SANDIA REPORT
SAND2002-3312
Unlimited Release
Printed October 2002

An Approach to Wireless Communications at Sandia National Laboratories

Edward L. Witzke

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.doe.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/ordering.htm

SAND2002-3312
Unlimited Release
Printed October 2002

An Approach to Wireless Communications at Sandia National Laboratories

Edward L. Witzke
Advanced Networking Integration Department
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-0806

Abstract

Wireless communication plays an increasing role in military, industrial, public safety, and academic computer networks. Although in general, radio transmitters are not currently permitted in secured areas at Sandia, wireless communications would open new opportunities, allowing mobile and pervasive user access. Without wireless communications, we must live in a "non-mainstream" world of fixed, wired networks, where it becomes ever more difficult to attract and retain the best professionals.

This report provides a review of the current state of wireless communications, which direction wireless technology is heading, and where wireless technology could be employed at Sandia. A list of recommendations on harnessing the power of wireless communications is provided to aid in building a state-of-the-art communication environment for the 21st century at Sandia.

Acknowledgements

The author wishes to thank his following Sandia colleagues for their contributions to, and/or review of, portions of this report:
David Beck
Doug Brown
John Eldridge
Steve Gossage
John Long
Del Packwood
Perry Robertson
Tom Tarman
Jeff Taylor
Dallas Wiener
Bill Young

The author also wishes to thank the many members of the user community that contributed ideas, requirements, and directions to this study.

Contents

1 Problem Statement 5
2 Current State of Wireless Technology 6
2.1 Cellphones and Pagers 6
2.2 PDAs and Pocket PCs 11
2.3 Computer Networks 12
3 How Might Wireless Technology Evolve? 18
4 Where Should Sandia Strive to Be? 20
5 Issues for the Sandia Environment 24
6 Where Could Wireless Technology Be Applied at Sandia? 26
6.1 Unclassified Environment 27
6.2 Classified Environment 28
7 Recommendations for the Path Forward 29
7.1 Implement Diffused Infrared Infrastructure Mode LANs Inside the Limited Areas 30
7.2 Create a Map of the Classified Computing and Communications Resources at Sandia 30
7.3 Implement Strict Configuration Control over the Location of Classified Computing and Communications Resources at Sandia 30
7.4 Perform an RF Mapping of the Sandia, NM Facilities 31
7.5 Implement a System to Allow the Use of Two-Way Pagers, both Inside and Outside the Limited Areas 31
7.6 Implement 802.11a Wireless Infrastructure Mode LANs Outside the Limited Areas 31
7.7 Allow the Use of Approved Type 1 Wireless Devices in the Secure Network 32
7.8 Replace Copper Data Cables by Fiber Optic Cables and Wireless LANs in the SCN 32
7.9 Perform a Study to Remedy Coupling Issues 32
7.10 Cluster Classified Computing Resources into Bounded Enclaves 33
7.11 Perform a Study of How to Implement Wireless Voice Communications within the Limited Areas 33
7.12 Implement 802.11a Infrastructure Mode Networks Inside the Limited Areas 33
7.13 Implement Diffused Infrared LANs on the SCN 34
8 Bibliography 35
Appendix A Acronyms and Abbreviations 38

Figures

Figure 1. Infrastructure Mode Versus Ad Hoc Mode Networks. 14
Figure 2. Office Communications Today. 21
Figure 3. Office Communications Tomorrow. 22

Tables

Table 1. Summary of Cellular Telephone Technologies 10
Table 2. 802.11 and HiperLAN/2 Comparison. 16
Table 3. Summary of Wireless Computer Network Technology. 17
Table 4. Summary of User Community Interest in Wireless Connectivity. 26

1 Problem Statement

Wireless communication plays an increasing role in military, industrial, public safety, and academic computer networks. Although in general, radio transmitters are not currently permitted in secured areas at Sandia, wireless communications would open new opportunities, allowing mobile and pervasive user access. Examples of this include the ability to have network connectivity to a laptop computer in areas that don't have any (or don't have an adequate number of) wired network drops, email alerts during meetings or collaborative work sessions, and instant accessibility through voice and Short Message Service (SMS) connectivity. Without wireless communications, we must live in a "non-mainstream" world of fixed, wired networks, where it becomes ever more difficult to attract and retain the best professionals.

Wireless communication also needs to be examined from a cost comparison viewpoint. In addition to any productivity and convenience benefits, augmenting the wired infrastructure with wireless devices can reduce the cost of extending Sandia's computing networks.

For the purposes of this report, wireless communication is used in its broadest sense: communication without wires. Communication can be voice or data, streams or packets. Communication media not involving wires can use infrared, free-space optical, or radio frequency signals, each occupying a different portion of the electromagnetic spectrum.

This report endeavors to describe a potential future wireless end state for Sandia, how and where wireless technology might be used to achieve that state, and recommendations for migration toward that state. Also included in this report is a current description of wireless technology and a discussion of how it might evolve.

2 Current State of Wireless Technology

Wireless communications is literally communicating without wires. This encompasses radio frequency (RF), infrared (IR), and free space optical communication systems.

It is appropriate to open the discussion of wireless technology with an overview of some technical issues that are common to some or all of the technology implementations. *Path Loss* is the relationship between the received signal and the transmitted signal and quantifies the attenuation of a signal across the distance between the transmitter and the receiver. Not only are distance, transmit power level, receiver sensitivity, and antenna gain, factors in path loss, but also environmental conditions in the path of the signal that can cause attenuation (e.g. rain, fog, etc.). Another issue is *Shadow Fading*, where physical obstructions that are opaque to the signal, block or prevent signal reception in areas behind them (in relation to the signal source). Depending on the power level of the signal, the nature of the obstacle, and the proximity of the signal transmitter and receiver to the obstacle, the signal might be able to knife-edge over or around the obstruction. *Multipath* problems are caused by two or more differently delayed versions of the original signal arriving at the receiver at the same time. This phenomenon occurs when one copy of a signal travels a direct line to a receiver and a second copy of the same signal is reflected off of several objects before arriving at the receiver, thus taking longer to reach the receiver. Alternatively, there might be no direct path from the transmitter to the receiver and signals may take different paths being reflected off of a different number of surfaces, creating transmission paths of different lengths, and causing the same signal to arrive at various points in time. *Intersymbol Interference* is a special case of multipath interference and occurs when the arrival delay between different versions of the same signal approaches the duration of a data symbol, causing the symbols to overlap in varying degrees at the receiver. Finally, *Co-channel Interference* is the distortion of received radio signals by nearby systems using the same, or harmonics of the same, frequency.

As one can see, all of these issues apply to RF communication systems, some of them apply to IR systems, and only path loss and shadow fading are relevant to free space optical communications.

2.1 Cellphones and Pagers

2.1.1 Cellular telephone systems

As cellular telephone system technology advances, the data transmission capabilities and rates increase. This could potentially provide wireless data connectivity to laptop computers and various handheld data devices.

Most, if not all cellphones include features such as call logs, multiple ring tones, menu navigation keys, battery and reception indicators, and memory for a phone book, in addition to basic wireless telephony. More advanced cellphones also include text messaging, a color display, multiple modes of operation (e.g. combinations of frequency

bands, modulation types, circuit vs. packet switched, etc.), voice activated dialing, music players, gaming options, email access, web browsing, or Java applications. Very advanced cellphones blur the line between the cellular telephone and the wireless telephony-enabled Personal Digital Assistants (PDAs).
The first generation wireless technologies (1G) are analog systems designed to carry only voice transmissions. These (and successive generation) systems are based on *cells*, where each cell is a geographic area (actually a volume, since height is a factor in hilly terrain or when tall buildings are involved) in which there is radio coverage by a given cell phone tower. Several of these 1G systems are briefly described.

The Advanced Mobile Phone System (AMPS) is a 1G circuit switched system that uses FM modulation in the ranges of 824-849 MHz and 869-894 MHz. AMPS is based upon Frequency Division Multiple Access (FDMA) and provides 832 channel pairs. An end wireless device (handset) transmits on the lower channel and receives on the higher channel of a frequency pair. AMPS was deployed throughout much of the world, starting in 1983 [29], and still sees widespread use, especially in the United States where there is extensive AMPS coverage.

Total Access Communication System (TACS) is a variant of AMPS that operates in the 890-950MHz band and uses a somewhat narrower channel spacing (25 KHz vs. 30 KHz) than AMPS. Deployment of this system began in 1985 in the United Kingdom [29]. Extended Total Access Communication System (ETACS) operates in a larger frequency band (872-960 MHz) using the same 25 KHz channels. These systems are still in use in the United Kingdom, but are being replaced by GSM systems. (GSM systems will be described later in this section.)

The Nordic Mobile Telephony (NMT) system was first deployed in Denmark, Finland, Norway, and Sweden and has subsequently been deployed in more than 40 countries around the world since 1981 [29]. NMT is also a 1G, FDMA, circuit switched technology using FM modulation. NMT 450 operates in the 453-468 MHz band with a channel spacing of 25 KHz. NMT 900 operates in the 890-960 MHz band with a channel spacing of 12.5 KHz. NMT 450 is reputed to operate well in rough terrain, such as that found in Scandinavia. NMT 450 is still widely used, particularly in Russia, and will probably migrate to a CDMA variant operating in a 450 MHz band. (CDMA systems will be described later in this section.)

Because these 1G systems are all analog, FM modulated, FDMA systems, there is no inherent security. Scanner radios, such as those used to monitor public service (police and fire) radio bands, can be used to eavesdrop on 1G cellular telephone calls. In addition, the identifying information needed to clone a 1G cell phone can be captured off the air and decoded. By programming the right pieces of this information into another 1G cellular handset, an interloper can make his phone appear to the cellular network as belonging to someone else, and therefore having his usage billed to someone else.

Second generation wireless technologies (2G) are descendants of the analog 1G systems initially deployed in the 1980s. 2G systems are designed to improve capacity and voice

quality beyond that of the 1G systems and provide the ability to carry digital computer data. Digital data could be carried over the 1G AMPS network in analog form, similar to the way it is carried over an analog wired telephone network when using a modem. This could be performed by attaching a device, similar in function to a modem, between the computer and the cellphone. The current, commonly deployed systems in the United States are based upon 2G technology. The 2G offerings are briefly described in the following paragraphs.

Cellular Digital Packet Data (CDPD) is an overlay that can be deployed on top of an AMPS or TDMA network. It is used to transmit and receive packet switched computer data over idle channels of an existing 1G cellular telephone voice network at a data rate of 19.2 Kbps.

Code Division Multiple Access (CDMA) is a digital 2G technology employing Direct Sequence Spread Spectrum (DSSS) in the 900 MHz and 1900 MHz bands. 2G CDMA systems (also known by the trademark cdmaOne) move voice and data packets in a packet switched fashion, unlike the circuit switching of the 1G AMPS systems and the Public Switched Telephone Network (PSTN). The rate for passing computer data over these CDMA systems is 14.4 Kbps. CDMA systems have a frequency reuse factor (that is, the number of different frequency sets required by a cell cluster) of one, which means the same frequencies can be re-used in adjacent cells.

The wireless communication technology, TDMA (formerly known as D-AMPS) uses TDMA techniques to divide up its available radio spectrum. It is a digital, circuit switched, 2G upgrade to 1G AMPS [29]. 30 KHz channels of the 824-894 MHz band (same frequency band as used for 1G AMPS) are divided into time slots to support three digital users in the same space as one AMPS user. TDMA systems can support computer data transmission at up to 9.6 Kbps.

Global System for Mobile Communication (GSM) is a digital, circuit switched 2G technology using a combination of FDMA and Time Division Multiple Access (TDMA) techniques in the 890-960 MHz, 1710-1880 MHz, and 1850-1990 MHz bands. (The 1900 MHz band is used for GSM systems in the United States.) The available bandwidth is split into channels (FDMA) with each one of the channels then essentially divided into eight time slots (TDMA), allowing up to eight users per channel. (Each channel is made up of two frequencies, where the higher frequency of the pair carries transmissions from the Base Transceiver Station of a cell to the mobile equipment, commonly a cellphone, and the lower frequency of the channel pair carrying transmissions back to the Base Transceiver Station.) GSM systems can also use frequency hopping to minimize interference and alleviate multipath fading. GSM systems can have computer data rates of 9.6 Kbps per channel. Today, GSM technology is used by more than one out of every 10 people in the world [12]. GSM systems are installed in more than 170 countries [12].

Personal Communications Services (PCS) is not really a technology, but rather an artifact of the U.S. Federal Communications Commission (FCC). The FCC created PCS to encompass mobile and ancillary fixed communications providing services to individuals

and business, and set aside the radio spectrum between 1850 MHz and 1990 MHz for this use [29]. Even though there are products currently on the market bearing the name "PCS", PCS is actually a concept and a set of frequency bands. In the United States, GSM services are operated in the PCS band (1850-1990 MHz). Also in the United States, Sprint PCS supplies service using CDMA technology in the same band. Even some CDPD services are reputed [29] to be offered in this band! The PCS concept does make use of cells, and performs handoffs if users move between cells. PCS systems do employ frequency reuse if they are based on GSM technology, but do not if they are based on CDMA technology.

Currently there are three predominate 2G wireless technologies operating in the United States (GSM, CDMA, and TDMA). Even though the role of TDMA is expected to diminish (being replaced by GSM), the United Stated is expected to lag behind Europe and Japan due to the simultaneous deployment of two incompatible 2G technologies (CDMA and GSM). On a worldwide market scale GSM is by far the most popular of the 2G standards [29], although CDMA enjoys wider acceptance in the United States.

As stated earlier, computer data rates of the 2G technologies vary from 9.6 Kbps for GSM and TDMA systems, up to 19.2 Kbps for the CDPD technology. (CDMA systems come in somewhere between at 14.4 Kbps.) A desire to increase data rates, and provide advanced features, is driving the deployment of third generation wireless technology (3G). Although it is technically possible to go from 2G to 3G, it is cost-prohibitive for the service providers to make the technology change in a single step. Because of this, an intermediate step (2.5G) was proposed and is being implemented.

High Speed Circuit Switched Data (HSCSD) is a 2.5G enhancement to GSM networks allowing circuit switched data transmission at 28.8 Kbps that is available in certain parts of the world (not the United States). General Packet Radio Services (GPRS) is a 2.5G evolution of GSM that packet switches digital voice and data at rates up to 171.2 Kbps. With appropriate transceivers and GPRS data terminals, it can be used over existing GSM networks. Trial GPRS systems are in use. EDGE is another 2.5G technology that fits between GPRS and 3G technologies such as Wideband CDMA (WCDMA) on the path from GSM and TDMA to the 3rd generation wireless devices. EDGE is built upon the GPRS air interface and network hardware, but uses new coding schemes and adaptive modulation to move data faster and improve the efficiency of the communication channel. The maximum data rate for EDGE systems is over 384 Kbps. According to a business news story on "TheStreet.com" from June 20, 2002 [18], Nokia is, and will continue to be, supplying EDGE infrastructure equipment to AT&T.

IS-95B is the next (2.5G) iteration of CDMA and can move packet switched data at up to 65 Kbps. IS-95B networks have been in commercial service since 1999 in Korea. The 3G product on this path is cdma2000. It preserves the network operators' investments in earlier (cdmaOne, IS-95B) systems, and will be able to move data at rates from 14.4 Kbps (on cdmaOne networks) up to 2 Mbps (on second phase, cdma2000 3x networks).

2.5G systems are the leading-edge, state-of-the-art at this time. 3G systems are starting to be deployed in the United States and may soon become the state-of-the art, although full deployment of 3G systems will be based upon market realities and user demand. The cellular phone technologies described in this section are summarized in Table 1.

Table 1. Summary of Cellular Telephone Technologies.

Technology	Generation	Analog or Digital	Freq. Range or Band	Switching	Voice/Data	Data Rate
AMPS	1	A	824-849 MHz & 869-894 MHz	Circuit	V	N/A
TACS	1	A	890-950 MHz	Circuit	V	N/A
ETACS	1	A	872-960 MHz	Circuit	V	N/A
NMT	1	A	453-468 MHz, 890-960 MHz	Circuit	V	N/A
CDPD	2	D	AMPS Networks	Packet	D	19.2 Kbps
CDMAone	2	D	900 MHz band, 1850-1990 MHz	Packet	V,D	14.4 Kbps
TDMA	2	D	AMPS Networks	Circuit	V,D	9.6 Kbps
GSM	2	D	890-960 MHz, 1710-1880 MHz, 1850-1900 MHz	Circuit	V,D	9.6 Kbps
HSCSD	2.5	D	GSM Networks	Packet	V,D	28.8 Kbps
GPRS	2.5	D	GSM Networks	Packet	V,D	171.2 Kbps
EDGE	2.5	D	GSM, TDMA Networks	Packet	V,D	384 kbps
IS-95B	2.5	D	CDMAone Networks	Packet	V,D	14.4Kbps – 65 Kbps
CDMA2000	3	D	1920-1980 MHz & 2110-2170 MHz	Packet	V,D	14.4 Kbps – 2Mbps
W-CDMA	3	D	1920-1980 MHz & 2110-2170 MHz	Packet	V,D	2Mbps

2.1.2 Paging Systems

Paging systems operate on their own networks, separate and distinct from the cellular telephone networks. Pagers are available in one-way, one and a half way, and two-way paging varieties. Pagers operate at lower power than cell phones and in a different part of the radio spectrum, not the cellular bands. For greater coverage, paging services are available through satellite.

One-way pagers range from simple pagers that pass along a series of numeric digits to alphanumeric pagers that can not only receive paging messages but also email messages. One and a half way pagers are similar to one-way pagers in that they can receive paging and email messages; however one and a half way pagers may also reply to messages. The reply is typically from a list of "canned" messages. Each pager contains a list of common, limited responses, called canned responses. An example of a canned response would be, "I'll meet you there." Two-way pagers are actually small email terminals with tiny keyboards and memory for an address book. Some of these, like the RIM (Research

in Motion) BlackBerry, are intended to integrate with corporate email solutions. Two-way pagers can also include calendar and date book functions, encompassing some of the territory covered by PDAs.

2.2 PDAs and Pocket PCs

Personal Digital Assistants (PDAs) are small computers that run a limited set of applications. They are basically handheld organizers that store contact information, allow the taking of notes, and offer scheduling and event (timer) notification. They can also store and retrieve information (such as that relating to daily expenses, job and project assignments, etc.), provide "mini readers" for the reading of books, and access corporate data networks and the Web.

Various models of the Palm® as well as all models of the Sony Clié™ and Handspring® PDA have infrared ports to enable wireless communication with other PDAs. Some Palm units have an integrated RF transceiver to provide wireless Internet access. Others may include a Mobile Internet Kit, which permits you to access email and the Internet with a data-enabled mobile phone. All Handspring PDAs include expansion slots that can accommodate, among other things, an RF communication module.

With cellular telephones offering extended features such as calculators, expanded (beyond just telephone numbers) contact information, and event notification, and PDAs offering email and Web browsing capabilities, the line between cellphones and PDAs is becoming blurred. Indeed, the Kyocera Smartphone is not only a cellular telephone, but also offers an address and date book, memo pad, To Do List, and since it runs the Palm OS, any other Palm application. Likewise, cell phones in the Samsung SPH-I300 series combine the functionality of cell phones with the PDAs and are compatible with Palm OS applications. Similarly, the Nokia 9290 Communicator, running the Symbian operating system, combines a cell phone with a small computer sporting a 640 x 200 pixel color display to browse the web, read books and pdf files, view jpeg pictures, and perform organizer functions.

Other RF connection possibilities for attaching to local data networks from a PDA include 802.11b and Bluetooth modules. (Bluetooth and 802.11b are described in a later section.)

The capabilities of a Pocket PC are similar to those of a laptop computer, but more limited. Many Pocket PCs use the Windows CE operating system from Microsoft. Pocket PCs have full color screens that are typically larger than those found on cellphones and PDas. Some Pocket PCs have keyboards; others do not. In some cases, Pocket PCs can be used as thin clients, with a terminal server.

Pocket PCs can have wireless access through data-capable cellphones, wireless modems, CDPD devices, and 802.11b wireless LAN cards (to be described in a later section). These can have the form factor of a Type II PCMCIA card or a clip-on "sled" device. Postage stamp-sized devices for SD slots are currently under development [29].

2.3 Computer Networks

2.3.1 IR

Direct beam radiation comes in a direct line from the source. Direct-beam infrared (DBIR) is mainly characterized by the need for a line-of-sight between the transmitting and receiving devices. When using DBIR communications, the transmitted pattern must be adjusted to reasonably align (within beam width and distance specifications) with the receiver.

The Infrared Data Association (IrDA) is the trade association responsible for defining infrared data and control standards. IrDA standards define serial DBIR data transmission at distances up to 1.0 meters with bit error rate of 1 in 10^9 in daylight illumination levels. (Typically, usable connections can even be reached at 2 meters.) Data rates in the standards range from 2400 bits per second to 4 Mbps. Increased distances (outside of the IrDA standards) can be attained by decreasing the data link rates.

Because DBIR is very much point-to-point oriented, it is well suited for connecting certain peripheral devices (e.g. keyboard, mouse, etc.) to a computer or connecting two devices (PDA to PDA, laptop to laptop, PDA to laptop, etc.) for data exchange. Using lenses to focus the beam, DBIR can also be used to provide a wireless bridge between Local Area Networks (LANs).

Diffuse radiation is scattered out of the direct beam by refraction and reflection. Diffused infrared (DFIR) fills an enclosed area, using the rooms surfaces (e.g. walls, ceiling) and surfaces of objects in the room (e.g. tables, cabinets) to bounce the IR signal between the transmitter and the receiver. Diffused IR does not require alignment to establish or maintain a communication link. Diffused IR links provide robustness against shadowing and provide coverage similar to radio waves within a room, making them suitable for nomadic access in limited range environments, but they can be subject to multipath interference, which limits their rate of communication. DFIR communication technologies require higher power than DBIR to cover the same distance, but IR signals do not penetrate walls or ceilings.

Commercial DFIR products are on the market. One manufacturer of these products (Spectrix Corp.) has a system that operates at a data rate of 4 Mbps and includes PC cards for a laptop (to fit into a Type II PCMCIA slot), IR “antennas”, and Wireless Hub Routers (that serve as the controllers and protocol gateways for the system). The Wireless Hub Router can control eight or 16 antenna units and contains a 10/100 Base T uplink to connect into a wired Ethernet network.

The IEEE 802.11 standard (to be discussed in a later section) provides not only for several RF physical or PHY layers, but also a diffused infrared PHY layer operating at 1 (and optionally 2) Mbps using Pulse Position Modulation. Currently (circa summer 2002), there seem to be no 802.11 infrared devices available.

Because IR signals do not penetrate walls and are heavily attenuated by windows, diffused infrared is a possible technology candidate to provide wireless data networking over comparatively short distances (6-30 meters) in confined or bounded indoor areas. Within these kinds of areas, DFIR is an especially suitable choice when, for security or interference reasons, RF communications are restricted.

2.3.2 Wireless Optical

Existing construction (buildings, roads, etc.) could make installing extensions to wired (copper or fiber) networks cost prohibitive. For ad hoc situations requiring new data communications between buildings or technical areas, such as one-time events or limited duration projects, installing wired infrastructure may not be cost effective. One possible solution is to use air as the transmission medium in a free-space optical networking system.

The Lucent Wavestar Optic Air system used dense wavelength-division multiplexing (DWDM) technology to deliver up to 10 Gbps over a 5 Km distance [4]. A system like this could be positioned in tall buildings or on rooftops (so a clear line-of-sight can be obtained) to bridge LANs together in a temporary or permanent fashion.

Unfortunately, the Lucent Wavestar Optic Air system is now a discontinued product. Terabeam makes several free space optic products based on the same technology. The Elliptica 7000 series supports Fast Ethernet (100 Mbps) and OC-3 (155 Mbps) transmissions, while the Magna 8000 series supports Gigabit Ethernet (1 Gbps) and OC-12 (622 Mbps) transmissions. LightPointe and other vendors supply systems that operate at rates from 10 Mbps to 2.5 Gbps over distances ranging from a hundred meters to several kilometers [34].

2.3.3 RF

The Institute of Electrical and Electronics Engineers (IEEE) has an approved standard, IEEE 802.11, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, for wireless networking. Three PHY layers were defined in 802.11, Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum and Infrared light. Supplements *a* and *b* added Coded Orthogonal Frequency Division Multiplexing and High Rate Direct Sequence Spread Spectrum to the physical layer alternatives. Full discussion of spread spectrum communications is outside the scope of this report and can be found in other sources (e.g. various reference/text books [2][23][31]).

Products conforming to the IEEE 802.11b standard use High Rate Direct Sequence Spread Spectrum (HR/DSSS) with Complementary Code Keying (CCK) modulation for data transmission at 5.5 Mbps or 11 Mbps with the ability to back down to 2 Mbps or 1 Mbps if necessary. Optionally, CCK modulation can be replaced with Packet Binary Convolutional Coding (PBCC). 802.11b-compliant devices have 3 non-overlapping channels in the unlicensed 2.4 GHz Industrial, Scientific, and Medical (ISM) band.

Numerous manufactures make these 802.11b access points and PCMCIA/Cardbus LAN interfaces. The ORiNOCO 802.11b cards (by Agere Systems) have a (Lucent Technologies proprietary) connector to accommodate an external antenna for a greater (or possibly shorter) operational range.

Rather than using spread spectrum communications, IEEE 802.11a devices use Coded Orthogonal Frequency Division Multiplexing (COFDM or coded OFDM). They operate at rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps using 8 non-overlapping channels in the 5 GHz Unlicensed National Information Infrastructure (U-NII) band. Not only does this allow faster data communications and higher capacity systems, but has the advantage of operating in a less crowded band. (Bluetooth devices, microwave ovens, some cordless telephones, and other devices, compete with 802.11b products in the 2.4 GHz ISM band.) Several manufactures (including Proxim, Intel, Linksys, and SMC) have 802.11a offerings in their product lines. One company (Agere) sells wireless access points that can accommodate two radio cards (Orinoco AP-2000 Access Point) thereby enabling support for both 802.11a and 802.11b wireless networks, simultaneously.

As of summer 2002, IEEE 802.11g has not yet been ratified as a standard. If this comes to fruition, it will combine various aspects of the 802.11a and 802.11b specifications. 802.11g devices would communicate at rates up to 54 Mbps (like 802.11a devices), but in the 2.4 GHz ISM band (like 802.11b devices). 802.11g products are supposed to be backward compatible with 802.11b devices, thereby preserving investment and making migration easier, but 802.11a devices will enjoy a first-to-market advantage over any 802.11g devices for the 54 Mbps market.

Both 802.11a and 802.11b support two modes in which they can operate. When in *infrastructure mode* the various 802.11 interface cards communicate to a wireless access point, which is connected to the wired network. In *ad hoc mode* the 802.11 interface cards communicate with each other directly, in a peer-to-peer manner. These modes of networking are compared in Figure 1.

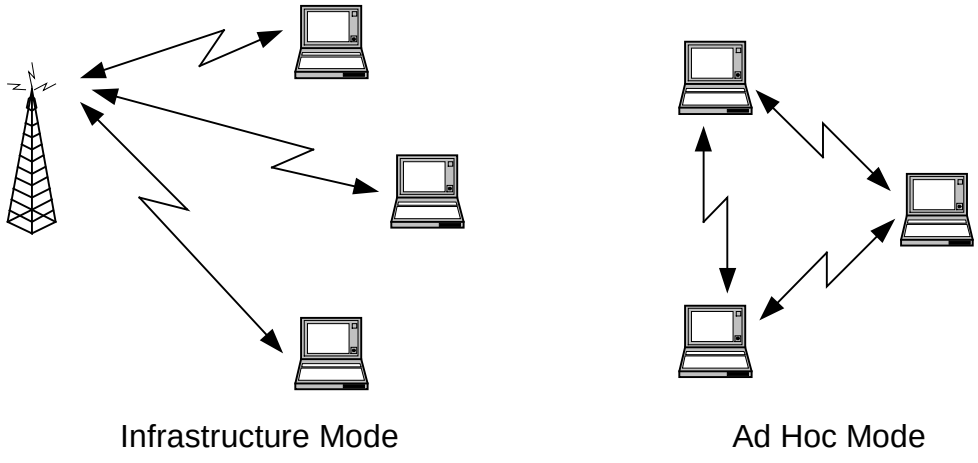

Figure 1. Infrastructure Mode Versus Ad Hoc Mode Networks.

Some 802.11 access points with high-gain antennas, or other RF equipment with directional antennas (e.g. the Alvarion BreezeLINK series) can be used to wirelessly bridge wired or wireless LANs. Depending on the configuration, these can be point-to-point or point-to-multipoint bridges. These bridges can operate over a range up to 30 miles or more.

Many 802.11b and 802.11a wireless LAN devices operate at distances up to several hundred feet indoors and over 1000 feet outdoors. As well as permitting an extended operating range or mobile operating conditions, these devices raise many security issues, especially in light of the claims that the Wired Equivalent Privacy (WEP) implemented in 802.11 products does not actually provide privacy [11][28][1][5]. These products have been shown to have flaws in their security protocols and implementations, and their operations at the data link layer, making them susceptible to session hijacking, data manipulation, and cryptanalytic attacks to derive the WEP encryption/decryption key. The port-based network access control proposed in IEEE 802.1x still contains protocol flaws that leave 802.11 networks susceptible to session hijacking and man-in-the-middle attacks [19].

Currently, answers to some of the security issues may be found in the proper placement of 802.11 devices combined with appropriately configured IPSec Virtual Private Network (VPN) tunnels and/or through add-on security products. One such product, AirFortress by Fortress Technologies provides a layer two encryption and access control solution. AirFortress employs dynamic session keys (with Diffie-Hellman key exchange), AES or Triple DES encryption, and SHA-1 frame authentication to provide privacy and authentication. Software on each wireless client intercepts the packet produced by the network driver before it is transmitted, and encrypts the frame, including the MAC address (thereby defeating attacks based upon MAC address spoofing). The wireless access point receives the transmitted frame and passes it to the AirFortress Wireless Security Gateway, which decrypts the frame and authenticates it before passing it on to the wired network. Access control server software allows for blacklisting of lost or stolen client systems. The software clients and the Wireless Security Gateways supplied by Fortress Technologies as part of the AirFortress wireless security solution are blind as to whether 802.11a or 802.11b hardware is being used in the network, since the AirFortress components reside outside of the radio link.

Similar add-on security products are available from SMC Networks, NetMotion Wireless, ReefEdge, and Bluesocket [25]. Both VPNs and these various add-on security products work with products that are operating in infrastructure mode. They are not suitable for peer-to-peer communication in ad hoc networks.

HiperLAN is a networking standard developed in Europe by the European Telecommunications Standards Institute (ETSI) for high performance RF networks. It is designed for the 5.15-5.30 GHz band. HiperLAN Type 1 has a maximum data rate of about 23.5 Mbps. HiperLAN/2 can operate up to 54 Mbps. The HiperLan MAC protocol has a feature called intraforwarding, which allows messages sent to nodes that do not have direct connections, to be forwarded by other nodes. This feature can be used to

overcome range limitations and allows a wireless LAN to be extended without adding access points or a wired network backbone. The HiperLAN MAC protocol also exploits the fact that a receiver can sense or detect a signal at a much greater range than it can decode the signal. This enables it to (at least partially) overcome "hidden node" problems [2] by inhibiting its own transmissions upon sensing other, possibly interfering transmissions. Devices built on the HiperLAN standards do not enjoy the popularity, at least in the United States, that 802.11 products do. Selected characteristics of 802.11 and HiperLAN/2 are compared in Table 2.

Table 2. 802.11 and HiperLAN/2 Comparison.

Characteristic	**802.11**	**802.11b**	**802.11a**	**HiperLAN/2**
Frequency Band	2.4 GHz	2.4 GHz	5 GHz	5 GHz
Maximum Physical Data Rate	2 Mb/s	11 Mb/s	54 Mb/s	54 Mb/s
Connectivity	Connection-less	Connection-less	Connection-less	Connection-oriented
Spectrum Division	FHSS or DSSS	DSSS	Single carrier in sub-channel	Single carrier with dynamic frequency selection
Encryption	RC4	RC4	RC4	DES, 3DES
Radio Link Quality Control	None	None	None	Link adaptation

Bluetooth was developed as a full-duplex, short range radio link to connect up to 8 portable or mobile devices at a raw data rate of 1 Mbps. (The actual full-duplex data rate is about 430 Kbps, while asymmetric data rates of 723.2 Kbps can be achieved in one direction with a return rate of 57.6 Kbps.) Bluetooth is intended to connect personal computers, computer peripheral devices (keyboards, printers, etc.), PDAs, mobile phones, and consumer electronic products (headphones, digital cameras, MP3 players, etc.) in piconets (two to eight Bluetooth devices communicating with each other). Bluetooth uses FHSS in the 2.4 GHz ISM band with a range of about 10 m. Higher transmission power can extend the operational range to 100 m or more.

Bluetooth devices can associate with each other in an ad hoc fashion. One device will act as a master and all other associating devices will be slaves in a piconet. Alternatively, a Bluetooth wireless access point can be a master device to control slaves within its operating range (picocell). The first available Bluetooth wireless access point, the WIDCOMM BlueGagte 2100, can link 7 Bluetooth devices simultaneously, plus a 10/100Base-T connector to uplink into an Ethernet. Add-in cards are available from several vendors for PDAs and laptop or personal computers, but interoperability issues may still be present.

2.3.4 Wireless Computer Network Technology Summary

As this section indicates, there are many competing RF technologies for building wireless computer networks. These are summarized in Table 3. No one solution will meet the needs of every network user at Sandia National Laboratories. RF, infrared, and wireless optical systems may be mixed into the wired networks for differing purposes in differing

areas. If multiple RF solutions are chosen, we must be careful when attempting to integrate systems using the same frequency band. There is great potential for co-channel interference causing reduced performance as the various technologies compete with each other for bandwidth.

Table 3. Summary of Wireless Computer Network Technology.

Characteristic	DBIR	DFIR	Free Space Optical	Bluetooth
Portion of Spectrum	Infrared	Infrared	Near-infrared	RF (2.4 GHz)
Modulation or Spectrum Division	Pulse Modulation	Pulse Modulation	DWDM	FHSS
Raw Data Rate	4 Mb/s	4 Mb/s	10 Gb/s	1 Mb/s
Typical Range	6 ft.	50 ft. (1000 sq. ft.)	3 mi.	30 ft.
Line-of-sight required?	Y	N	Y	N
Penetrates Walls?	N	N	N	Y
Intended Commercial Use	Short range point-to-point links	LANs	Bridging of networks	Connect computer peripheral devices and consumer electronic devices into piconets

Table 3 (continued). Summary of Wireless Computer Network Technology.

Characteristic	802.11	802.11a	802.11b	HiperLAN/2
Portion of Spectrum	RF, Infrared	RF (5 GHz)	RF (2.4 GHz)	RF (5 GHz)
Modulation or Spectrum Division	FHSS, DSSS, Pulse Position Modulation	COFDM	HR/DSSS with CCK modulation or PBCC	Single carrier with Dynamic Frequency Selection
Raw Data Rate	2 Mb/s	54 Mb/s	11 Mb/s	54 Mb/s
Typical Range	300 ft . – 3300 ft.	325 ft. – 1150 ft.	300 ft. – 1000 ft.	???
Line-of-sight required?	N	N	N	N
Penetrates Walls?	Y	Y	Y	Y
Intended Commercial Use	LANs	LANs	LANs	LANs, 3G mobile networks

RF systems introduce complications such as radio waves not being contained or bounded by buildings and fences, unintended emissions caused by cross coupling of data, and network intrusions caused by outsiders attacking RF communication sessions and access points. There are technological and policy approaches (described in later sections of this report) that may make RF technology palatable for certain uses. Other technological research and development, combined with possible changes in laws or policies may expand the range of uses.

3 How Might Wireless Technology Evolve?

This section must be prefaced by the fact that the author's crystal ball is of no higher quality or is no clearer than the next person's. These are the observations of the author.

Cellular telephone systems are headed into the 2.5 and 3rd generation, but slower than equipment manufacturing companies and service providers expected. Third generation cell phone systems will incorporate data transfer rates significant enough to be used in data communication networks. The author believes the line between cell phones and PDAs will disappear, as cell phones get more memory (to store contact information, appointments, etc.) and Bluetooth and/or infrared interfaces, while PDAs become equipped with voice applications and cellular network interfaces.

At the other end, the line between Pocket PCs and PDAs will blur, since PDAs are just miniature computers that support various applications, including organizer applications. Adding in phone capabilities resulting from the convergence of cellular phones and PDAs gives large, bulky cell phones or cellular telephony-capable Pocket PCs. Indeed, the Pocket PC Phone Edition is now available from several vendors including Voicestream and AT&T Wireless.

The author views this as becoming a bi-polar market with extremely capable devices sized in the range of current PDAs to Pocket PCs and incorporating the functions of a laptop (including organizer applications), cell phone, GPS receiver, etc. at one end of the market, and a class of compact, moderately capable (cell phone, organizer, web browser, and possibly GPS combination) devices at the other pole. Although Nokia is moving in this direction with the 9290 Communicator, that device (which incorporates a keyboard and a cell phone) will not run programs such as a version of Microsoft Office. Its touted "PC compatibility" is limited to document (calendar, contact, text, etc.) files being compatible with windows, allowing for easy synchronization with a Windows-based PC.

Direct-beam infrared and Bluetooth technologies will be more extensively used for connecting input and output devices to PDAs and computers. Both of these technologies should see expanded service for the interconnection and synchronization of computers and PDAs.

The use of 802.11b for wireless LANs is growing quickly, despite its security weaknesses. Whether security is fixed in the 802.11 standards, or by some add-on components, or even not fixed at all in the near future, the author expects the use of 802.11b equipment to continue to increase, but be augmented (and eventually superceded) by 802.11a networks. Because of the crowded conditions in the 2.4 GHz ISM band, 802.11b and 802.11g performance will suffer as more and more devices are brought into use. 802.11a offers greater potential for expansion, operating in a less crowded band and having more non-overlapping channels. Within indoor areas where there exist security or radio frequency interference concerns, the author sees a viable niche for diffused infrared LANs.

In any endeavor larger than a home or small office, there will not be a “one size fits all” solution. Elements of multiple technologies will be integrated together to provide adequate capabilities with the requisite flexibility.

4 Where Should Sandia Strive to Be?

Discussions with a cross-section of the user community brought forth the following needs and interests regarding wireless communications at Sandia. Many of these desires are based upon portability and convenience; some require full mobility. Portability allows a user to be connected to the network while at various stationary locations. Although portability does not, in itself, imply a wireless connection, it may require one in order to be convenient enough to be used. Mobility allows a user to be continuously connected to the network while in transit or on the move. Mobility always implies a wireless connection to the network. Mobility is a superset of portability, requiring not only location management functions, but also handoff functions.

There was strong interest in having the ability to process incoming and outgoing email while in meetings, both inside and outside the limited areas. There was also strong interest in two-way paging capability (again both inside and outside the limited areas), especially in devices like the RIM BlackBerry, which combine these functions.

Some interest was expressed in easily using laptop computers in conference rooms without the bother of connecting cables. Interest was also expressed in wireless connectivity for laptops while on the road (e.g. airports, hotels, conferences, trade shows, meeting rooms at other companies/facilities equipped with wireless networking). There was some interest in using wireless data communications to connect computers in offices and labs to the corporate infrastructure, in lieu of wired communication drops, to reduce expenses and wiring complexity. Additionally, some interest was expressed in connecting classified computing resources to the classified network, wirelessly, in order to reduce the cost of extending secure network services into places not wired for such.

Garnering limited interest was the ability to use cellular telephones within the limited areas at Sandia, ad hoc wireless networking within offices (so someone could easily bring files with them when coming to meet or discuss an issue), and cordless telephones (as to not be tethered to a wall or fixed point when working on a problem in a laboratory).

It was generally agreed that for the future Sandia will need ubiquitous wireless communications for voice, short message service (SMS), PDAs, and such, inside the limited areas, because that is the new way of life for recent college graduates. The way that they have been taught and conditioned to interact with each other and collaborate to solve problems revolves around instant and continuous wireless connectivity. This also seems to be a path to higher productivity for senior personnel.

Based on the inputs from the user community, Sandia should ultimately strive to create an environment of mobile wireless connectivity supporting voice, SMS, and email. Portable wireless access to the data network should be pervasive. Fixed wireless connectivity for data and voice should be a tool, to be considered as a practical alternative to wired communications. All this should be accomplished using commercially available, off-the-shelf equipment.

This would enable small, portable, computing devices to be easily used in many working locations, both inside and outside the limited areas. It would also make full use of the new generation of employees steeped in information technology and its exchange, and improve productivity of "legacy" employees. Costs could also be reduced due to the ease of installing wireless communications versus the cost wiring individual communications drops.

This will require not only new equipment, but also changes in policy, new ways of thinking and conducting business, fresh approaches to old problems, and analysis of impacts on existing wireline equipment. Balancing the advantages – listed above – of wireless communications, are the security concerns that arise because the data transmissions are not necessarily bounded by walls and may be coupled to fortuitous conductors. Some of these issues are discussed in Chapter 5.

If security was not a concern, Sandia could be mostly wireless and untethered today. (Some users would still need wired infrastructure to support their data rate requirements.) Because security concerns are an integral part of operations at Sandia, we must look at how best to harness the power of the oncoming flood of wireless communications. We could try to build a symbolic dam to turn away the flood (as has largely been done in the past), but this approach will leave us falling further and further behind the state-of-the-art of communications. This will eventually prove costly in terms of finding equipment (both computing and communications) to meet our requirements, and in terms of attraction and retention of personnel. Additionally, cracks and leaks are already starting to appear in the dam, as explained in Chapter 6. At some point the dam will crumble and no one will be able to keep wireless communications out of Sandia and other facilities. A far better tack will be to plan for the oncoming flood and migrate to wireless connectivity in an orderly manner.

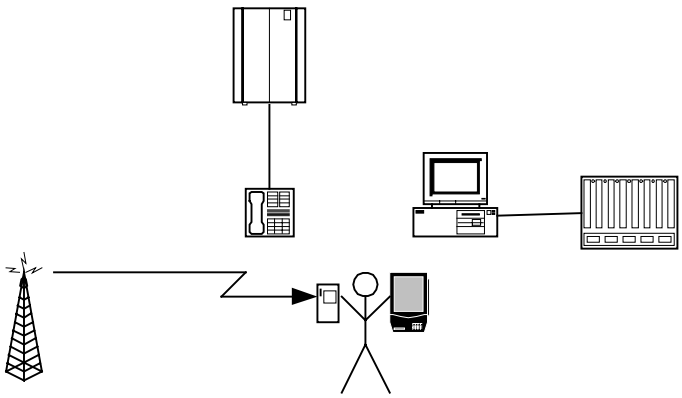

Figure 2. Office Communications Today.

Today's office is depicted as Figure 2, where the employee has a wired telephone, a wired computer, a one-way pager, and an unconnected PDA. An aggressive position would be to push technology and policy to allow seamless, wireless connectivity of phones, telephony-equipped PDAs, and computers (portable or stationary), as shown in Figure 3. This would not only address the current requests by the user community, but

also encompass the new untethered, instantly communicating, information-based employee. This approach would involve:

- Wireless RF data networks (both inside and outside the limited areas) everywhere except the most secure places, where diffused IR networks would be used; and
- Cellular phones and PDAs in most parts of the campus, allowing instant communications via voice, SMS, and email.

This would provide productivity and cost benefits by:

- Instant accessibility of colleagues,
- Instant accessibility by supervisors,
- Instant access to information resources,
- Improved information exchange,
- Elimination of costs incurred by carrying multiple devices (pager, cell phone, PDA, etc.) and the associated reduction in costs of supporting multiple systems, and
- Granting the ability to make productive use (returning calls and messages, processing email, etc.) of otherwise dead time (e.g. walking across the complex, waiting for the start of a meeting).

In this approach (shown in Figure 3) most people would have one mobile device to handle voice communications, text messages, appointments and contacts, basic email, and simple web browsing. This eliminates the need to carry a pager, forward calls (because your phone goes with you) except to voice mail, be tethered to one point in an office or lab, and fumble between a phone and a PDA or other organizer. (Devices that combine these functions are already starting to appear on the market.) A second device that would be portable but not necessarily mobile, such as a laptop computer with wireless connectivity, would provide heavy duty email and web browsing capabilities along with traditional computing applications. This could lead to an environment where only a small portion of the entire campus remains wired.

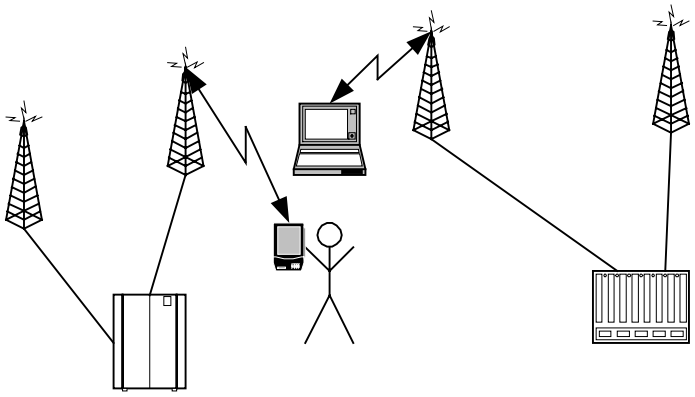

Figure 3. Office Communications Tomorrow.

A more conservative approach, possibly appropriate for a security-conscious national laboratory, would entail a near term component that could be implemented with today's technology and minimal changes to policies. This would be a stepping stone on the path

to the ultimate goal of ubiquitous wireless communications. Specific capabilities to achieve in the nearer term, are:

- Two-way paging,
- Wireless network connections for processing email,
- Wireless connectivity of laptop computers in conference rooms, and
- Wireless connectivity of laptops back to corporate networks while on the road.

This would provide immediate productivity benefits through improved efficiency of:

- Interaction with colleagues,
- Accessing resources, and
- Information exchange.

Wireless connectivity of laptops back to corporate networks while traveling, is now treated the same as connectivity through a wireless LAN at home to Sandia's corporate network [30]. Assuming proper protections and configurations are in place, this can be approved locally at Sandia, without needing to be sent for approval to the local DOE office [21].

Wireless connectivity of laptop computers in conference rooms and allowing the use of BlackBerry-type pager/email terminals inside the limited areas would meet the remaining, most pressing, near term wireless demands. RIM is providing a customized version of BlackBerry software with S/MIME support to be used by the National Security Agency and plans to continue working with NSA "to address the unique requirements of security conscious organizations such as the Department of Defense" [3].

Any chosen approach should be tempered by an analysis of, from an internal infrastructure view, what information makes sense to be migrated entirely off of wired media to wireless media? At what points in time and the development of a wireless infrastructure, should what information be moved from the wired to the wireless world? What information or functions should forever stay wired? If specific needs or requirements are identified in this analysis, these needs may delay or accelerate the development and deployment of the wireless infrastructure.

5 Issues for the Sandia Environment

Speaking in this section as the devil's advocate, what are some of the possible security issues with wireless communications in a secure area?

- It may be possible with cellular handsets, as it is possible with ISDN telephones, to remotely open the microphone for covert listening, via the network infrastructure.
- Functionality of cellular telephones can be changed "on the fly," as new or modified functions can be downloaded, over the air waves, to the SIM card.
- If phone/PDA units contained a GPS transceiver, those units used in combination with other information could potentially pinpoint (within meters) the location of sensitive information.
- Security, as implemented by wireless networking cards conforming to the IEEE 802.11 standards, is weak. Interlopers from outside a given perimeter could exploit internetworking data connections, attack local and remote systems, and steal information. Compounding this is the false sense of security given by WEP.
- Information could possibly be coupled into wireless access points in a wireless extension to a wired network. A discussion of information coupling can be found on pages 78-80 of Computer Security Technology [8] or pages 203-205 of Computer and Communications Security [7].
- Because radio waves do not stop at building walls or fences, both intentional and unintended emissions are difficult to control.

The way to address these issues is with a combination of technology tools and policy changes. Changes in existing laws might also be explored. Possible partial solutions to one or more of the above issues follow.

- Strict configuration control can enforce separation of various computing/networking/power resources and wireless access points. A possible configuration control tool would be a map of the entire Sandia campus, with locations of classified computing and communications resources identified by their GPS coordinates.
- Move to reduce or eliminate copper wiring within the classified infrastructure; allow only fiber optic cables for wired connections in classified networks.
- Policy changes to cluster classified computing into bounded enclaves, rather than allowing classified drops and terminals in any office in the limited areas. (This may also aid in controlling access to classified data and removable media containing classified data, because there would be fewer points/locations to control.)
- Create "cones of silence" where no classified discussions or emanations are permitted.
- Use isolation transformers or batteries to power wireless access points to prevent information coupling [8].
- Examine the use of Liquid Crystal Display (LCD) monitors rather than Cathode Ray Tube (CRT) display terminals to reduce information coupling.

- Encrypt/decrypt all classified information with a Type 1 algorithm at the points where it enters/leaves the network, thereby making the network itself, unclassified.
- Although destructive interference can currently be illegal in the United States per Federal Communication Commission (FCC) regulations, a change in the laws to allow limited interference under certain conditions could enable jamming of cell phones, PDAs with RF interfaces, Bluetooth devices, and laptops with RF LAN interfaces when near devices processing sensitive information.
- Lower power transmitters and lower gain antennas for RF networking devices would reduce their range, the distance at which their emissions could be received.
- VPNs and add-on security products may secure current 802.11b and 802.11a products.
- Now that industry knows what is technically possible, and can learn from its mistakes, an entirely new wireless data communication architecture that incorporates security from the start could be developed for next generation wireless networking deployment.
- A Sandia owned and operated cellular phone system may, in much the same way as the Sandia owned and operated telephone switch, defeat the ability to remotely open the handset microphone for covert listening.
- Just as collaboration with standards bodies and vendors in the past has resulted in standards and products incorporating functions to meet Sandia's needs, future collaboration with cellular terminal equipment manufactures and industry groups may be able to produce design changes to ensure microphones cannot be controlled remotely and to eliminate or restrict the ability to reprogram cellular handsets through SIM downloads. Other collaborations could ensure security-friendly RF devices for use at government facilities.

These issues will not go away and must be faced, if not for productivity, convenience, or social/cultural reasons, then for technological reasons. Article number 103284 from HPCwire ("Intel Details New Technology for Cheaper Chips," August 16, 2002) states that Intel Corporation is seeking to combine multiple features, including wireless networking (presumably in the RF portion of the spectrum), on the same chip with microprocessors.

If RF wireless networking becomes pervasive as a part of every computer chip, DOE and NNSA will have to make some difficult decisions. Will the labs go back to pre-computer days? A return to slide rules and typewriters could mean hiring every able-bodied man and woman in the country to perform calculations and type up the results. This would not only bankrupt the country, but would likely pose a greater security risk than wireless networking! Custom computer chips without built-in wireless networking, fabricated specifically for the U. S. Government would be a somewhat cheaper, but not necessarily any more feasible, solution. It is quite conceivable that at some point, whether we want it or not, whether users require it or not, **we will be forced to deal with RF-based wireless networks and their associated emissions throughout the working environment.** Policies (and possibly laws) will have to change, and new developments to mitigate unwanted side effects will have to advance, in order to accommodate the ongoing march of technology.

6 Where Could Wireless Technology Be Applied at Sandia?

Table 4 recaps the interests of the user community (from Chapter 4) and shows how pieces of technology match up to provide possible solutions. Also shown are potential issues with the technology. Not shown in the table as an issue, because it is needed for all solution technologies, is strong authentication.

Table 4. Summary of User Community Interest in Wireless Connectivity.

Interest	Possible Solution	General Issues
Process incoming and outgoing email while in meetings (both inside and outside the limited area)	Portable wireless laptops, Network-connected PDAs, Two-way pagers	Information coupling, Weak RF LAN security, RF emissions
Two-way paging (both inside and outside the limited area)	Two-way paging terminals, Cellular telephones	Information coupling, RF emissions, Lack of cell phone security
Easily using laptops in conference rooms	802.11 RF LANs, Diffused IR LANs	Information coupling, Weak RF LAN security, DHCP, RF emissions, Containment of IR
Wireless connectivity back to the corporate infrastructure while on the road	802.11b RF LANs combined with VPNs	Weak RF LAN security (covered by IPSec [30] and slight modifications to existing security policy[21])
Wireless data communications in offices and labs in lieu of wired communication drops	802.11 RF LANs, Diffused IR LANs	Information coupling, Weak RF LAN security, RF emissions, Containment of IR
Wireless data connections to SCN	802.11b RF LANs with Type 1 encryption, Diffused IR LANs	Information coupling, Weak RF LAN security, RF emissions
Wireless voice communication	Cellular telephones, Telephony enabled PDAs, Voice over IP (VoIP) using small data processing devices (e.g. Pocket PCs)	Lack of cell phone security, Information coupling, Weak RF LAN security, RF emissions, Microphone use with data processing devices
Ad hoc wireless networking within offices	802.11 RF LANs, Diffused IR LANs, Direct-beam IR ports, Bluetooth ports	Information coupling, Weak RF LAN security, RF emissions, Troubleshooting, Containment of IR
Untethered voice communications with an office or lab in the limited area	Cordless telephones, Bluetooth telephone headsets, Cellular telephones	Information coupling, RF emissions, Lack of cell phone security

The way to migrate into the wireless world is to break the problem into manageable pieces and deal with each piece individually, but in the context of the overall problem. For each piece of the problem:

- Propose a new position, based on the desired goal and the available (or soon to be available) technology;
- Identify the risks involved;
- Identify protection measures to mitigate the risks; and
- Develop a migration path leading to the new position.

Key issues that any risk mitigation strategies will need to address, include:

- Proximity to classified processing and communications;
- Emanations and coupling; and
- Wired media (cable) selection.

Also to be noted here, as it applies to both the classified and unclassified environments, is that we have not performed an exhaustive examination of the Sandia facilities to see what physical limitations exist, especially RF-dead zones. This information could be useful in many ways, including determining where to place classified computing enclaves.

6.1 Unclassified Environment

Wireless technology is here! Direct-beam IR is in use between PDAs inside the limited areas. With local approvals, and conformance to existing security policies and recommended practices, 802.11 wireless data networks can be used in conjunction with Sandia computers at home, in airports, and at conferences and trade shows [30]. This enables increased productivity in road warriors and telecommuters.

Access points for 802.11 RF networks could be installed in locations outside the limited areas such as conference rooms that are outside the fence, and the cafeteria. Diffused IR access points could be installed inside the limited area. This would be a relatively easy way to provide untethered portability for email and collaborative applications.

The RIM BlackBerry, customized for DoD/NSA, holds promise for two-way paging and fully mobile email processing at Sandia. A Sandia-specific version of instant messaging software could be developed to provide an instant message capability not only between portable wireless laptop computers, but also with computers connected to the wired infrastructure.

Each of these items (802.11 RF, Diffused IR, BlackBerry) are potentially a piece of the solution. An analysis, as described above, should be performed for each of these pieces, stating how it would be used, what the risks are, how the risks can be managed to an acceptable level, and a plan for implementation and roll-out.

In the longer term, the issues of RF in the limited areas and ubiquitous wireless connectivity will have to be addressed. Policy and technical issues will need to be solved so RF devices – be they voice phones, PDAs, or computers – can be used anywhere, inside or outside the technical areas. Some of the “solution pieces” listed in Chapter 5

(fiber optic cables, isolated power, “No Classified” zones, LCD monitors, a Sandia cellular system, etc.) may be applied to achieve this.

6.2 Classified Environment

In classified environments, the use of the Harris SecNet 11 PCMCIA cards can provide wireless connectivity, secured to the level of secret [14]. These cards use Type 1 encryption with the Baton algorithm [14] for communicating text, voice, and video data over 802.11b wireless networks. They accept optional antennas or a power amplifier via an SMA-style connector [14]. The wireless access point is a box that accepts one SecNet 11 PCMCIA card and can be wired to an existing secure network. This could reduce the cost of extending secure networking services, while at the same time, providing office-to-office (or intra-office) untethered portability.

Because IR signals are much more easily contained than RF signals, diffused IR could also be used in the classified environment. DFIR could be used in closed conference rooms and large office/work spaces where everyone has the required clearance and a common need-to-know. DFIR, in addition to the Harris SecNet 11 RF cards, will not only aid in providing untethered portability, but also help to reduce the amount of copper cabling in the SCN.

7 Recommendations for the Path Forward

The following sections contain an ordered list of recommendations on harnessing the power of wireless communications to provide one portion of a state-of-the-art communication environment for the 21st century. Further formal study to determine exact risks and details of risk mitigation strategies is recommended before installing new communications hardware.

This ordered list of recommendations dovetails onto the recent work of Del Packwood regarding approvals for RF at SNL-controlled premises. It is expected to extend the work of Packwood and Taylor [21][30], providing a path forward to an environment of ubiquitous wireless connectivity.

With streamlined, local approvals [21][30] we can now use RF wireless networking with Sandia-owned equipment in stand-alone networks. We can also use Sandia-owned computers in RF wireless LANs at home, conferences, trade shows, and airports to connect back into the Sandia corporate network. The recommendations in the following sections are intended to carry Sandia forward, in an orderly manner, into a world of portability and mobility.

The reason that the recommendation regarding the implementation of diffused infrared access points (section 7.1) is listed first, is because it does not require a great deal of further study and is comparatively easy to implement within existing policy, technology, and infrastructure. The recommendations in sections 7.2 and 7.4 provide foundation information upon which other items of the list can draw when they are implemented. Recommendation 7.5 on two-way pagers will need some further study, but I believe much of the work already performed by DoD, NSA, and RIM can be leveraged to accommodate BlackBerry devices in the DOE environment. Once the recommendations in sections 7.2-7.4 are implemented, recommendation 7.6 on wireless LANs outside the limited areas, becomes fairly straightforward in light of augmentation by a layer 2 encryption/access control product (as recommended by Lockheed Martin Information Systems [15]) and Packwood's recent work [21] on local approvals for RF at Sandia. Recommendation 7.7 on Type 1 wireless LANs will need more study on policy issues, but has technology available on the shelf. The recommendations in sections 7.8 through 7.10 provide more foundation material for later recommendations (7.11-7.12). Bringing 802.11 into the limited areas (section 7.12) not only builds on the earlier recommendations and will need much more study of, and possible changes to, policies, but will build on the knowledge and experience gained in implementing 802.11 wireless LANs outside the limited areas (section 7.6). Finally, once the DFIR equipment of recommendation 7.1 has been replaces by 802.11 equipment inside the limited areas (section 7.12), the DFIR gear can be reused in specialized applications, as per recommendation 7.13.

7.1 Implement Diffused Infrared Infrastructure Mode LANs Inside the Limited Areas

Evaluate equipment from vendors such as Spectrix and install a diffused IR access point in most conference rooms inside the limited area. Connect these DFIR access points into the existing wired LAN (SRN) in that building. This effectively creates a wireless module that can be deployed in a safe, secure environment. It is a building block that can be replicated time and again throughout the SRN. Implementation should start with the conference rooms in one building and expand to serve other buildings. This would provide portable access to the corporate network in conference rooms for email processing and resource sharing, without the necessity of connecting a cable from a client laptop into the wired network. In addition, this could possibly be used in offices to increase portability and reduce the number of wired communication drops to the office.

General risks, such as unbounded propagation of the electromagnetic waves is mitigated by the using IR portion of the spectrum. IR signals do not pass through walls, floors, and ceilings. Conference room doors should be closed to contain the IR within the room. IR signals can pass through windows, but are attenuated when doing so. In spite of this attenuation, and because of the fact that excessive light in the room can hamper the effectiveness of DFIR networking equipment, shades or blinds over the windows should be drawn when the DFIR networking equipment is in use.

7.2 Create a Map of the Classified Computing and Communications Resources at Sandia

Using a GPS receiver to determine location, we should undertake a project at the Sandia facilities in Albuquerque, to record the location of all classified computing and communication resources. This can consist of a tabular form data file with the name and description of the resource and the GPS coordinates of its location. This information should be rendered onto a map of the Sandia Albuquerque facilities.

This data file and any reports and maps produced from it may be classified, but knowing this data would aid in developing a plan of where RF-based wireless networking could be employed. Having this information available would also aid in space management. Currently, office and laboratory space is managed on a “Quality of Space” basis and when the space will next need refurbishment. This information, and that developed under recommendation 7.4, could enable space management that also considers “Quality of Security” and the availability of communications. This may provide revelations about the ease or difficulty of the consolidation recommended in section 7.10.

7.3 Implement Strict Configuration Control over the Location of Classified Computing and Communications Resources at Sandia

A configuration control plan should be devised and implemented to ensure Sandia has a corporate knowledge of all details of the computing and communications resources for classified work. This should include information about the type of equipment, how it is powered, what communication media it employs, and other details needed to analyze

whether RF-based wireless networking could be employed in the vicinity of the various classified computing and communications resources. To keep this data current and useful, it should be updated whenever classified computing or communication resources are relocated, augmented, or retired.

7.4 Perform an RF Mapping of the Sandia, NM Facilities

Perform a radio frequency mapping of the Sandia, New Mexico, facility to determine how to obtain the maximum radio coverage with the fewest antennas and lowest transmit power. This should also identify "dead spots", where there is no RF coverage.

7.5 Implement a System to Allow the Use of Two-Way Pagers, both Inside and Outside the Limited Areas

Evaluate two-way paging equipment – such as the version of the RIM BlackBerry customized for DoD/NSA [3] – and various supporting equipment (i.e. gateways, antennas, etc.) to determine suitability for use at Sandia. This should include an examination of the pertinent DoD/NSA policies regarding the customized BlackBerry, and recommendations for changes in DOE polices concerning the selected device. Once approved, procure support equipment and a limited number of devices, and initiate a pilot installation of two-way pagers.

Capabilities of the devices (in light of any DoD/NSA customizations) and DoD/NSA/DOE/NNSA policies will have to be evaluated to determine the risks involved and what mitigative actions may be necessary. The RIM BlackBerry seems to use a server or gateway that sits behind a firewall on a corporate intranet, but we would need to learn much more detail about the specific architecture in order to properly evaluate the system.

7.6 Implement 802.11a Wireless Infrastructure Mode LANs Outside the Limited Areas

To provide portable, convenient, and untethered access to the Sandia corporate data network outside of the limited areas, 802.11a RF networks in the 5 GHz U-NII band should be established. 802.11a equipment should be used to provide higher data rates (up to 54 Mbps) and operation in the less-crowded 5 GHz portion of the spectrum. Operation in the 5 GHz band by the 802.11a equipment avoids potential future spectrum conflicts with equipment that operates in the 2.4 GHz ISM band (e.g. Bluetooth, cordless telephones) using different modulation techniques.

To remedy the security problems inherent in 802.11 networks, a layer 2 encryption and access control product, such as AirFortress by Fortress Technologies (using AES or Triple DES), should be used with the wireless LAN equipment. Other information provided by mapping and configuration tools regarding the location of, and distance to, classified computing and communications resources will need to be obtained (see sections 7.2 and 7.3) to proper analyze the remaining associated risks.

By combining the 802.11a networking equipment with a layer 2 encryption/access control product, this too effectively creates another wireless module that can be repeatedly deployed. It is another building block that can be replicated time after time outside the limited areas, allowing connections to the SON. Note that constraints relating to the proper separation or distance from classified operations must be observed.

7.7 Allow the Use of Approved Type 1 Wireless Devices in the Secure Network

Examine wireless LAN equipment employing Type 1 encryption algorithms (such as the SecNet 11 equipment by Harris Corporation) and the relevant DOE/NNSA policies to determine what steps must be performed or which policies must be changed, and in what manner, to allow the use of Type 1 encrypted wireless LAN equipment in the SCN. Equipment of this nature can easily and cost-effectively extend secure networking services, reduce the amount of copper cable in the SCN, and provide untethered portability of classified computing equipment. To keep configuration and location data bases (sections 7.2, 7.3) current, a range of operation (e.g. building or building/room combination) will need to be associated with each portable, classified device (e.g. computer).

7.8 Replace Copper Data Cables by Fiber Optic Cables and Wireless LANs in the SCN

Replacement of copper cables within the SCN by fiber optic cables eliminates certain data coupling effects [7], since optical fibers neither emanate signals nor serve as antennas to receive signals. Fiber optic cables also provide greater bandwidth, and therefore allow faster data rates than copper wires. In areas that do not require the fastest data rates, but can benefit from ease of portability of computing equipment, wireless extensions to the SCN (section 7.7) can augment fiber optic cables, replacing copper wiring for data communication.

7.9 Perform a Study to Remedy Coupling Issues

As technology evolves, many things change. Some years ago at Sandia, the required separation between a telephone and a classified computing or communication resource was 6 feet. Over the years, this has decreased by an order of magnitude to about six inches to one foot. It is time to revisit required separations due to RF, data, and power coupling in light of the newer technologies (e.g. LCD monitors and isolation transformers) available in the marketplace. Analyze the remaining problems and devise solutions to the various coupling issues. This will allow network designers to find what the minimum separations should really be between classified computing and communication equipment and unclassified wireless communication equipment.

7.10 Cluster Classified Computing Resources into Bounded Enclaves

Cluster classified computing resources into bounded enclaves and protect these enclaves (i.e. electromagnetically shield the enclave, prohibit the presence of RF devices not equipped with Type 1 encryption, etc.). Where remote access to these enclaves is absolutely needed, use fiber optic communication cables and low emission LCD terminals (along with shielded cases for the electronics) to minimize coupling (section 7.9).

This topic will need much more study. It will require information generated by recommendations 7.2 and 7.4. It will need the configuration controls of section 7.3. A consensus would have to be developed with facilities (concerning space management) and the users of the classified computing resources.

7.11 Perform a Study of How to Implement Wireless Voice Communications within the Limited Areas

A key consideration when thinking about wireless voice communications within the limited areas is ensuring the RF transmitting devices do not pick up and transmit classified voice conversations or emanations. One idea to study would be the feasibility of creating "cones of silence" where no classified or sensitive discussions or emanations are permitted. This way, cell phones could be used within these cones of silence, for even if a cell phone with an open microphone was transmitting, little or no useful information would leak. Another item to study would be the feasibility of installing a Sandia owned and operated cellular telephone system. Although this would have the advantage of Sandia control over the cellular infrastructure (and possibility the ability to reprogram the phones to a known set of attributes and functions upon entering the Sandia premises), there is a risk of obsolescence. It may be expensive to purchase the spectrum license and keep the equipment up-to-date. (One aspect to explore would be, just how current would the system have to remain?) Other options to examine include: Voice over IP (VoIP), using the ever-shrinking data devices (PDAs, Pocket PCs) to communicate voice over a wireless data network; cordless telephones (operating in the 2.4 GHz ISM band) reporting to numerous base stations (where each base station could handle many handsets); and commercial cellular handsets that have been modified to not accept SIM downloads or be able to have their microphone opened remotely.

7.12 Implement 802.11a Infrastructure Mode Networks Inside the Limited Areas

Once the locations of classified computing and communication resources are identified and controlled (sections 7.2 and 7.3), copper wiring is removed from the classified network portion of the cable plant (section 7.8), coupling issues have been remedied (section 7.9), classified computing resources have been separated into enclaves (section 7.10), and experience has been gained with 802.11 products (section 7.6), implementation of 802.11a networks (along with a layer 2 encryption product such as AirFortress) inside limited areas is recommended. This will require study of, and possibly changes to DOE/NNSA policies, but much of the groundwork should have been performed through

the earlier recommendations in this list. Again, 802.11a equipment is recommended, for the same reasons as in section 7.6.

7.13 Implement Diffused Infrared LANs on the SCN

In locations where classified information must be processed, but Type 1 encrypted wireless devices (like the Harris SecNet 11 PCMCIA cards) cannot be used, implement diffused IR LANs if the areas can be bounded (e.g. conference room, a bullpen office where everyone is working on the same project). This will need to be accompanied by policies requiring closed doors without windows (or having shades, blinds, or other suitable covering over the windows in the doors) and shades or blinds to cover the room's windows while the DFIR networking devices are in use. This will further bound the room, limiting the propagation of the IR signals.

8 Bibliography

1. William A. Arbaugh, Narendar Shankar, and Y.C. Justin Wan, Your 802.11 Wireless Network has No Clothes, in *Proceedings of the First International Conference on Wireless LANs and Home Networks*, held in Singapore, December 5-7, 2001, World Scientific, 2001.

2. Benny Bing, *High-Speed Wireless ATM and LANs*, Artech House, Boston, 2000.

3. "BlackBerry Meets Department of Defense's Advanced Wireless Security Standard," press release, http://www.rim.com/news/press/pr-19_08_2002.shtml, August 19, 2002.

4. John Blyler, Understanding Optics In a Wireless World, in *Wireless System Design*, pp. 65-69, April 2001.

5. Nikita Borisov, Ian Goldberg, and David Wagner, Intercepting Mobile Communications: The Insecurity of 802.11, in *Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking*, held in Rome, Italy, July 16-21, 2001, ACM, 2001.

6. Walter R. Bruce III, *Wireless LANs End to End*, Hungry Minds, New York, 2002.

7. James Arlin Cooper, *Computer and Communications Security*, Mcgraw-Hill, New York, 1989.

8. James Arlin Cooper, *Computer-Security Technology*, Lexington Books (D. C. Heath and Co.), Lexington, MA, 1984.

9. Andy Dornan, Why Wi-Fi Will Die, in *Network Magazine*, http://www.networkmagazine.com/article/NMG20020701S0017, July 7, 2002.

10. Amitava Dutta-Roy, Fixed Wireless Routes for Internet Access, in *IEEE Spectrum*, vol. 36, pp.61-69, September 1999.

11. Scott Fluhrer, Itsik Mantin, and Adi Shamir, Weaknesses in the Key Scheduling Algorithm of RC4, in *Eight Annual Workshop on Scelected Areas in Cryptography*, held in Toronto, Canada, August 16-17, 2001, Springer-Verlag (part of the Lecture Notes in Computer Science series), 2001.

12. GSM Association, http://www.gsmworld.com/technology/gsm.shtml, 2002.

13. Vipul Gupta and Sumit Gupta, Securing the Wireless Internet, in *IEEE Communications*, vol. 39, pp. 68-74, December 2001.

14. Harris Corporation, http://www.govcomm.harris.com/secure-comm/secnet11.pdf, 2002.

15. Keith Hollister, Network Security for Internal Wireless LAN Deployments, white paper, Lockheed Martin Information Systems.

16. Joseph Y. Hui, Wireless Optical Ad-Hoc Networks for Embedded Systems, in *Conference Proceedings of the 2001 IEEE International Performance, Computing, and Communications Conference*, held in Phoenix, AZ, April 4-6, 2001, IEEE, 2001.

17. Kenneth Li, Microsoft Aims at Corporate Wireless Users, on *TheStreet.com*, http://www.TheStreet.com/tech/kennethli/10035034.html, July 31, 2002.

18. Kenneth Li, Nokia Reduces Its Second-Half Forecast, on *TheStreet.com*, http://www.TheStreet.com/tech/kennethli/10028187.html, June 20, 2002.

19. Arunesh Mishra and William Arbaugh, *An Initial Security Analysis of the IEEE 802.1X Standard*, Technical Report CS-TR-4328, UMIACS-TR-2002-10, University of Maryland, College Park, Maryland, February 6, 2002.

20. Randall K. Nichols and Panos C. Lekkas, *Wireless Security*, McGraw-Hill, New York, 2002.

21. Del Packwood, of SNL Computer Security Department, personal conversation, August 26, 2002.

22. Kaveh Pahlavan, Ali Zahedi, and Prashant Krishnamurthy, Wideband Local Access: Wireless LAN and Wireless ATM, in *IEEE Communications Magazine*, vol. 35, pp. 34-40, November 1997.

23. Ray H. Pettit, *ECM and ECCM Techniques for Digital Communication Systems*, Lifetime Learning Publications, London, 1982.

24. Port-Based Network Access Control, IEEE 802.1x-2001, Institute of Electrical and Electronics Engineers, Piscataway, NJ, 2001.

25. Cornell W. Robinson III and Dave Molta, Elite Solution Secures WLANs, in *Network Computing*, pp. 48—65, June 10, 2002.

26. Tamir Shaanan, IrGate Takes on Bluetooth and IrDA, in *Wireless System Design*, pp. 43-45, February 2002.

27. Spectrix Corporation, http://www.spectrixcorp.com/products.html, 2000.

28. Adam Stubblefield, John Ioannidis, and Aviel D. Rubin, *Using the Fluhrer, Mantin, and Shamir Attack to Break WEP*, AT&T Labs Technical Report TD-4ZCPZZ, AT&T, Florham Park, NJ, August 2001.

29. Winston Steward and Bill Mann, *Wireless Devices End to End*, Hungry Minds, New York, 2002.

30. Jeff Taylor, of SNL Computer Security Department, personal conversations, August 26-30, 2002.

31. Don J. Torrieri, *Principles of Military Communication Systems*, Artech House, Boston, 1982.

32. Upkar Varshney and Ron Vetter, Emerging Mobile and Wireless Networks, in *Communications of the ACM*, vol. 43, pp. 73-81, June 2000.

33. Brian Van Leeuwen, Juan Espinoza, Jr., and Peter Sholander, *Effective Protocols foe Mobile Communications and Networking*, SAND98-2753, Sandia National Laboratories, Albuquerque, NM, December 1998.

34. Heinz A. Willebrand and Baksheesh S. Ghuman, Fiber Optics Without Fiber, in *IEEE Spectrum*, vol. 38, pp. 40-45, August 2001.

35. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE 802.11-1999, Institute of Electrical and Electronics Engineers, Piscataway, NJ, 1999.

36. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-speed Physical Layer in the 5 GHz Band, IEEE 802.11a-1999, Institute of Electrical and Electronics Engineers, Piscataway, NJ, 1999.

37. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band, IEEE 802.11b-1999, Institute of Electrical and Electronics Engineers, Piscataway, NJ, 1999.

38. Wireless Network Security (Draft), Special Publication 800-48, National Institute of Standards and Technology, Gaithersburg, MD.

39. Anthony D. Wood and John A. Stankovic, Denial of Service in Sensor Networks, in *IEEE Computer*, vol. 35, pp. 54-62, October 2002.

Appendix A Acronyms and Abbreviations

1G First Generation wireless technology

2G Second Generation wireless technology

2.5G Intermediate step between second and third generation wireless technologies

3G Third generation wireless technology

AES Advanced Encryption Standard

AMPS Advanced Mobile Phone System

CCK Complementary Code Keying

CDMA Code Division Multiple Access

CDPD Cellular Digital Packet Data

COFDM Coded Orthogonal Frequency Division Multiplexing

CRT Cathode Ray Tube

DBIR Direct-beam infrared

DES Data Encryption Standard

DFIR Diffused infrared

DoD (U.S.) Department of Defense

DOE (U.S.) Department of Energy

DSSS Direct Sequence Spread Spectrum

DWDM Dense wavelength-division multiplexing

EDGE Enhanced Data rates for GSM and TDMA/136 Evolution, or Enhanced Data rates for Global Evolution, or Enhanced Data rates for GSM Evolution

ETACS Extended Total Access Communication System

ETSI European Telecommunications Standards Institute

FCC (U.S.) Federal Communications Commission

FDMA Frequency Division Multiple Access

FHSS Frequency Hopping Spread Spectrum

FM Frequency Modulation

GPRS General Packet Radio Services

GSM Global System for Mobile Communication

HiperLAN High Performance LAN

HR/DSSS High Rate Direct Sequence Spread Spectrum

HSCSD High Speed Circuit Switched Data

IEEE Institute of Electrical and Electronics Engineers

IPSec Internet Protocol security

IR Infrared

IrDA Infrared Data Association

ISM Industrial, Scientific, and Medical

LAN Local Area Network

LCD Liquid Crystal Display

MAC Medium Access Control

NMT Nordic Mobile Telephony

NNSA National Nuclear Security Administration

NSA National Security Agency

OFDM Orthogonal Frequency Division Multiplexing

PBCC Packet Binary Convolutional Coding

PCMCIA Personal Computer Memory Card International Association

PCS Personal Communications Services

PDA Personal Digital Assistant

PHY Physical Layer

PSTN Public Switched Telephone Network

RF Radio Frequency

RIM Research in Motion

SIM Subscriber Identity Module

SMS Short Message Service

TACS Total Access Communication System

TDMA Time Division Multiple Access

U-NII Unlicensed National Information Infrastructure

VoIP Voice over IP

VPN Virtual Private Network

WCDMA Wideband CDMA

WEP Wired Equivalent Privacy

DISTRIBUTION:

1	MS 0103	J.P. VanDevender, 12100	1	MS 0806	J.H. Naegle, 9336
1	MS 0139	C.S. Leishman, 9904	1	MS 0806	R.R. Olsberg, 9336
1	MS 0630	D.H. Schroeder, 9411	5	MS 0806	L.G. Pierson, 9336
1	MS 0630	M.J. Murphy, 9600	1	MS 0806	T.J. Pratt, 9336
1	MS 0662	T. Klitsner, 9623	1	MS 0806	J.A. Schutt, 9336
1	MS 0662	M.E. Adams, 9624	1	MS 0806	J.D. Tang, 9336
1	MS 0662	C.A. Quintana, 9624	1	MS 0806	T.D. Tarman, 9336
1	MS 0662	M.D. Snitchler, 9624	1	MS 0806	L.F. Tolendino, 9336
1	MS 0775	M.H. Pendley, 5852	1	MS 0806	D.J. Wiener, 9336
1	MS 0775	M.J. Eaton, 5852	10	MS 0806	E.L. Witzke, 9336
1	MS 0784	R.E. Trellue, 6501	1	MS 0812	M.J. Benson, 9334
1	MS 0784	M.J. Skroch, 6512	1	MS 0812	L.D. Byers, 9334
1	MS 0785	M.D. Torgerson, 6514	1	MS 0812	J.H.Maestas, 9334
1	MS 0785	R.L. Hutchinson, 6516	1	MS 0812	P.L. Manke, 9334
1	MS 0785	B.P. Van Leeuwen, 6516	1	MS 0812	B.L.Weaver, 9334
1	MS 0785	W.F. Young, 6516	1	MS 0812	B.C. Whittet, 9334
1	MS 0801	A.L. Hale, 9300	1	MS 0813	R.M. Cahoon, 9327
1	MS 0801	W.F. Mason, 9320	1	MS 0813	D.N. Packwood, 9327
1	MS 0801	M.R. Sjulin, 9330	1	MS 0813	R.A. Suppona, 9327
1	MS 0806	M.J. Ernest, 9323	1	MS 0813	J.L. Taylor, 9327
1	MS 0806	P.C.R. Jones, 9332	1	MS 0822	P.D. Heermann, 9227
1	MS 0806	J.P. Abbott, 9332	1	MS 0822	C.F. Diegert, 9227
1	MS 0806	C.D. Brown, 9332	1	MS 0826	J.D. Zepper, 9143
1	MS 0806	J.P. Long, 9332	1	MS 0839	R.L. Craft, 16000
5	MS 0806	L. Stans, 9336	1	MS 0864	P.E. Linke, 3112
1	MS 0806	J.P. Brenkosh, 9336	1	MS 0874	P.J. Robertson, 1751
1	MS 0806	J.M. Eldridge, 9336	1	MS 0874	K.L. Gass, 1751
5	MS 0806	S.A. Gossage, 9336	1	MS 1361	D.F. Beck, 5323
1	MS 0806	T.C. Hu, 9336	1	MS 1125	J.J. Harrington, 15252
1	MS 0806	B.R. Kellogg, 9336	1	MS 9011	H.Y. Chen, 8915
1	MS 0806	L.G. Martinez, 9336	1	MS 9012	S.C. Gray, 8930
1	MS 0806	M.M. Miller, 9336	1	MS 9012	R.D. Gay, 8930

1	MS 9018	Central Technical Files, 8945-1
2	MS 0899	Technical Library, 9616
1	MS 0612	Review & Approval Desk, 9612 For DOE/OSTI