Seamless access to multiple wireless data networks

A Wireless Data Network Infrastructure at Carnegie Mellon University

ALEX HILLS AND DAVID B. JOHNSON

In order to support mobile computing research, including the development of software which will allow seamless access to multiple wireless data networks, a wireless data network infrastructure is being built at Carnegie Mellon University. This infrastructure will allow researchers and other members of the campus community to use mobile computers to gain access to data networks while they are on-campus, or off-campus in the greater Pittsburgh area. The infrastructure will initially include two different types of wireless networks, a low-bandwidth wide area system and a high-bandwidth local area system, each of which will provide access to the campus computer network. Since the campus network is called "Andrew" (after Andrew Carnegie and Andrew Mellon), the new wireless infrastructure has been dubbed "Wireless Andrew."

This article describes the Wireless Andrew infrastructure being built. First, an overview of the infrastructure and the characteristics of the two types of wireless networks used are presented. Next, each of these networks is described in more detail. The technology used, its implementation in the wireless network infrastructure, and current deployment experience are discussed. Finally, the lessons learned and present conclusions are summarized.

An Overview of the Infrastructure

Our approach to wireless data networks is based on the notion that it is unlikely that a single wireless network will be able to meet all mobile computing needs that will evolve. It is far more probable that many wireless networks will be available, each of which will provide service over a variety of geographical coverage areas at various speeds and at a variety of price levels. Each network will serve a niche, but none will meet all needs. Accordingly, mobile computer users will need to be able to access multiple networks in order to meet their needs.

A mobile computer, in order to take advantage of the highest-speed or most capable network available, will need to be able to work with any of two, three, or even more wireless networks. Furthermore, a mobile user would, in general, like to be connected to the wireless network best able to meet the application's needs at the lowest usage cost. When moving beyond the range of one wireless network, a user would generally like to be connected to another automatically.

As part of the Wireless Andrew infrastructure at Carnegie Mellon, we are building a high-speed wireless data network on campus, using AT&T WaveLAN wireless local area network (LAN) technology to provide high-speed (2 Mb/s) service over a large portion of the campus. In addition, outside the wireless LAN service area, we are using the lower-speed (19.2 kb/s) Cellular Digital Packet Data (CDPD) service [1]. With both the CDPD and wireless LAN networks operational, properly equipped mobile computers will be able to use both networks. Table 1 summarizes some of the important characteristics of these two networks.

We are currently using laptop computers equipped with Personal Computer Memory Card Industry Association (PCMCIA) wireless LAN interfaces and on-board CDPD modems, and we expect to continue their use in the near term. We are developing software for use on this infrastructure, with which mobile computer users will be able to seamlessly move between the wireless LAN and CDPD networks [2]. The infrastructure is intended to be used both by researchers developing the software, and by the faculty, staff, and students of the Carnegie Mellon community.

Low-Bandwidth Wide Area Component

In order to support mobile connections to our campus network from throughout the greater Pittsburgh area, we have elected to use the CDPD service [1] offered by Bell Atlantic NYNEX Mobile. Like other wide area wireless services, it operates at a low data bit rate. Since CDPD supports the Internet Protocol (IP) [3], CDPD service can easily be integrated into an existing IP network.

Details of Technology Used

CDPD is a relatively new service for wide-area data communication with wireless mobile hosts. The original version of the CDPD System Specification (Release 1.0) [1] was developed by IBM and released in July 1993 by a consortium of the major U.S. cellular telephone carriers, consisting of Ameritech Mobile Communications, Bell Atlantic Mobile Systems, Contel Cellular, GTE Mobile Communications, McCaw Cellular Communications, NYNEX Mobile Communications, PacTel Cellular, and Southwestern Bell Mobile Systems. The CDPD

1070-9916/96/$05.00 © 1996 IEEE

standard is now controlled by an open trade organization known as the CDPD Forum, which released a revision of the CDPD standard (Release 1.1) in January 1995.

CDPD uses the existing infrastructure of the analog Advanced Mobile Phone Service (AMPS) cellular telephone network to transmit data, utilizing idle channels in the cellular system to provide a connectionless digital data packet service. When a channel is not being used for voice service, it can be used to send and receive packets from a CDPD-equipped mobile station. Existing cellular channels can thus be shared between voice and data service, although CDPD uses only time *between* voice calls, not silence periods *within* any voice call, for sending data; voice service always has priority over CDPD service for access to a channel. A CDPD cellular carrier may also remove some channels from voice service and dedicate them exclusively to CDPD service, although this is not the normal configuration. CDPD can be used whenever one is within range of a CDPD-equipped cell site. The coverage area of each cell site is typically in a range from one to ten miles in radius, depending on the configuration installed by the cellular carrier. An array of cell sites normally covers all of a metropolitan (or larger) area.

CDPD operates at layers 1 and 2 of the Open Systems Interconnection (OSI) model (physical and data link) and provides service to either of two layer 3 (network) protocols: IP [3] or the International Standards Organization (ISO) Connectionless Network Protocol (CLNP). The service operates at a raw data bit rate of 19.2 kb/s, although actual throughput is well below that figure. The deterministic protocol overhead bits required for additional levels of headers (beyond IP) and for forward error correction (FEC) coding and other functions reduces the available bandwidth to a maximum of 13 kb/s from the mobile user to the base station and 12 kb/s from the base station to the mobile user [4]. This bandwidth is further reduced by contention in gaining access to the channel. In our own measurements in Pittsburgh, the usable throughput of CDPD is between 9 and 11 kb/s.

The current CDPD standard includes two types of compression that may improve the usable transmission throughput. The original CDPD standard (Release 1.0) provided for use of "header compression" for packets carrying transport- and network-level protocols that support header compression. For example, Transmission Control Protocol (TCP) header compression [4] removes the fields from the combined TCP [5] and IP [3] headers that do not change between sequential packets on the same TCP connection; the 40 bytes of combined TCP and IP headers can typically be reduced to 3 bytes. The headers for other IP transport protocols, such as User Datagram Protocol (UDP) [6], are not compressed, and TCP header compression is not supported by all CDPD implementations. In particular, the Bell Atlantic NYNEX Mobile system in Pittsburgh which we are using does not yet support TCP header compression. In addition to header compression, Release 1.1 of the CDPD standard added support for V.42bis data compression, used on recent circuit-switched telephone modems. V.42bis can compress some data by as much as a factor of 3 or 4, but few CDPD systems or modems, including the Bell Atlantic NYNEX Mobile system in Pittsburgh, have been upgraded yet to support Release 1.1 of the standard.

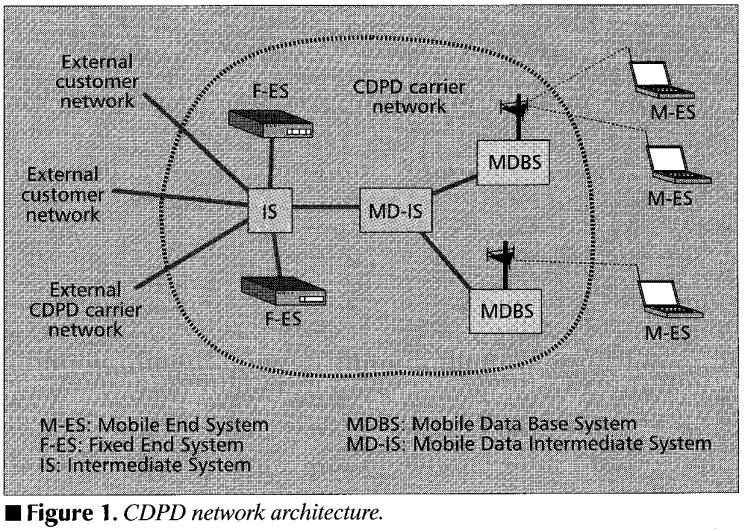
A CDPD network serves a mobile computer (Mobile End System — M-ES) through a radio link to a nearby cell site equipped with a Mobile Data Base Station (MDBS), as shown in Fig. 1. The MDBS, in turn, communicates with a Mobile Data Intermediate System (MD-IS), which routes packets to and from the MDBSs and is typically located at the cellular carrier's mobile telephone switching office (MTSO). Each MD-IS serves a number of MDBSs, and there may be one or more MD-ISs in a CDPD network. Also part of the CDPD network may be a number of "off-the-shelf" routers (Intermediate Systems — ISs), which connect to conventional IP or CLNP networks on which are located stationary host computers or servers (Fixed End Systems — F-ESs). A "CDPD modem" is typically used to provide the CDPD functions of an M-ES; when a customer initially establishes CDPD service with a cellular carrier, the carrier assigns an IP (or CLNP) address to the M-ES (to the CDPD modem), which is used for routing packets to the M-ES.

	CDPD	WaveLAN
Base station coverage radius	1–10 miles	100–800 ft
Raw transmission data bandwidth	19.2 kb/s	2 Mb/s
Typical user data throughput	9–11 kb/s	0.5–1.5 Mb/s
Typical round-trip latency between mobile and stationary computer	450–600 ms	5–30 ms

■ **Table 1.** *Carnegie Mellon "Wireless Andrew" infrastructure network characteristics.*

Costs experienced by CDPD users are based on the number of packets and the number of kilobytes of data transported between the M-ES and MDBS. This differs significantly from the pricing model used by cellular carriers for conventional circuit-switched voice service, where prices are based on a charge per minute of connect time. There are no connect time charges on CDPD, as there is no connection. To use CDPD, the CDPD modem does not dial a telephone number and connect to a remote system. Instead, individual data packets (either IP or CLNP) are sent over the air to the MDBS using the CDPD "air interface" protocol, for forwarding through the MD-IS to other M-ESs registered with CDPD, or to any F-ESs or ISs on any wired network connected to the CDPD system.

In each cell, the MDBS is responsible for channel usage. The MDBS selects the channel to be used for CDPD within



■ **Figure 1.** *CDPD network architecture.*

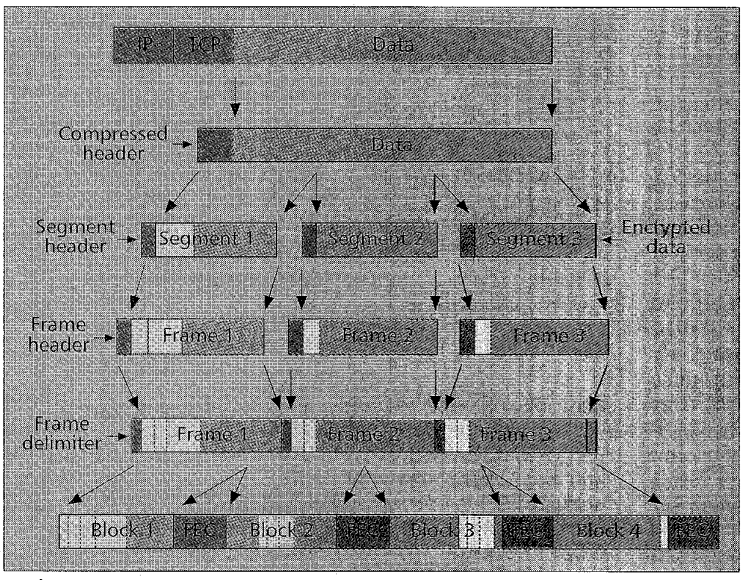


Figure 2. *CDPD packet transmission processing.*

the cell, and "hops" from one channel to another if the channel it is using is taken by the cell for voice service. The M-ESs in the cell will follow the MDBS to the new channel, either by receiving an explicit channel hop command from the MDBS or by scanning all cellular channels to find the one being used by CDPD. When an M-ES initially begins use of CDPD (such as at boot time), it must also scan all cellular channels to find the one being used by CDPD.

In sending a packet over the air in a CDPD system, a number of processing steps are performed; Fig. 2 shows a simplified view of these steps. First, the header of the packet may be compressed, such as with TCP header compression [4] as described above. The packet is then divided into *segments*, and a segment header is added to each; the segment header includes an identifier indicating the type of header compression applied to the packet (present in all segments, but only meaningful in the first segment of a packet) and a protocol number to indicate which type of network protocol (IP or CLNP) is contained in the segment. The data of each segment is also encrypted using the RC4 encryption algorithm [7]. Next, each segment is encapsulated with the addition of a data link header to form a *frame*; the frame header includes sequence numbers to maintain the order of frames in transit, and an identifier for multiplexing separate data link connections (such as to separate data packets from CDPD administrative packets). The resulting frames are then concatenated together, with flag bits added to delimit the individual frames, and the resulting bit sequence is divided into a series of fixed-sized *blocks*; each block also has Reed-Solomon FEC codes added, allowing errors in transmission to be corrected by the receiver. The resulting stream of blocks is then sent digitally over the 30-kHz AMPS channel being used by CDPD.

The *forward link channel* (from MDBS to M-ES) is a broadcast channel with no contention. The MDBS simply transmits blocks on this channel for any of the M-ESs registered in the cell. Interspersed in this data stream are "channel idle" and "decode status" flag bits, used to approximate the *carrier sense* and *collision detection* functions of carrier sense multiple access with collision detection (CSMA/CD) in IEEE 802.3 (Ethernet) networks, using a protocol called digital sense multiple access with collision detect (DSMA/CD). An M-ES wishing to transmit a block on the *reverse link channel* (from M-ES to MDBS) listens to the forward link channel until a flag bit from the MDBS indicates that the reverse link channel is idle. It then transmits its block on the reverse link channel and checks the following decode status flag bit on the forward link channel. If the flag bit indicates that the block was not successfully received by the MDBS, a collision or other wireless transmission error has occurred, and the block is retransmitted later by the M-ES. After transmitting one block, an M-ES may continue to transmit consecutive blocks (up to a maximum number of blocks) without needing to reacquire the channel, as long as the decode status flag bit indicates that the previous block was successfully received by the MDBS.

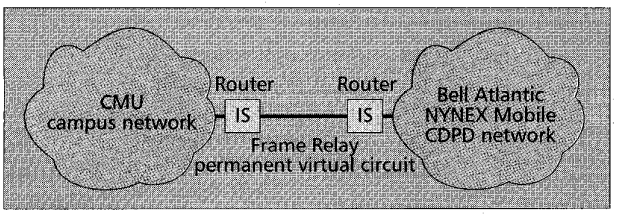
Implementation Details

To use CDPD, the service must be ordered from a cellular carrier, and CDPD modem equipment for the M-ESs must be purchased; furthermore, to allow communication between M-ESs and F-ESs on an existing data network, a wired connection from the CDPD system to the existing network must be installed. We initially selected the Pacific Communications Sciences Inc. (PCSI) Ubiquity 1000 modem when we began using CDPD in October 1994 because it was the only CDPD modem available at that time capable of on-board installation in a portable computer. The Ubiquity 1000 is designed to be installed in the internal floppy disk drive bay, replacing the floppy drive, on IBM ThinkPad 750 series, 755C, or 755Cs laptop computers; it includes a small telescoping antenna that integrates with the ThinkPad. We are now also using the IBM Wireless Modem for Cellular/CDPD, which is designed to be installed in a PCMCIA Type II PC Card slot and includes a small external radio and antenna unit.

The CDPD network can provide communication between M-ESs without the use of wired data networks, since an MD-IS can route packets between the MDBSs serving two M-ESs. To provide connections to a fixed host computer or to a wired data network, however, it is necessary to connect a router associated with the CDPD network to the fixed host or to a router which is part of the wired network. Since CDPD can carry IP packets, it is natural to imagine a CDPD network connected directly to the Internet. However, this is not yet generally possible for many CDPD carriers due to the restrictions placed on the regional Bell operating companies as a result of the 1982 AT&T divestiture. This limitation is expected to change at some point in the future, and CDPD customers are currently able to connect their own wired networks into the CDPD system through their CDPD cellular carrier.

Since we wanted to provide our mobile computers with access to all of Carnegie Mellon's campus network, we needed to install a wired connection to Bell Atlantic NYNEX Mobile's CDPD network. We purchased a Cisco router specifically for this purpose and linked it to a Wellfleet router already installed at Bell Atlantic NYNEX Mobile, as illustrated in Fig. 3. The connection between the routers is accomplished using a 56 kb/s Frame Relay permanent virtual circuit. Although the 56 kb/s service is adequate for our immediate needs, we plan to upgrade it to a T1 (1.544 Mb/s) link as our CDPD usage increases.

On the mobile computers, we are currently running primarily Microsoft Windows, and are using FTP Software's PC/TCP implementation of the TCP/IP networking protocols. PC/TCP provides a number of Internet applications, including telnet, FTP, and electronic mail, and is compatible with the



■ **Figure 3.** *Interconnecting CDPD and the campus network.*

Windows Sockets (WinSock) application programming interface (API) [8]. We are also running the NetBSD version of UNIX on the mobile computers using CDPD in some research projects.

The Ubiquity 1000 modem provides a serial port interface to the IBM ThinkPad through the floppy disk drive connector inside the ThinkPad's case. The modem implements the serial line IP (SLIP) protocol [9] on this serial port for communicating IP packets to and from the ThinkPad, and we are using the built-in SLIP implementation in PC/TCP and NetBSD. The IBM Wireless Modem for Cellular/CDPD includes an NDIS [10] device driver for Microsoft Windows, allowing PC/TCP to interface to the modem on the PCMCIA PC Card (we are not yet using the IBM modem under NetBSD). With both modems, though, the protocol used to interface to the CDPD modem is separate from the protocol used over the CDPD network, which is defined by the CDPD standard.

Deployment and Experience to Date

With the establishment of the CDPD-to-campus Frame Relay link in October 1994, wireless access to our campus network became possible from anywhere in the greater Pittsburgh area. When cellular carriers put roaming arrangements in place for CDPD, the coverage area will, of course, be much larger. The new service has so far been used primarily for e-mail, and it is quite adequate in that application. Subjectively, the response time and speed are close to what one would experience using a 9.6 kb/s dial-up telephone connection through a modem, although the high latency (about 500 ms) is noticeable in interactive usage, such as when typing over a telnet connection.

Coverage and capacity planning are serious issues for cellular carriers, but since a CDPD user is buying service from a carrier, the user need only ascertain that the service provided by the carrier is adequate. Although the Pittsburgh area is composed of hilly terrain, the base stations (cell sites) in the Bell Atlantic NYNEX Mobile network have been located appropriately for this terrain. CDPD coverage is thus comparable to what one experiences in Pittsburgh or another city when using a cellular telephone. In Pittsburgh, the CDPD coverage extends over most of the Bell Atlantic NYNEX Mobile territory around the city and surrounding areas.

When signals are weak or voice service usage is heavy, a user may experience a significant delay as the M-ES seeks to access the CDPD channel. As CDPD becomes more popular, this could become a serious problem, although we have not yet found it to be so. There are occasional delays of at least several seconds, though, when the MDBS hops to a new channel and the M-ES must scan the channels to find the MDBS again. Such delays can be somewhat more common during times of the day when there is high demand for cellular voice service (such as in the afternoon as commuters drive home from work), but we have not yet found this to be a significant problem.

The CDPD standard itself is still quite new, and cellular carriers are still working to fully deploy and gain experience with it. Based on our own experience to date with CDPD, we believe it will be a valuable component of our wireless data network infrastructure, allowing us to extend the coverage of our wireless infrastructure to seamlessly provide support for mobile users in the greater Pittsburgh area.

High-Bandwidth Local Area Component

To complement this low-bandwidth CDPD service and to provide an infrastructure with much higher speed capability, we are building a high-speed wireless network on the Carnegie Mellon campus as part of Wireless Andrew. We are using AT&T WaveLAN wireless LAN equipment [11] to provide this high-speed service.

Details of the Technology Used

Wireless LANs were originally intended to allow LAN connections where premise wiring systems are inadequate to support conventional wired LANs. Now, because the equipment is available in PCMCIA PC Card form, wireless LANs have come to be identified with mobility. Wireless LANs can be used to provide service to mobile computers throughout a building or campus.

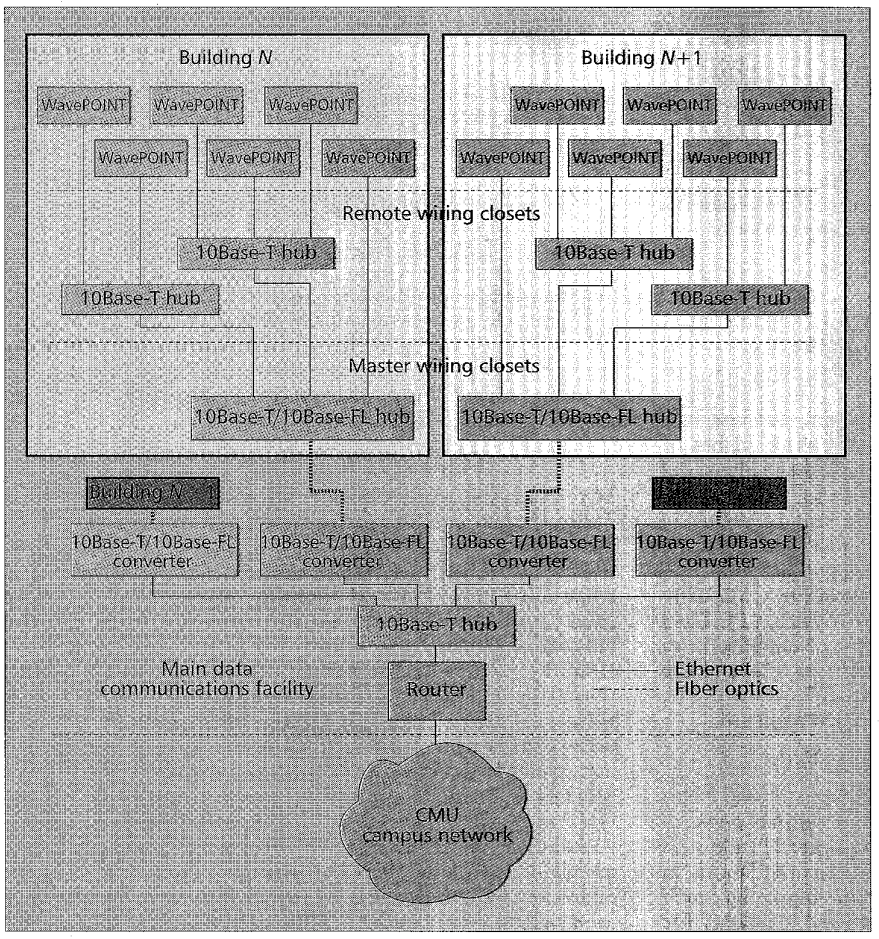
Many wireless LANs operate in the unlicensed industrial, scientific, and medical (ISM) bands at 915 MHz (902–928 MHz), 2.4 GHz (2.4–2.4835 GHz), and 5.7 GHz (5.725–5.85 GHz). Spread-spectrum techniques are used in these products, typically direct-sequence spread spectrum (DSSS) at 915 MHz or frequency-hopping spread spectrum (FHSS) at 2.4 GHz or 5.7 GHz. This use of spread spectrum is required for license-free operation in the ISM bands by the Federal Communications Commission (FCC) in the United States and its equivalents in other countries. Other wireless LAN products are available which operate in the licensed 18 GHz band and at infrared frequencies [12].

Wireless LANs operate at speeds up to a few megabits per second, with radio ranges typically from 50 ft to over 1000 ft, depending on the specific product and the environment in which it operates. Many of these products can be interfaced directly to IEEE 802.3 (Ethernet) or 802.5 (token ring) wired LANs. A new standard, IEEE 802.11, is being developed to allow interoperability between wireless LANs [13], but since the IEEE 802.11 standard has not yet been adopted, wireless LANs currently use proprietary protocols and generally do not interoperate with each other.

We selected AT&T's 915 MHz WaveLAN wireless LAN equipment for use in our network. WaveLAN equipment is also available for the 2.4 GHz ISM band, although this version has not yet been released as a product in the United States. Hardware compatible with AT&T WaveLAN is also sold by Solectek Corporation and Digital Equipment Corporation.

WaveLAN uses DSSS (in both the 915 MHz and 2.4 GHz products) to spread its transmissions over a wide bandwidth [14], allowing its transmissions to be robust against various kinds of interference and multipath effects. With DSSS, a "pseudo-random" spreading code is used, consisting of a sequence of bits (called "chips"), to modulate the transmitted data signal. At the receiver, the received signal is correlated using the known spreading code to recover the data. WaveLAN operates at a raw data bit rate of 2 Mb/s, which is spread using a spreading code of 11 chips/bit, for a transmission rate of 22 Mchips/s. All WaveLAN units use the same spreading code, which is fixed in the WaveLAN hardware.

Transmissions use the CSMA with collision avoidance (CA) medium access scheme [14], which is similar to the CSMA scheme used in IEEE 802.3 (Ethernet) LANs. With



■ **Figure 4.** *High-speed local area wireless infrastructure connections.*

wireless transmissions, the collision detect (CD) technique used in wired LANs cannot be done effectively, since a transmitter's signal strength at its own antenna will be so much stronger than the signal from any other transmitter. Instead, CSMA/CA adds a number of features to the basic CSMA scheme to greatly reduce the number of collisions that might occur if only CSMA (without CD) were used. With CSMA, a transmitter listens for "carrier" (the presence of another transmission) before attempting to transmit its own packet; if carrier is present, the transmitter defers until the end of the transmission in progress before again attempting transmission. CSMA/CA adds a further random "back-off" delay before this new transmission attempt, to avoid the likelihood of a collision as multiple deferring transmitters all attempt transmission at the same time once the transmission in progress completes.

Like other wireless LANs, the AT&T WaveLAN product line includes both "access points," which AT&T calls WavePOINT units, and host network adapters, which AT&T calls WaveLAN units. The WaveLAN host network adapter is available as a Type II PCMCIA PC Card with a small external radio and antenna unit. The WavePOINT access point is designed to be mounted in a fixed position and connected to a wired LAN, allowing WaveLAN-equipped mobile computers to communicate with the wired LAN. The access point operates as a transparent medium access control (MAC)-level bridge to forward packets to and from the wired LAN as needed [15].

Each WavePOINT is assigned a unique 16-bit network identification designator (NWID), used to distinguish packets transmitted by one access point from those transmitted by another. The WaveLAN transmission format consists essentially of a standard Ethernet frame with the NWID prepended to each frame. The receiver filters received packets in the WaveLAN host adapter based (in part) on the NWID of the access point it is using. This technique avoids the logical interference from packets transmitted in overlapping coverage areas of different WavePOINTs, although such transmissions can still physically interfere and do consume bandwidth in both coverage areas.

Like some other wireless LANs, the AT&T WaveLAN product allows "roaming," the ability for mobile computers to continue to receive service as they move from the coverage area of one access point to another. In order for this service to be provided, it is necessary that the wireless LAN system know in which access point coverage area each mobile computer is located. Thus, the tables of the bridges contained in each access point must be updated as mobile computers move from one access point coverage area to another.

The WaveLAN roaming functionality is called "WaveAROUND" and involves the addition of a beaconing and a sign-on protocol to the system [14]. Each WavePOINT periodically broadcasts a "beacon" packet, which mobile computers using WaveLAN monitor in order to detect when they have moved from the coverage area of one WavePOINT to another. When the signal strength received by a mobile computer from its current access point falls below a defined threshold, the mobile computer places its WaveLAN unit into NWID-promiscuous mode to allow it to also receive the beacon signals from other nearby access points. When a suitable new access point is identified, the WaveLAN unit is set to again filter received packets based on the NWID of the new access point, and the mobile computer uses the sign-on protocol to register with the new WavePOINT. The sign-on protocol also serves to update the forwarding tables in the old and new WavePOINTs and in any other learning MAC-level bridges on the wired network connecting the two WavePOINTs [15].

In wireless LANs, peer-to-peer (mobile-to-mobile) communication can be provided in one of two ways. In some wireless LANs, it is possible for a mobile to communicate directly with another mobile. In other wireless LANs, two mobiles, even though they are both within the coverage area of the same access point, can communicate only by having their transmissions relayed by the access point. The AT&T WavePOINT/WaveLAN products use the former approach.

In laying out a multiple-access-point wireless LAN installation, one must take care in locating the access points to ensure that adequate radio coverage will be provided throughout the service area. There is an additional issue in a wireless

LAN in which direct peer-to-peer communication between mobile computers is supported without relaying by the access point. In this case, one must reduce the coverage area of each access point in a way which will ensure that any two mobiles within the coverage area will be within radio range of each other. This reduction in coverage areas is generally done by reducing the distance between neighboring access points by half, and means that more access points will be needed to cover a given service area. Such reduction in coverage area is not necessary where peer-to-peer service is provided by relaying communication through the access point. In our installation, we have worked with AT&T to modify the WavePOINT access points such that peer-to-peer service can be provided through the access points, thus giving each access point the maximum possible coverage area.

Because wireless LAN equipment is rarely used in such a large system, we are proceeding cautiously in introducing the service to the campus community to be sure that the wireless LAN service is reliable and stable before usage is attempted on a large scale.

Implementation Details

We are installing WavePOINT access points in 12 buildings on campus in order to provide complete WaveLAN coverage for all areas in these buildings and their adjacent outside spaces. These buildings constitute most of the campus classroom and administrative buildings. We estimate that approximately 200 WavePOINT units will be required to reach this level of campus coverage.

Figure 4 illustrates how the WavePOINT units are connected to our campus network. We are installing a new IEEE 802.3 backbone network on campus to connect the WavePOINT units in each building with the rest of the campus wired network through a separate router located in the main campus data communications facility. In each building, each WavePOINT is connected to a Synoptics IEEE 802.3 10Base-T hub located either in the building's master wiring closet or in a remote wiring closet on a floor of the building. These hubs, in turn, are connected by multimode fiber cable to a 10Base-T hub which is central to the high-speed wireless network. This hub connects to a Cisco router. The WavePOINT units and hubs are powered by the campus 110 VAC system.

This structure allows us to operate the high-speed wireless network independent of the campus network and to disconnect the two if necessary. We consider this arrangement necessary at least until the wireless network is stable and considered a fully operational system. This structure also allows separating traffic on the wireless LAN backbone network from traffic on the rest of the campus network. The Cisco router connecting the wireless backbone to the rest of the campus filters packets based on destination address and only passes packets to and from the wireless backbone as needed. For example, this allows us to avoid passing the packets used for the WaveAROUND sign-on protocol between a mobile computer's old and new WavePOINT access point, over the main campus network backbone.

As with CDPD, we are primarily using the FTP Software PC/TCP implementation of the TCP/IP protocols on our IBM ThinkPad laptop computers running Microsoft Windows. The WaveLAN units include an NDIS [10] device driver for interfacing to the TCP/IP protocol stack. We are also using the WaveLAN units with NetBSD UNIX running on the ThinkPads and have written a UNIX WaveLAN device driver and PCMCIA PC Card support for NetBSD to support this. The UNIX device driver supports the full WaveLAN protocol, including WaveAROUND roaming.

Deployment and Experience To Date

In contrast to CDPD service, where coverage is primarily the responsibility of the cellular carrier, a user of wireless LAN equipment must take responsibility for installing access points carefully, in a way that provides complete coverage of the service area. The layout should be based on measurements, not just on "rule-of-thumb" calculations. These measurements involve extensive testing and careful consideration of radio propagation issues when the service area is large, such as an entire campus as in our installation.

Because the coverage area of an access point is relatively small, terrain is not a propagation issue. Rather, the layout and construction of buildings determine the coverage area of each access point. AT&T rates the WaveLAN/WavePOINT transmission range at up to 800 ft in an open environment, but this rated range may be reduced to 100–200 ft through walls and other partitions in typical office environments. Wood, plaster, and glass are not serious barriers to the WaveLAN radio transmissions, but brick and concrete walls can be significant barriers; the greatest barrier to radio transmissions commonly found in office environments is metal, such as in desks, filing cabinets, reinforced concrete, and elevator shafts. Even a carefully considered access point design layout may have to be modified after installation is complete in order to remedy coverage gaps.

Because wireless LAN equipment is rarely used in such a large system, we are proceeding cautiously in introducing the service to the campus community to be sure that the wireless LAN service is reliable and stable before usage is attempted on a large scale. We plan to announce the service as available for research support and experimental use after we have accomplished the following tasks.

Coverage Verification – We will carry out coverage testing to be sure that targeted areas are in fact receiving complete coverage.

Trouble Reporting and Tracking System – We will establish a system to report and track problems on the wireless LAN system.

Network Management Tools – We will establish a rudimentary network management system for the access points, hubs, and routers associated with the wireless LAN system.

Hardware and Software Tools – We will procure and make available to the campus the hardware (e.g., host network adapters) and software needed to support a variety of application software running on a number of specified hardware platforms.

We began installation work for the WavePOINTs and new backbone network for connecting them in May 1995, and as of November 1995 had completed installation and testing in five buildings. Our testing revealed some coverage gaps in a few buildings, which we are currently working to correct with the installation of a small number of additional WavePOINTs. The system is currently capable of supporting PC-compatible computers but does not yet support Macintosh platforms. Since Macintosh computers are so commonly used on our campus, AT&T is working with us to develop support for these as well. It is anticipated that such support will be available by summer 1996.

Related Work

A number of other universities are currently also planning or deploying wireless data network infrastructures. Purdue University is developing a campus-wide wireless network, called Crosspoint [16], based on the Solectek AIRLAN wireless LAN product. Solectek AIRLAN uses the same hardware technology as the AT&T WaveLAN system we are using, and is built under license from AT&T. In Crosspoint, each AIRLAN unit is connected to a base-station computer, and the base stations are connected using an ATM backbone. The Crosspoint network runs a custom protocol between base stations to support sign-on of a mobile computer with a base station, providing roaming of mobile computers between base stations. Crosspoint uses an ATM backbone in order to support the large number of routing messages that may be generated between base stations, for example, as students move from one class to another.

At Stanford University, a new project called MosquitoNet [17] is studying operating system and application issues in mobile and wireless computing, and is building an experimental platform for their research. They are utilizing the Ricochet microcellular wireless data network service being deployed by Metricom in the San Francisco Bay Area and planned for deployment in other major metropolitan areas in the United States. The Metricom service uses FHSS in the 915 MHz ISM band to transmit wireless data packets at a raw data rate of 100 kb/s. Ricochet uses small radio units mounted on street lights, utility poles, and buildings, each with a range of about 2–5 miles. A subset of the radio units also have a wired network connection, and the Ricochet routing software forwards packets at a rate of about 2–10 hops/s between wireless radios to reach one of these wired access points. The approximate user data throughput of the system is 10–40 kb/s.

The system is currently capable of supporting PC-compatible computers but does not yet support Macintosh platforms. Since Macintosh computers are so commonly used on our campus, AT&T is working with us to develop support for these as well.

The InfoPad Project at the University of California at Berkeley is building InfoNet, a wireless data network that will allow multimedia communication with small portable terminals, called "pads" [18]. The wireless link for InfoNet is currently provided by two different types of networks, each serving one direction of the communication with the pads. For communication from a base station to a pad, InfoNet uses commercial radio components manufactured by Plessy, operating at 700 kb/s, and for communication from a pad to a base station, wireless LAN units manufactured by Proxim are used, operating at 244 kb/s. The backbone network connecting the base stations is currently Ethernet, although an ATM backbone is planned.

Also at the University of California at Berkeley, the Bay Area Research Wireless Access Network (BARWAN) Project is developing a wide-area wireless data service featuring a number of different wireless networks, each operating at a different scale, including regional area, wide area, metropolitan area, campus area, in-building, and in-room. The BARWAN Project seeks to integrate these different networks together seamlessly, sharing much the same vision as our Wireless Andrew infrastructure and some of the research being conducted on it [2]. Like the MosquitoNet Project at Stanford University, BARWAN is using the Metricom Ricochet microcellular data network service. They are also integrating use of the Hughes Direct Broadcast Satellite system into the network. The Hughes "DirecPC" service provides downlink facilities only (wireless data sent to a mobile computer), but operates at a raw data rate of 12 Mb/s. The DirecPC system thus must be used together with a separate (slower) network link for the uplink traffic (from the mobile computer).

Conclusion

The Wireless Andrew wireless data network infrastructure that has been described is expected to be invaluable in its ability to support research in mobile computing and wireless networking at Carnegie Mellon University. Some of the research projects that are already using this infrastructure include the following:

- Automatic connection to the most appropriate network and handoff to another network when appropriate [2]. The appropriateness of a network depends on its coverage area, speed, error rate, and usage cost in relation to the needs of a particular application.
- Scalable and transparent support for IP routing in an environment in which hosts are mobile. This is the "mobile IP" problem [2]. CDPD and WaveLAN each handle host mobility internally, but IP address assignment differs between these two networks, and we are using mobile IP to switch routing between these networks as well as between base stations on other types of networks that do not support their own protocols for internal host mobility.
- Mobile access to information, including the caching and consistency of files in a distributed file system environment [19]. These are challenging issues with wireless links because of their unreliable characteristics relative to wired links.
- Image and video compression techniques which can adapt to the bandwidth of the wireless link, including when switching between networks with different connection qualities [20]. For example, when switching from a 2 Mb/s wireless LAN link to a 19.2 kb/s CDPD link, the compression algorithms should adapt to the change in available network bandwidth.

This infrastructure will also enable faculty, staff, and students at Carnegie Mellon to access the facilities of the campus network and the Internet from around campus and around the greater Pittsburgh area. This will also serve as a source of empirical data on how mobile computers and wireless data network service are actually used by people.

Acknowledgments

We wish to thank John Leong, Richard Hovey, Robert Baron, Charles Bartel, and Pete Bronder for their contributions to this work. The work reported here is supported by Carnegie Mellon's Information Networking Institute, the National Science Foundation, Bell Atlantic NYNEX Mobile, and Bell Communications Research.

References

[1] CDPD Consortium, "Cellular Digital Packet Data System Specification," Release 1.0, July 1993.
[2] D. B. Johnson and D. A. Maltz, "Protocols for Adaptive Wireless and Mobile Networking," *IEEE Pers. Commun.*, this issue.
[3] J. B. Postel, ed., "Internet Protocol," Internet Request for Comments (RFC) 791, Sept. 1981.

[4] V. Jacobson, "Compressing TCP/IP Headers for Low-Speed Serial Links," Internet RFC 1144, Feb. 1990.
[5] J. B. Postel, ed., "Transmission Control Protocol," Internet RFC 793, Sept. 1981.
[6] J. B. Postel, "User Datagram Protocol," Internet RFC 768, Aug. 1980.
[7] B. Schneier, *Applied Cryptology: Protocols, Algorithms, and Source Code in C*, 2nd ed., [John Wiley & Sons, New York, 1996].
[8] M. Hall et al., "Windows Sockets: An Open Interface for Network Programming under Microsoft Windows," ver. 1.1, Jan. 1993.
[9] J. Romkey, "A Nonstandard for Transmission of IP Datagrams over Serial Lines: SLIP," Internet RFC 1055, June 1988.
[10] 3Com Corporation and Microsoft Corporation, "Microsoft/3Com LAN Manager Network Driver Interface Specification," ver. 2.0.1, Oct. 1990.
[11] B. Tuch, "Development of WaveLAN, an ISM Band Wireless LAN," *AT&T Tech. J.*, vol. 72, no. 4, July/Aug. 1993, pp. 27–37.
[12] D. F. Bantz and F. J. Bauchot, "Wireless LAN Design Alternatives," *IEEE Network*, vol. 8, no. 2, Mar./Apr. 1994, pp. 43–53.
[13] IEEE, "Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications," Draft Standard 802.11 D2.0, July 1995.
[14] AT&T Wireless Communications and Networking Division, "Data Manual: WaveLAN Air Interface," doc. no. 407-0024785, rev. 2 (draft), July 1995.
[15] R. Perlman, *Interconnections: Bridges and Routers*, [Addison-Wesley, Reading, MA, 1992].
[16] D. E. Comer, J. C. Lin, and V. F. Russo, "An Architecture for a Campus-Scale Wireless Mobile Internet," Tech. Rep. CSD-TR 95-058, Dept. of Comp. Sci., Purdue Univ., 1995.
[17] M. G. Baker, "Changing Communication Environments in MosquitoNet," *Proc. Workshop on Mobile Comp. Sys. and Apps.*, Dec. 1994, pp. 64–68.
[18] M. T. Le *et al.*, "InfoNet: The Networking Infrastructure for InfoPad," *Digest of Papers: COMPCON Spring 1995*, Mar. 1995.
[19] M. Satyanarayanan, Mobile Access to Information, *IEEE Pers. Commun.*, this issue.
[20] J. M. F. Moura et al., "Video over Wireless," *IEEE Pers. Commun.*, this issue.

This infrastructure will also enable faculty, staff, and students at Carnegie Mellon to access the facilities of the campus network and the Internet from around campus and around the greater Pittsburgh area, and serve as a source of empirical data on how mobile computers and wireless data network service are actually used by people.

Biographies

ALEX HILLS is Vice Provost for Computing Services and chief information officer at Carnegie Mellon University, where he is also a Distinguished Service Professor of Engineering and Public Policy. He is responsible for the University's academic computing, telecommunications, and data network facilities, and is also involved in wireless communications research activities. Professor Hills joined Carnegie Mellon after serving as executive director of the University of Alaska Computer Network. He was extensively involved in developing the telecommunications networks in rural Alaska and was deputy commissioner of the Alaska Department of Administration. He holds a B.S. in electrical engineering from Rensselaer Polytechnic Institute, an M.S. in electrical engineering from Arizona State University, and a Ph.D. in engineering and public policy from Carnegie Mellon University.

DAVID B. JOHNSON is an assistant professor in the School of Computer Science at Carnegie Mellon University, and also holds a courtesy appointment as an assistant professor in the Electrical and Computer Engineering Department. His research interests include network protocols, distributed systems, and operating systems. He has worked actively within the Mobile IP Working Group of the Internet Engineering Task Force (IETF) for the past three years and is one of the principal designers of the current IETF Mobile IP protocol. Prior to joining the faculty at Carnegie Mellon in 1992, he was on the faculty at Rice University in the Computer Science Department. He holds a B.A. in computer science and mathematical sciences, an M.S. in computer science, and a Ph.D. in computer science, all from Rice University.