability between WLAN equipment in multivendor environments. The initial IEEE 802.11 standard specified a 2.4GHz operating frequency with data rates of 1 Mbps and 2 Mbps (Geier, 2002a). When deploying a wireless LAN using the initial specification, either FHSS or DSSS can be selected.

IEEE 802.11a - An extension of the IEEE 802.11 specification (Geier, 2001). IEEE 802.11a-compliant WLAN solutions employ Orthogonal Frequency Division Multiplexing (OFDM) technology and support data rates up to 54 Mbps in the 5 GHz frequency band.

IEEE 802.11b - An extension of the IEEE 802.11 specification (Geier, 2001). IEEE 802.11b-compliant WLAN solutions employ DSSS technology and support data rates up to 11 Mbps in the 2.4 GHz frequency band (Geier, 2001). Most present-day WLAN installations comply with IEEE 802.11b, which is also the basis for Wi-Fi certification from the Wi-Fi Alliance (Geier, 2002a).

IEEE 802.11g - An evolving extension of the IEEE 802.11 specification ("*Wireless LAN glossary*," 2002). IEEE 802.11g-compliant WLAN solutions employ OFDM technology and support data rates up to 54 Mbps in the 2.4 GHz frequency band. The IEEE 802.11g extension will implement all mandatory elements of the IEEE 802.11b extension and allow IEEE 802.11b clients to associate with IEEE 802.11g-compliant APs (Geier, 2002a).

IEEE 802.11i - An evolving security extension of the IEEE 802.11 standard that specifies encryption that is stronger than WEP (Vaughan-Nichols, 2002). IEEE 802.11i replaces WEP's RC4 encryption algorithm with Temporal Key Integrity Protocol (TKIP) and AES.

IEEE 802.1x - A security protocol defined by the IEEE 802.11 specification ("*802.11 security*," 2002). Combined with an authentication protocol such as EAP-TLS or EAP-TTLS, IEEE 802.1x-compliant WLANs provide port-based access control and mutual authentication between clients and APs via an authentication server. IEEE802.1x-enabled WLANs also provide a method for distributing encryption keys dynamically to WLAN devices.

Independent Basic Service Set (IBSS) - A set of wireless devices operating without an AP (Gast, 2002). Devices in an IBSS network operate in ad hoc or peer-to-peer mode.

Industrial, Scientific, and Medical (ISM) Bands - Bands of frequencies originally reserved internationally for non-commercial use of RF electromagnetic fields for industrial, scientific, and medical purposes ("*ISM band*," 2002). The ISM bands are defined by the International Telecommunications Union-Telecommunications Standards Section (ITU-T). IEEE 802.11-compliant WLANs operate in an ISM band.

Infrared (IR) - Invisible light waves with wavelengths between .75 and 1,000 microns (Geier, 1999b). Direct infrared platforms support point-to-point connections and are dependent on direct line of sight for transporting data (Littman, 2002). Diffuse infrared platforms support multipoint-to-multipoint connections and are not dependent on a direct line of sight for information transport.

Initialization Vector (IV) - A term used to describe the exposed key in a cryptographic header (Gast, 2002). The IEEE 802.11b WEP initialization vector is 24 bits in length.

Institute of Electrical and Electronics Engineers (IEEE) - The IEEE is an organization of more than 377,000 engineers, scientists, and students in 150 countries ("*About the IEEE*," 2002). The IEEE is engaged in setting standards for computers and communications and produces 30 percent of the world's published literature in electrical engineering, computers, and control technology.

Infrared Data Association (IrDA) - IrDA is an international organization that creates and supports low cost, interoperable infrared data interconnection standards ("*The*

Infrared," 2002). IrDA's membership is composed of hardware, systems, software, and communications manufacturers.

Infrared Link Access Protocol (IrLAP) - IrLAP is an IrDA protocol that enables the establishment of a logical relationship and the transmission of data between two IrDA-compliant machines (Rodbell, 2002).

Infrared Physical Medium Dependent (PMD) - The PMD sub-layer of the Physical Layer enables the actual transmission and reception of data between two IR stations ("*Reducing total cost,*" 2002). The PMD service interfaces with the air and modulates and demodulates frame transmissions.

Infrared Physical Layer Convergence Procedure (PCLP) - The PCLP layer delivers incoming frames from the infrared medium to the Medium Access Control (MAC) layer ("*Physical,*" 2002). The PLCP layer communicates with the MAC layer through the Physical Layer Service Access Point (PLSAP).

IP Security Protocol (IPSec) - A group of protocols developed by the Internet Engineering Task Force (IETF) to secure packet exchange at the IP layer ("*IPSec,*" 2002). IPSec enables secure transmissions via Virtual Private Networks (VPNs).

IrDA Link Management Protocol (IrLMP) - The IrLMP is a protocol for IrDA-compliant devices that enables walk-up, ad hoc connection between devices (Seaborne, Williams, & Novak, 1996). The protocol supports the operation of concurrent and independent multiple software applications.

IrDA Serial IR (IrDA-SIR) - IrDA-SIR is the physical layer that enables half-duplex IR connections with data rates up to 115.2 Kbps (Freedman, 2002).

Keyguard - A proprietary encryption method developed by Symbol Technologies to provide an advanced mechanism for securing Symbol WLANs ("*MobiusGuard*," 2002). Keyguard is an enhancement of the TKIP encryption standard.

Lightweight Authentication Protocol (LEAP) - A proprietary version of the Extensible Authentication Protocol (EAP) developed by Cisco Systems to secure WLANs ("*Cisco's use*," 2002). LEAP enables user-based central authentication in addition to per-user WEP session keys.

Local Multipoint Distribution System (LMDS) - A line of sight digital wireless transmission technology that supports fixed wireless access point-to-multipoint networking solutions (Littman, 2002). LMDS business networks support downstream transfer rates ranging between 51.84 Mbps and 155.52 Mbps. The technology is designed to connect the last mile from a carrier to a large building or campus with high-bandwidth communications ("*LMDS*," 2002).

Logical Link Control (LLC) - LLC is one of two sublayers of Layer 2 of the OSI Reference Model ("*The 7 Layers*," 2002). The LLC layer controls flow control, frame synchronization, and error checking.

MAC Service Data Unit (MSDU) - A MSDU is the higher-level data such as multicast packets transferred by the MAC to another MAC on the network (Gast, 2002). The primary service of the IEEE 802.11 standard is to deliver MSDUs between LLC connections to the network (Geier, 1999a).

Medium Access Control (MAC) - The function in IEEE networks that mediates the use of network capacity and determines which stations are allowed to use the medium for transmission (Gast, 2002).

Mini PCI (Mini Peripheral Component Interconnect) - Mini PCI is a specification that defines a small form factor version of the PCI card ("*Mini PCI*," 2002). Mini PCI cards use a qualified subset of the same electrical definitions, signal protocol, and configuration definitions as the conventional PCI specification.

Modern Systems Development Life Cycle (MSDLC) - A process used by systems analysts, engineers, and programmers to build information systems (Whitten et al., 1994). The five phases of the MSDLC are Systems Planning, Systems Analysis, Systems Design, Systems Implementation, and Systems Support.

Multichannel Multipoint Distribution System (MMDS) - MMDS is a line of sight digital transmission technology that enables fixed wireless broadband transmissions and employs protocols that include TDMA, FDMA, and OFDM (Littman, 2002). In Ireland, Mexico, and the United States, MMDS implementations operate in the 2.596-2.644 and 2.686-2.689 GHz licensed frequency bands. MMDS was initially designed to provide one-way cable television service to customers in remote areas. Subsequently, the technology was enabled to provide two-way data and Internet services to subscribers. MMDS channels are 6 MHz wide and operate on frequencies licensed by the Federal Communications Commission (FCC) ("*MMDS*," 2002).

Multimedia Mobile Access Communication (MMAC) - A wireless LAN standard created by the MMAC Committee of the Ministry of Post and Telecom (MPT) in Japan ("*Multimedia Mobile*," 2002). The MPT created the MMAC Committee to study next-generation broadband mobile communication systems (Prasad & Prasad, 2001a). MMAC systems are able to transmit high-quality multimedia content to mobile users at ultrahigh rates.

Narrowband - A term used to describe wireless systems that transmit in a narrow band of frequencies ("*Narrowband*," 2002). The width of this frequency band is typically between 12.5 KHz and 25 KHz (Prasad & Prasad, 2001b). Narrowband technology was initially developed by amateur radio operators.

Offset Codebook Mode (OCM) - A mode of AES operation, OCM simultaneously enables privacy and authentication services (Rogaway, 2002). In addition to being simple and efficient, OCB use a provable-security paradigm. Provable-security schemes are those whose assurance does not stem from a failure to find attacks but from proofs and associated bounds and definitions.

Orthogonal Frequency Division Multiplexing (OFDM) - A modulation technique that divides a wide frequency band into multiple narrow frequency bands (Gast, 2002). The transmitted data are inverse multiplexed across multiple subchannels. Inverse multiplexing is a technique that breaks up a high-speed transmission into several low-speed transmissions. The IEEE 802.11a and IEEE 802.11g standards are based on OFDM.

Peripheral Component Interconnect (PCI) - A local data bus standard originally developed by Intel ("*Conventional PCI*," 2002). The PCI specification provides for plug and play, high-speed data connections between a computer's peripheral devices and the Central Processing Unit (CPU). PCI is a 64-bit bus that is most often implemented as a 32-bit bus.

Personal Computer Memory Card International Association (PCMCIA) - PCMCIA is an international standards body and trade organization founded in 1989 and comprised of over 200 member companies ("*About PCMCIA*," 2002). The association

was established to promote standards for integrated circuit cards and interchangeability among Personal Computers (PCs). The small, credit card-sized devices developed by member companies are called PC Cards.

Personal Data Assistant (PDA) - A PDA is a handheld computer that serves as a Personal Information Manager (PIM) (Freedman, 2002). Common applications that are supported on PDAs include e-mail, a calendar, an address book, a task list, and a notepad. Wirelessly enabled PDAs are also able to access company LANs and the Internet (Gray & Cowley, 2002).

Physical Layer (PHY) - The Physical Layer is Layer 1 of the OSI Reference Model (Freedman, 2002). Layer 1 provides services to transmit bits over the network and deals only with the electrical and mechanical characteristics of the signals and signaling methods.

Programmable Logic Controller (PLC) - A computer used in manufacturing facilities to control process applications (Freedman, 2002). PLCs are typically RISC-based (Reduced Instruction Set Computer-based) microprocessors designed to operate in real-time, industrial environments.

Protected Extensible Authentication Protocol (PEAP) - A proposed standard for IEEE 802.1x authentication ("*PEAP*," 2002). PEAP enables one-time token authentication, password change, and user database extensibility.

Quality of Service (QoS) - QoS is a term used to describe the ability to define a level of performance in data communications systems (Mitchell, 2002). The goal of QoS is to provide guarantees on ability of a network to deliver predictable results. Elements of network performance covered by QoS are availability, bandwidth, latency, and error rate.

RC4 - A stream cipher symmetric key algorithm defined by IEEE 802.11. RC4 uses a variable length key up to 256 bytes to initialize a 256-byte state table (Rivest, 2002). The state table is then used to generate a stream that is XORed with the plain text to be encrypted. An exclusive OR (XOR) is a Boolean logic operation that is true if only one of the inputs is true, but not both (Freedman, 2002).

Remote Authentication Dial-In User Service (RADIUS) - A network access control technology that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service ("*Remote Authentication*," 2002). RADIUS access solutions are the de facto industry standard for the authentication of dial-in users.

Small Office Home Office (SOHO) - A term used to describe a business or office that consists of 10 or fewer employees and/or computers ("*WiFi Alliance*," 2002).

System Control and Data Acquisition (SCADA) - A term used to describe a computer system that collects and analyzes real-time data ("*SCADA*," 2002). SCADA systems are employed by the manufacturing, energy, oil, and gas refining industries to control and monitor manufacturing equipment.

T-1 - A 1.544 Mbps point-to-point dedicated, digital circuit provided by the telephone companies ("*T-1 carrier*," 2002). A T-1 connection is composed of 24 individual channels. Each channel has a data transfer rate of 64 Kbps and can be configured to carry voice or data traffic.

Temporal Key Integrity Protocol (TKIP) - A wireless security protocol that enables initialization, vector hashing, and message integrity checking to counteract

passive snooping and determine if packets have been modified by an unauthorized user (*"Enhancing wireless,"* 2002).

Terminal Node Controller (TNC) - A device that converts digital signals from a computer to signals that a ham radio is able to modulate and transmit (Geier, 2001).

Terminal Service (TS) - An option of Microsoft Windows NT 4.0 and Microsoft Windows 2000 Server operating systems that enables multiple client computers to run a server application simultaneously (Freedman, 2002). All application logic is performed in the server. Client computers only display screen changes and the user interface.

Time Division Duplexing (TDD) - A transmission method, developed by Bell Labs, that divides the entire bandwidth of the transmission medium into a sequence of timeslots (Littman, 2002). Each timeslot uses the entire frequency range for an assigned interval of time. TDM adjusts time intervals to promote efficient use of the available bandwidth.

Time Division Multiple Access (TDMA) - A technology for delivering digital wireless service (*"TDMA,"* 2002). TDMA uses Time Division Multiplexing (TDM) to enable a single frequency to support multiple, simultaneous data channels. TDMA divides a radio frequency into time slots that are allocated to multiple calls.

Time Division Multiple Access/Time Division Duplexing (TDMA/TDD) - A communications technique that uses a single channel to transmit and receive data (Freedman, 2002). In addition, the technology interleaves multiple digital signals onto the same channel.

Total Cost of Ownership (TCO) - An expression that recognizes the cost of technology is often far greater than the technology's initial purchase price (*"Reducing*

total cost," 2002). For example, the initial cost of a PC is only a small fraction of the total cost of using, connecting, maintaining, and disposing of the PC.

Ultra High Frequency (UHF) - A term used to describe the band of electromagnetic frequencies from 300 MHz to 3 GHz (Freedman, 2002).

Ultrawideband (UWB) - UWB is a short-range wireless technology that enables transmission and reception of very short baseband signals without a carrier (Siwiak & Huckabee, 2002). The technology reuses previously allocated RF bands by spreading RF energy thinly in a wide spectrum.

Universal Serial Bus (USB) - A hardware interface used to connect peripherals such as a mouse, scanner, and keyboard to a computer (Freedman, 2002).

Very High Frequency (VHF) - A term used to describe the electromagnetic frequencies in the range from 30 MHz to 300 MHz (Freedman, 2002).

Virtual Private Network (VPN) - A private network that is configured within a public network such as the Internet (Freedman, 2002). A VPN employs access control and encryption to ensure that only authorized users are able to access the network and that the data cannot be intercepted. VPN security mechanisms include tunneling protocols such as Generic Routing Encapsulation (GRE) and Layer Two Tunneling Protocol (L2TP) and encryption protocols such as IPSec (Vaughan-Nichols, 2002).

Very Small Aperture Terminal (VSAT) - An earthbound device used to receive satellite data, voice, and video transmissions ("*VSAT,*" 2002). The very small component of the acronym refers to the three to six feet diameter of the VSAT dish antenna. A VSAT system consists of two parts. The first is a transceiver that is placed outdoors in line of sight of the satellite. The second is an interface device that is placed indoors to

connect the transceiver to the user's PC or network. While early VSAT systems were only able to achieve data rates of 56 Kbps, current systems, designed for SOHO venues, are capable of downlink data rates of 2 Mbps and uplink data rates of 19.2 Kbps (Littman, 2002).

WEPlus - A proprietary extension to the IEEE WEP encryption developed by Agere Systems (Baxter, 2001). WEPlus enhances WEP security by eliminating the propagation of the weak key patterns identified by Fluhrer, Mantin, and Shamir (2001).

Wideband Code Division Multiple Access (W-CDMA) - W-CDMA is a high-speed 3G mobile wireless technology that supports both circuit-switched and packet-switched operations (Littman, 2002). W-CDMA solutions enable transmission rates up to 2 Mbps and provide Quality of Service (QoS) assurances for multimedia applications.

Wideband Frequency Hopping (WBFH) - This FHSS technology operates in the 2.4 GHz frequency band (Paulo & Wolf, 2000). Unlike standard frequency hopping systems that use a 1 MHz wide channel for transmission, WBFH systems employ a 5 MHz wide channel. This wider transmission channel supports transmissions ranging from 2 Mbps to 10 Mbps.

Wi-Fi Alliance - A nonprofit international association formed in 1999 to certify the interoperability of broadband Fixed Wireless Access (FWA) Ethernet LAN products based on the IEEE 802.11 specification (Littman, 2002; "What is Wi-Fi," 2002). The organization has 193 member companies, and more than 522 WLAN products have received Wi-Fi certification ("What is Wi-Fi," 2002). Certified products feature Wi-Fi

logos. The Wi-Fi Alliance was formerly known as the Wireless Ethernet Compatibility Alliance (WECA).

Wi-Fi Protected Access (WPA) - A WLAN security standard issued by the Wi-Fi Alliance (Grimm, 2002). WPA is designed to replace WEP and addresses WEP security weaknesses such as highjacking and man-in-the-middle attacks by supporting a higher level of encryption and the dynamic exchange of encryption keys.

Wired Equivalent Privacy (WEP) - An optional IEEE 802.11 wireless security protocol designed to enable frame transmission privacy similar to a wired network (Geier, 1999b). WEP-enabled systems generate secret shared encryption keys that both destination and source stations use to encrypt transmissions.

Wireless Application Protocol (WAP) - A secure standard that supports instant access to information from handheld wireless devices such as mobile phones, pagers, two-way radios, and smart phones ("WAP," 2002). WAP-enabled systems provide a complete environment for wireless applications that includes a wireless equivalent of Transmission Control Protocol/Internet Protocol (TCP/IP).

Wireless Local Area Network (WLAN) - A computer network covering a local area such as an office or a home that uses radio waves instead of wires as a carrier ("*Wireless LAN*," 2002). Early WLANs included industry-specific solutions and proprietary protocols that were replaced in the late 1990s by standards-based solutions such as IEEE 802.11b-compliant and HomeRF-compliant WLANs.

Work in Progress (WIP) - A term used to describe the portion of a manufacturing company's inventory that is neither raw materials nor finished goods

(Wasp, 2002). A WIP consists of materials that will be integrated into sub-assemblies as part of the process of building a finished product.

Summary

The rate at which companies are deploying wireless LAN technologies has 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 units in 2005. WLAN technologies provide companies with many competitive advantages when properly leveraged.

In this chapter, this investigator began by describing the problem to be investigated and the goal to be achieved. The focus of this research is to define procedures for enabling large manufacturing enterprises to effectively plan, design, and implement WLAN technologies. The goal of this research is to provide a model for those companies to use when deploying WLAN technologies in offices, manufacturing facilities, and employee residences. An analysis of the relevance and significance of the research along with a discussion of barriers and issues related to achieving the goal were presented. Limitations and delimitations associated with the investigation were also reviewed. Finally, research questions related to the inquiry and definitions of key terms that will be used throughout the paper were provided.

Chapter 2

Review of Literature

The literature review that follows establishes the rationale and framework for this investigation. The review begins with a historical overview of the research literature and follows with a discussion of literature specific to the subject of planning, designing, and implementing WLANs in a global manufacturing enterprise. The literature review is organized into seven subject areas: wireless LAN technologies, wireless LAN standards and wireless standards associations, wireless LAN security, wireless LAN initiatives, wireless LAN vendor offerings, wireless LAN service providers, and wireless LAN strategy.

Historical Overview

According to Geier (2001), Radio Frequency (RF) and network technologies first complemented one another in 1971 with a project called ALOHANET. 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 (Geier, 2001). Armyros (1992) adds that all stations in the network transmitted packets to the master station on Oahu without regard for other network traffic. 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 (Armyros, 1992). Although this first system was inefficient, ALOHNET successfully replaced costly and unreliable telephone lines with the first packet radio network.

The American Radio Relay League (ARRL) and the Canadian Radio Relay League (CRRL) began promoting the use of wireless connectivity in the 1980s (Geier, 1999b). Amateur radio hobbyists, active in the ARRL, interconnected their PCs 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 PCs to analog signals. These signals were then broadcast using a packet switching technique.

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 in 1985 (Geier, 1999b). The ISM bands occupy radio spectrum between the 902 MHz and the 5.85 GHz frequencies. According to 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 1997.

WLANs have been in use since 1990 (Prasad & Prasad, 2001b). These networks are primarily based upon spread spectrum technologies developed by the United States military during World War II. Spread spectrum technologies transmit voice and data over a range of frequencies using either the Frequency Hopping Spread Spectrum (FHSS) or the Direct Sequence Spread Spectrum (DSSS) modulation techniques. Newer systems

that operate in the 5 GHz frequency band achieve higher data rates using Orthogonal Frequency Division Multiplexing (OFDM) (Prasad & Prasad, 2001b). In addition to spread spectrum technology, WLAN systems employing infrared and UHF narrowband technologies are also in limited use.

Wireless LAN Technologies

Literature related to wireless LAN technologies is reviewed in the following sections. These WLAN technologies include UHF narrowband, spread spectrum, ultrawideband, and infrared.

Ultra High Frequency (UHF) Narrowband

UHF narrowband technology was originally developed by amateur radio operators (Prasad & Prasad, 2001b). The term narrowband describes wireless systems that transmit in a narrow band of frequencies ("*Narrowband*," 2002). The width of this frequency band is typically between 12.5 KHz and 25 KHz (Prasad & Prasad, 2001b). Existing UHF narrowband systems transmit in both licensed and unlicensed frequencies between 300 MHz and 3 GHz 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.

According to Jensen (1999), UHF narrowband has a number of disadvantages. These disadvantages include regulatory barriers limiting operation at data rates above 56 Kbps because a broad section of the radio spectrum is required to accomplish this and government regulators are reluctant to allocate additional bandwidth in the highly utilized

UHF band. UHF frequencies are subject to interference and propagation anomalies that limit performance (Jensen, 1999). 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. In a typical system, the installation process involves assembling equipment, configuring antennas, verifying radio link performance, and installing network software.

Spread Spectrum

The spread spectrum radio transmission technique continuously varies the signal patterns and frequencies of the transmitted signal ("*Spread Spectrum*," 2002). Spread spectrum systems in contrast to narrowband systems use more bandwidth than required for transmission. Perez-Jimenez, Riera, and Lopez-Hernandez (2001) further state that since spread spectrum transmissions are difficult to detect, intercept, and decode, the transmissions are more secure than narrowband transmissions. Spread spectrum radio transmission was first proposed by the military to prevent radio signals from being jammed or monitored by the enemy (Perez-Jimenez et al., 2001). However, spread spectrum systems are more complex than narrowband systems and were only adopted by the commercial sector after low cost integrated Digital Signal Processors (DSPs) became available in high quantity. Both narrowband and spread spectrum transmission systems support transmissions in the same frequency band.

Spread spectrum systems typically utilize DSSS and FHSS technologies to enable wireless network operations (Littman, 2002). OFDM technology is employed in newer systems to achieve increased data rates (Prasad & Prasad, 2001b).

Direct Sequence Spread Spectrum (DSSS).

The DSSS modulation method spreads the data over a coded stream that uses the full bandwidth of the radio channel (Perez-Jimenez et al., 2001). This is accomplished by combining the data signal with a higher data rate bit sequence, or chipping code, that divides the data using a spreading ratio. The primary reason to select the DSSS transmission method is the technology's ability to share the same spectrum by employing different chipping codes. For example, the IEEE 802.11b standard supports the use of Complementary Code Keying (CCK) modulation method for enabling data rates of 5.5 Mbps and 11 Mbps. A higher data rate extension of DSSS, CCK is less prone to multipath propagation interference (Petrick, 2002). With data rates reaching 11 Mbps, DSSS enabled WLANs support broadband applications and services (Littman, 2002).

Frequency Hopping Spread Spectrum (FHSS).

FHSS systems use conventional techniques to modulate a data signal with a carrier signal (Littman, 2002). The carrier frequency changes or hops multiple times per second following a sequence that is generated by pseudo-random algorithms. Consequently, FHSS transmissions are secure and extremely difficult to monitor because the FHSS receiver must utilize the sequence code to follow the frequency hops (Perez-Jimenez et al., 2001). Furthermore, Fast Frequency Hopping (FFH) refers to FHSS systems in which the hopping rate is faster than the bit rate. Slow Frequency Hopping (SFH) occurs when the hopping rate is slower than the bit rate.

When interference occurs, FHSS signals are retransmitted at different frequencies during subsequent hops (Littman, 2002). FHSS systems operating in the spectrum between the 2.400 and 2.483 GHz RF bands are required by FCC regulations to utilize a minimum of 75 hopping frequencies. FHSS technology supports data rates reaching 2 Mbps.

Orthogonal Frequency Division Multiplexing (OFDM).

OFDM is a spread spectrum modulation technique that divides a wide frequency band into multiple frequency bands that are narrow and precisely spaced (Gast, 2002). The orthogonality that this spacing provides prevents demodulators from receiving frequencies other than their own. The transmitted data are inverse multiplexed across multiple subchannels. Inverse multiplexing is a technique that breaks up a high-speed transmission into several low-speed transmissions. OFDM is employed by WLAN solutions based on the IEEE 802.11a and IEEE 802.11g standards. OFDM is capable of supporting data rates that are five times greater than the rates enabled with IEEE 802.11b CCK modulation.

Spread Spectrum Interference.

Spread spectrum systems are virtually unaffected by interference from conventional sources radiating in fixed and narrow areas of the frequency band ("*DSSS and FHSS*," 2002). However, these systems are affected by other spread spectrum systems operating in the same or adjacent frequency bands. The greater the number of FHSS devices in an area, the higher the probability that the systems will hop to the same frequency at the

same time. When this occurs, a small number of FHSS systems are able to prevent nearby DSSS systems from communicating. On the other hand, since DSSS systems are always transmitting on every frequency in the band, a FHSS system in the immediate area may not find a clear channel ("*DSSS and FHSS*," 2002).

Typically, DSSS system quality degrades at a greater rate than FHSS systems when competing for common air space ("*DSSS and FHSS*," 2002). For example, IEEE 802.11b WLANs that employ DSSS technology and 2.4 GHz FHSS cordless phones occupy the same frequency band. When placed in close proximity, the systems' transmissions often interfere with one another. The extent of the interference is variable and dependent on the hardware manufacturer, wireless device placement, and the construction and placement of objects such as walls and windows in the area. In most cases, IEEE 802.11b-compliant devices are impacted to a greater degree than FHSS cordless phones, thereby resulting in decreased transmission quality from factors such as lost packets, decreased signal to noise ratio, and decreased throughput.

Ultrawideband (UWB)

Leeper (2001) defines Ultrawideband (UWB) technology as a short range, low power wireless technology with a bandwidth greater than 25 percent of the radio system's center frequency. In addition, UWB systems emit very narrow pulses over a wide spectrum of frequencies (Leeper, 2001). First developed in the 1980s, UWB is primarily used in radar systems and to identify objects hidden underground or behind barriers.

The FCC's recent approval of UWB technology utilization in commercial applications and concomitant advances in low cost, low power switching technology, enable the use

of UWB technology in consumer-grade communication devices (Paulson, 2002). Paulson (2002) adds that the technology is most appropriate for small devices with limited power capacities such as smart cellular phones and Personal Digital Assistants (PDAs). In addition, UWB devices have low power and broadly spread signals for secure transmission. UWB devices employ a modulation technique that also ensures privacy, and only the UWB receiver is able to demodulate the exact pulse sequence generated by the UWB transmitter (Peretz, 2002). Interference between UWB appliances and other devices is minimal. UWB signals appear to be background noise to other devices.

Infrared

Infrared (IR) technology operates using invisible light waves with wavelengths between .75 and 1,000 microns (Geier, 1999b). These wavelengths exist in the portion of the electromagnetic spectrum that is just below visible light and are generated by Light Emitting Diodes (LEDs). Wireless implementations based on IR technology operate at distances ranging from zero meters to one meter and greater and support one-way or half-duplex and two-way or full-duplex data exchange (Littman, 2002).

Direct infrared platforms support point-to-point connections and are dependent on direct line of sight for transporting data (Littman, 2002). In contrast, diffuse infrared platforms support multipoint-to-multipoint connections and are not dependent on a direct line of sight for information transport. IR technology is flexible and reliable and is integrated into devices that include laptops, printers, PDAs, digital cameras, portable scanners, credit card readers, and overhead projectors.

Wireless LAN Standards and Wireless Standards Associations

Literature related to wireless LAN standards and the standards associations that develop and support the standards is reviewed in the following sections. The WLAN standards include the IEEE 802.11, IEEE 802.11 b, IEEE 802.11a, IEEE 802.11g, and IEEE 802.11x specifications and extensions developed by the IEEE organization. The ETSI HiperLAN-1 and HiperLAN-2 standards and the Japan Ministry of Post and Telecom (MPT) MMAC standard are also investigated. Finally, the HomeRF Working Group's HomeRF 1.0 and HomeRF 2.0 standards are explored.

IEEE 802.11

IEEE 802.11 is the first international standard for wireless LANs developed by the IEEE (O'Hara & Petrick, 1999). The IEEE is an organization of more than 377,000 engineers, scientists, and students in 150 countries ("*About the IEEE*," 2002). The IEEE is engaged in setting standards for computers and communications and produces 30 percent of the world's published literature in electrical engineering, computers, and control technology.

The IEEE 802.11 standard was adopted by the IEEE in 1997 and was subsequently revised in 1999 (Prasad, Kamerman, & Moelard, 2001). IEEE 802.11 is officially titled the IEEE Standard for wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. The standard establishes the framework for enabling wireless connectivity between mobile devices within the local area. Similar to other IEEE 802 standards such as IEEE 802.3 and IEEE 802.5, the IEEE 802.11 specification provides a

foundation for delivering MAC Service Data Units (MSDUs) between peer Logical Link Controls (LLCs) (Prasad et al., 2001).

Components of the IEEE 802.11 architecture include the station, the AP, the Basic Service Set (BSS), the Independent Basic Service Set (IBSS), and the Extended Service Set (ESS) (O'Hara & Petrick, 1999). A BSS consists of an AP and associated stations. An ESS is comprised of two or more BSSs in the same subnet. In contrast, an IBSS is made up of wireless devices communicating in a peer-to-peer or ad hoc mode without the use of an AP (O'Hara & Petrick, 1999).

The IEEE 802.11 standard supports three physical layers: DSSS, FHSS, and Infrared (IR) Physical Layer (PHY) (O'Hara & Petrick, 1999). The DSSS PHY and the FHSS PHY use the 2.4 GHz spectrum as the transmission medium. 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.

IEEE 802.11b.

According to Rappaport (2002), 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. The IEEE 802.11b standard is also known as Wireless Fidelity (Wi-Fi). The Wi-Fi logo was

created by the Wi-Fi Alliance to designate products that are compatible with the IEEE 802.11b standard (Rappaport, 2002).

IEEE 802.11b-compliant FWA Ethernet LANs transmit in ISM RF bands between the 2.400 GHz and 2.483 GHz frequencies and support license-exempt operations in fields that include education, government, business, and medicine (Littman, 2002). IEEE 802.11b-compliant systems support data, voice, and video transmission at rates reaching 11 Mbps, and WEP is employed to ensure transmission integrity (Littman, 2002).

Specifically, the IEEE 802.11b standard defines DSSS transmissions with data rate capabilities of 11 Mbps, 5.5 Mbps, 2 Mbps, and 1 Mbps (Rappaport, 2002). Furthermore, the IEEE 802.11 standard defines data rate in terms of available bit rate (O'Hara & Petrick, 1999). Available bit rate is often mistaken for aggregated data throughput. For example, the average aggregate data throughput of an IEEE 802.11 wireless network is between 75 percent and 85 percent of the data rate.

In addition to the IEEE organization, the Wi-Fi Alliance, a nonprofit international association formed in 1999, certifies the interoperability of broadband Fixed Wireless Access (FWA) Ethernet LAN products based on the IEEE 802.11 specification (Littman, 2002; "What is Wi-Fi," 2002). The organization has 193 member companies, and more than 522 WLAN products have received Wi-Fi certification ("What is Wi-Fi," 2002). Certified products feature Wi-Fi logos. The Wi-Fi Alliance was formerly known as the Wireless Ethernet Compatibility Alliance (WECA).

Wi-Fi certified IEEE 802.11b-compliant devices interoperate at the maximum data rate possible (Gast, 2002). This is accomplished using a data rate selection mechanism that automatically and dynamically determines and selects the transmission rate for

optimal communications. For example, when a transmission fails, a Wi-Fi certified device retransmits the lost message at the same data speed (Gast, 2002). If the second attempt fails, the device automatically switches to a slower rate to attempt retransmission. Transmissions at lower data rates may provide greater wireless range.

IEEE 802.11a.

Another physical layer extension to IEEE 802.11 is IEEE 802.11a (Rappaport, 2002). IEEE 802.11a-compliant FWA LANs enable the transmission of bandwidth-intensive data, voice, and video at data rates reaching 54 Mbps in the license-exempt U-NNI (Unlicensed-National Network Infrastructure) spectrum (Littman, 2002). The U-NNI spectrum is between the 5.15 GHz and 5.25 GHz frequencies and the 5.75 GHz and 5.825 GHz frequencies. Unlike IEEE 802.11b, which uses the Complimentary Code Keying (CCK) modulation scheme, the IEEE 802.11a standard employs OFDM to achieve higher data rates and overcome multipath interference (Rappaport, 2002).

As well as supporting greater throughput than IEEE 802.11b, IEEE 802.11a specifies eight non-overlapping channels in comparison to the three that are supported by the IEEE 802.11b specification (Crump, 2001a). Therefore, IEEE 802.11a-compliant solutions support operations in densely populated areas such as airports, convention centers, schools, and stock exchanges.

In contrast, IEEE 802.11b-compliant solutions operate in a lower frequency band and penetrate solid objects better than IEEE 802.11a-compliant networks (Crump, 2001a). These characteristics make IEEE 802.11a-compliant WLANs better suited for SOHO environments while IEEE 802.11b-compliant WLANs are most appropriate in

environments with obstacles and large coverage areas such as manufacturing plants, warehouses, distribution centers, and retail outlets (Crump, 2001a).

IEEE 802.11g.

The IEEE 802.11g Task Force, which was established by the IEEE 802.11 Working Group subsequent to the passage of the IEEE 802.11a and IEEE 802.11b extensions, recently drafted the IEEE 802.11g extension (Littman, 2002; “*Wireless LAN glossary*,” 2002). The IEEE 802.11g draft extension specifies data rates reaching 54 Mbps in the 2.4 GHz band (“*Wireless LAN glossary*,” 2002). Like the IEEE 802.11a extension, the IEEE 802.11g draft extension employs OFDM to achieve higher data rates. In addition, IEEE 802.11g-compliant solutions will be backward compatible with IEEE 802.11b-compliant systems since IEEE 802.11g-compliant solutions will implement all mandatory elements of the IEEE 802.11b extension and allow IEEE 802.11b-compliant clients to associate with IEEE 802.11g-compliant APs (Geier, 2002a). Finally, like IEEE 802.11b-compliant WLANs, IEEE 802.11g-compliant WLANs are most appropriate in environments with obstacles and large coverage areas such as manufacturing plants, warehouses, distribution centers, and retail outlets.

IEEE 802.11x.

IEEE 802.1x is a security protocol defined by the IEEE 802.11 specification (“*802.11 security*,” 2002). The IEEE 802.1x protocol describes how IEEE 802.1x-compliant WLANs employ the EAP authentication protocol to authenticate users via a RADIUS authentication server (Funk, 2002a). EAP traffic flows between the user's machine and

the RADIUS server, with the Access Point (AP) as the conduit. After successful authentication, the RADIUS server informs the AP, which then connects the user to the network (Funk, 2002a).

Since IEEE 802.1x is an asymmetric protocol, IEEE 802.1x-compliant networks authenticate the user, but the user does not authenticate the network (Funk, 2002a). Therefore, an attacker can fool the mobile station into connecting with the attacker's AP instead of the legitimate AP. This man-in-the-middle attack allows the attacker to eavesdrop on data transmitted between the mobile station and the legitimate AP. However, when IEEE 802.1x is combined with an authentication protocol such as EAP-TLS or EAP-TTLS, IEEE 802.1x-compliant WLANs provide port-based access control and mutual authentication between clients and APs via an authentication server ("*802.11 security*," 2002). IEEE802.1x-enabled WLANs also provide a method for distributing encryption keys dynamically to WLAN devices.

The evolving IEEE 802.11i security extension is also intended to eliminate man-in-the-middle attacks and other security weakness in the IEEE 802.11 family of specifications and extensions (Vaughan-Nichols, 2002). The IEEE 802.11i extension will specify encryption that is stronger than WEP. IEEE 802.11i replaces WEP's RC4 encryption algorithm with Temporal Key Integrity Protocol (TKIP) and Advanced Encryption System (AES).

European Telecommunications Standards Institute (ETSI)

The ETSI is a multinational body of 912 members from 54 countries with regulation and standardization authority over much of Europe ("*ETSI*," 2002). ETSI

represents administrations, network operators, manufacturers, service providers, and research bodies. The Institute develops a wide range of telecommunications, broadcasting, and information technology standards and technical documentation ("ETSI," 2002). Examples include the Global System for Mobile Communications (GSM), HiperLAN-1, and HiperLAN-2 standards.

High Performance Radio Local Area Network-Type 1 (HiperLAN-1).

The HiperLAN-1 specification defines operations, capabilities, and services enabled by Radio LAN (RLAN) solutions (Littman, 2002). HiperLAN-1 supports wireless connectivity between network nodes such as PCs, printers, servers, and consumer electronics equipment. The specification was developed by the ETSI in the mid 1990s and supports functionality similar to IEEE 802.11 (Rappaport, 2002). In addition, the European standard defines asynchronous data rates up to 20 Mbps in the 5 GHz frequency band ("ETSI HIPERLAN/1," 2002). HiperLAN-1-compliant networks are designed to operate at a distance of 50 meters and in vehicles moving at speeds up to 35 kilometer per hour (Rappaport, 2002).

High Performance Radio Local Area Network-Type 2 (HiperLAN-2).

HiperLAN-2 is a radio LAN (RLAN) specification, developed by the ETSI, that supports wireless operations and communications services in infrastructure-based and ad hoc configurations (Littman, 2002). HiperLAN-2-compliant systems operate in the license-exempt spectrum between the 5.15 GHz and 5.25 GHz frequencies, the 5.25 GHz and 5.35 GHz frequencies, and the 5.725 GHz and 5.825 GHz frequencies and are

capable of data rates reaching 54 Mbps at the Physical Layer (Littman, 2002; “*ETSI HIPERLAN/2*,” 2002).

According to Geier (2001), HiperLAN-2 and IEEE 802.11a technologies have similar physical layers and a connectionless protocol. However, HiperLAN-2 technology, an outcome of the Asynchronous Transfer Mode (ATM) development effort, employs more elements of ATM technology than elements of Ethernet technology (Geier, 2001).

HiperLAN-2 solutions provide Quality of Service (QoS) support for video, voice, and images in venues that include homes, offices, schools, hospitals, and factories.

HiperACCESS and HiperLINK.

In addition to the HiperLAN-1 and HiperLAN-2 specifications, HiperACCESS and HiperLINK were defined by the ETSI (Prasad & Prasad, 2001a). HiperACCESS systems operate in multiple frequency bands and provide fixed wireless broadband point-to-point communications with a typical data rate of 25 Mbps. Bolle (1998) adds that HiperACCESS systems provide long range and fixed radio connections to customer premises. In addition, HiperACCESS systems were designed to compete with and to complement other broadband wired access systems such as Digital Subscriber Line (DSL) and cable modems (Bolle, 1998).

HiperLINK technology, which operates in the 17 GHz frequency band, was developed as an interconnection between HiperLAN and HiperACCESS systems (Prasad & Prasad, 2001a). HiperLINK technology also provides data rates up to 155 Mbps and is capable of supporting multimedia applications. The combination of HiperLAN, HiperLINK, and HiperACCESS technologies yields a 100 percent wireless network solution.

Japan Ministry of Post and Telecom (MPT) Multimedia Mobile Access Communication (MMAC)

The Ministry of Post and Telecom (MPT) in Japan created the 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 by the MMAC standard: 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 that range between 3 GHz and 60 GHz (Prasad & Prasad, 2001a). This technology is appropriate for mobile video telephone conversations. MMAC Ultrahigh Speed WLAN systems transmit data at rates reaching 156 Mbps in the 30 GHz to 300 GHz frequency band and facilitate indoor videoconferences. Prototype MMAC WLAN systems operating in the 60 GHz band have demonstrated the feasibility of ATM and Ethernet interfaces with data rates reaching 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 data rates between 20 Mbps and 25 Mbps. Minor differences between Wireless ATM (WATM) and HiperLAN-2 exist in the protocol for intercellular synchronization. MMAC Ethernet wireless systems are compatible with the IEEE 802.11a standard. The fourth type of MMAC system is

Wireless Home-Link (Prasad & Prasad, 2001a). These systems are designed for indoor use and are able to transmit at data rates reaching 100 Mbps using frequencies that range between 3 GHz to 60 GHz. Wireless Home-Link systems are effective for the transmission of multimedia content between PCs and audiovisual equipment.

HomeRF Working Group

The HomeRF Working Group (HomeRF WG) is an organization of more than 100 computer, communications, and microelectronics manufacturers (Riera & Perez-Jimenez, 2001). The HomeRF WG develops and publishes specifications for wireless voice and data networking applications in the home in addition to fostering the development of wireless devices that support the delivery of streaming audio, streaming video, and broadband wireless Web connection outside the home (Littman, 2002). Standards published and promoted by the HomeRF WG include HomeRF 1.0 and HomeRF 2.0. Unlike the IEEE 802.11b standard, which was designed for corporate environments, HomeRF standards were developed to meet the needs of consumers in home networking applications ("*Home networking*," 2001).

HomeRF 1.0.

The HomeRF1.0 standard enables data rates from .8 Mbps to 1.6 Mbps in the 2.4 GHz frequency band (Prasad & Prasad, 2001a). HomeRF 1.0-compliant systems utilize the FHSS transmission technique with hop times of 300 microseconds. In addition, HomeRF 1.0-compliant networks provide a range of up to 50 meters, adequate to cover the typical home and yard.

HomeRF 2.0.

The second-generation HomeRF 2.0 standard enables new types of devices, applications, and services that include streaming video and CD (Compact Disc) quality audio ("*Home networking*," 2001). The HomeRF 2.0 standard employs Wideband Frequency Hopping (WBFH) and supports data rates up to 10 Mbps in the 2.4 GHz frequency band within a range of 50 meters (Prasad & Prasad, 2001a). HomeRF 2.0-compliant systems are backward compatible with HomeRF 1.0-compliant devices.

Caswell (2001) observed that devices using HomeRF 2.0 technology are in direct competition with those compliant with the IEEE 802.11b Wi-Fi standard. Proponents of the HomeRF 2.0 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 (Caswell, 2001). According to Caswell (2001), HomeRF 2.0-compliant WLANs' use of frequency hopping makes the solutions more secure and less susceptible to interference than IEEE 802.11b-compliant solutions. However, WiFi's market penetration currently offsets any disadvantages the technology possesses (Batista, 2000).

Infrared Data Association (IrDA)

The Infrared Data Association (IrDA) is an international organization established in 1992 to create and support low cost, interoperable, infrared data interconnection standards ("*The Infrared*," 2002). IrDA members include hardware, systems, software, and communications manufacturers. IrDA standards support a wide range of

communications, computing, and consumer devices and facilitate point-to-point, point-to-multipoint, and multipoint-to-multipoint connections (Littman, 2002).

The IrDA standard specifies the three levels of a network's architecture (Geier, 1999b). These levels are the IrDA Serial IR (IrDA-SIR) physical layer protocol, the Infrared Link Access Protocol (IrLAP) data link protocol, and the IrDA Link Management Protocol (IrLMP). IrDA-SIR enables half-duplex data rates at 115 Kbps. IrLAP enables the establishment of a logical relationship and the transmission of data between two IrDA-compliant machines (Rodbell, 2002). Finally, IrLMP specifies the mechanism to multiplex and handshake two or more simultaneous data streams and enables walk-up, ad hoc connection between devices (Santamaria, Vento-Alvarez, Rabadan, & Perez-Jimenez, 2001; Seaborne et al., 1996).

IrDA specifications also support high-speed networks (Littman, 2002). For example, the Fast Infrared (FIR) standard supports data rates up to 4 Mbps, and the Very Fast Infrared (VFIR) specification supports data rates reaching 16 Mbps.

According to Santamaria, Vento-Alvarez, Rabadan, and Perez-Jimenez (2001), 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. The interfaces between these elements are not defined in the IrDA standard (Santamaria et al., 2001).

The IrDA also publishes specifications to clarify the functionality of Infrared LAN (IrLAN) protocols (Littman, 2002). Typically, the IrLAN protocol is a passive protocol that defines a bi-channel interface between a protocol server and a protocol client (Santamaria et al., 2001). The IrLAN protocol enables an IrDA-compliant computer to connect to a LAN through an AP or to communicate with another computer as though the

IrDA-compliant computer is attached to a LAN. In addition, the IrLAN protocol allows an IrDA-compliant computer to attach to a LAN through a second LAN-attached computer (Santamaria et al., 2001). In this case, the second LAN-attached computer acts as an AP or gateway to the wired LAN.

Wireless LAN Security

According to Pescatore (2002), 85 percent of the wireless security incidents from the present-day until 2005 will be device-related instead of over-the-air related. Wireless devices are easily lost or stolen. Ensuring that the data on these devices are safe from unauthorized viewing is critical (Pescatore, 2002). Although the number of over-the-air security incidents is projected to be significantly lower, weaknesses in IEEE 802.11 security have been extensively explored in the literature. While WLANs offer users mobility within a networked environment, WLANs also have an increased risk of penetration from attackers capable of intercepting data and gaining access to network resources (Nichols & Lekkas, 2002).

Brewin (2001) observed that wireless security concerns have delayed WLAN deployments in many cases. For example, the Andersen Cancer Center in Houston put a hold on a pilot project to provide WLAN access at the center's five-building campus because of security issues (Brewin, 2001b). Best Buy deactivated the WLANs used in company stores (Smith, 2002). The corporate decision was made after a message was posted anonymously on the Internet that described how an in-store, point-of-sale WLAN could readily be penetrated by individuals in an adjacent parking lot.

Although the rate of enterprise WLAN implementations has slowed as a consequence of security issues, more than \$1.5 billion worth of IEEE 802.11 hardware is currently in service (Taschek, 2002). IT managers responsible for WLAN projects must weigh the risks before proceeding (Nichols & Lekkas, 2002). In addition, managers must counter the risk with an acceptable level of security relative to the nature of the enterprise data, corporate information policies, and government regulations. Decisions to employ WLAN technologies must take into consideration the safeguards needed to protect the integrity of enterprise resources and address employee health concerns.

IEEE 802.11 Security Vulnerabilities

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

Walker (2000) analyzed WEP encapsulation as defined by IEEE 802.11. The IEEE 802.11 standard defines the five elements used in WEP to encrypt the contents of data frames: four shared keys, a RC4 stream cipher encryption algorithm, a 24-bit Initialization Vector (IV), transport encapsulation, and the cyclic redundancy code (CRC) of the frame payload (Walker, 2000). According to Walker (2000), the inherent deficiency of the WEP encapsulation design was created by an attempt to adapt the RC4 security algorithm to an environment for which RC4 was not appropriate. In addition,

Walker (2000) proved the impossibility of solving WEP security problems by simply increasing the size of the secret key.

Walker (2000) established a series of recommendations to address WEP weaknesses. The recommendations included a new encryption cipher, a session key derivation algorithm, and a new WEP encapsulation. Specifically, the AES block cipher should serve as the basis for all of the proposed changes. A block cipher is a mathematical function that produces one output from two inputs ("*Block cipher*," 2002). In addition, an algorithm derived session key should be employed in the case of a manually configured WEP secret key. Walker (2000) also proposed that a redesigned WEP encapsulation should employ 128-bit AES as the cipher along with the use of AES in Offset Codebook Mode (OCB). In addition, a 32-bit sequence number should be used to indicate the number of frames to send under the present key.

Borisov, Goldberg, and Wagner (2001) described practical WEP attack techniques that employed keystream reuse and data dictionaries. A known weakness of stream ciphers is that reusing the same key to encrypt two messages can reveal plaintext information about both messages (Borisov, Goldberg, & Wagner, 2001). WEP employs the RC4 stream cipher. Once the plaintext of a message is obtained, an attacker is able to build a decryption dictionary of keystreams and decrypt subsequent ciphertext with very little work.

Secure protocol design is not a trivial task (Borisov et al., 2001). A thorough understanding of cryptographic properties is vital to the design of a secure WLAN standard. Also important are the reuse of previous designs and the public review of new designs by the cryptographic community. For example, the design of the IP Security

(IPSec) Protocol dealt with link-layer security and the dangers of using a CRC to ensure message integrity (Borisov et al., 2001). A public review of WEP before enactment may have revealed the flaws that currently exist in the standard.

Arbaugh, Shankar, and Wan (2001) discussed how a large number of organizations assume IEEE 802.11b-compliant WLANs are secure. This assumption is unsound because the access control mechanism employed by the IEEE 802.11b standard is flawed (Arbaugh, Shankar, & Wang, 2001). Weaknesses include insecurities related to Ethernet MAC address Access Control Lists (ACLs) and shared key authentication. Ethernet MAC ACLs do not provide adequate security because an attacker can easily determine the MAC addresses permitted to access the network because the addresses are transmitted in plaintext. In addition, WEP shared key authentication is exploited by monitoring mutual authentication messages and using the fixed structure of the message authentication protocol to decrypt the ciphertext. According to Arbaugh et al. (2001), a major overhaul of the current IEEE 802.11b standard is the only way to eliminate the security weaknesses.

The security of IEEE 802.11-compliant solutions was also compromised with the public release of the AirSnort and WEPcrack software tools that capture and decrypt WEP encryption keys (Delio, 2001). AirSnort and WEPcrack are practical demonstrations of the weaknesses in the key scheduling algorithm of RC4 stream cipher as explained by Fluhrer, Mantin, and Shamir (2001). The WEP RC4 encryption algorithm is made up of a user configured secret key concatenated with an IV (Fluhrer et al., 2001). The IV is determined by the transmitting station and varies with each transmitted frame.

Fluhrer et al. (2001) analyzed the key scheduling algorithm of RC4 that derives the initial state from a variable key size and described important weaknesses of the process. One weakness is the existence of a large number of weak IV keys. Weak keys are secret keys with a value for which RC4 will exhibit regularities in encryption or, in other cases, a poor level of encryption. Fluhrer et al. (2001) explained how the awareness of only a small number of weak keys is sufficient to derive the secret key and decrypt a WEP-secured transmission.

According to Bruestle and Hegerle (2002), 9,000 weak keys out of 16 million possible keys can be generated using 128-bit WEP. By capturing 2,000 to 4,000 packets with weak keys, the AirSnort application can decrypt a WEP password (Bruestle & Hegerle, 2002). Gast (2002) observed that the time required to decrypt a 128-bit password is directly proportional to the traffic on the WLAN. AirSnort requires approximately eight hours to recover a key from an IEEE 801.11b-compliant WLAN with a 30 percent traffic load (Gast, 2002).

Subsequent to the release of AirSnort, Agere Systems, a WLAN equipment manufacturer, announced a security enhancement to the company's Orinoco line of WLAN products (Baxter, 2001). The enhancement, WEPplus, prevents hacker programs such as AirSnort from exploiting the WEP weak key component by implementing WEP encryption in a manner that avoids the use of the IVs responsible for the generation of weak keys. WEPplus is interoperable with all IEEE 802.11b-compliant WLAN devices.

In addition to WLAN security weaknesses related to the IEEE 802.11 vulnerabilities and hacker tools such as AirSnort, problems resulting from unauthorized rogue WLAN connections also plague corporate WLANs (Chen, 2002). Gartner Research estimated

that at least 20 percent of businesses with LANs have rogue APs attached to company networks. WLAN monitoring tools such as AirMagnet, AiroPeek, NetStumbler, and WaveScanner allow network managers to locate rogue APs while walking or driving around company facilities (Chen, 2002).

Wireless LAN Security Enhancements

One of the greatest threats to WLAN security is the failure of network administrators to use any type of security (Garcia, 2002). Gartner Research estimated that 70 percent of all WLAN installations were initially implemented with little or no security (Crump, 2001b). Often WLANs are deployed with WEP disabled and Extended Service Set Identifiers (ESSIDs) set to broadcast periodically. The ESSID is an identifier applied to wireless APs and clients that allows devices on the same wireless network to recognize one another (Garcia, 2002). When wireless APs and clients are configured to broadcast the ESSID in plaintext, hackers are able to identify potential targets. Disabling this broadcast obscures the identity of the WLAN and hinders intruders.

The Wi-Fi Alliance recommends that one or more of the following steps be taken (Garcia, 2002). The first is to ensure that WEP is enabled. Next, the default ESSID should be changed and MAC address filtering should be applied. If available, session keys and a VPN system should be used. Finally, PC disk drives and file folders should be password protected.

In response to IEEE 802.11 WEP security weaknesses, third-party manufacturers developed a new class of hardware-based VPN products for WLANs (Garcia, 2002). Devices from ReefEdge, Blue Socket, SMC Networks, Vernier Networks, Netmotion,

Red-m, and Fortress Technologies increase security by isolating WLAN APs and clients from the wireline LAN (Garcia, 2002). Along with third-party solutions, wireless device manufacturers also develop proprietary security schemes. Agere's Advanced Mobile Security Architecture, Cisco's Lightweight Extensible Authentication Protocol technology (LEAP), 3Com's Dynamic Security Link, and Symbol's Keyguard provide advanced encryption mechanisms, user-based central authentication, and per-user session keys.

The IEEE formed Task Group I (TGi) to strengthen WLAN security (Garcia, 2002). TGi recommended the use of Temporal Key Integrity Protocol (TKIP) as a short-term solution. Compatible with existing IEEE 802.11b-compliant hardware, TKIP employs a method called fast-packet rekeying that changes encryption keys on a regular basis. In addition, TGi recommends the use of the IEEE 802.1x standard to secure WLANs.

Originally designed for wired networks, IEEE 802.1x provides a standard framework for granting port-based network access control (Garcia, 2002). Under IEEE 802.1x, a WLAN client is authenticated by an AP using an Extensible Authentication Protocol (EAP) compliant Remote Authentication Dial-In User Service (RADIUS) server. The RADIUS server uses the machine MAC address or a user password for authentication.

Since the IEEE 802.1x standard does not specify a method to implement EAP, various solutions have been developed (Garcia, 2002). EAP solutions available for deployment include EAP-MD5 (Message Digest 5), EAP-TLS (Transport Level Security), EAP-TTLS (Tunneled Transport Level Security), and Protected Extensible Authentication Protocol (PEAP). These EAP solutions vary in the use and management of security certificates and tokens. According to Funk (2002), the use of IEEE 802.1x is supported

by enterprise WLAN product manufacturers such as Agere, Avaya, Enterasys, Intermec, and Proxim. These manufacturers also endorse the use of IEEE 802.1x with EAP-TTLS (Funk, 2002b). IEEE 802.1x eliminates numerous flaws inherent in WEP. However, in the long term, the IEEE standards body intends to replace the flawed RC4 implementation with the AES security protocol by endorsing the IEEE 802.11i specification (Gast, 2002).

Finally, in response to increasing concerns about the vulnerabilities of WEP, the Wi-Fi Alliance in conjunction with the IEEE developed the Wi-Fi Protected Access (WPA) specification (Grimm, 2002). WPA is designed to replace WEP and addresses WEP security weaknesses such as hijacking and man-in-the-middle attacks by supporting a higher level of encryption and the dynamic exchange of encryption keys. WPA will be forward-compatible with the IEEE 802.11i security specification currently being developed by the IEEE (Grimm, 2002). Existing Wi-Fi certified products are software upgradeable to operate using WPA enabled security enhancements.

Wireless LAN Health and Safety Considerations

Consumer advocates and health awareness groups such as the Wireless Consumers Alliance have expressed health and safety concerns regarding devices that emit RF energy ("*Do wireless LANs*," 2002; "*WCA*," 2001; "*Wireless radio*," 2002). Health concerns have focused on RF emissions from microwave devices, cellular telephones, and WLAN devices. In 1993, Dr. George Carlo, an epidemiologist conducted a study that found genetic damage from cellular telephone radiation. In addition, Kenneth Foster, a bioengineering professor at the University of Pennsylvania, has cast doubt on the validity

of Specific Absorption Rate (SAR) unit of measure ("WCA," 2001). Cellular telephone manufacturers self-certify the SAR values of telephones with the FCC as an indication of safe device operation. In contrast to Carlo's investigation, two newer studies published in the New England Journal of Medicine and the American Journal of Medicine concluded that there is no connection between cellular telephone use and genetic damage and that further study was needed ("WCA," 2001).

Although there is scientific disagreement about the effect of cellular telephone radiation, the Standards Coordinating Committee 28 of the IEEE, the National Radiological Protection Boards (NRPB), and the International Radiation Protection Association's International Radiation Committee (IRPA/INIRC) have independently issued similar recommendations for the exposure to RF electromagnetic energy ("*Do wireless LANs*," 2002). In November 1992, the American National Standards Institute (ANSI) approved the IEEE C95.1-1991 standard that stated there were no verified reports of injury to human beings who have been exposed to electromagnetic fields within the frequency and SAR ranges specified in previous ANSI standards ("*Wireless radio*," 2002).

The operating frequencies, SARs, and output power of hand-held cellular telephones are within ANSI safe operating guidelines ("*Wireless radio*," 2002). In addition, the 600 milliwatts (mW) output power of the typical cellular phone is 20 times greater than the output power of an IEEE 802.11b-compliant WLAN device ("*Do wireless LANs*," 2002). Moreover, since radio waves fade rapidly over distance, human beings are exposed to a negligible quantity of RF energy in the area of a WLAN system.

Wireless LAN Initiatives in the Corporate Arena

According to Gartner Dataquest, corporations are leading the adoption of WLAN technology in the United States (Mostafa, Byrne, & Bruederle, 2001). However, the deployment of WLANs in large enterprises is developing more slowly (Campbell, 2001). Large enterprise WLANs are growing at a sluggish pace compared to those in small-sized and mid-sized businesses because of difficulty demonstrating WLAN cost justification to Chief Information Officers (CIOs) focused on cost savings. In addition, company size often determines the goals associated with WLAN implementation. For example, small companies view WLAN technology as an infrastructure solution and not a business solution. On the other hand, large enterprises see WLAN benefits as including employee flexibility and mobility.

General Motors

According to Moozakis (2001), General Motors (GM) Corporation is implementing WLANs throughout company plants and offices. The wireless project is one of GM's top technology priorities (Moozakis, 2001). GM's wireless deployment encompasses both new and existing facilities. The goal of the project is to give employees faster access to business information as they move about multiple work environments.

Cisco Aironet WLAN hardware is the standard at GM (Moozakis, 2001). GM estimates these IEEE 802.11b-compliant devices will provide more than enough bandwidth to handle the applications the system will support. The company does not have a master plan listing wireless applications. However, GM does plan to include wireless applications for managing inventory and remotely monitoring forklift trucks. Additional

wireless applications will be justified on a project-by-project basis. In addition, GM intends to use wireless LAN technology to connect temporary construction trailers that are typically hardwired (Moozakis, 2001).

Intel

Another example of a large company deploying WLAN technology is Intel Corporation ("*Wireless 802.11*," 2001). Intel is deploying IEEE 802.11b technology across the enterprise. In addition, the company is replacing desktop PCs with laptop PCs. In the present-day, more than 55 percent of the company's employees use mobile PCs worldwide. Benefits from the WLAN deployment include enhanced productivity and improved morale. For example, project teams are able to find documents, view presentations, send e-mail, and conduct Web searches while participating in project meetings.

Office Depot

Orenstein (2001) commented on Office Depot's use of IEEE 802.11b technology to extend the company's intranet to store managers and employees on the sales floor. The company selected Compaq iPaq Pocket PCs along with Symbol Technologies wireless Network Interface Cards (NIC)s to serve as the wireless application platform (Orenstein, 2001b). The goal of Office Depot's WLAN deployment is to give managers the ability to track sales and inventory numbers while walking around the store. In addition, customer product inquiries can be quickly answered by sales associates using wireless handhelds. One of Office Depot's ongoing challenges is to familiarize 30,000 employees with a

variety of product information. The company envisions the new wireless application platform coupled to an existing product knowledge database as a cost effective solution to this problem (Orenstein, 2001b).

Corrugated Supplies Company

Corrugated Supplies Company is another example of WLAN technology deployed in a manufacturing environment (Joch, 2001). The company produces corrugated cardboard in a 100,000 square foot manufacturing plant. After wirelessly enabling the entire facility with an IEEE 802.11b WLAN, the company significantly improved the order ship-through rate to 50 percent of orders within 24 hours. The gain was attributed to business process improvements and operating efficiencies brought on by the use of forklift-mounted wireless data entry terminals. In addition to the in-building WLAN, the company installed a 22 Mbps building-to-building wireless bridge and eliminated the cost of a T-1 data connection.

WLAN Vendor Offerings

During the 1990s, WLAN hardware manufacturers transitioned from high-cost, proprietary, low-bandwidth WLAN systems to low-cost, standards-based, high-bandwidth solutions (Dulaney, 2002). WLAN hardware based upon the IEEE 802.11b standard was introduced in late 1999 (Janowski & Chang, 2002). Since then, IEEE 802.11b-compliant hardware has become both mature and reasonably priced. For example, a low-cost AP may be purchased for less than \$200 and a wireless NIC for less than \$50 (Janowski & Chang, 2002).

The number of manufacturers offering WLAN products has grown to more than 20 (Henderson, 2002). Companies manufacturing enterprise WLAN systems include Agere, Cisco, Enterasys, Intermec, Proxim, and Symbol (Dulaney, 2002). Cisco has been targeting large enterprises with product innovations in the areas of management and security. In addition to APs and wireless NICs, manufacturers offer a variety of WLAN interfaces ("*Wireless network*," 2002). Examples include wireless print servers, Peripheral Component Interconnect (PCI) wireless adapters, Universal Serial Bus (USB) wireless adapters, Compact Flash wireless adapters, Ethernet-to-wireless bridges, and wireless digital cameras.

PC manufacturers such as Dell, Compaq, and Toshiba offer IEEE 802.11 wireless solutions as an integral part of notebook computers (Sicher, 2002). Along with plug-in WLAN PCMCIA (Personal Computer Memory Card International Association) PC Cards, PC manufacturers install internal Mini PCI embedded wireless NICs. Present-day IEEE 802.11b technology is being replaced by embedded and plug-in multi-band radios and NICs that are compatible with a range of technologies including IEEE 802.11a, IEEE 802.11g, General Packet Radio Service (GPRS), and CDMA2000 (Sicher, 2002). Computer manufacturers such as Dell, Compaq, and Toshiba view this multi-band approach as the most effective way of integrating the growing number of wireless solutions available in the marketplace.

WLAN hardware manufacturers such as Intel, Proxim, Symbol, Linksys, and Netgear recently began releasing IEEE 802.11a APs and radio NICs (Geier, 2002b; Molta & Laxminarayanan, 2002). This has complicated the process of determining which WLAN technology effectively suites the needs of a particular enterprise. One solution may lie in

proposed WLAN radio cards capable of supporting multiple standards such as IEEE 802.11a, IEEE 802.11b, and IEEE 802.11g along with 3G (Third-Generation) protocols. For example, Atheros Communications manufactures a chip set with support for IEEE 802.11a, the IEEE 802.11g draft standard, and the IEEE 802.11b standard (Churchill, 2002).

Wireless LAN Service Providers

Wireless LAN service providers offer broadband connectivity to mobile users in public areas called “hot spots” (Redman & Chapman, 2002, p. 1). These hot spots include airports, hotels, convention centers, and restaurants. Mobile employees equipped with IEEE 802.11b WLAN hardware are able to use a VPN, access e-mail, or execute enterprise applications. The services compliment the 2.5G (2.5 Generation) and 3G digital cellular communications services that are just beginning to roll out. However, these services do not provide the bandwidth required by in-building mobile users. For example, deployments by AT&T Wireless and T-Mobile, based on 2.5G GPRS technology, provide a maximum transfer rate of 144 Kbps (Mitchell & Kay, 2001). 3G cellular communications solutions such as CDMA2000 and Wideband Code Division Multiple Access (W-CDMA) are capable of transmission rates of 2.4 Mbps and 2.0 Mbps respectively (Littman, 2002).

Analysts predict that by 2005, over 80 percent of professional notebook PCs worldwide will have an IEEE 802.11 interface and 10 percent of the broadband Internet connections will be available through WLAN service providers (Keene & Calvert, 2002). Factors accelerating the growth of publicly accessible WLANs include low deployment

costs and the relatively low cost of remote access to high-bandwidth service in comparison to 3G cellular communications services. In addition, site operators of hotels, airports, retail outlets, municipal buildings, and railroad terminals have an active interest in wireless networking technology and the value publicly accessible WLANs provide (Keene & Calvert, 2002).

The primary WLAN service providers in the United States include T-Mobile, WiFi Metro, and Wayport (Redman & Chapman, 2002). These companies offer IEEE 802.11b wireless connections in hundreds of locations across the country. The number of publicly accessible APs is expected to grow to 41,000 by 2007 ("*Public WLANs*," 2002). In addition to these service providers, companies such as Boingo, iPass, and GRIC resell multiple WLAN services so that users do not have to limit selection to just one wireless network (Redman & Chapman, 2002). Boingo also provides users with a wireless sniffer program that identifies available commercial, private, and free wireless networks.

In Europe, Sonera, and Telia offer IEEE 802.11b WLAN service to customers in Scandinavia (Keene & Calvert, 2002). The company's service provides WLAN access to intranet applications and the Internet in hotels, convention centers, motorway services, railway stations, and airports. In summary, publicly accessible WLANs in the United States and overseas are just beginning to emerge and will remain secondary to wide-area cellular networks. Publicly accessible WLAN coverage needs improvement and analysts estimate that coverage will not be adequate until 2004.

Wireless LAN Strategy

Enterprises preparing to install WLANs should implement them as part of an overall wireless strategy (Sbihli, 2002). This wireless strategy should be separate from, yet link to, a company's technology and business strategies. A wireless strategy is necessary for three important reasons. First, not having a strategy is a strategy. The lack of a wireless strategy allows employees, departments, and facilities to implement freely any type of WLAN technology. Inevitably, this lack of a plan leads to an environment in which multiple standards, devices, and applications exist. WLAN technologies deployed in such a manner are difficult, if not impossible, to manage and secure (Sbihli, 2002).

The second reason to have a wireless strategy is to leverage investments (Sbihli, 2002). For example, without a strategy a company might install WLANs in manufacturing facilities to interconnect plant-floor automation controllers. However, these WLANs may not satisfy the requirements of a new project to provide plant dockworkers with an efficient way to perform shipping, receiving, and inventory functions. Finally, the third reason to develop a wireless strategy is to create tangible business value. This value is created by executing projects in a logical manner with the highest potential for a return. In addition, avoiding applications not suited for WLAN technology creates value (Sbihli, 2002). For example, utilizing a WLAN to interconnect fixed Computer Aided Design (CAD) workstations would provide operators a less than optimal work environment due to the substantial data rate and bandwidth requirements of the workstations.

The process of creating a WLAN strategic plan is addressed by Whitten et al. (1994) in a discussion of Phase 1, the Systems Planning Phase, of the MSDLC. In the Systems

Planning Phase, the investigator identifies and prioritizes those WLAN technologies and applications that will return the most business value (Whitten et al., 1994). The first step of the Systems Planning Phase is to study the business mission and to develop business requirements to achieve the mission. For example, a company with a business mission to respond faster to customer order status requests might have a business requirement for sales representatives to access order information while moving about company manufacturing facilities.

The second step of the Systems Planning Phase is to use these business requirements to develop the high-level information architecture for WLAN systems that mirror and support the business mission (Whitten et al., 1994). This step begins by defining the status of network technology deployed in the enterprise, restating goals based on the requirements, and identifying resources available for allocation (Rosser, 1997). Examples include the mapping of areas where WLAN connectivity would have the greatest impact, and the adoption of WLAN solution standards.

Finally, the third step of the Systems Planning Phase is the evaluation of the business area and information architecture to identify and prioritize WLAN implementation projects (Whitten et al., 1994). This step weighs the proposed WLAN projects and determines which to execute and why (Rosser, 1997). Considerations should include changing WLAN standards and the predictability of the technology. A description of the projects along with the reasons why the projects are chosen is a key aspect of this step. One example would be the installation of wireless barcode scanners to support a business initiative to monitor and reduce a manufacturing facility's Work in Progress (WIP) inventory.

Summary of Knowns and Unknowns

The principal focus of this investigation will be to define procedures for enabling large manufacturing enterprises to effectively plan, design, and implement WLANs. WLANs have been in use since 1990 (Prasad & Prasad, 2001b). A great deal has been written about WLAN technologies, standards, security, hardware, deployment, tactics, and strategy. For example, seminal papers by Walker (2000), Arbaugh et al. (2001) from the University of Maryland, and Borisov et al. (2001) from the University of California at Berkeley demonstrated the weaknesses of IEEE 802.11 access control mechanisms (Gast, 2002). In addition, Mishra and Arbaugh (2002) subsequently pointed out problems with the IEEE 802.1x security protocol, one proposed method of strengthening IEEE 802.11 security.

While the insecurity of IEEE 802.11b-compliant is known, what is not clear is the most effective method to secure existing and future enterprise WLANs (Geier, 2001). In addition, when deployments are global in scope, the most appropriate WLAN standard is also uncertain. Standards include IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, HiperLAN-1, HiperLAN-2, MMAC, and HomeRF. As existing wireless standards continue to develop and new standards are created, a number of challenges must be addressed by those responsible for the deployment of WLANs across a global manufacturing enterprise. These challenges include questions about the effectiveness of WLAN security solutions, the ease of installation and management of WLANs, and the long-term viability and interoperability of differing WLAN technologies

Contribution to the Field

This research will contribute to the field of information systems by providing a model to plan, analyze, design, implement, and support enterprise WLAN deployments. The model will be based upon lessons learned from a case study of four WLAN projects conducted by the investigator at AAM: Wireless Connectivity in Executive Conference Rooms, AAMatHome, Enhanced WLAN Security, and Wireless Connectivity on the Plant-Floor.

There is considerable debate about the effectiveness, capabilities, and functions of WLAN solutions (Dulaney, 2002; Geier, 1999; Rogak, 2001; Sbihli, 2002). In addition, there is a real need for a WLAN deployment model that encompasses the diverse environments and issues encountered in global manufacturing enterprises by Chief Information Officers (CIOs), Chief Technical Officers (CTOs), information systems managers, network engineers, and WLAN architects. The goal of this research is to create such a model.

Summary

The review of literature provided above established the background of the investigation. The chapter began with a 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 literature was organized into seven subject areas: wireless LAN technologies, wireless standards and wireless standards associations, wireless LAN security, wireless LAN initiatives, wireless LAN vendor offerings, wireless LAN service providers, and wireless

LAN strategy. In addition, a summary of what is known and unknown about the topic along with a discussion of the contribution the study will make to the field of information systems were presented.

Chapter 3

Methodology

In this chapter, this investigator began by describing the methodology that will be employed by this researcher during the course of the investigation. The chapter begins with a discussion of the case study method. This method will provide the conceptual framework for the research. Next, the role the MSDLC method in this investigation and the primary audience for the study are described. The chapter continues with an examination of the specific procedures that will be utilized to conduct the study. This is followed by a discussion of how results will be presented along with an explanation of the projected outcomes of the research. In addition, the resource requirements for the investigation are explained. Finally, a discussion of the reliability and validity of the results are provided along with a summary of the chapter.

Research Method to Be Employed

The case study method will be used by the investigator to provide the framework for the inquiry. Specifically, the model that will be developed as the goal of this investigation will be based on an in-depth case study of WLAN projects to be implemented by the researcher at AAM, previous research reported in the literature, and the MSDLC strategy defined by Whitten et al. (1994). Four WLAN initiatives are the subject of the case study: Wireless Connectivity in Executive Conference Rooms, AAMatHome, Enhanced WLAN

Security, and Wireless Connectivity on the Plant-Floor. These projects will be implemented simultaneously using the MSDLC systems analysis and design method as described by Whitten et al. (1994). In addition, the MSDLC method will be used as the framework for the model, which is the goal of the research.

Case Study

According to Yin (1994), a case study is an empirical analysis that investigates contemporary events when the delineation between the occurrences and context is not readily apparent. In general, case studies are the correct research strategy when “how” or “why” questions are being asked (Yin, 1994, p. 6). Other instances that favor the use of the case study method are when the focus is contemporary as opposed to historical or when the researcher has very little control over events. Although considered a form of qualitative research, case studies often contain a mix of qualitative and quantitative evidence. In addition, case study research does not always include direct observation as a data source. Researchers using the case study method seek to describe, understand, and explain (Winegardner, 1998).

There are three common types of case studies: exploratory, explanatory, and descriptive (Tellis, 1997). Exploratory case studies are frequently conducted prior to the definition of research questions and hypotheses. However, the framework of the research is always constructed first. These pilot endeavors are useful in deciding which protocols will be used in the final project. In addition, exploratory studies are suitable when the existing knowledge and the available literature are limited or a major component of the study is uncertain (Yin, 1994).

Explanatory case studies are appropriate in causal research such as when an investigator seeks to identify patterns and to relate methodically one observed variation to another (Winegardner, 1998). Questions related to “how” and “why” are most likely to foster an explanatory case study (Yin, 1994, p. 6). Finally, descriptive case studies begin with a descriptive theory that covers the depth and scope of the case being studied (Yin, 1994). The use of pattern matching in descriptive case studies is relevant as long as the predicted pattern of variables is defined before data are collected. In addition, both descriptive and explanatory cases studies are able to communicate research-based information about an event to individuals outside the field of study. This ability to converse with the non-specialist extends the role of these case study types beyond that of other research methodologies.

When designing a case study, the researcher should consider five components of the process: study questions, study propositions, unit of analysis, linking data to propositions, and criteria for interpreting results (Yin, 1994). Defining the research questions is the first task in conducting a case study. These will most likely be how and why questions. The research questions should enable the researcher to achieve the goal and be answerable in the research environment (Gillham, 2000).

Next, the study’s propositions, which are often derived from the questions, are developed to aid in focusing on the goals of the study (Yin, 1994). The unit of analysis component defines the primary unit of analysis such as employee, groups, departments, or manufacturing facility. Finally, the fourth component, linking the data to propositions, and the fifth component, selecting criteria for interpreting the findings, are the data analysis steps of the case study design process. Although a case study design should lay

the foundation for the data analysis, these components are often the least developed part of a case study design.

Modern Systems Development Life Cycle (MSDLC)

The MSDLC method will play two important roles during the investigation. First, the MSDLC method will provide the framework for the model, which is the end result of the research. Second, the MSDLC approach will serve as the framework for execution of the WLAN initiatives at AAM. The following is a brief overview of the MSDLC method.

MSDLC is a disciplined approach to developing and implementing IT solutions (Whitten et al., 1994). The method is used by engineers, systems analysts, programmers, and IT project managers to construct computer applications and information systems such as an enterprise WLAN. The MSDLC method consists of five high-level phases, specifically, the Systems Planning, Systems Analysis, Systems Design, Systems Implementation, and Systems Support Phases. The primary difference between the MSDLC and the classic Systems Development Life Cycle (SDLC) is the addition of the Systems Planning Phase (Whitten et al., 1994). The classic SDLC method consists of only four high-level phases, specifically, the Systems Analysis, Systems Design, Systems Implementation, and Systems Support Phases.

Phase 1 of the MSDLC involves Systems Planning (Whitten et al., 1994). The goal of Phase 1 is to discover and prioritize information systems that would most benefit the enterprise. Decisions in the form of information systems plans and formal projects are derived from the company's business mission and existing system characteristics and limitations.

Phase 2 of the MSDLC is Systems Analysis (Whitten et al., 1994). Unlike Systems Planning, the scope of Phase 2 is a single information systems application. In Phase 2, a specific business problem is analyzed and then the business requirements for an information system to solve the problem are determined. The key deliverable of Phase 2 is a business requirements statement that explains what users need.

Phase 3, the Systems Design Phase, involves an examination of a single information systems application (Whitten et al., 1994). The purpose of Phase 3 is to design a computer-based solution that fulfills previously determined business requirements. The technical design statement, which is the result of Phase 3, describes how the system will meet the business requirements.

Next, Phase 4, the Systems Implementation Phase, assembles the technical components to produce the new or improved information system (Whitten et al., 1994). In addition to a production system that meets the day-to-day needs of the organization, system documentation and training are also important components of Phase 4.

Finally, Phase 5 is the Systems Support Phase (Whitten et al., 1994). The maintenance of the production information system is the focus during this period. The Systems Support Phase continues until the system is replaced or no longer required. At that time, the five-step MSDLC process begins all over again.

In light of the above discussion of the case study method and the MSDLC approach, an explanatory case study of AAM WLAN initiatives implemented using the MSDLC model should yield answers to the research problem. The focus of the investigation is contemporary, and the primary question to be answered by the investigation is how to effectively plan, design, and implement WLAN technologies in a large manufacturing

enterprise. As discussed by Yin (1994), “how” questions are likely to lead to the use of an explanatory case study (Yin, 1994, p. 6). In addition, the MSDLC model is well suited for the implementation of information technologies such as those to be deployed as part of AAM’s four WLAN initiatives (Whitten et al., 1994).

Audience

The primary audience of the case study will be IT managers, network engineers, WLAN architects, CIOs, and CTOs. As is often the case with explanatory case studies, the investigator also intends to communicate with individuals outside the field of study (Yin, 1994).

Specific Procedures to Be Employed

The specific procedures to be employed during this investigation will follow the case study guidelines as defined by Yin (1994) and the MSDLC approach as described by Whitten et al. (1994). First, the MSDLC framework will be used to plan, design, and implement four WLAN initiatives at AAM. Next, the case study method will be employed to analyze, interpret, and report the results of the AAM WLAN deployment.

AAM Wireless LAN Initiatives

The implementation and investigation of the AAM WLAN initiatives will be carried out with AAM’s full support. The company’s CIO granted the wireless project full approval and funding on December 12, 2001 (see Appendix A for signed approval letter).

The researcher who is Advanced Technology Manager of AAM's IT Department will serve as project manager for the WLAN initiatives.

The following sections provide detailed descriptions of the four AAM WLAN initiatives: Wireless Connectivity in Executive Conference Rooms, AAMatHome, Enhanced Wireless LAN Security, and Wireless Connectivity on the Plant-Floor. Topics included are the background, goal and scope, assumptions, managerial and technical considerations, functional and physical constraints, target population, resources, MSDLC timeline, and determination of success for each of the WLAN projects.

Wireless Connectivity in Executive Conference Rooms.

AAM senior executives travel to each of the company's manufacturing facilities on a quarterly basis to conduct operations reviews. The productivity and efficiency of the visited plant are examined during these meetings. While attending the all day meetings, managers are unable to access corporate computer applications without considerable effort and inconvenience since multiple PCs are not available in the executive conference rooms (Blair, 2002). In addition, only a limited number of the executives have laptop computers to bring to the meetings.

The goal of the executive conference room WLAN initiative will be to provide AAM senior leadership with access to corporate applications such as e-mail, Factory Information System (FIS), Enterprise Resource Planning (ERP), and the Internet during quarterly operations reviews. The wireless coverage provided in these conference rooms will also be available for employees at other meetings. In addition, employees working in

adjacent office areas will benefit because each AP will provide coverage for an area much larger than the typical conference room (Geier, 2001).

This project will include the evaluation, selection, and installation of 25 IEEE 802.11b-compliant wireless APs at AAM locations worldwide. In addition, approximately 70 AAM laptops will be configured to connect to the conference room WLANs. The executive conference rooms at 12 AAM locations will be enabled with WLANs. These locations include Detroit Corporate Headquarters, Detroit Gear and Axle Plant, Detroit Forge Plant, Three Rivers Driveline Plant, MSP Industries, Rochester Technical Center, Global Procurement Center, Colfor Manufacturing, Buffalo Gear and Axle Plant, Tonawanda Forge Plant, AAM de Mexico, and Albion Automotive.

The following assumptions are made related to the project. Many executives attending the operations reviews have minimal PC and networking expertise. Therefore, the process of connecting to a conference room WLAN must be transparent. In addition, it is assumed that if an executive does not currently have a laptop computer, one will be provided as part of the project.

Managerial and technical considerations include the ability of the existing network support team to remotely configure and manage the wireless devices with little or no support at the local venue. In addition, the initial installation of the WLAN equipment in many cases must be plug and play because of the limited expertise at the local site.

Each WLAN device must be standards-compatible and interoperate with the company's PC hardware and software and on-site network infrastructure. WLAN devices must be unobtrusive once installed. AAM executive management is concerned with aesthetics.

The target population that will benefit from the conference room WLAN initiative is the regular attendees of the quarterly operations review meetings. This group includes the AAM executive staff along with the management staff at each of the plants. In addition, other AAM employees will be able to use the WLAN when the operations review meetings are not in session.

The researcher, acting in the role of Project Manager, will handle day-to-day project activities. In addition, AAM network engineers along with IT support personnel from each AAM facility will provide assistance. Project-related software, hardware, and laptop computers will be purchased with funds allocated from the IT Department budget.

The timeline to complete the executive conference room WLAN project is estimated to extend over a four to six month period. The Systems Planning Phase or Phase 1 and the Systems Analysis Phase or Phase 2 should be completed in one month. The Systems Planning Phase of the project will identify the locations of all operations review conference rooms along with other locations in which wireless connectivity can have a positive impact on AAM's executive leadership. The Systems Analysis Phase of the project will determine the business requirements of the WLAN systems that will be needed to connect executives during operations review meetings. Phase 2 will also include a detailed review of user needs, current network infrastructure, and existing conference room environments.

The Systems Design Phase or Phase 3 of the project should be completed in one to two months. Phase 3 will focus on the WLAN design and include the selection, purchase, and testing of available WLAN hardware along with the management software required to manage remotely all network attached wireless devices. Next, the Systems

Implementation Phase or Phase 4 is expected to last from one to three months. Phase 4 will focus on WLAN and laptop computer hardware and software procurement, configuration, installation, and testing. In addition, system documentation and training will be developed and distributed during the Systems Implementation Phase. Finally, the Systems Support Phase or Phase 5 of the WLAN project will be ongoing until the conference room WLAN equipment is either upgraded or replaced.

The success of the WLAN initiative in the executive conference rooms will be determined by factors that include the system's effectiveness and transparency to the users. In addition, the amount of time and money required to install the WLAN along with the reliability of the wireless network will be important factors. Finally, the scalability of the WLAN for use in other office areas throughout AAM will be an important measure.

AAMatHome.

AAM provides remote access to the AAM network through a dial-up modem pool (Blair, 2002). The slow data rate of these connections limits the effectiveness of AAM's remote users. Consequently, only a limited number of employees utilize the remote access service.

The goal of the AAMatHome project will be to investigate the use of WLAN technologies for AAM's executive staff to use at residential locations. The project will include the evaluation, selection, and implementation of a wireless solution to enable AAM's executive staff to access AAM applications. Integral to the project will be the installation of broadband Internet connections along with WLANs. In addition, a VPN

server and a Terminal Services (TS) server will be installed on the AAM LAN to facilitate the connection of AAMatHome users to commonly used AAM applications via fast, secure connections. These applications will include Microsoft Office Pro, Microsoft Project, Microsoft Outlook, Microsoft Publisher, Microsoft Visio, FIS, ERP, and the AAM Portal.

Assumptions will be made related to this project. The first is that high-speed broadband service will be available to the selected residences. In addition, the PCs that will facilitate access to the AAMatHome service will be loaded with the Microsoft Windows 2000 or Windows XP operating systems.

Managerial and technical considerations include the ability to remotely configure and monitor the residential WLAN. This will allow for a proactive response in resolving networking problems and minimize the downtime experienced by the executive users. In addition, the WLAN equipment will also need to facilitate the connection of other household computers to the Internet.

All WLAN devices must interoperate with the broadband Internet Service Provider's (ISP's) Customer Premises Equipment (CPE) in addition to existing computer and network equipment in the residence. WLAN devices must be located in close proximity to the broadband ISP's equipment and be unobtrusive once installed. The location of existing telephone or cable television cabling will often determine the position of WLAN devices because of the time and expense required to relocate the in-place wiring.

The target population that will benefit from the AAMatHome initiative will be members of AAM's executive staff. In addition, if existing home computers are connected to the WLAN, other household occupants may potentially benefit.

The researcher, acting in the role of Project Manager, will work with the Advanced Technology Systems Engineer to handle day-to-day project activities. In addition, the assistance of technicians from the broadband service provider will be necessary. Project-related software, hardware, and laptop computers will be purchased with funds allocated from the IT Department budget.

The timeline to complete the AAMatHome project is estimated to extend over a 12 to 14 month period. The Systems Planning Phase or Phase 1 and the Systems Analysis Phase or Phase 2 should be completed in one month. The Systems Planning Phase of the project will identify the locations of all the executive residences to be connected. The Systems Analysis Phase of the project will determine the business requirements of the WLAN, broadband service availability, and VPN and TS servers that will be needed to connect the executive residences to AAM applications and the Internet. Phase 2 will also include a detailed review of user needs, VPN and TS applications, and the availability of broadband service providers.

The Systems Design Phase or Phase 3 of the project should be completed in two months. Phase 3 will focus on the WLAN, VPN, and TS design and include the selection, purchase, and testing of WLAN, VPN, and TS hardware and software. Next, the Systems Implementation Phase or Phase 4 is expected to last from nine to 11 months. Phase 4 will focus on the procurement, configuration, and test of the WLAN, VPN and TS servers, and broadband hardware, software, and services. In addition, system documentation and training will be developed and distributed during the Systems Implementation Phase or Phase 4. Finally, the Systems Support Phase or Phase 5 of the AAMatHome project will be ongoing until the service is either upgraded or replaced.

The success of the AAMatHome initiative will be determined by factors that include the speed, reliability, and convenience with which AAM's executive staff is able to connect wirelessly to AAM's applications and the Internet. In addition, the applicability of the AAMatHome service model to the residences of AAM's other employees will be a factor.

Enhanced Wireless LAN Security.

Information systems security is a primary concern of the AAM IT Department. Issues related to the insecurity of IEEE 802.11 wireless networks must be addressed as the company deploys these technologies as part of the WLAN initiatives discussed in this research (Walker, 2000). The goal of the enhanced WLAN security initiative is to minimize the risk to AAM's information systems from the addition of WLAN devices to the company's network infrastructure.

The scope of the WLAN security 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 solution (Borisov et al., 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 Systems Implementation Phase or Phase 4 of this project include hardware-based VPN products manufactured by ReefEdge, Blue Socket, SMC Networks, Vernier Networks, Netmotion, Red-m, and Fortress Technologies (Garcia, 2002). Software-based WLAN security solutions from Microsoft and Funk Software will also be evaluated. In addition, the

project will evaluate, select, and implement a tool to detect unauthorized wireless APs that are illegally attached to the AAM network. The threat from unauthorized APs has increased significantly since the release of wireless hacking tools such as AirSnort (Delio, 2001).

Assumptions will be made related to this project. The first is that IEEE 802.11b WEP security will not adequately protect AAM's IT resources. In addition, it will be assumed that if an enhanced security solution is not implemented at AAM, the company's wireless and wireline networks will be exposed to attack from cyberintruders.

Managerial and technical considerations include the ability of the existing IT security and network teams to deploy, configure, and manage the selected security solution with existing resources from a central location. In addition, the solution must be upgradeable as new wireless security risks are identified in the literature. The security solution must also be transparent to the wireless user and not require the use of physical tokens for authentication. Finally, the security solution must not significantly affect WLAN data throughput.

The target population that will benefit from the enhanced WLAN security initiative is the AAM organization. Enhanced WLAN security will protect AAM's information assets. In addition, increased WLAN security in the residences of AAM executives will guard their PCs and information resources from unauthorized exposure.

A number of resources will be required to complete the WLAN security project. The researcher, acting in the role of Project Manager, will work with the Advanced Technology Systems Engineer to handle day-to-day project activities. In addition, the

assistance of AAM's security and network engineers will be necessary. Project-related software and hardware will be purchased with funds allocated from the IT budget.

The timeline to complete the enhanced WLAN security initiative is estimated to extend over a 12-month period. The Systems Planning Phase or Phase 1 and Systems Analysis Phase or Phase 2 should be completed in two to four months. The Systems Planning Phase of the project will identify and prioritize which IT assets, corporate information, and manufacturing equipment that would be most at risk if WLAN security were compromised. The Systems Analysis Phase of the project will determine which wireless security solution is most appropriate for use by AAM. Phase 2 will also include a detailed review of corporate wireless security requirements.

The Systems Design Phase or Phase 3 of the project will take two to three months to complete. Phase 3 will focus on the security architecture that includes the selection and testing of proprietary and standards-based wireless security hardware and software. Next, the Systems Implementation Phase or Phase 4 of the project is estimated to take four to six months to finish. Phase 4 will concentrate on the procurement, configuration, installation, and test of the security solution. In addition, system documentation and training will be developed and distributed during the Systems Implementation Phase. Finally, the Systems Support Phase or Phase 5 of the enhanced WLAN security project will be ongoing until the security solution is either upgraded or replaced.

The success of the WLAN security initiative will be determined by a number of factors. These include the level of protection the system provides to AAM's wireless and wireline networks and the reliability and scalability of the solution as the use of wireless LANs increases in AAM facilities.

Wireless Connectivity on the Plant-Floor.

The AAM Detroit Forge Plant has been forging automotive driveline products since 1918 (Manardo, 2001b). The facility produces axle shafts, output shafts, pinions, connecting rods, rod caps, and stabilizer bars for light trucks using a variety of special purpose automation and robotics that include 6-axis, electric, servo-controlled part transfer robots and numerically controlled bending lines. The facility has an existing network infrastructure that consists of an ATM fiber optic backbone linked to Ethernet and Fast Ethernet wired connections interfaced to the client desktops (Blair, 2002). However, the Programmable Logic Controllers (PLCs) that operate the manufacturing automation used to forge axles and bend stabilizer bars and the Die Fabrication Area's Computerized Numeric Controllers (CNCs) that drive the part machining centers are isolated with no network connectivity.

AAM's corporate direction is to provide comprehensive real-time reporting of the products manufactured in company facilities (Leo, 1997). This information is made available to associates at all levels using a SCADA application called FIS (Factory Information System). A significant portion of the total cost and effort to implement FIS in one of AAM's facilities comes from the installation of the network infrastructure required to link factory-floor automation controllers to FIS servers.

The goal of the initiative to establish wireless connectivity on the plant-floor will be to investigate the ability of wireless technologies to reduce both the cost and time required to implement FIS at the Detroit Forge Plant (Tiagunov, 2002). The scope of the project will be to connect wirelessly a select number of PLCs located in the factory with six FIS

gateway computers. In addition, 19 machining center CNCs will be connected wirelessly to a Direct Numerical Control (DNC) server located in the plant's die fabrication area. These WLANs will be installed as a substitute for the proprietary wired Data Highway and wired serial RS-232 networks that are currently used to interconnect plant-floor systems in AAM facilities.

Assumptions will be made related to this project. The first is that the WLAN to be designed and deployed will also be installed at AAM's other facilities in the future. In addition, it will be assumed that the data throughput, security, connectivity, and hardware requirements of the WLAN are common across AAM's facilities.

Managerial and technical considerations include completing the project without interrupting manufacturing operations and minimizing the impact of physical interferences on WLAN operation. For example, the large metal part racks that are continuously moved about the facility have the potential to impact WLAN coverage areas (Geier, 2001). Interference sources will be further identified as part of a site survey that will be conducted during the Systems Design Phase or Phase 3 of the project.

A number of functional and physical constraints are anticipated during the course of the project. Functional constraints will include logical items such as limited IP addressing space and a corporate requirement to isolate all plant-floor networks from the company's business infrastructure (Blair, 2002). Physical constraints will include the harsh forging environment in which the WLAN equipment will be required to operate.

The target population that will benefit from the WLAN project are the Detroit Forge Plant employees (Tiagunov, 2002). A less expensive and timelier method of

interconnecting plant-floor automation controllers will increase operational efficiency and provide the company an additional means of remaining competitive.

A number of resources will be required to complete the WLAN project at the Detroit Forge Plant. These include the researcher, acting in the role of Project Manager, along with the facility's IT Project Manager and FIS Engineer who will handle day-to-day project activities. In addition, the efforts of AAM's network engineers and Detroit Forge Plant electricians will be required to varying degrees throughout the project.

Project-related hardware, software, and additional contract labor will be procured using funds allocated from the IT budget.

The MSDLC timeline to complete the WLAN initiative at the Detroit Forge Plant is expected to extend over a 10 to 12 month period. The Systems Planning Phase or Phase 1 and Systems Analysis Phase or Phase 2 should be completed in one month. The Systems Planning Phase of the project will identify and prioritize production processes and the related automation equipment that benefit from a wireless FIS connection. The Systems Analysis Phase of the project will determine the wireless and wireline solutions to interconnect the selected manufacturing equipment to FIS. Phase 2 will include a detailed review of user needs, current network and manufacturing systems, and the existing manufacturing environment.

The Systems Design Phase or Phase 3 of the project should be completed in one to two months. Phase 3 will focus on the WLAN design and include the selection and testing of available WLAN devices along with interface hardware to connect plant-floor controllers to the wireless network. Next, the Systems Implementation Phase or Phase 4 is estimated to take between nine and 10 months to complete. Phase 4 is expected to take

considerably longer than the first three phases because the scheduling of WLAN device installation must accommodate varying product manufacturing schedules. The Systems Implementation Phase will also concentrate on WLAN and interface hardware procurement, assembly, configuration, installation, and testing. In addition, system documentation and training will be developed and distributed during Phase 4. Finally, the Systems Support Phase or Phase 5 will be ongoing until the new equipment is either replaced or upgraded.

The success of the plant-floor WLAN initiative at the Detroit Forge Plant will be determined by such factors as the amount of time and money required to install the WLAN. In addition, the effectiveness and reliability of the finished network will be considered along with the WLAN's applicability in AAM's other facilities.

Case Study

The case study segment of the investigation will be designed as an embedded, single-case, explanatory study. According to Yin (1994), the first step in the case study process is the definition of the research design. The following sections begin with a discussion of the five components of case study design: study questions, study propositions, unit of analysis, linking data to propositions, and criteria for interpreting results (Yin, 1994). Next, the data gathering and evidence analysis stages will be specified.

Design.

According to Yin (1994), the definition of research questions is one of the most important steps in conducting a case study. This researcher will answer the following questions during the course of the case study:

- What are effective procedures for planning, designing, and implementing a WLAN solution in a large manufacturing enterprise?
- What are the key factors that contribute to WLAN deployment?
- What are the major benefits and limitations associated with WLAN utilization?
- What WLAN standards and technologies are currently available for deployment?
- What existing and projected WLAN technologies are most appropriate for deployment?
- What mechanisms adequately secure the integrity of WLAN transmissions?
- What WLAN strategies should be employed to ensure the most effective use of wireless technology?

The purpose of the questions is to provide direction to the case study (Yin, 1994). A thorough review of the literature was a key component in the formulation of the questions. The fundamental question that will guide the case study of AAM WLAN initiatives is how WLANs are effectively planned, designed, and implemented in a large manufacturing enterprise. Answering this question along with the others listed in Chapter 1 are major goals of the case study.

Defining the study's propositions is the next component of the design process (Yin, 1994). The study propositions serve as delimiters and help focus the study on aspects

important to the study questions. The propositions for the case study of WLAN initiatives at AAM include the following:

- Issues encountered and resolved during AAM's deployment of WLAN technologies will be typical of those encountered by other large manufacturing enterprises (Chen, 2002; Coffee, 2002; Crump, 2001b; Dulaney, 2002; Geier, 1999, 2001; Moozakis, 2001; MSI Editors, 2001; Rogak, 2001; Sbihli, 2002).
- WLAN technologies that will be deployed by AAM will be suitable for use by other large manufacturers (Chen, 2002; Coffee, 2002; Crump, 2001b; Dulaney, 2002; Geier, 1999, 2001; Moozakis, 2001; MSI Editors, 2001; Rogak, 2001; Sbihli, 2002).
- The lessons learned from the AAM WLAN initiatives will be applicable to WLAN initiatives in similar manufacturing environments (Chen, 2002; Coffee, 2002; Crump, 2001b; Dulaney, 2002; Geier, 1999, 2001; Moozakis, 2001; MSI Editors, 2001; Rogak, 2001; Sbihli, 2002).
- The MSDLC methodology is replicable and will therefore support a framework that other large-sized manufacturing companies will be able to follow in developing WLAN solutions (Geier, 1999, 2001; Sbihli, 2002; Whitten et al., 1994).
- The MSDLC methodology serves as a framework for planning, designing, and implementing a WLAN solution in a global manufacturing enterprise (Geier, 1999, 2001; Sbihli, 2002; Whitten et al., 1994).

The third component of case study design is the definition of the unit of analysis or what the "case" is (Yin, 1994, p. 21). For this case study, the primary unit of analysis will

be the process used to plan, design, and implement the AAM WLAN initiatives. In addition, secondary units of analysis such as AAM WLAN effectiveness will be used to support the validity of the model developed from the study.

The fourth component of case study design is linking data to propositions (Yin, 1994). This component involves relating several pieces of information from the same case study to some theoretical proposition. The fifth component includes establishing criteria for interpreting the findings of the study. Data gathered during the case study will be analyzed to show how the issues encountered, methodology utilized, and technologies deployed in the AAM WLAN initiatives will be applicable to other large manufacturing enterprise WLAN deployments. Criteria for interpreting the study's findings will include the MSDLC system design model. Linking the actual process used during the AAM WLAN initiatives with the MSDLC strategy will demonstrate the appropriateness and capabilities of the MSDLC method as a framework for planning, designing, and implementing a WLAN solution in a global manufacturing enterprise.

Data Gathering.

The next step in the case study process is the gathering of empirical materials such as official documents, remarks in context, and personal writings (Hamel, Dufour, & Fortin, 1993). According to Gillham (2000), there are six main types of evidence for use in a case study: documents, records, interviews, detached observation, participant observation, and physical artifacts. The researcher will maintain the quality of the evidence by following three principles related by Yin (1994): use multiple sources of evidence, create a case study database, and maintain a chain of evidence.

Consequently, the case study of AAM WLAN initiatives will rely on four primary sources of evidence: AAM corporate documents, project-related documents, interviews, and participant observation. Unpublished activity reports, project journals, and network documentation will provide detail about the AAM WLAN initiatives deployment process. The participant-observer perspective will be provided by the researcher who will be employed by AAM as the project manager for the WLAN initiatives.

In addition, data will be organized and documented using a computerized reference database and an electronic project journal. The chain of evidence will be maintained by making frequent reference to relevant portions of the case study database in the report and by including the circumstances under which the data are collected in database records (Yin, 1994).

Evidence Analysis.

The next step in the case study process is analysis of the data (Gillham, 2000). According to Yin (1994), evidence analysis is one of the least developed and most difficult aspects of a case study. Therefore, an examination of chronological events will be used to analyze the empirical materials collected during the case study of AAM WLAN initiatives. This arraying of events into a chronology will allow the researcher to determine causal events over time (Yin, 1994). In addition, temporal diagrams such as Gantt and flow charts will assist this researcher in linking the AAM WLAN initiatives deployment process to the MSDLC model.

Formats for Presenting Results

Following the evidence analysis phase, the case study report is written (Gillham, 2000). Gillham (2000) observed that the basic way of presenting a case study report is a narrative that follows the sequence of events and logic of the investigation. The case study report of AAM WLAN initiatives will use this technique and follow a chronological structure to describe and explain project events and how the events relate to the MSDLC model. This common approach to report composition will organize the case study evidence in sequential order (Yin, 1994). The use of this method will also serve to validate any causal propositions drawn by this researcher.

In light of recommendations by Yin (1994), the case study report will be drafted in reverse chronological order to reduce the greater emphasis and attention usually given earlier events in chronological case studies. Once drafts are completed in this manner, this researcher will present the final case study report in a normal chronological sequence.

Finally, the findings narrated in the case study report will be used, along with previous research as reported in the literature to develop the model, which is the goal of this investigation. The MSDLC method of systems analysis and design will provide the framework for this model. The purpose of the model based on research findings and the MSDLC strategy will be to facilitate the deployment of WLANs in large manufacturing enterprises (Whitten et al., 1994).

Projected Outcomes

The key outcome of this research will be an effective model for planning, designing, and implementing a WLAN solution in a global manufacturing enterprise. This model will be based on previous research literature, the MSDLC strategy defined by Whitten et al. (1994), and the results of the case study.

Resource Requirements

A number of resources will be required during the course of the proposed research. Published and unpublished literature will include textbooks, scholarly journals, online resources, AAM project activity reports and journals, and AAM network documentation. The use of AAM computer hardware, software, and facilities will also be required.

In addition, the assignment of this researcher, as project manager for the WLAN initiatives, and the assistance of select members of AAM's IT staff, will be necessary as well. Funding from AAM will also be needed to purchase and install the required hardware and software. Importantly, approval from AAM to provide the aforementioned resources and to conduct the case study was given on December 12, 2001 (see Appendix A for signed approval letter).

Reliability and Validity

A number of strategies will be applied during the course of the research study to ensure the investigation's reliability and validity and to enable replication of the research by others. First, as noted, a variety of empirical materials will be used to ensure the depth of the study (Hamel et al., 1993). The case study report will also be drafted in reverse

chronological order to avoid the overemphasis of earlier events that frequently characterizes the chronological approach to explanatory case study reporting (Yin, 1994). In addition, the chain of evidence will be maintained by frequently referencing relevant portions of the case study database in the report (Yin, 1994).

Furthermore, the researcher will verify empirical generalizations by considering how the case might be typical or atypical and by comparing the characteristics of the case with information about large manufacturing enterprises to which the generalizations are intended (Gomm, Hammersley, & Foster, 2000). The researcher will also validate the study by having the draft report reviewed by peers and participants in the research (Yin, 1994). This validating procedure, sometimes referred to as “member checking,” can improve the quality of the report (Stake, 1995, p. 115).

Summary

In Chapter 3 above, the methodology that will be employed by this researcher during the course of the investigation is described. The chapter began with a discussion of the case study method that will provide the conceptual framework for the research. Next, the role the MSDLC method will play during the investigation and the primary audience for the study are explained. This chapter continued with an examination of the specific procedures that will be utilized to conduct the study. A discussion of how results will be presented and an explanation of the projected outcomes of the research are provided. In addition, the resource requirements for the investigation are delineated. Finally, a discussion of reliability and validity of the results is provided.

Chapter 4

Expectations

Anticipated Benefits

An anticipated benefit of conducting the proposed research will be the development of a model for the deployment of WLAN technologies in a large-sized manufacturing enterprise. This model will benefit large enterprises as they begin and continue the installation of WLANs (Wheat et al., 2001). Network design engineers have struggled for years to streamline the design and implementation process, and WLAN technologies have further complicated this process with the addition of new standards and security issues.

Projected Outcomes

The key outcome of this research will be an effective model for planning, designing, and implementing a WLAN solution in a large-sized manufacturing enterprise. This model will be based on previous research literature, the MSDLC strategy defined by Whitten et al. (1994), and the results of the case study of AAM WLAN initiatives.

Practical Applications of the Findings

The use of WLANs in large manufacturing enterprises will continue to grow rapidly in the near future (Coffee, 2002). IT professionals will be called upon to deploy them quickly and efficiently. A model to organize the deployment of these networks will be of

practical use to information systems managers, network engineers, WLAN architects, CIOs, and CTOs because the model will be specifically tailored to their operating issues and environments.

Constraints and Limitations of the Study

Several constraints will influence the scope and focus of the study. These restrictions will limit the wireless technologies deployed, the size of the conference room WLAN and AAMatHome user groups, and the length of time allotted for project completion. For example, the focus of one of the projects will be the use of WLAN technologies by users with new laptops configured with the Microsoft Windows 2000 operating system. In addition, the projects must be deployable with limited resources and no negative effect on manufacturing operations.

In addition to the aforementioned constraints, a number of restrictions beyond the control of the researcher will influence the study. These include limitations related to corporate business objectives, resource availability, and changing WLAN standards and technologies. For example, the wireless initiatives that will serve as the subject of the case study were selected based on appropriateness to the research and ability to return immediate value to the corporation. Resource availability, both monetary and IT staff, will be another limiting factor. The wireless projects will be funded from a predefined departmental expense budget, and staff resources will be required to complete the projects along with their regular work activities.

Recommendations for Additional Studies

The proposed research will develop a model for the deployment of WLANs in global manufacturing enterprises. However, the investigation will not study the effects of company size on the structure and effectiveness of the model. Future studies may examine the need to modify the model to be more applicable to WLAN deployments in small and medium size businesses. In addition, the study of WLAN deployments in large and small government organizations may also prove beneficial.

Multimode wireless systems capable of interoperating with IEEE 802.11a-compliant, IEEE 802.11b-compliant, IEEE 802.11g-compliant, and 3G devices will soon become available. Future investigations may also study the effects of enhanced wireless technologies on the relevance of the model.

Contributions to the Field

The proposed research will significantly contribute to the field of study by providing a model to plan, analyze, design, implement, and support enterprise WLANs. This model will be based upon lessons learned from a case study of four WLAN initiatives conducted by the investigator at AAM: Wireless Connectivity in Executive Conference Rooms, AAMatHome, Enhanced WLAN Security, and Wireless Connectivity on the Plant-Floor.

There is considerable theory, as presented in the literature review, related to WLAN technologies and issues. However, there is also a real need for a WLAN deployment model that encompasses the rapidly changing technologies, diverse environments, and issues encountered in global manufacturing enterprises by CIOs, CTOs, information systems managers, network engineers, and WLAN architects. The goal of the proposed

research is to create such a model. In addition, this model will provide future investigators with a basis for additional research and the advancement of knowledge in the areas of office, residential, plant-floor, and enhanced security WLAN deployments.

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 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 all-in-one device 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.

Arbaugh, W., Shankar, N., & Wang, J. (2001). Your 802.11 wireless network has no clothes. *University of Maryland*. Retrieved August 4, 2002, from <http://www.cs.umd.edu/~waa/wireless.pdf>.

The authors, researchers at the University of Maryland, discussed the explosive growth of wireless networks in the last few years. In addition, the paper pointed out the misconception many large organizations share that WLANs are secure. In fact, the article demonstrated that all existing IEEE 802.11b security mechanisms are completely ineffective. The paper began by providing background information on the IEEE 802.11b standard and the security mechanisms the IEEE 802.11b standard employs. These included WEP, open system authentication, shared key authentication, closed network access control, access control lists, and key management.

The article contributed to the research project by enumerating the weaknesses in the access control mechanisms employed by the IEEE 802.11b standard. These included insecurities related to Ethernet MAC ACLs, the shared key authentication flaw, and Lucent Technology's proprietary access control mechanism. Finally, the authors recommended a major overhaul of the current IEEE 802.11b standard.

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., & 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 the 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, the CFO, or the 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), 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.

Borisov, N., Goldberg, I., & Wagner, D. (2001, July 16-21). *Intercepting mobile communications: The insecurity of 802.11*. Paper presented at the Seventh Annual International Conference on Mobile Computing and Networking, Rome, Italy. The authors, wireless researchers at the University of California, Berkeley and Zero-Knowledge Systems, reported the discovery of security flaws in the WEP protocol included in the IEEE 802.11 standard. The paper began with a brief introduction to the IEEE 802.11 standard, the WEP protocol, and the security threats the protocol was created to address. This was followed by an explanation of the security principles violated by the protocol along with a discussion of potential countermeasures. In addition, the paper explained the practicality of a WEP attack, the risks of keystream reuse, the use of decryption dictionaries, and CRC vulnerabilities such as message modification, message injection, and authentication spoofing.

The paper illuminated the research project with a discussion of lessons learned from WEP protocol insecurities. Secure protocol design is not a trivial task and a thorough understanding of cryptographic properties is vital. Also important are the reuse of previous designs and the public review of new designs. For example, the design of the IPSec dealt with similar link-layer security issues. In addition, a public review of the WEP protocol before the technology's enactment would have revealed many of the flaws that currently exist in the standard.

Brederveld, L., Prasad, N., & Prasad, A. (2001). IP Networking for Wireless Networks. In N. Prasad & A. Prasad (Eds.), *WLAN Systems and Wireless IP for Next Generation Communications* (pp. 127-147). Boston, MA: Artech House. The authors, a developer of WLAN products for Agere Systems and Ph.D. candidates studying WLAN technologies, discussed issues related to high-level IP protocols and the technologies' use with WLANs. The paper began with a brief overview of the protocol layers of a generic WLAN system. These included bridging, routing, protocol filtering, Internet Control Message Protocol (ICMP), Ethernet link integrity, and Dynamic Host Configuration Protocol (DHCP). In addition, issues related to IP address space, TCP/IP, DHCP, Address Resolution

Protocol (ARP), Network Address Translation (NAT), and QoS were discussed. The article also presented a possible top-to-bottom and end-to-end QoS solution to employ with WLANs.

The paper illuminated the research project with a discussion of security protocols and the technologies' application to WLANs. The RADIUS protocol is often used to maintain central control of user profiles in addition to authentication, service authorization, and accounting. Another method utilizes information from the IP layer security protocol in combination with MAC layer security mechanism such as IEEE 802.1x. In the case of IEEE 802.1x, authentication at the access point is provided only if the wireless client is authenticated by the network server. Once authenticated, the encryption key exchange is performed.

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. CIOs, CTOs, and consultants were the intended audience of the text. The book provided a brief summary of the wireless web 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 delivery and wireless connectivity for convenience and personalized services.

The book contributed to the research project with a discussion of the relationship between wireless and Extensible Markup Language (XML). XML, a data representation technology, facilitates content delivery to mobile devices and platforms. Examples of XML-based wireless initiatives are SyncML, Wireless Markup Language (WML), and Extensible Hypertext Markup Language (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.

Desai, A. (2001). Secure connections. *Enterprise Systems*. Retrieved July 9, 2002, from <http://www.esj.com/features/article.asp?EditorialsID=47>.

The author, a technical architect for QuickArrow Corporation, discussed different methods of securely connecting remote users to a corporate intranet. Traditional solutions included Integrated Services Digital Network (ISDN), frame relay, ATM, and T-class lines for connecting distributed environments. Problems associated with these solutions are related to implementation, administration, and cost. In addition, the bandwidth available to individual users is fixed and unused bandwidth is not available for redistribution. Along with these traditional solutions, VPNs now provide an alternative method to connect remote users.

The article illuminated the research project with a discussion of VPN technologies and the technology's role in connecting remote users and branch offices. In addition, the use of VPNs to secure the WLAN environment was described. For example, weaknesses in the IEEE 802.11 WEP protocol may be overcome using a VPN. VPNs provide an added layer of authentication and data encryption. VPNs also offer other business benefits that include cost savings, support for new broadband technologies, and scalability using the Internet instead of dedicated leased lines. The paper also provided a description of available VPN protocols along with a table that highlighted the advantages and disadvantages of each.

Dubie, D., Jacobs, A., & Ohlson, K. (2002). Wi-Fi @ work. *Network World*. Retrieved April 1, 2002, from <http://www.nwfusion.com/wifi/2002/sideonline.html>.

The authors, staff writers for Network World magazine, discussed WLAN deployments at a couple of medical facilities, a casino, a hotel, and a shipping company. These included St. Luke's Episcopal Health System, Anderson Cancer Center, Penticton, Lakeside Casino, the Venetian Hotel, Famous Footwear, and Federal Express. A number of physical obstacles were encountered during the WLAN installation at St. Luke's. For example, the IT Department found that the metal beds of the elevators interrupted the connection between wireless laptops and access points. Similar problems occurred in areas of the hospital near microwave ovens. The WLAN deployment at Anderson Cancer Center revealed the use of unauthorized wireless networks by many of the staff.

The article illuminated the research project by reporting the advantages of wireless LAN technology when deployed in real life situations. For example, Federal Express installed a network with more than 10,000 wireless access points. The five-year deployment is estimated to have increased staff productivity by 30 percent. In addition, when Famous Footwear installed wireless LANs in 50 shoe stores, the company reduced pricing errors by 75 percent. Employees in each shoe store now use wireless handheld barcode scanners to perform daily point-of-sale and inventory tasks.

Dulaney, K. (2002). *WLAN: Strategizing for broadband connectivity*. Paper presented at the Wireless Access and Mobile Business Solutions Conference, Chicago, Illinois.

The author, a vice president in Gartner's Research organization, discussed the current state of WLAN broadband connectivity. Topics reviewed included IEEE 802.11b-compliant WLANs, evolving WLAN standards, WLAN security directives, WLAN vendor ratings, WLAN access point location planning, and enterprise markets. The applications for WLAN technologies in vertical markets are substantial. Vertical applications that will continue to grow are in education, healthcare, and warehousing. In these markets, the greatest return on investment will be realized from applications where the cost of network cabling is significant. Other considerations for calculating the benefits of WLANs include network backup, temporary installations, freedom of movement, and the need to access real-time information from anywhere.

The paper contributed to the research project with several conclusions to be considered when developing a WLAN strategy. These included a recommendation to deploy hardware from a single vendor to minimize security issues until IEEE 802.11i security enhancements become available. In addition, IEEE 802.11a was not seen as a replacement for IEEE 802.11b, and enterprises should deploy WLANs with the expectation of an IEEE 802.11a upgrade becoming a possibility. Finally, as Bluetooth devices become prevalent, interference with IEEE 802.11b-compliant WLANs will become an issue.

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-compliant 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 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 author 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.

Fluhrer, S., Mantin, I., & Shamir, A. (2001). *Weaknesses in the key scheduling algorithm of RC4*. Paper presented at the Selected Areas in Cryptography, 8th Annual International Workshop, SAC 2001, Toronto, Canada.

The authors, wireless researchers at Cisco Systems and the Weizmann Institute, reported on weaknesses in the key scheduling algorithm of RC4. RC4 is a widely used stream cipher in software applications. The paper began with an introduction to RC4 and previous attacks on RC4. Next, the invariance weakness of the key scheduling algorithm was described along with an analysis of the propagation of weak key patterns. The paper also identified a large number of weak initialization vector keys. Awareness of only a small number of weak keys was sufficient to derive the secret key. In addition, the paper demonstrated the correlation between secret key bits and bits of the output stream for a large class of weak keys. The article also presented the details of the known initialization vector attacks in which the initialization vector precedes or follows the secret key.

The article illuminated the research project by highlighting the inherent weaknesses of WEP as defined by the IEEE 802.11b standard. The passive cipher text-only WEP attack outlined in the paper was able to recover secret keys of variable length in a short period. In addition, the recovery time varied only linearly with the length of the key for both 24-bit and 128-bit initialization modifiers.

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, WAP and 3G systems, RF optimization techniques, and 3G data services for W-CDMA, CDMA2000, GPRS, and Enhanced Data Rate for Global Evolution (EDGE) networks. The intended audience of the book was telecommunications engineers, 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 systems.

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 WAP, Bluetooth, and WLANs. WAP, for example, specifies a microbrowser that employs the new WLM standard that 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-compliant systems are an excellent example of this acceptance.

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 MAC 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 a 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.

Hulton, D. (2002). Practical exploitation of RC4 weaknesses in WEP environments.

Dachb0denLabs. Retrieved 5/16/2002, from

<http://www.dachb0den.com/projects/bsd-airtools/wepexp.txt>.

The author, co-founder and CEO of Nightfall Security Solutions, LLC, discussed IEEE 802.11b WEP weaknesses and outlined flaws in the RC4 encryption key scheduling algorithm the standard employs. The WEP RC4 stream cipher uses a 24-bit IV. This vector is concatenated with a 40-bit or a 104-bit secret shared key to form a 64-bit or 128-bit key that is used as the RC4 seed. The 24-bit IV is most often generated by a pseudo random number generator. The article also provided an explanation of WEP packet structure and practical WEP assaults such as the brute force attack, FMS attack, and first byte attack. The brute force attack is often optimized using a wordlist or statistical analysis of the IVs.

The paper contributed to the research project by detailing methods of exploiting WEP weaknesses and by recommending solutions to secure wireless networks dependent on WEP for security. These included manually entering WEP keys, changing WEP keys frequently, using MAC filtering, and configuring the wireless network as untrusted or closed.

Janowski, D., & Chang, S. (2002). The lay of the wireless LAN. *PC Magazine*. Retrieved July 8, 2002, from <http://www.pcmag.com/article2/0,4149,69271,00.asp>.

The authors, editors in the PC Magazine Networking Infrastructure Group, presented a comprehensive review of available WLAN hardware devices. The article began with a discussion of WLAN technologies along with existing and future WLAN standards. This was followed by a table comparing the positive and negative features of the IEEE 802.11b, IEEE 802.11a, and IEEE 802.11g extensions. For example, although the IEEE 802.11a standard was approved before the IEEE 802.11b standard, IEEE 802.11a-compliant technology was more difficult to develop, and products based upon the technology were released years after IEEE 802.11b-compliant products.

The article contributed to the research project with the results of performance tests conducted on IEEE 802.11b-compliant and IEEE 802.11a-compliant devices. IEEE 802.11b-compliant product manufacturers frequently advertise products as having 11 Mbps throughput. Testing revealed an actual throughput of 4 Mbps to 6 Mbps. A significant portion of the 11 Mbps maximum throughput was utilized for radio signal control and network protocol information. In addition, IEEE 802.11a-compliant devices with an advertised throughput of 54 Mbps achieved approximately 27 Mbps throughput during the tests.

Kamerman, A., & Prasad, A. (2001). Performance Analysis. In N. Prasad & A. Prasad (Eds.), *WLAN Systems and Wireless IP for Next Generation Communications* (pp. 213-239). Boston, MA: Artech House.

The authors, a developer of WLAN products for Agere Systems and a Ph.D. candidate studying WLAN technologies, briefly discussed the results of several theoretical and simulation performance analyses of IEEE 802.11-compliant systems available in the open literature. The paper continued with a presentation of measured performance results related to net throughput, channel degradation, power save, and QoS. Net throughput measurements were based on the file transfer time with a group of six wireless stations. The throughput of an IEEE 802.11b-compliant device was determined to be just over 5 Mbps. In addition, an IEEE 802.11a-compliant device had a net throughput of 28 Mbps.

The article illuminated the research project with a discussion of QoS and the IEEE 802.11 standard. QoS dependent applications such as teleconferencing, telesurveillance, and video-on-demand were investigated. The data throughput requirements of a good quality teleconference and telesurveillance were 468 Kbps and 512 Kbps respectively. Video-on-demand required 2 Mbps data throughput for a good quality connection. The bandwidth requirements of video-on-demand were significantly less than those for video broadcasting that required 240 Mbps. The requirements for video-on-demand were less demanding because buffering technology was employed.

Kamerman, A., Prasad, A., Prasad, N., Moelard, H., & Brederveld, L. (2001). Deployment. In N. Prasad & A. Prasad (Eds.), *WLAN Systems and Wireless IP for Next Generation Communications* (pp. 241-263). Boston, MA: Artech House.

The authors, developers of WLAN products for Agere Systems and Ph.D. candidates studying WLAN technologies, investigated issues critical to the network deployment of IEEE 802.11b-compliant WLANs. These included coverage, cell planning, interference, power management, and data rate. The article began with a discussion of the worldwide allocation and use of frequency bands and power levels for wireless LANs. This was followed with a brief description of the hardware and software functionality built into the typical IEEE 802.11b-compliant NIC. In addition, the predeployment analysis process was discussed. Issues such as access point density and the type of radio environment were illuminated.

The paper contributed to the research project with an explanation of WLAN propagation and coverage issues. These issues were related to indoor and outdoor environments, fading and shadowing, and coverage range. In addition, the effects of noise and interference on the reliable operation of a wireless system were discussed. WLAN system operational limits such as noise limitations, minimum receive level, and interference limitations were highlighted. Finally, the roles of outdoor and directional antenna were detailed.

Keely, D. (2001). A security strategy for mobile e-business. *IBM Global Services*, 1-23. The author, Wireless Security Competency Leader within the IBM Security and Privacy Service Organization, assessed the importance of privacy and security relative to recent developments in wireless technology. The paper outlined the requirements to develop secure wireless services and reported on the risks and threats created by mobile e-business. In addition, the paper discussed strategies for creating solutions and processes to secure wireless applications. Examples of solutions were firewalls, content/e-mail filtering, anti-virus, intrusion detection, and secure device management. The processes typically included risk management, security validation, security monitoring, technical standards, and privacy.

The paper contributed to the research project by providing a security roadmap for mobile e-business. The key steps in planning and implementing an effective wireless security solution included defining clear objectives, understanding business goals, and identifying points of vulnerability. Finally, the seven components of a security roadmap were explained. These were managing the risks, gaining executive buy-in, formalizing the plan, developing an end-to-end security architecture, implementing a business oriented security solution, testing and validating the solution, and establishing a review cycle.

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), Signaling System 7 (SS7), ISDN, and Advanced Intelligent Network (AIN). The authors also described mobile services that included mobile database overflow, failure restoration, number portability, prepaid service, international roaming, and WAP. Advanced industrial developments in PCS technology were also 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, EPOC, 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 that utilize voice and handwriting recognition technologies.

Mishra, A., & Arbaugh, W. An initial security analysis of the IEEE 802.1x standard. *National Institute of Standards*. Retrieved July 11, 2002, from <http://www.cs.umd.edu/~waa/1x.pdf>.

The authors, researchers in the University of Maryland's Department of Computer Science, provided a security analysis of the IEEE 802.1x standard. The long-term security architecture for the IEEE 802.11 standard utilizes the IEEE 802.1x specification as the basis for access control, authentication, and encryption key management. The paper identified and operationally verified two weaknesses in IEEE 802.1x specification. These were session hijacking and man-in-the-middle attacks. The article began with an introduction to WLANs and followed with an explanation of the basic security mechanisms of IEEE 802.11-compliant technology.

This paper illuminated the research project because organizations are beginning to adopt IEEE 802.1x-compliant security solutions to overcome weaknesses in the IEEE 802.11 WEP protocol. The article found that the use of the IEEE 802.1x protocol fails to enable strong access control and authentication. The authors were able to mount successfully man-in-the-middle and session hijacking attacks. The attacks exploited design flaws within IEEE 802.11, IEEE 802.1x, and EAP technologies. The paper concluded that attacks against IEEE 802.1x-compliant systems could be easily prevented by adding message authentication to IEEE 802.11 management messages and EAP and by ensuring the synchronization of the various state machines.

Moelard, H., Kamerman, A., Prasad, A., & Prasad, N. (2001). System Design and Implementation Aspects. In N. Prasad & A. Prasad (Eds.), *WLAN Systems and Wireless IP for Next Generation Communications* (pp. 149-211). Boston, MA: Artech House.

The authors, developers of WLAN products for Agere Systems and Ph.D. candidates studying WLAN technologies, discussed the system design and implementation aspects of IEEE 802.11b technology. The paper began with a description of the IEEE 802.11b standard and followed with a review of different practical topologies. These included AP-based topologies, residential gateway-based topologies, peer-to-peer group, station as AP, and outdoor links. In addition, the article reviewed IEEE 802.11b technologies related to software architecture, system scalability, power management, power control, and automatic rate fallback.

The paper contributed to the research project by outlining creative methods of implementing IEEE 802.11b-compliant networks. For example, automatic load balancing is often used to divide the traffic load between access points and client stations. Stations monitor how clearly the access point is received and the load on the access point. The access point allowing the highest potential data rate is then selected. Finally, interference from microwave ovens, cordless telephones, and Bluetooth devices must be factored into IEEE 802.11b-compliant network implementations.

Molta, D. (2001). The survivor's guide to 2002. *Network Computing*. Retrieved December 30, 2001, from <http://www.networkcomputing.com/shared/printArticle?article=nc/1226/1226f4fu1l.html&pub=nmc>.

The author, a senior technology editor for Network Computing and assistant professor in the School of Information Studies at Syracuse University, discussed the key areas of mobile and wireless technology that will have significant growth in 2002. These included WPANs, WLANs, WWANs, fixed-access wireless networks, mobile devices, and mobile applications. For example, the worldwide WLAN market is predicted to increase to approximately \$3.8 billion by 2006.

The article contributed to the research project with a discussion of the WLAN and WWAN markets. WLAN technology has been most successful in key vertical markets where mobility and cable replacement have the greatest benefit. In addition, the marketing appeal of having a wireless campus has accelerated the growth of WLANs in colleges and universities. In medium and large enterprises, WLAN deployments are complex. Often, departmental WLAN systems are established without the approval of the Information Technology Department. In addition, enterprise WLAN deployments are often delayed by issues such as security, cost, performance, and the viability of existing standards.

Moozakis, C. (2001). GM's wireless leap. *Internet Week*. Retrieved July 17, 2002, from <http://www.internetweek.com/newslead01/lead102501.htm>.

The author, a senior editor for Internet Week magazine, reported plans by GM to install wireless LANs throughout company offices and plants. GM's wireless deployment encompasses both new and existing facilities. The goal of the project is to give employees faster access to business information as they move about

multiple work environments. Cisco Aironet WLAN hardware is the standard at GM. These devices are IEEE 802.11b-compliant and will provide more than enough bandwidth to handle the applications the system will support.

The article contributed to the research project with a discussion of the cost savings that GM expects to realize from the WLAN deployment. GM does not have a master plan listing the applications the company plans to enable wirelessly. However, GM does plan to include applications for managing inventory and remotely monitoring forklift trucks. Additional wireless application will be justified on a project-by-project basis. In addition, GM is planning to use wireless LAN technology to connect temporary construction trailers that are typically hardwired.

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 wireless threats, cryptographic countermeasures, application solutions, and hardware solutions. Wireless threats to air-to-ground interfaces and satellite system vulnerabilities are also examined. In addition, advanced encryption technologies that included stream ciphers, elliptic curve cryptography, Rijndael, and the AES were discussed relative to the technologies' ability to secure wireless communications.

The book contributed to the research paper with a discussion of the security principles and flaws of WLANs, WAP, TLS, Bluetooth, and Voice Over IP (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 are considered legitimate and convenient, the methods 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 developed by the IEEE. Topics covered in the text included 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 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.

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.

The authors, telecommunications engineers and researchers, began the paper with an introduction and general description of the IEEE 802.11 standard. This was followed by a discussion of the MAC and physical layers for IEEE 802.11 wireless LAN radio systems. In addition, the physical layer for infrared IEEE 802.11 wireless LANs was described. Since the standard only specifies the MAC and physical layers, wireless devices are able to employ the same LLC used by other IEEE 802 systems. A primary goal of the IEEE 802.11 standard was to achieve upper layer functionality without having to take into account the differences between wired and a wireless networks. For this reason, issues related to link losses, security, fading, and node authentication, were incorporated as MAC or physical layer services.

The paper contributed to the research project by providing a detailed description of the minimum requirements that went into the design of the IEEE 802.11 MAC protocol. These requirements centered around the issues of throughput, delay, transparency to different physical layers, fairness of access, battery power consumption, maximum number of nodes, maximum coverage area, cochannel access and interference, impromptu peer-to-peer connectivity, roaming, multicasting, capture effect insensitivity, and support for priority and non-reciprocal traffic. In addition, another important consideration was the effect of RF transmission on human safety.

Pescatore, J. (2002, March 11-13). *Security on the fly*. Paper presented at the Gartner Wireless Access, Mobile Business Solutions Conference, Chicago, Illinois.

The author, a vice president at Gartner Research, identified the five components of mobile access security: personal firewalls, access control, malicious content protection, over-the-air security, and corporate policies. The paper began by explaining why 85 percent of wireless security incidents from the present-day until 2005 will be device-related instead of over-the-air related. Wireless devices are easily lost or stolen and ensuring that the data on these devices is safe from unauthorized viewing is critical. The paper continued with a review of wireless

technologies, the five levels of hacking, the complexity of standards, WLAN access risks, the IEEE 802.1x standard, personal firewalls, WAP end-to-end security, and Secure Sockets Layer (SSL) technology.

The paper contributed to the project with recommendations for securing wireless devices and networks. These included the use of VPNs on all WLANs and the installation of personal firewall software on wireless laptops. In addition, the article recommended against the creation of wireless authentication /authorization silos and the use of heavyweight security protocols when simple SSL is adequate. Finally, the inability of wireless standards to keep up with developing technologies makes it prudent to choose only one WLAN device manufacturer.

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.

The authors, a Ph.D. candidate studying WLAN technologies and researchers assigned to WLAN development at Lucent Technologies, provided an in-depth explanation of the IEEE 802.11 standard. The paper began with an overview that detailed the standard's features, topology, and logical architecture. This was followed by a discussion of MAC layer functionality. These functions included interframe spacing, distributed coordination, fragmentation, point coordination, scanning, association, authentication, encryption, roaming, and power management. In addition, the four physical layers of the standard were reviewed: DSSS, FHSS, OFDM, FHSS, and IR. Finally, the ongoing activities of the IEEE 802.11 standards committee were discussed. These included enhanced MAC, and a single global standard in the 5 GHz band.

The paper contributed to the research project with a review of IEEE 802.11 security as defined by the Enhanced Security Network (ESN) standard. The ESN standard provides security features not found in the basic IEEE 802.11 architecture. Features included are enhanced authentication mechanisms, key management algorithms, dynamic association-specific cryptographic keys, and other enhancements. The ESN standard also takes advantage of work done by other standards groups to avoid the duplication of functions at the MAC layer that are already performed at higher layers. One example is the use of IEEE 802.1x ports.

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.

The authors, Ph.D. candidates studying WLAN technologies, focused on five categories of wireless technology: cellular, WLAN, WPAN, cordless technologies, and FWA. The article began with an overview of several evolving and emerging wireless technologies. These included the GPRS, EDGE, IEEE 802.11, HiperLAN-2, Bluetooth, and the Digital Enhanced Cordless Telephone (DECT) data system. In addition, a comparison of existing standards, data rates,

and mobility was provided. The WLAN standards discussed included those from the IEEE, the MPT in Japan, and the ETSI.

The paper illuminated the research project with a discussion of existing WLAN standards and technologies. These included IEEE 802.11, HiperLAN, MMAC, and HomeRF. A comparison of IEEE 802.11b, IEEE 802.11a, HiperLAN-2, MMAC, and HomeRF technical features and security provisions was also provided. Finally, the paper reported the past and present work of the IEEE 802.15 group in developing existing and future WPAN standards. These include the existing Bluetooth 1.0 standard along with the IEEE 802.15.3 standard that supports data rates as high as 55 Mbps and guaranteed support for multi-media traffic.

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.

The authors, Ph.D. candidates studying WLAN technologies, briefly explained WLAN technologies together with standardization efforts currently taking place. The paper began with a history of WLANs. This included a WLAN timeline that detailed the first use of spread spectrum technology in 1940, the use of narrowband technology in 1980, and the ratification of the IEEE 802.11b standard in 1999. The paper continued with a discussion of WLAN benefits that included mobility, speed of deployment, and scalability. DSSS and FHSS technologies were also explored along with wireless propagation issues such as attenuation, fading, spreading, and shifting.

The paper contributed to the research project with a discussion of standardization work in the field of WLANs. This included the work of the IEEE 802.11 Working Group, the ETSI, and the Japanese MMAC. In addition, the article detailed the worldwide allocation of radio frequency spectrum and power levels for WLAN systems along with the associated industry standard. Finally, the paper discussed the overall market demand for WLAN services and the reasons behind the rapid growth of wireless communications. These included increased mobility, decreased wiring complexity, and increased flexibility.

Railsback, K. (2001). Strategy: Building a wireless infrastructure. *InfoWorld*. Retrieved May 18, 2002, from

<http://www.infoworld.com/articles/tc/xml/01/05/07/010507tctcap.xml>.

The author, associate technical director at the InfoWorld Test Center, provided a systematic method for deploying wireless LAN technology in a business organization. One factor considered was the interoperability of wireless access points with existing network routers and switches. Another factor was whether the WLAN devices were supported by existing network management systems such as Unicenter, Tivoli, and Openview.

The article illuminated the research project by discussing seven steps of a WLAN deployment. These included needs evaluation, planning, trial rollout, testing, training, production rollout, and ongoing maintenance. The most efficient method of accomplishing the production rollout is to complete the process in phases. For example, implementing a WLAN in one department at a time allows the IT staff to maintain high service levels while adjusting to the new technology. Monitoring and maintenance are an important phase of a WLAN deployment and the existing network management platform should track the performance of and identify problems with new wireless resources.

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. WLANs 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 design fundamentals such 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, IEEE 802.11g, HiperLAN, Broadband Radio Access Network (BRAN), Bluetooth, fixed wireless, and LMDS. The chapter on wireless networking was particularly relevant with coverage of cellular telephone networks along with the new 3G interface standards: CDMA2000, EDGE, GPRS, UMTS, and W-CDMA.

Reynolds, M. (2001). Technology analysis: What's up with WEP? *Gartner.com, HARD-WW-DP-0093*, 1-6.

The author, a vice president in Gartner's Dataquest organization, discussed strategies and enabling technologies to address mobile security and privacy issues. The author began by describing five security weaknesses in IEEE 802.11-compliant systems. These included the technology's attractiveness to external parties, the use of plaintext to carry TCP/IP network protocols, the default transmission of unencrypted data, and the ability to decode both 40-bit and 128-bit WEP keys in a short period.

The paper contributed to the research project with a concise explanation of 40-bit and 128-bit WEP weaknesses. For example, a state-of-the-art personal computer is capable of cracking a 40-bit WEP key in just a few hours. This length of time is significantly decreased by the predictability of TCP/IP packets. WEP 128-bit encryption is unable to be cracked in the same manner. However, the protocol is weakened by the use of a relatively small number of initialization vectors. It is

feasible for a fast personal computer to capture samples of all possible initialization vectors and associated blocks of the key stream and to create a codebook that is able to decrypt all data packets in just a few hours.

Riera, J. (2001). The HiperLAN Standard. In A. Santamaria & F. Lopez-Hernandez (Eds.), *Wireless LAN Standards and Applications* (pp. 109-149). Norwood, MA: Artech House.

The author, a telecommunications engineer and professor of radio communications, provided a concise review of the HiperLAN standard developed by the European Telecommunications Standards Institute (ETSI). The paper began with a review of HiperLAN terminology, which was followed by a discussion of the HiperLAN physical layer, Channel Access Control (CAC), and MAC protocols. HiperLAN compatible systems share five common features; high bit rates of 23 Mbps, virtually unlimited coverage, dynamic network configuration, high traffic capacity, data encryption, and power-saving functions.

The article illuminated the research paper with a discussion of three additional HiperLAN standards: HiperLAN-2, HiperACCESS, and HiperLINK.

HiperLAN-2 systems provide local wireless access to moving and stationary ATM, IP, and UMTS networks. In addition, HiperLAN-2 systems operate in the unlicensed 5 GHz band and have a high bit rate of 25 Mbps. The HiperACCESS standard supports operation in the licensed 3 GHz to 60 GHz band and provides increased ranges up to 5 kilometers using directional gain antennas. Finally, the HiperLINK standard is intended to support ultrahigh speed point-to-point links with high bit rates of 155 Mbps.

Riera, J., & Perez-Jimenez, R. (2001). Upcoming Standards and Future Trends. In A. Santamaria & F. Lopez-Hernandez (Eds.), *Wireless LAN Standards and Applications* (pp. 183-211). Norwood, MA: Artech House.

The authors, telecommunication researchers, provided a summary of upcoming standards and future trends in wireless communications. The factors influencing these trends included the widespread use of standards-based systems, the time to agree upon a new standard, the data interchange needs of our information society, the success of mobile communications, and the inconvenience, cost, and installation difficulties of wired infrastructures. In addition, the paper reviewed the evolution of existing wireless standards and discussed new wireless standards. The standards reviewed were HiperLAN, IEEE 802.11, IrDA, Bluetooth, Wireless ATM, and HomeRF. Often the speed of technological innovation requires existing wireless standards to be updated with additional features or new applications.

The paper illuminated the research project with a look into the future. The paper envisioned a future significantly influenced by wireless technology. For example, mobile telephony will far surpass wired telephony with 90 percent of the population having mobile phones. Fixed access to home and offices will be provided by microwave and millimeter-wave links, and short-range wireless technologies will provide connectivity within homes and offices. Finally, Internet

access will be provided by microwave and millimeter-wave links, and by third and fourth generations of mobile communications.

Rogak, L. (2001). Productivity and the enterprise. *Wireless Internet*. Retrieved October 13, 2001, from http://www.wirelessinternetmag.com/news/0104/0104_features_enterprise.htm. The author, an editor for Wireless Internet Magazine, discussed the increasing demand for corporate IT managers to develop an enterprise wireless strategy. The article suggested that IT managers begin by asking themselves which functions or departments within their enterprise would realize the greatest benefit from the mobile access to data. This leads to a further investigation of cost effectiveness, scalability, training, and measurable results. Although wireless connectivity is available, it does not make good business sense for every user or application. In addition, one interdepartmental user group may effectively be served by a wireless LAN and another group that is frequently out of the office by a wireless WAN. If a wireless WAN is appropriate, then the decision to use a wireless application service provider or an off-the-shelf solution would have to be made.

The article contributed to the research project with a case study of a wireless implementation by Pacific Mechanical Services, a heating, ventilation, and cooling company in California. The goal of the implementation was to communicate with 15 company technicians who traveled to a variety of work sites throughout the day. The company selected FX Central, a wireless application service provider to supply three systems: dispatch, record keeping, and service calls. The ROI for the project was estimated to be six to nine months based upon an efficiency improvement of two percentage points.

Santamaria, A., & Lopez-Hernandez, F. (2001a). Introduction. In A. Santamaria & F. Lopez-Hernandez (Eds.), *Wireless LAN Standards and Applications* (pp. 1-8). Norwood, MA: Artech House.

The authors, professors of circuit analysis and optical communications, introduced wireless LANs. The article began with a discussion of worldwide wireless LAN standards and continued with a summary of future wireless systems. These standards included IEEE 802.11, HiperLAN, and IRDA. All three standards share a common application environment that includes the expansion of existing wired networks and the installation of new wireless networks.

The paper contributed to the research project with a discussion of five environments in which wireless and mobile systems are used. These included home-cell environments for in-house applications, picocell environments for in-building systems, macrocell environments for applications covering suburban areas, and the global environment for applications using satellite-based systems. In addition, the paper provided an overview of third-generation wireless networks will offer service with data rates up to 2 Mbps.

Santamaria, A., & Lopez-Hernandez, F. (Eds.). (2001b). *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.

Santamaria, A., Melian, V., & Minano, J. (2001). Application Scenarios. In A. Santamaria & F. Lopez-Hernandez (Eds.), *Wireless LAN Standards and Applications* (pp. 151-181). Norwood, MA: Artech House.

The authors, telecommunications engineers and researchers, began with a discussion of the deployment of WLAN technology in two areas: indoor applications and building-to-building interconnections. The application scenarios that were provided involved WLAN installations in public buildings, business environments, domestic buildings, and the industrial sector. The wireless installation requirements in these scenarios were dependent on the communication infrastructure already installed at each location and involved the extension of existing indoor wireline networks and new installations of wireless communication systems. In addition, the wireless interconnection of buildings close to existing wired networks were described. The advantages offered by WLAN systems in these scenarios were related to mobility, portability, and ease of reconfiguration.

The paper contributed to the research project with a discussion of WLAN technologies and products. Several organizations involved in the development and commercialization of WLAN communications systems were reviewed. These included the Wireless LAN Association (WLANA), the Wi-Fi Alliance, the Wireless LAN Interoperability Forum (WLIF), the Bluetooth Special Interest Group (Bluetooth SIG), the HomeRF alliance, and the Broadband Wireless Internet Forum (BWIF). In addition, a detailed inventory of mobile computing product and component manufacturers was provided.

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.

The authors, WLAN and infrared communication systems researchers, began with a description of the IrDA (Infrared Data Association) and the IrDA standard. This paper continued with a discussion of the IrDA physical layer, the serial infrared link access protocol, IrDA link management protocol, and IrDA transport protocol. The authors also reviewed IrLAN a passive protocol that defines a bi-channel interface between a protocol server and a protocol client. The IrLAN protocol enables an IrDA-compliant computer to connect to a LAN through an access point or to communicate with another computer as though the IrDA-compliant computer was attached to a LAN. In addition, the IrLAN protocol allows an IrDA-compliant computer to attach to the LAN through a second LAN attached computer.

The paper illuminated the research project with a discussion of the basic components of the IrDA structure. These included the IR physical layer, IrLAP, IrLMP, IrLAN, and IrCOMM. These components allow the standard to adapt to the varying complexity of IR devices. Printers, for example, employ simple access and connectivity protocols, while a network server may utilize the IrLMP and IrLAN protocols. In addition, devices with simpler communications needs could use the IrDA LITE protocol, which was designed for devices requiring less complex software and hardware.

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 author 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 description of 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 described a healthcare application for capturing the medical costs at the time and location the costs occur. Finally, the text presented short-term 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, an executive at 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 author 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.

Stanley, D. (2002). Orinoco wireless LAN security. *Agere Systems*. Retrieved July 11, 2002, from

http://www.orinocowireless.com/upload/documents/March_7_02_ORiNOCO_Wireless_LAN%20_Security_Response2.pdf.

The author, a system architect for the Wireless Communication and Networking Division of Agere Systems, responded to a security analysis of the IEEE 802.1x standard conducted by Mishra and Arbaugh from the University of Maryland. The paper discussed IEEE 802.1x implementations specific to the Orinoco brand of WLAN systems and two types of attacks: session hijacking and man-in-the-middle. The attack scenarios that were considered included EAP-TLS authentication and the session hijacking attack, EAP-TTLS authentication and the session hijacking attack, access server authentication and the session hijacking attack, and access server authentication using CHAP.

The paper contributed to the research project by demonstrating how the use of encryption and mutual authentication methods with the IEEE 802.1x standard, eliminates the weaknesses outlined in the security analysis written by Mishra and Arbaugh. In addition, the man-in-the-middle attack described by Mishra and Arbaugh would at most result in a denial of service attack. The attacker would not gain access to the network and encrypted data would not be compromised. In addition, the upcoming IEEE 802.11i standard addresses denial of service attacks.

Walker, J. (2000). Unsafe at any key size; An analysis of the WEP encapsulation. *IEEE, doc.: IEEE 802.11(00/362)*.

The author, a network security architect with Intel Corporation, analyzed the vulnerabilities of WEP encapsulation as defined by the IEEE 802.11 standard. The paper sought to prove the infeasibility of solving WEP security problems by simply increasing the secret key size. The paper began with an overview of WEP encapsulation. The IEEE 802.11 standard defines the five elements used in WEP to encrypt the contents of data frames: four shared keys, a RC4 stream cipher encryption algorithm, a 24-bit initialization vector, a transport encapsulation, and the cyclic redundancy code of the frame payload. Next, the article discussed WEP initialization vector problems. For example, WEP keys are not replaced frequently enough to maintain system security.

The paper contributed to the research paper by providing a thorough analysis of WEP security weaknesses and a list of changes to address them. The recommendations included a cipher, a key derivation algorithm, random data suggestions, and a new WEP encapsulation. The Advanced Encryption System (AES) block cipher served as the basis for all of the proposed changes. For example, a redesigned WEP should employ 128-bit AES as the cipher along with the use of AES in Offset Codebook Mode (OCB). In addition, a 32-bit sequence number should be used to indicate the number of frames to send under the present key.

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 broadband wireless communications. Individuals with a thorough understanding of digital communications and spread spectrum/CDMA were the intended audience. The author described recent research developments in broadband wireless communications 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 an investigation of 4G mobile communications. 3G mobile systems are currently being deployed worldwide. These systems 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, 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 communication devices. In addition, WLAN coverage in hotels and public buildings will not become ubiquitous until 2015, and 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 the history of wireless communications, the physics behind the technology, the components of a wireless network, the OSI 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 in the workplace 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 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, 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. Case studies 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

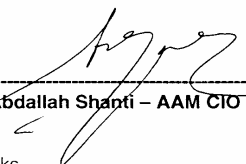
From: Wolak, Ronald
Sent: Wednesday, December 12, 2001 8:47 AM
To: Shanti, Abdallah
Subject: Ph.D. Dissertation Topic Approval
Importance: High

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

- 3Com unveils industry's first Wi-Fi certified workgroup bridge extending the reach of wireless connectivity.* (2002). Retrieved October 16, 2002, from http://www.3com.com/corpinfo/en_US/pressbox/press_release.jsp?INFO_ID=7569.
- 802.11 security beyond WEP.* (2002). Retrieved December 8, 2002, from <http://www.80211-planet.com/tutorials/article.php/1377171>.
- About PCMCIA.* (2002). Retrieved December 1, 2002, from <http://www.pcmcia.org/about.htm>.
- About the ARRL.* (2002). Retrieved December 4, 2002, from <http://www.remote.arrl.org/aarrl.html>.
- About the IEEE.* (2002). Retrieved November 30, 2002, from http://www.ieee.org/portal/index.jsp?pageID=corp_level1&path=about&file=index.xml&xsl=generic.xsl.
- Abramson, N. (2002). ALOHAnet; The first packet radio network. *Rochester Institute of Technology*. Retrieved October 12, 2002, from <http://www.rit.edu/~elp7807/imm/project1/alohanet.html>.
- Agere Systems announces the Orinoco AP-200.* (2002). Retrieved October 16, 2002, from <http://www.agere.com/NEWS/PRESS2002/031302a.html>.
- Agrawal, A. (2002). 3G. *SearchNetworking.com*. Retrieved December 3, 2002, from http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci214486.html.
- Arbaugh, W., Shankar, N., & Wang, J. (2001). Your 802.11 wireless network has no clothes. *University of Maryland*. Retrieved August 4, 2002, from <http://www.cs.umd.edu/~waa/wireless.pdf>.
- 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 http://www.wirelessweek.com/index.asp?layout=print_page&doc_id=59318.
- Batista, E. (2000). FCC: HomeRF gets up to speed. *Wired News*. Retrieved May 9, 2002, from www.wired.com/news/technology/0,1282,38564,00.html.

- Baxter, S. (2001). Agere Systems is first to solve wireless LAN wired equivalent privacy issue. *Broadband Wireless Exchange*. Retrieved August 11, 2002, from <http://www.bbwxchange.com/news/agere111301.htm>.
- Blackwell, G. (2001). Assessing total cost of ownership. *802.11 Planet*. Retrieved December 17, 2001, from http://www.80211-planet.com/columns/article/0,4000,1781_917751,00.html.
- Blair, R. (2002). *AAM NetWeb: Web-based network documentation*. Unpublished manuscript, American Axle and Manufacturing.
- Block cipher*. (2002). Retrieved December 4, 2002, from http://www.wikipedia.org/wiki/Block_cipher.
- Blunk, L., & Vollbrecht, J. (1998). PPP Extensible Authentication Protocol (EAP). *Internet FAQ Consortium*. Retrieved December 7, 2002, from <http://www.faqs.org/rfcs/rfc2284.html>.
- Bolle, A. (1998). HIPERACCESS status and plans. *Ericsson*. Retrieved July 31, 2002, from <http://nwest.nist.gov/mtg3/papers/bolle.pdf>.
- Borisov, N., Goldberg, I., & Wagner, D. (2001, July 16-21). *Intercepting mobile communications: The insecurity of 802.11*. Paper presented at the Seventh Annual International Conference on Mobile Computing and Networking, Rome, Italy.
- Bourin, B. (2001). High performance radio mobility in LANs. *ETSI*. Retrieved December 20, 2001, from http://www.etsi.org/literature/aa_oldtokeep/stateart/bourin.htm.
- Brewin, B. (2001a). New wireless LAN standard receives IEEE approval. *Computerworld*. Retrieved December 21, 2001, from http://www.computerworld.com/itresources/rcstory/0,4167,STO66052_KEY68,00.html.
- Brewin, B. (2001b). Security fears prompt delays in cancer center wireless program. *Computerworld*. Retrieved December 21, 2001, from <http://www.computerworld.com/mobiletopics/mobile/story/0,10801,63396,00.html>.
- Bruestle, J., & Hegerle, B. (2002). AirSnort FAQ. *Shmoo Group*. Retrieved August 11, 2002, from <http://airsnort.shmoo.com/>.
- Campbell, C. (2001). Wireless LAN services: Addressing user expectations. *Gartner Dataquest, MBLC-WW-DP-0102*(August 16).

- Caswell, W. (2001). Which standard is better for teleworkers: Wi-Fi or HomeRF? *Network World*. Retrieved May 9, 2002, from www.nwfusion.com/forum/2001/0409faceoffhomerf.html.
- CCK. (2002). Retrieved December 5, 2002, from <http://www.webopedia.com/TERM/C/CCK.html>.
- Chen, A. (2002). Sniffing out rogue wireless LANs. *eWeek*. Retrieved May 16, 2002, from <http://www.eweek.com/article2/0,3959,7744,00.asp>.
- Churchill, S. (2002). Single chip - Dual band. *DailyWireless*. Retrieved August 17, 2002, from <http://dailywireless.org/modules.php?name=News&file=article&sid=193>.
- Cisco's use of EAP/LEAP in wireless communications*. (2002). Retrieved, from <http://support.asl.co.uk/observer/wireless/EAP-LEAP.htm>.
- Coffee, P. (2002). Ready or not, Wireless enterprise IT is here today. *eWeek*. Retrieved October 24, 2002, from <http://www.eweek.com/article2/0,3959,647522,00.asp>.
- Conventional PCI 2.3 - An evolution of the conventional PCI local bus specification*. (2002). Retrieved December 1, 2002, from <http://www.pcisig.com/specifications/conventional>.
- CPE. (2002). Retrieved December 5, 2002, from <http://www.webopedia.com/TERM/C/CPE.html>.
- Crump, B. (2001a). *Maximizing efficiency: 802.11a vs. b vs. g*. Paper presented at the Winning with Wireless Conference, Troy, Michigan.
- Crump, B. (2001b). *Wireless security: Overcoming the obstacles*. Paper presented at the Winning with Wireless Conference, Troy, Michigan.
- Curl, D. (2001). Finding the way forward in wireless technologies. *GlobalTechnoScan.com*. Retrieved December 20, 2001, from <http://www.globaltechnoscan.com/21stFeb-27thFeb01/wireless.htm>.
- Delio, M. (2001). Wireless networks in big trouble. *Wired News*. Retrieved December 19, 2001, from <http://www.wired.com/news/print/0,1294,46187,00.html>.
- Digital signal processor*. (2002). Retrieved December 5, 2002, from http://www.wikipedia.org/wiki/Digital_signal_processor.
- Do wireless LANs pose a health risk to consumer?* (2002). Retrieved December 5, 2002, from <http://www.wlana.org/learn/health.htm>.

- DSSS and FHSS spread spectrum.* (2002). Retrieved August 27, 2002, from http://www.arcelect.com/DSSS_FHSS-Spead_spectrum.htm
- Dulaney, K. (2002). *WLAN: Strategizing for broadband connectivity*. Paper presented at the Wireless Access and Mobile Business Solutions Conference, Chicago, Illinois.
- EAP.* (2002). Retrieved October 16, 2002, from http://www.microsoft.com/windows2000/en/server/help/sag_RRAS-Ch1_71.htm.
- Enhancing wireless LAN security.* (2002). Retrieved October 16, 2002, from <http://www.computerworld.com/news/2002/story/0,11280,67990,00.html>.
- ETSI general information.* (2002). Retrieved December 12, 2002, from <http://www.etsi.org/aboutetsi/home.htm>.
- ETSI approves HiperACCESS core standards for Broadband Fixed Wireless Access.* (2002). Retrieved December 1, 2002, from <http://www.etsi.org/search/frameset/home.htm?CiScope=%2F&CiMaxRecordsPerPage=10&TemplateName=query&CiSort=rank%5Bd%5D&HTMLQueryForm=search.htm&UserRestriction=hiperaccess>.
- ETSI HIPERLAN/1 standard.* (2002). Retrieved November 30, 2002, from <http://www.etsi.org/technicalactiv/hiperlan/hiperlan1.htm>.
- ETSI HIPERLAN/2 standard.* (2002). Retrieved November 30, 2002, from <http://www.etsi.org/technicalactiv/hiperlan/hiperlan2.htm>.
- FHSS.* (2002). Retrieved December 7, 2002, from <http://www.webopedia.com/TERM/F/FHSS.html>.
- Flickenger, R. (2002). *Building Wireless Community Networks* (First ed.). Sebastopol, CA: O'Reilly & Associates.
- Fluhrer, S., Mantin, I., & Shamir, A. (2001). *Weaknesses in the key scheduling algorithm of RC4*. Paper presented at the Selected Areas in Cryptography, 8th Annual International Workshop, SAC 2001, Toronto, Canada.
- Freedman, A. (2002). *Computer Desktop Encyclopedia* (Vol. 15.2). Point Pleasant, PA: The Computer Language Company.
- Funk, P. (2002a). Comments on "An Initial Security Analysis of the IEEE 802.1X Standard". *Funk Software*. Retrieved December 16, 2002, from http://www.funk.com/radius/Solns/umdresp_wp.asp.

- Funk, P. (2002b). Industry embraces 802.1x WLAN standard and EAP-TTLS security protocol. *Funk Software*. Retrieved October 16, 2002, from http://www.funk.com/PressReleases/8021x_partner_pr.asp.
- Gantt chart*. (2002). Retrieved December 7, 2002, from http://searchsystemsmanagement.techtarget.com/sDefinition/0,,sid20_gci331397_00.html.
- Garcia, A. (2002). Making the insecure secure. *PC Magazine*. Retrieved August 11, 2002, from <http://www.pcmag.com/article2/0,4149,24492,00.asp>.
- Garg, V. (2001). *Wireless network evolution: 2G to 3G*. Upper Saddle River, NJ: Prentice Hall.
- Gast, M. (2002). *802.11 Wireless Networks: The Definitive Guide*. Sebastopol, CA: O'Reilly & Associates.
- Geier, J. (1999a). Overview of the IEEE 802.11 standard. *Wireless-Nets*. Retrieved December 1, 2002, from http://www.wireless-nets.com/articles/whitepaper_overview_80211.htm.
- Geier, J. (1999b). *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.
- Geier, J. (2002a). 802.11 alphabet soup. *Internet.com*. Retrieved December 8, 2002, from <http://www.80211-planet.com/tutorials/article.php/1439551>.
- Geier, J. (2002b). 802.11a becomes a contender. *Network World*. Retrieved August 17, 2002, from <http://www.nwfusion.com/reviews/2002/0617bg1.html>.
- Gillham, B. (2000). *Case Study Research Methods*. New York: Continuum.
- Gomm, R., Hammersley, M., & Foster, P. (2000). *Case Study Method*. Thousand Oaks, California: Sage Publications.
- Gray, D., & Cowley, S. (2002). Palm rolls out wireless i705, Drops flip-up antenna. *IDG News Service*. Retrieved December 1, 2002, from <http://www.nwfusion.com/news/2002/0125palm.html>.
- Grimm, C. (2002). Wi-Fi Alliance announces standards-based security solution to replace WEP. *Wi-Fi Alliance*. Retrieved December 3, 2002, from <http://www.weca.net/opensection/ReleaseDisplay.asp?TID=4&ItemID=118&StrYear=2002&strmonth=10>.

- Hamel, J., Dufour, S., & Fortin, D. (1993). *Case Study Methods*. Newbury Park, California: Sage Publications.
- Health concerns*. (2001). Retrieved December 5, 2002, from <http://www.wirelessconsumers.org/healthconcerns.html>.
- Henderson, T. (2002). Buyer's guide: Wireless LANs. *Network World*. Retrieved August 17, 2002, from <http://www.nwfusion.com/reviews/2002/0617bgtoc.html>.
- Home networking technologies*. (2001). Retrieved December 17, 2002, from <http://homerf.org/data/tech/consumerwhitepaper.pdf>.
- HomeRF*. (2001). Retrieved December 8, 2002, from <http://www.webopedia.com/TERM/H/HomeRF.html>.
- Honeywell goes wireless*. (2002). Retrieved August 25, 2002, from www.bitpipe.com/data/detail?id=1010690741_864&type=RES&x=902992285.
- Hot spot*. (2002). Retrieved November 30, 2002, from http://www.webopedia.com/TERM/h/hot_spot.html.
- IEEE 802.11b High Rate Wireless Local Area Networks*. (2001). Retrieved December 21, 2001, from http://www.intel.com/network/connectivity/resources/doc_library/documents/pdf/np1692-01.pdf.
- IPSec*. (2002). Retrieved November 30, 2002, from <http://www.webopedia.com/TERM/I/IPsec.html>.
- ISM band*. (2002). Retrieved December 1, 2002, from http://www.wikipedia.org/wiki/ISM_band.
- Janowski, D., & Chang, S. (2002). The lay of the wireless LAN. *PC Magazine*. Retrieved July 8, 2002, from <http://www.pcmag.com/article2/0,4149,69271,00.asp>.
- Jensen, M. (1999). A guide to using low-cost radio communication systems for telecommunication in developing countries - An African perspective. *International Research Development Centre*. Retrieved May 9, 2002, from www.idrc.ca/acacia/03866/wireless.
- Joch, A. (2001). Business case: Thinking outside the boxes. *Network Magazine*. Retrieved August 29, 2002, from <http://networkmagazine.com/article/NMG20010521S0006>.

- Keene, I., & Calvert, J. (2002). Public wireless LAN hot spots: Worldwide trends and forecasts. *Gartner Research, TELC-WW-EX-0393*(August 9), 1-4.
- Komagan, C. (2000). Wireless 3G: The future of wireless. *Scient*. Retrieved December 3, 2002, from http://allnetdevices.com/developer/white/2000/06/30/wireless_3g.html.
- Krazit, T. (2001). Study: Wireless networking unchained in 2001. *Computerworld*. Retrieved December 21, 2001, from 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.
- Leo, F. (1997). *Plant-wide FIS design* (11025.1-08). Detroit, Michigan: American Axle and Manufacturing.
- Lipschultz. (2001). Security haunts the Wireless Web. *InternetWeek*. Retrieved December 20, 2001, from <http://www.internetweek.com/indepth01/indepth071001.htm>.
- Littman, M. (2002). *Building Broadband Networks*. Boca Raton, Florida: CRC Press.
- LMDS. (2002). Retrieved November 30, 2002, from <http://www.webopedia.com/TERM/L/LMDS.html>.
- Manardo, K. (2001a). AAM: Company profile. *American Axle and Manufacturing*. Retrieved December 9, 2001, from http://www.aam.com/about/about_profile.html.
- Manardo, K. (2001b). AAM: Forging Division. *American Axle and Manufacturing*. Retrieved October 5, 2002, from http://aam.com/global/global_forgingdiv.html#Detroit.
- Martec. (2002). What is solid modeling? Retrieved December 5, 2002, from <http://www.martec.us/CAD-CNC%20Information.htm>.
- Mini PCI. (2002). Retrieved December 1, 2002, from http://www.pcisig.com/specifications/conventional/mini_pci.
- Mitchell, B. (2002). QoS. *Computer Networking*. Retrieved December 1, 2002, from <http://compnetworking.about.com/library/glossary/bldef-qos.htm>.
- Mitchell, R., & Kay, R. (2001). Unfulfilled promises. *Computerworld*. Retrieved November, from

<http://www.computerworld.com/mobiletopics/mobile/story/0,10801,63949,00.html>.

MMDS. (2002). Retrieved November 30, 2002, from <http://www.webopedia.com/TERM/M/MMDS.html>.

MobiusGuard features advanced mechanism for authentication, encryption, virtual private network (VPN) tunneling, and network architecting. (2002). Retrieved October 16, 2002, from http://www.symbol.com/news/pressreleases/pr_wireless_mobiusguard.html.

Molta, D. (2001). WaveBase: A gateway to wireless heaven. *Network Computing*. Retrieved July 28, 2002, from <http://www.networkcomputing.com/1222/1222f2.html>.

Molta, D., & Laxminarayanan, S. (2002). Perfect harmony. *Network Computing*. Retrieved July 25, 2002, from www.networkcomputing.com/1313/1313f3.html.

Moozakis, C. (2001). GM's wireless leap. *Internet Week*. Retrieved July 17, 2002, from <http://www.internetweek.com/newslead01/lead102501.htm>.

Mostafa, M., Byrne, J., & Bruederle, S. (2001). Corporations lead the adoption of wireless LAN technology in the United States. *Gartner Dataquest, MBLC-WW-DP-0102*(February 19).

Multimedia Mobile Access Communication Systems. (2002). Retrieved October 13, 2002, from <http://www.arib.or.jp/mmac/e/what.htm>.

Narrowband. (2002). Retrieved October 6, 2002, from http://searchnetworking.techtarget.com/sDefinition/0,290660,sid7_gci212622,00.html.

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

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, D. (2001a). Microsoft's wireless road ahead. *Business 2.0*. Retrieved December 17, 2001, from <http://www.business2.com/articles/web/print/0,1650,36308,FF.html>.

- Orenstein, D. (2001b). Wireless moves to the ground floor. *Business 2.0*. Retrieved August, from <http://www.business2.com/articles/web/0,1653,17772,00.html?ref=cnet>.
- Paulo, G., & Wolf, M. (2000). FCC Approves WBFH, Much to Proxim and Home RF's delight. *Cahners In-Stat Group*. Retrieved October 14, 2002, from <http://www.instat.com/insights/networking/2000/09fccapproves.htm>.
- Paulson, L. D. (2002, May, 2002). US approves new uses for wireless technology. *IEEE Computer*, 35, 27.
- PEAP. (2002). Retrieved October 15, 2002, from http://www.cisco.com/en/US/tech/tk722/tk723/tk76/tech_protocol_home.html.
- Peretz, M. (2002). Ultra Wideband: The ultimate disruptive technology. *Ultrawideband Planet.com*. Retrieved July 31, 2002, from http://www.ultrawidebandplanet.com/technology/article/0,,10850_1355831,00.html.
- 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.
- Pescatore, J. (2002, March 11-13). *Security on the fly*. Paper presented at the Gartner Wireless Access, Mobile Business Solutions Conference, Chicago, Illinois.
- Petrick, A. (2002). IEEE 802.11b - Wireless Ethernet. *CommsDesign.com*. Retrieved July 31, 2002, from <http://www.commsdesign.com/main/2000/06/0006stand.htm>.
- Physical (PHY) Layer. (2002). Retrieved October 13, 2002, from http://www.informit.com/content/index.asp?product_id=%7B85189561-10E7-4D4D-861D-C7030DE2AB09%7D&st=%7B5403B8D0-9308-4B84-9F63-8040DAD445DF%7D.
- 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.

- Public WLANs growing rapidly in U.S.* (2002). Retrieved August 18, 2002, from http://www.80211-planet.com/news/article/0,,1481_970661,00.html.
- Railsback, K. (2001). Strategy: Building a wireless infrastructure. *InfoWorld*. Retrieved May 18, 2002, from <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.
- Redman, P., & Chapman, J. (2002). Wireless LAN: Opportunities in service provider markets. *Gartner Research, M-15-5030*(March 8).
- Reducing total cost of ownership.* (2002). Retrieved October 5, 2002, from <http://www.compstar.com/TCO.htm>.
- Remote Authentication Dial-In User Service.* (2002). Retrieved December 8, 2002, from http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214249,00.html.
- Reynolds, M. (2001). Technology analysis: What's up with WEP? *Gartner.com, HARD-WW-DP-0093*, 1-6.
- 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.
- Rivest, R. (2002). RC4 encryption algorithm. *North Carolina Agricultural and Technical State University*. Retrieved October 15, 2002, from http://www.ncat.edu/~grogans/algorithm_history_and_descriptio.htm.
- Rodbell, M. (2002). IrLAP: Infrared Wireless Link Access Protocol. *Communication Systems Design*. Retrieved October 14, 2002, from <http://www.commsdesign.com/main/9802art2.htm>.
- Rogaway, P. (2002). OCB mode. *University of California - Davis*. Retrieved October 16, 2002, from <http://www.cs.ucdavis.edu/~rogaway/ocb/ocb.htm>.
- Rosser, B. (1997). Preparing an IT Strategic Plan. *Gartner Research, TU-443-171*(November 25).
- 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.
- Sbihli, S. (2002). *Developing a Successful Wireless Enterprise Strategy*. New York: Wiley Computer Publishing.

- SCADA. (2002). Retrieved October 5, 2002, from <http://80211-planet.webopedia.com/TERM/S/SCADA.html>.
- Scott, R. (1999). Understanding cyclic redundancy check. *4D*. Retrieved December 5, 2002, from <http://www.4d.com/ACIDOC/CMU/CMU79909.HTM>.
- Seaborne, A., Williams, S., & Novak, F. (1996). Infrared Data Association Link Management Protocol. *Infrared Data Association*. Retrieved December 1, 2002, from <http://www.irda.org/standards/pubs/IrData.zip>.
- Sicher, A. (2002). *Wireless Overview*. Round Rock, Texas: Dell Computer.
- Singhal, S. (2001). *The seven deadly sins of wireless LANs*. Fort Lee, NJ: ReefEdge.
- Siwiak, K., & Huckabee, L. (2002). An Introduction to Ultra Wide Band Wireless Technology. In B. Bing (Ed.), *Wireless Local Area Networks* (pp. 244). New York: Wiley-Interscience.
- Smith, B. (2002). Best Buy boots WLAN after alleged security breach. *Wireless Week*. Retrieved May 4, 2002, from http://www.wirelessweek.com/index.asp?layout=story&doc_id=84413&verticalid=110&vertical=Wireless+Internet&industry=Broadband.
- Smith, R. (2001). Deciphering the Advanced Encryption Standard. *Networkmagazine.com*. Retrieved December 3, 2002, from <http://networkmagazine.com/article/NMG20010226S0010>.
- Spread spectrum*. (2002). Retrieved December 8, 2002, from http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci213041,00.html.
- Stake, R. (1995). *The Art of Case Study Research*. Thousand Oaks, California: Sage Publications.
- T-1 carrier*. (2002). Retrieved November 30, 2002, from http://www.webopedia.com/TERM/T/T_1_carrier.html.
- Taschek, J. (2002). How much wireless security is enough? *eWeek*. Retrieved July 27, 2002, from <http://www.eweek.com/article2/0,3959,3643,00.asp>.
- TDMA*. (2002). Retrieved November 30, 2002, from <http://www.webopedia.com/TERM/T/TDMA.html>.
- Tellis, W. (1997). Introduction to case study. *The Qualitative Report*, 3(2), 1-12.

- The 7 Layers of the OSI model.* (2002). Retrieved December 1, 2002, from http://www.webopedia.com/quick_ref/OSI_Layers.asp.
- The Infrared Data Association.* (2002). Retrieved December 1, 2002, from <http://www.irda.org/about/index.asp>.
- The wireless wave.* (2001). Retrieved December 17, 2001, from <http://www.manufacturingsystems.com/archives/2001/apr/ms0401f7.asp>.
- Tiagunov, P. (2002). *Detroit Forge FIS*. Detroit, Michigan: American Axle and Manufacturing.
- Vaughan-Nichols, S. (2002). Beyond WEP. *Internet.com*. Retrieved December 7, 2002, from <http://www.80211-planet.com/tutorials/article.php/1490451>.
- VSAT. (2002). Retrieved November 30, 2002, from <http://www.webopedia.com/TERM/V/VSAT.html>.
- Walker, J. (2000). Unsafe at any key size; An analysis of the WEP encapsulation. *IEEE, doc.: IEEE 802.11(00/362)*.
- WAP. (2002). Retrieved November 30, 2002, from <http://www.webopedia.com/TERM/W/WAP.html>.
- Wasp. (2002). Work in progress. *Wasp Bar Code*. Retrieved October 16, 2002, from http://www.waspbarcode.com/barcode_education/work_in_progress.asp.
- What is Amateur Radio?* (2002). Retrieved October 13, 2002, from <http://www.rac.ca/faqham.htm>.
- What is Wi-Fi?* (2002). Retrieved December 3, 2002, from <http://www.weca.net/OpenSection/index.asp>.
- Wheat, J., Hiser, R., Tucker, J., Neely, A., & McCullough, A. (2001). *Designing a Wireless Network*. Rockland, MA: Syngress Publishing.
- Whitten, J., Bentley, L., & Barlow, V. (1994). *Systems Analysis and Design Methods* (Third ed.). Burr Ridge, Illinois: Irwin.
- WiFi Alliance - Glossary of terms.* (2002). Retrieved October 6, 2002, from <http://www.wi-fi.org/opensection/glossary.asp#S>.
- Winegardner, K. (1998). The Case Study Method of Scholarly Research. *Graduate School of America*. Retrieved December 9, 2001.

- Wireless 802.11 security in a corporate environment*. (2001). Retrieved December 1, 2001, from http://www.intel.com/ebusiness/products/related_mobile/wp012602.htm.
- Wireless LAN*. (2002). Retrieved December 3, 2002, from http://www.wikipedia.org/wiki/ISM_band.
- Wireless LAN glossary*. (2002). Retrieved October 13, 2002, from http://www.ksys.info/wlan_glossary.htm.
- Wireless LANs: Improving productivity and quality of life*. (2001). Retrieved December 1, 2001, from http://newsroom.cisco.com/dlls/sage_report.pdf.
- Wireless network solutions*. (2002). Retrieved August 28, 2002, from <http://www.dlink.com/products/DigitalHome/Wireless/11b/11bWireless.htm>.
- Wireless radio health concerns*. (2002). Retrieved December 5, 2002, from http://www.tycowireless.com/products/wireless_health.html.
- Yin, R. (1994). *Case Study Research: Design and Methods* (Second ed.). Thousand Oaks, California: Sage Publications.