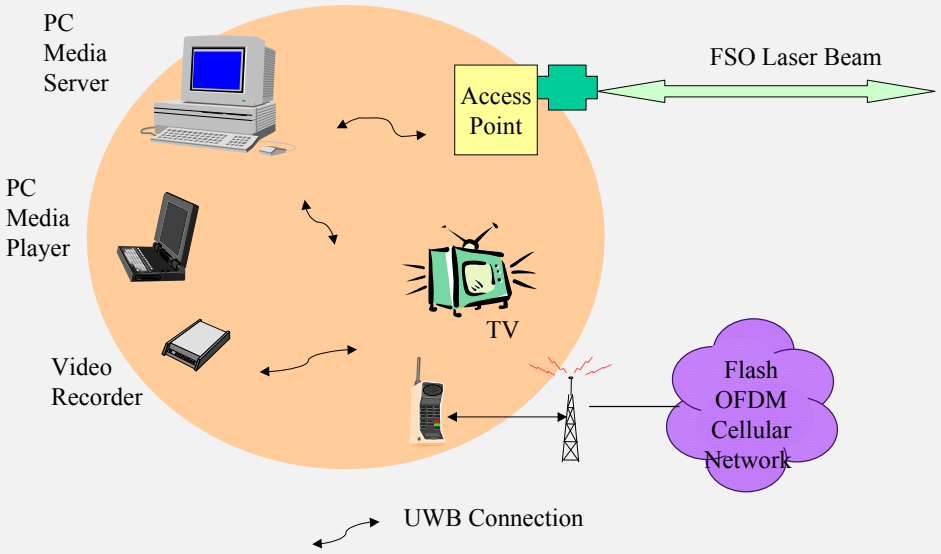
10 Emerging Wireless Networks: UWB, FSO, MANET, and Flash OFDM

Example: A Future Wireless Broadband Scenario

Consider a future wireless home in which all home devices (computers, VCRs, TVs) are "connected" to each other through broadband wireless networks. The main candidate for such networks is UWB because it offers very high data rates for applications such as remote video viewing over very short distances. This home could be connected to the Internet over wireless local loop technology such as free space optics. The high data rate telephone services could be provided through Flash OFDM. The following configurations shows such a scenario in which users at home and offices can access the Internet and also use the handsets for voice, video and multitude of other applications over broadband wireless networks.



10.1 Introduction

A great deal of research and industrial work is currently underway in different aspects of wireless networking. Work ranges from optimization of physical-layer communication technologies to the development and enhancement of higher-level protocols and applications that enhance end-user capabilities. Many different efforts are concentrating on broadband wireless communications and new models for using mobile communications. Many of these

efforts are not new; in fact many (such as UWB and FSO) have been around in the military segment for a while and are now being allowed for general commercial applications.

It is virtually impossible to cover all emerging technologies in this rapidly advancing field. We have chosen a few that appear to have great industrial impact. Examples of the wireless network technologies covered include Powerline Communication (PLC), Ultra Wideband (UWB), Free Space Optics (FSO), Mobile Ad Hoc Networks (MANETs), wireless sensor networks (WSNs), and Flash OFDM (Orthogonal Frequency Division Multiplexing). We took a quick look at many of these technologies in the previous chapters. The purpose here is to provide additional details and point to sources for further studies.

Chapter Highlights

- Powerline communication (PLC) networks are the LANs that use existing powerlines to carry data. The main idea is to use a "powerline modem" that transfers data which can be then carried over regular powerlines that are all around us.
- Ultra Wideband (UWB) is a promising new technology in the areas of wireless personal area networks. It offers very high data rates over very short distances.
- Free Space Optics (FSO) is a line-of-sight technology that uses lasers for wireless optical communication in a wireless local loop environment.
- Mobile Ad Hoc Network (MANET) is a set of wireless mobile nodes forming a dynamic autonomous network without an access point.
- A wireless sensor network (WSN) typically consists of thousands of sensor devices interacting with each other in an ad hoc structure. The sensors collect a variety of data and transfer it to chosen neighboring sensors until it gets to a target machine (e.g., a data collection and analysis site).
- Flash OFDM (Orthogonal Frequency Division Multiplexing) is an attractive alternative to 3G cellular networks.

The Agenda
- Powerline Networks, UWB, and FSO
- MANETs and Wireless Sensor Networks
- Flash OFDM and Synthesis

10.2 Powerline Communications Networks

10.2.1 Overview

Powerline communication (PLC) networks use existing powerlines to carry data. Although not strictly wireless, PLC can be discussed under wireless networks because you do not need *additional* wires for communications. The main idea is quite simple. For years, we have been

using telephone lines that were designed to carry voice to transmit data by using *modems*. Can a "powerline modem" be designed that can transmit data by using the regular powerlines that are all around us? The answer is yes – and this is the foundation for the excitement. Initial predictions for the growth in PLCs were almost unbelievable. For example, according to analysts from Cahners Instat/MDR, powerline technology will grow from an $18M business in 2001 to a $190M one in 2002 (955% growth) and thereafter at a steady rate. Although some of these predictions have not materialized due to the tremendous popularity of other alternatives such as 802.11, PLC is still an interesting area of work.

Although the idea is not new, now it is becoming technically and economically feasible. For example, electrical lines were used by radio amateurs during World War II to establish underground communication lines. At present, the technology is far more mature in Europe than in the US. The primary driver behind PLC is the widespread availability of electric lines. While cable and DSL connections are still being built, 98.9% of US homes are connected to a power supply. Even today, phones are still around only 95%.

10.2.2 Powerline Communications Characteristics

Developments in PLC are proceeding in two directions: home networking and broadband WANs. Figure 10-1 shows an example of a PLC home network that consists of two networks that are interconnected through the home wiring. The upstairs network is a wireless network and the downstairs network is an Ethernet LAN. The two LANs are connected to powerline adapters that connect computing devices to the home powerlines. The powerline adapters are essentially the "powerline modems" that translate data signals to the powerline signals. These adapters let you exploit your home's existing electrical wiring for computing purposes. In particular, you can turn the existing electrical wiring of a home into the backbone of a home network. The vision is that you have to just plug in a PLC adapter outlet in your home to connect to a network. In addition to the adapters, repeater units are available to repeat signals and combat noise.

The main appeal of PLC is that you can communicate with your home devices and set up a home network by using the existing powerlines in your home. Proponents of PLC-based home networks feel that it is fast, reliable, simple to install, and moderate in cost. In addition, because there are more power outlets (on average, each room has 3 electrical outlets) than phone jacks in a typical home, you can connect your devices anywhere.

10.2.3 Powerline Communications Market

While PLC-based home networking is the main area of development at present, many utilities are investigating this technology for broadband services. The main driver here is to use PLC as a way to expand their business and meet demand that is not being met by cable modems and DSL. The electric utility companies want to use the existing electric distribution systems to take the role of broadband pipelines for network communications. The utilities are excited because they see another strategic value for their already installed infrastructure. Another reason is that several management functions such as billing are already being provided by the electric utilities, so new investment for billing is not needed. PLC-based broadband services are currently available in Germany and Sweden. Several companies, such as ConEd and American Electric Company, in the US are also getting into it.

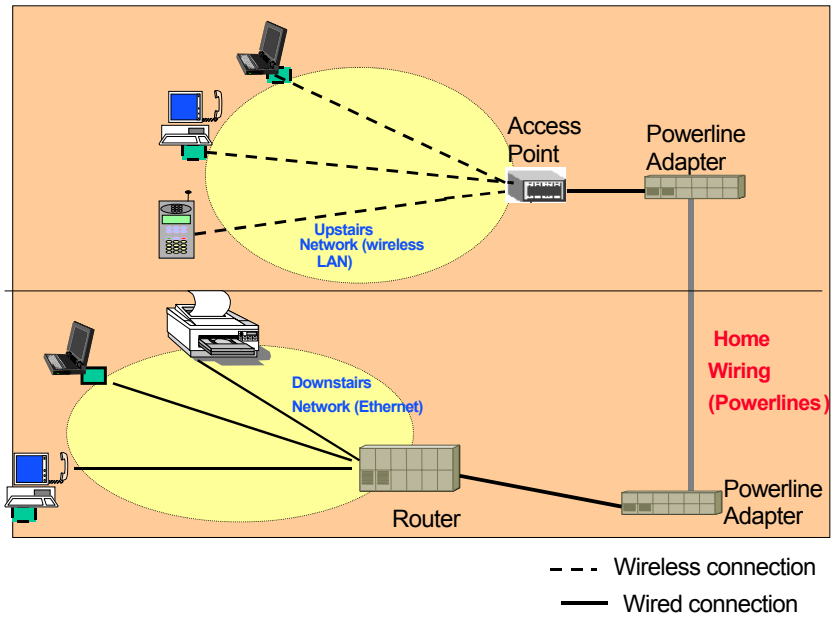


Figure 10-1: A Powerline Communication Home Network

While the work on broadband PLC is underway, most attention at present is being paid to position PLC as an alternative to wireless Ethernet (IEEE 892.11b) LANs. In general, PLC-based LANs are easier to install, have longer range than wireless networks, and provide better security. Table 10-1 summarizes the tradeoffs between wireless LANs and PLC LANs. However, there are several potential drawbacks to PLCs also. Before PLC becomes a commercial reality, it must overcome several technical hurdles such as the following:

- Tests have shown PLC data rates between 6 Mbps to 14 Mbps. As we know, 802.11g can deliver up to 54 Mbps. Thus PLCs must deliver higher data rates to compete.
- The distance limit of 1000 feet may not cover larger offices and homes. Also the signals weaken as they progress through the network.
- Powerlines are inherently noisy (signal-to-noise ratio is inadequate) and prone to attenuation. In addition, interference from other appliances and RF on the line can be very high.
- Modern electric power systems use transformers to convert electricity into different voltages. Digital signals cannot be transmitted through transformers. How to bypass line transformers and other devices is a good question.
- The PLC setups are flexible but not really mobile. This is a weakness when compared with wireless networks.
- Security is an issue because PLC is a shared medium; thus messages must be encrypted. In addition, worker safety is a major concern because PLC equipment is installed on power lines.

Active progress is being made to address these issues. Most PLC vendors have made great progress developing devices that allow digital and analog signals to bypass transformers. To support PLC, feeders are typically segmented to maintain throughput and to keep data transmissions secure. RF (radio frequency) interference has historically been PLC's biggest problem. More shielding has been the typical solution to this problem. For worker security, transformers must not allow medium voltages to leak into them, or a line worker could be electrocuted. The most commonly proposed solution in this area is to educate the field crew about the dangers before the PLC devices are deployed.

Significant work is going on in this area. Information can be obtained from websites such as www.gigafast.com, www.linksys.com, and www.homeplug.org.

Table 10-1: Wireless Ethernet Versus Powerline

Factor	IEEE 802.11b (Wireless Ethernet)	Powerline
Data Rate	11 Mbps	14 Mbps
Distance	150 feet, w/ distance affecting speed	1000 feet before signal interruption
Security	40-bit and wireless (piggy-backing)	DES 56-bit plus physical connection
Interference with other LANs (Bluetooth), microwaves, home RF, etc	2.4 GHz band is congested and leads to interference	Eliminates some interference with adapters but it is a serious problem
Cost	Base station: $180 PC cards: $80 – $100	Adapters: $120 -$150 PC cards: $80 – $100 Router: $80
Can every PC in home watch DVD (requires 6 Mbps per PC for video transfer)	No	Yes

10.3 Ultra Wideband Wireless (UWB)

10.3.1 Introduction

Ultra Wideband (UWB) is a promising technology in wireless local and personal area networks. As shown in Table 10-2, UWB provides high data rates (around 50 Mbps) in very short distances (up to 10 meters). Simply stated, UWB is a radio or wireless system that uses narrow pulses (on the order of 1 to 10 nanoseconds) for communication and sensing (short-range radar). UWB faces stiff competition from existing technologies, and the adoption of UWB by the IEEE 802.15 Working Group has been slow. But UWB has an established and proven track record in military applications (it was originally developed in the 1960s for the military and classified for many years). In addition, UWB has several attractive characteristics such as high security, very low power consumption, very high throughput, and ability to operate without the requirement of spectrum licensing.

Table 10-2: Highlights of UWB

Factor	Key Points
Data Rate	50 Mbps
Coverage	10 m, typically less
Typical Applications	Military, Wireless Home Entertainment
Frequency Band	3.1 GHz – 10.6 GHz (usable frequency: 7.5 GHz)
Location Management	Low mobility in short distances
Physical Communication Considerations	– UWB pulses are very short and low-power. – There is no need for complex modulation because single pulses act as Morse code. – UWB spreads the signal without the use of complex spread-spectrum techniques.

After years of classified work, the Federal Communications Commission (FCC) recognized the significance of UWB in 1998 by creating a committee to conduct regulatory reviews of the technology. According to the FCC, UWB communications devices are restricted to intentional operation only between 3.1 and 10.6 GHz (other applications such as law enforcement, fire and rescue are restricted to operate between 1.99 and 10.6 GHz). Initial communications applications are further restricted to indoor operations, or to lower out-of-band emissions with outdoor handheld use. These restrictions limit the spectrum and power use by UWB Devices.

Figure 10-2 shows a sample UWB configuration for home entertainment. In this case, a VCR is "connected" to the TV through UWB instead of cables. Similarly, a desktop computer and a laptop are also UWB-enabled through UWB transceivers. Let us go through the following scenario. Suppose John wants to watch a movie by using the VCR. Then the VCR acts as a media server and John's TV acts as a media player. John's son Bob wants to watch a documentary that is stored on the desktop. Now the desktop acts as a media server and Bob's laptop becomes a media player. Note that all these devices are connected wirelessly through UWB. Other cable replacement options such as Bluetooth and Wi-Fi are not suitable because they are too slow for remote video viewing.

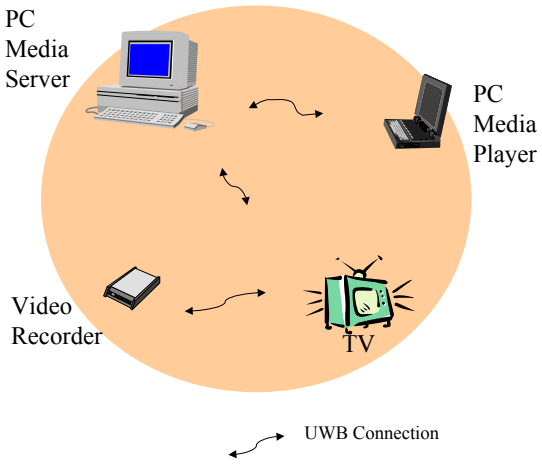


Figure 10-2: A Sample UWB Configuration

10.3.2 Technology Characteristics and Description

Basically, UWB transmissions are comprised of individual square wave pulses that are emitted at nanosecond intervals. The individual pulses are generated across a wide range of the frequency spectrum in what is known as the "noise floor"; i.e., UWB takes advantage of the pulses that are typically considered as noise. These pulses can be modulated to represent a digital value of 0 or 1 at the receiving end, therefore achieving digital data transmission when demodulated at the receiving end. UWB is based on communications systems with very narrow pulse widths and very wide bandwidths. These systems have instantaneous bandwidths of at least 25% of the frequency of the device. If a device operates at 10 GHz, it can have bandwidth of 2.5 GHz. Thus UWB devices have very high bandwidths and consequently high data rates.

Most communication systems have data signals that are modulated on carrier signals. For example, our voice is modulated on a carrier signal provided by the telephone company. In case of UWB, the data signals *are* the carrier signals. This removes the need for separate carrier signals. UWB basically uses extremely short, low-power pulses to communicate information. These extremely high frequencies of the millions of signals per second themselves carry the information and remove the need for a carrier. Thus UWB achieves wireless communications without using a radio frequency (RF) carrier and eliminates the need for RF licensing. Instead, it uses modulated pulses of energy less than one nanosecond in duration. UWB transmissions do not interfere with each other or with other conventional radio waves because the pulses are very short and have low power that is commonly considered as noise. Due to the low power of UWB, it operates in very short distances. For example, UWB has been used in emergency situations to detect bodies buried in rubble after collapse of a building.

UWB standards are being developed by the IEEE 802.15 working group for Wireless Personal Area Networks (WPANs). These standards have been developed for short-distance (30-feet, or 10-meter) wireless networks. The standards effort for UWB is being spearheaded by the 802.15.3a (WPAN Higher Rate) Task Group. This Task Group is chartered to develop a new standard for a higher speed (110 Mbps or greater) needed by streaming video and other multimedia applications. A new physical layer (PHY) is being developed by the Task Group for such high data rates. UWB is a strong player in this effort because it is a better choice compared to other short-range wireless systems (such as Bluetooth) because of its simpler device designs and higher data rates. These attributes can easily make it a better choice all around, for any type of short- or medium-range wireless applications with higher data rates. However, the progress is somewhat slow for a variety of reasons.

The main characteristics of UWB are:

- UWB requires no assigned spectrum because transmissions are sent across an ultra-wide band and at ultra-low power – too low to affect other users.
- UWB does not use the traditional radio frequency carriers employed by cellular, satellite, television, cable or other communications technologies. Current frequency-based technologies must operate in specific bands of an increasingly crowded radio spectrum, otherwise they would interfere with one another. Because UWB signals do not interfere with each other or with conventional RF carriers, UWB has opened up vast new possibilities as a new communications medium that can coexist with existing technologies.
- UWB is not line-of-sight**.** The fundamental physics of Ultra Wideband enables this technology to propagate through walls and other obstacles. That is why UWB technology is also used for things like "through-the-wall" imaging devices and ground penetration radar.

10.3.3 Applications of UWB Technology

UWB technology has been used for some time in Ground Penetrating Radar (GPR) applications and is now being developed for new types of imaging systems that would enable law enforcement, fire and rescue personnel to locate persons hidden behind a wall or under debris in crises or rescue situations. UWB imaging devices also could be used for security measures in construction and home repair industries, to locate fine electrical wiring and pipes hidden inside walls or underground. UWB devices can act as portable, high-performance, high-resolution radar and attain excellent penetration through walls, suitable for both imagers and sensors. Most UWB applications include the following:

Ground Penetrating Radar Systems (GPRs): GPR was originally developed for military purposes and public safety such as land-mine detection. GPRs operate only when in contact with, or within close proximity of the ground, for the purpose of detecting or obtaining the images of buried objects. Applications of GPRs include highway inspection to identify voids, locating pipes essential for safety, railroad bed inspection, forensics, detection and 3-D mapping of pipes and utilities before excavation, etc. It operates in the lower frequency band, in the range of 40 MHz to about 2.5 GHz. Due to FCC regulations, operation is restricted to law enforcement, fire and rescue organizations, scientific research institutions, commercial mining companies, and construction companies. The Radar Industry Coalition has been trying to petition the FCC for reconsideration of its stringent rules, in order to open GPR for other applications.

Wireless Home Entertainment: UWB could support wireless home entertainment because Wi-Fi cannot support the bandwidth demands of home entertainment. For example, a VCR could be "connected" to the TV through UWB instead of cables. In addition, camcorders could talk wirelessly to computers, and TVs could talk to DVDs, through UWB. Sony and Philips, for example, are both devoting resources to UWB to support this vision.

Wall and Through-Wall Imaging Systems: Wall-imaging systems are designed to detect the location of objects contained within a "wall," such as a concrete structure, the side of a bridge, or the wall of a mine. Through-wall imaging systems detect the location or movement of persons or objects that are located on the *other side* of a structure such as a wall. Operations are restricted to law enforcement, fire and rescue organizations, scientific research institutions, commercial mining companies, and construction companies. The systems operate below 960 MHz or in the frequency band 3.1-10.6 GHz, to detect the location of objects and identify them when obscured by foliage or contained within a wall such as a concrete structure, the side of a bridge, or the wall of a mine. Precision Range Gating[1] and Synthetic Aperture Radar (SAR) imaging experiments have demonstrated excellent images of objects obscured by dense foliage.

Add-ons to Wi-Fi LANs. While Wi-Fi LANs are quite popular, security concerns still linger. To compensate for Wi-Fi security weaknesses, wireless operators could sell UWB and W-iFi as a package to organizations that need military-grade security.

Medical Systems: A medical imaging system may be used for a variety of health applications to "see" inside the body of a person or animal. Operation must be at the direction of, or under the supervision of, a licensed healthcare practitioner. These devices must be operated in the frequency band 3.1-10.6 GHz.

Surveillance Systems: Surveillance systems operate as "security fences" by establishing a stationary RF perimeter field and detecting the intrusion of persons or objects in that field. Operation is limited to law enforcement, fire and rescue organizations, public utilities, and industrial entities. Although technically these devices are not imaging systems, for regulatory purposes they are treated in the same way as through-wall imaging and are permitted to operate in the frequency band 1.99-10.6 GHz.

10.3.4 Advantages and Disadvantages of UWB

UWB has several advantages. The main advantage is that UWB does not interfere with other radio communications in the environment. Thus, it can co-exist with available wireless communications systems such as IEEE 802.1X, and Bluetooth. Additionally, the pulses are

[1] Involves sampling the received video signal at a specified time after the transmit pulse has been radiated. This improves the sensitivity of short-range radars by eliminating reflections up to the point of the antenna reflection

very short and of low power. Moreover, there is no need for complex modulation because single pulses act as Morse code, and UWB spreads the signal naturally without the use of complex spread-spectrum techniques. High data bit rates can also be achieved in a short- to medium-range communication environment. Specifically:

- UWB is inherently a secure technology with multiple layers of security. The first layer is that UWB lies on the noise level, hence an attempting eavesdropper will not be able to decipher between noise and data unless they have access to proprietary coding schemes, algorithms, and modulation techniques. The next is the handshaking protocol invoked at the MAC level that only allows authorized parties to shake hands. Finally there are several encryption techniques that can be used for added security. For evidence, the military has used UWB technology for communications since the 1980s because of its security features.
- UWB technology promises to be less complicated and less expensive to design and use, resulting in quicker and wider adoption. Architecturally a UWB transceiver is much less complicated than a "narrowband" RF transceiver because it does not require the components to modulate a signal, leading to lower manufacturing and assembly costs.
- UWB is a more power-efficient technology. When comparing UWB and existing RF technologies in the same coverage area, UWB operates at a power level approximately 1000 times lower. The end result is longer-lasting battery life, which is an important consideration in wireless technology.
- UWB is less prone to interference. UWB technology uses extremely short, low-power pulses to communicate information. Due to the very high bandwidth of the signal, UWB signals are resistant to interference, since any interference would only possibly change one part of the signal's spectrum, leaving the rest of the spectrum unaffected by interferences.
- UWB operates in a fairly small footprint (10 meters and less) and as a result it has the advantage of frequency re-use. Multiple UWB systems can be meshed together such that they give a greater coverage area and still deliver high transfer rates in addition to being low in power consumption. However this feature requires serious analysis and development at the MAC layer, which is being researched and debated as the 802.15.3a standard by the IEEE.
- UWB works on top of existing systems and thus does not use an RF carrier signal. As a result, UWB provides relief to the bandwidth crunch that exists within the communications world. Since most of the RF spectrum has been auctioned off, the predicted growth of cell phones and handheld devices in the next five years is facing problems. Any technology that does not further exasperate the RF spectrum shortage is welcome.
- UWB can possibly become a global specification because it does not require frequency allocations. While global companies span the entire world, standards (and specifically frequency allocation) are decided on a national level. As a result, many products have to be designed for a specific country. UWB devices do not suffer from this "localization" because UWB operates on top of current specifications, thus it can become a globally interoperable RF technology.

However there are several possible disadvantages of UWB technology. Specifically:

- The FCC limitations restrict the possible data bit rate achievable and the distance of the transmission.
- The design of antennas can also be troublesome due to the broadband characteristics of the signal. There are not many tools available for antenna design for UWB.
- UWB, as stated previously, is implemented on top of currently allocated frequencies. This is a strength but also a possible weakness. The problem is that UWB could interfere

with communications that are using the same frequency range, such as the GPS or airline industries. The main argument comes from an alliance of more than 30 communications companies that make use of the specified spectrum: they are concerned about the integrity of their communications while UWB is running on top of their devices. More seriously, current regulations do not allow additional transmissions within certain frequency bands, in order to protect the integrity of the already-allowed transmissions [*RCR Wireless News*, January 29, 2003].

10.3.5 Concluding Comments about UWB

UWB provides high data rates (around 50 Mbps) over very short distances (10 meters). There are two main differences between UWB and existing "narrowband" technologies. First, UWB is defined as being greater than 25% of a center frequency or greater than 1.5 GHz wide, thus resulting in a much larger bandwidth. Second, UWB is implemented in a *carrier-less* fashion. "Narrowband" systems use radio frequency carriers to move a signal to the proper frequency range, whereas UWB modulates an impulse. As a result, the system occupies a frequency range on the order of one gigahertz, which gives a much larger bandwidth, thus allowing for much higher data rates than competing "narrowband" technologies. A simple comparison of such technologies can be seen in Table 10-3.

It can be noticed that UWB operates in the same distance range as Bluetooth. The 802.11 standard far exceeds the coverage area of both Bluetooth and UWB. However, the amount of power consumed by UWB mobile devices is lower, leading to greater power efficiency. Since the other three standards are limited to a smaller frequency spectrum, all of their bandwidth gains come from an effective SNR (signal-to-noise ratio), whereas because the bandwidth of UWB is so large, it allows for a much larger rate at a smaller energy output.

Table 10-3: Comparison of Wireless LAN Technologies with UWB

Standard	Bluetooth	802.11a	802.11b/g	UWB (projected)
Coverage	10 m	50 m	100 m	10 m
Frequency Band	2.4 GHz	5 GHz U-NII Band	2.4 GHz ISM Band	3.1 – 10.6 GHz
Usable Freq.	83.5 kHz	200 MHz	80 MHz	7.5 GHz
Data Rate	1 Mbps	54 Mbps	11 Mbps	50 Mbps

UWB Sources of Information

"UWB Unleashed." Pyramid Research Report, http://www.ppa.com.tw/Pyrawid/news/021231_Pyramid.htm

Aiello, R., et al. "Understanding UWB – Principles and Implications for Low-Power Communications – A Tutorial." Available at: http://www.discretetime.com/papers/03157r0P802-15_WG-Understanding_UWB_For_Low-Power_Communications-A_Tutorial.pdf

Blankenhorn, D. "Ultra Wideband." *Mobile Radio Technology*, January 1, 2003. Available at http://iwce-mrt.com/ar/radio_ultra_wideband/

Discrete Time Communications. "UWB Technology." http://www.discretetime.com/pages/technology.php

Federal Communications Commission. "FCC News." February 14, 2002. Available at http://www.fcc.gov/Bureaus/Engineering_Technology/News_Releases/2002/nret0203.html

Fontana, R. "Recent Applications of Ultra Wideband Radar and Communications Systems." Available at: http://www.multispectral.com/pdf/UWBApplications.pdf

Ground Penetrating Radar Industry Coalition. "Petition for Partial Reconsideration of the Ground Penetrating Radar Industry Coalition." June 5, 2002. Available at: http://www.geophysical.com/FCC%20Petition%20020617.pdf

Laine, D. "What's up with Ultra Wideband Technology – Part II." 24 June 1999. Available at http://wca.org/Year1999/laine/

Pulselink, Inc. "Bridged Ultra Wideband Architecture (BUWBA™)." Available at http://www.pulselink.net/wire_future.html

Pulselink, Inc. "Future of UWB over wire." Available at http://www.pulselink.net/wire_future.html

Wilson, James M. "Ultra-Wideband/a Disruptive RF Technology?" Intel Research & Development. September 10, 2002. Available at: http://www.intel.com/technology/ultrawideband/downloads/Ultra-Wideband_Technology.pdf

10.4 Free Space Optics (FSO) – A "New" Solution to the Last Mile

10.4.1 Overview

Free Space Optics (FSO) is a line-of-sight technology that uses laser beams in a wireless local loop environment. FSO uses optical waves to transmit data, but instead of enclosing the data stream in a fiber optic cable, the data is transmitted through the air (see Figure 10-3). FSO systems can support data rates between 1.25 and 150 Gbps (theoretically) with link lengths that can vary from more than 600 feet up to about a mile. The higher data rates and distances are achieved in clear, dry, and "non-intrusive" atmosphere. Common FSO networks support around 2.5 Gbps of data, voice and video communications between 1000 to 2000 feet. Most FSO equipment vendors supply products providing 100 Mbps, 155 Mbps (OC-3), 622 Mbps (OC-12) and up to 1 gigabit capacities. FSO transceivers can be located on a rooftop, on a corner of a building, or indoors behind a window to support the last mile. Although FSO appears to be point-to-point, FSO operations can be set up as point-to-multipoint where different laser beams from the provider site are directed to multiple subscribers.

Free Space Optics (FSO) systems could be a viable option for many applications in the last mile. Very few (only 5%) of commercial buildings in the U.S. have fiber optics to their door, although most are within a mile of a fiber-optic connection. FSO fills this "last mile" gap quite well. FSO provides short-term solutions for short-distance network bridges as well as an attractive offering for service providers to deliver all-optical networks. FSO technology operates at layer 1 and so is protocol-independent and can be used with ATM, SONET, Gigabit Ethernet or virtually any network. A major advantage of FSO, as we will discuss, is

that it is very secure because laser beams cannot be easily intercepted. In addition, FSO technology requires no spectrum licensing.

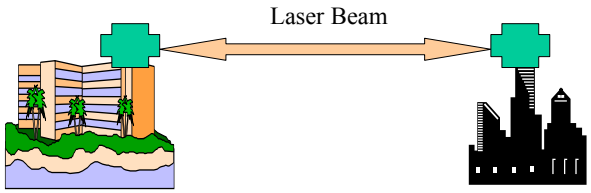


Figure 10-3: Conceptual View of FSO

Fiber-optic communication has gained wide acceptance in the telecommunications industry at the time of this writing. However, it is still relatively new and not well known in many markets. An FSO Alliance, comprised of virtually all significant players in the wireless sector, has been formed to promote and watch FSO activities. The Alliance website (http://www.free-space-optics.org/) is a rich source of information on FSO.

Table 10-4: Highlights of FSO

Factor	Key Points
Data Rate	Commercially available: 100 Mbps to 2.5 Gbps; research prototypes: up to 160 Gbps.
Coverage	600 feet to about a mile
Typical Applications	Broadband access for "last mile," especially suitable for highly secure and very fast data delivery in wireless local loop
Frequency Band	-TeraHertz spectrum (194 THz and 375 THz). - Frequency bands are unregulated and do not require licensing
Location Management	None, operates in a fixed wireless environment
Physical Communication Considerations	- Uses light waves instead of electromagnetic waves - Operates at layer 1, thus is independent of any protocols and can support Ethernet or any other higher-level protocols - Requires clear line of sight between the source and the destination .

10.4.2 Characteristics of Free Space Optics (FSO)

The technical foundation of FSO is the Alexander Graham Bell "photophone," experiment in the late nineteenth century before he invented the telephone. He converted voice sounds into telephone signals and transmitted them between receivers through free air space along a beam of light for a distance of about 600 feet. Although the Bell photophone did not become a commercial reality, it laid the foundation for FSO, which was developed in the last four decades for defense applications. The aerospace and defense applications established the foundation upon which today's commercial laser-based FSO systems are based.

FSO technology is relatively simple – it is similar to fiber optics but without the fiber cables. It uses similar optical transmitters and receivers. Each FSO unit consists of an optical transceiver with a laser transmitter and a receiver to provide full duplex capabilities. The FSO units use a high-power optical source (i.e., a laser), and a telescope that transmits light through the air to another telescope receiving the information. The receiving lens connects to a high-sensitivity receiver via optical fiber. FSO transceivers also include data processors and alignment systems. Light travels through air faster than it does through glass (fiber optic cables), so FSO can be thought of as optical communications at the speed of light.

FSO systems can function over distances of several kilometers. The main restriction is that there should be a clear line of sight between the source and the destination, and enough transmitter power. Since FSO is an optical technology, no spectrum licensing or frequency coordination with other users is required, and interference from or to other systems or equipment is not a concern. In addition, the point-to-point laser signal is extremely difficult to intercept – thus FSO is secure. FSO also has very low error rates. There is almost no practical limit to the number of separate FSO links that can be installed in a given location because FSO laser beams have extremely narrow widths.

The two wavelengths typically used for FSO transmissions are long wavelengths around 194 THz and short wavelengths around 375 THz. These wavelengths are used due to atmospheric propagation and the availability of fiber-based components. Signals at these wavelengths belong to the infrared spectrum and therefore are invisible. The technology can be globally deployed without requiring government licensing or certification. FSO products, however, need to comply with the International IEC safety standard.

10.4.3 Free Space Optics (FSO) Advantages

FSO provides many benefits:

- FSO's freedom from licensing and regulation translates into ease, speed and low cost of deployment.
- Since FSO transceivers can transmit and receive through windows, it is possible to mount FSO systems inside buildings, reducing the need to compete for roof space, simplifying wiring and cabling, and permitting FSO equipment to operate in a very favorable environment.
- The only essential requirement for FSO or optical wireless transmission is line of sight between the two ends of the link.
- FSO networks can close the last-mile gap and allow new customers access to high-speed MANs.

10.4.4 Free Space Optics (FSO) Security

The common perception of wireless is that it offers less security than wireline connections. In fact, FSO is far more secure than RF or other wireless-based transmission technologies, for several reasons (see the chapter on security for additional discussion):

- FSO laser beams cannot be detected with spectrum analyzers or RF meters.
- FSO laser transmissions are optical and travel along a line-of-sight path that cannot be intercepted easily. They require a matching FSO transceiver carefully aligned to complete the transmission. Interception is very difficult and extremely unlikely.
- The laser beams generated by FSO systems are narrow and invisible, making them harder to find and even harder to intercept and crack.
- Data can be transmitted over an encrypted connection, adding to the degree of security available in FSO network transmissions.

10.4.5 Free Space Optics (FSO) Challenges

The advantages of Free Space Optics (FSO) do not come without some cost. When light is transmitted through the air, as with these optical wireless systems, it must contend with many atmospheric issues – see the website of LightPointe (www.lightpointe.com) for an expanded discussion of the atmospheric issues:

- FSO is a line-of-sight technology. Thus all interconnecting points must be free from physical obstruction and able to "see" each other.
- Fog: The major challenge to FSO communications is fog. Rain and snow have little effect on FSO, but fog is different. The primary way to counter fog when deploying FSO is through a network design that shortens FSO link distances and adds network redundancies to find alternates.
- Absorption: Absorption occurs when suspended water molecules in the terrestrial atmosphere extinguish photons. Absorption attenuates the FSO beam and directly affects the availability of a system. The use of appropriate power and spatial diversity (multiple beams within an FSO unit) helps counter the absorption.
- Scattering and blocking: Scattering is caused when the light beam collides with scattering objects such as signs, bridges, and buildings. In scattering, there is no loss of energy, only a redistribution of energy that may have significant reduction in beam intensity for longer distances. Physical obstructions for FSO can be caused by flying birds that temporarily block a single beam. In addition, building sway, especially in high-rise buildings, can block FSO beams. Many companies, such as LightPointe, use multi-beam systems (spatial diversity) and other specialized techniques to overcome blocking and scattering.
- Scintillation: Heated air rising from the earth or man-made devices such as heating ducts can cause distortion of FSO beams.
- Safety: The two major concerns involve human exposure to laser beams (especially regarding eye safety), and high voltages within the laser systems and their power supplies. Standards have been established for laser safety and performance.

10.4.6 Case Study: FSO in Action

Vodacom is a large mobile telecommunications operator in several parts of the world. Vodacom embarked on an aggressive FSO deployment plan in South Africa (SA) by partnering with a UK firm, PAV Data Systems. The basic idea was to expand the cellular phone network in SA. As Vodacom rolled out more radio cell sites, the cell sites needed connections into the fixed network via 2 Mbps lines running over distances often less than 4 km. Leased line circuit was not an option because it could take up to eighteen months to install. Microwave technology was another option; microwave systems are competitive when transmitting over long distances (up to 60 km), but are not cost-effective over short links. The biggest problem with microwave systems (WLL and satellites) was that frequency spectrum allocation was strictly controlled by the SA Government and obtaining licenses could take months.

Vodacom started working with PAV to investigate feasibility of FSO. PAV originally supplied Vodacom with 25 FSO links, called SkyCell E1 products, each providing 2 Mbps point-to-point connectivity between cell sites and network lines. The main advantage of the FSO solution for Vodacom is that it operates in the infrared frequency band, thus the PAV's SkyCell products are free from government licensing. As a result, Vodacom had the solution it required in days, rather than months or years. Unlike leased lines, which carry rental costs, Vodacom bought the PAV SkyCell systems outright. In addition, the products can be relocated and reinstalled at minimal cost, within hours.

Vodacom increased its FSO operation into more than 200 PAV SkyCell connections running across its network. The PAV SkyCell systems, in many cases, are also being used to deliver backup links to leased line connections. Because of the theft of copper wires in South Africa, leased lines are somewhat unstable. For this reason, FSO technology plays an important role as a backup to leased lines. FSO also needs minimal maintenance. Once the systems have been installed, the main maintenance is that lenses need cleaning only once a year. FSO also seems to fit well with the future 3G cellular deployments in SA. The FSO network can be expanded easily to provide additional last-mile support for 3G networks.

Source: Vodacom case study: http://www.pavdata.com/partners_skyseries_case13.htm

10.4.7 FSO Summary

FSO uses point-to-point infrared lasers in the terahertz spectrum to support highly secure data rates in the range of 100 Mbps to 2.5 Gbps, over distances of several clear line-of-sight kilometers. Although new applications are emerging, FSO systems represent one of the most promising approaches for the last mile. As compared to the other alternatives of fiber-optic cables, wireless local loops, and copper-based technologies (i.e., cable modem, T1s or DSL), FSO systems have several attractive features for the last mile, such as low start-up and operational costs, rapid deployment, high security and high fiber-like bandwidths. Table 10-5 captures the main last-mile alternatives with their strengths and weaknesses. FSO is a particularly attractive option because, as mentioned previously, only 5 percent of the buildings in the United States are connected to fiber-optic infrastructure (backbone), yet 75 percent are within one mile of fiber. Thus as compared to the other options, FSO is well positioned for the last mile.

Table 10-5: Last-Mile Options Revisted

Option	Strengths	Weaknesses
Copper-based technologies (i.e., cable modem, T1s or DSL).	▪ Available almost everywhere ▪ Percentage of buildings connected to copper is much higher than fiber	▪ Low bandwidth (2 megabits to 3 megabits)
Fiber-optic Cable	▪ Very reliable means of providing optical communications.	▪ Digging, delays and associated costs to lay fiber ▪ Once deployed, it becomes a "sunk" cost and cannot be re-deployed if a customer relocates or switches to a another service
Radio Frequency (RF) Technology such as LMDS and MMDS	▪ Mature technology ▪ Longer ranges distances than FSO	▪ Requires immense capital investments to acquire spectrum license. ▪ Cannot scale to optical capacities of 2.5 gigabits – the current RF bandwidth ceiling is 622 megabits.
FSO	▪ Optical data rates and bandwidth scalability to Gbps range ▪ Low speed of deployment (hours versus weeks or months) ▪ Cost-effectiveness (on average, one-fifth the cost of installing fiber-optic cable). ▪ High security	▪ Short distance ▪ Relatively new technology in the commercial sector

FSO Sources of Information

"Free Space Optics – FSO: Wireless at the Speed of Light" – http://www.fsona.com/

http://www.nwfusion.com/links/Encyclopedia/F/568.html

"Free Space Optics: Technology, History, and Market Challenges" – www.freespaceoptics.org

"FSONA (Free Space Optical Networking Architecture)" – www.fsona.com

LightPointe White papers on FSO – www.lightpointe.com

Yahoo Free Space Optics News Group – groups.yahoo.com/group/fsonews/

Time to Take a Break

- Powerline Networks, UWB, and FSO
- MANETs and Wireless Sensor Networks
- Flash OFDM and Synthesis

10.5 Mobile Ad Hoc Networks (MANETs)[2]

10.5.1 Overview

A mobile ad hoc network (MANET), as described in a previous chapter, is a set of wireless mobile nodes forming a dynamic autonomous network. Simply stated, MANET is a wireless network without an access point. MANET nodes communicate with each other without the intervention of centralized access points or base stations. For example, the laptops of a group could establish a MANET during a meeting and then break up the network after the meeting is over. In such a network, each node acts both as a router and as a host. MANET is also defined as an autonomous system of mobile routers (and associated hosts) connected by wireless links that establish communication with each other. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably.

A MANET may operate in a standalone fashion, or may be connected to a corporate Intranet or the public Internet (see Figure 10-4). Due to the limited transmission range of wireless network interfaces, multiple hops may be needed to exchange data between nodes in a MANET. This is why MANETs are also known as "multi-hop networks."

[2] Many parts of this material are based on a presentation by Eva Kwan, Jason Poleski, and Eric Shoup.

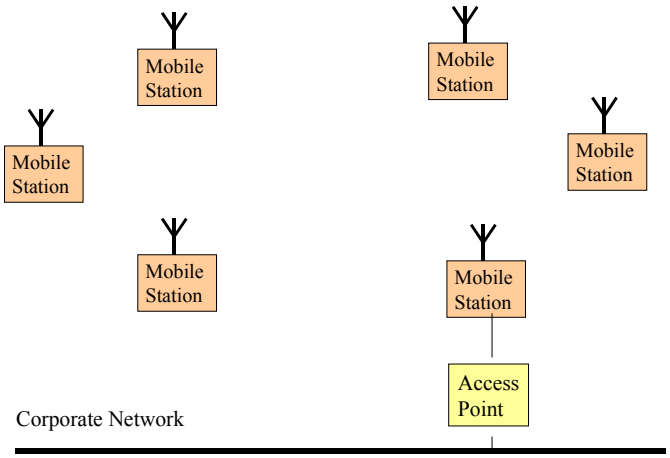


Figure 10-4: An Example of Mobile Ad Hoc Networks

Although several research and government projects have implemented MANETs, Bluetooth and Sun's Jini are the two main commercial examples. We have discussed Bluetooth in a previous chapter. Let us briefly look at Jini from Sun Microsystems. Jini is available for public use in commercial settings. For example, Jini could be used to dynamically provide access to a printer if a laptop moves into its range, and to allow 4G and 5G cellular phones to pass data directly from one to another without having to go to the BTSs or MTSOs. Jini is based on the standard Java technology and uses familiar networking technologies such as RMI (Remote Method Invocation) from Sun, CORBA from the Object Management Group (OMG), and SOAP from the Web Services initiative. Thus Jini can be quite flexible. Despite its flexibility, Jini has not been a great commercial success so far. For more details on Jini, see http://wwws.sun.com/software/jini/overview/index.html.

Is MANET a Wireless Sensor Network and Vice Versa?

MANET is a general concept that can be implemented in a wide variety of ways. A MANET can be formed, for example, between a PC and its attachments, between several laptops, or between sensors in a battlefield. Similarly, a wireless sensor network (WSN) is any wireless network configuration between various sensors. Although *most* WSNs use the MANET model, it is not necessary. A WSN may use a master/slave model, where a few sensors in a room may directly communicate with an access point instead of each other.

10.5.2 Examples of MANETs

Many examples of MANETs can be found in real life where an access point and existing infrastructure is not available. For example, battlefields and emergencies where no one has the time to establish access points are the prime examples of MANETs. Common examples of MANET are:

- Battlefield situations where each jeep and even each soldier's gun has a wireless card. These "nodes" form a MANET and communicate with each other in the battlefield. In addition, MANETs can be used to detect hostile movements in remote areas instead of

land mines (see the case study "MANETs as a Replacement for Land Mines" in Chapter 7).

- Emergency situations where, for example, a building has been destroyed due to fire, earthquake, or bombs. In such a case, it is important to set up a quick network. MANETs are ideal for such situations. For example, in emergency operations, police and fire fighters can communicate through a MANET and perform their operations without adequate wireless coverage.
- Group interactions such as communication setup in exhibitions, conferences, presentations, meetings, and lectures where the access points may not exist ahead of time. Group meetings are another example where different members of the team may want to communicate with each other in a different spot, such as a park on a nice day, instead of a pre-assigned conference room. Connecting cell phones to laptops and taxi cab networks are other examples of MANETs.
- Sensor devices may form a mobile ad hoc network of intelligent sensors (MANIS) for special situations. A MANIS can adapt to virtually any operational deployment due to the flexibility offered by the mobile ad hoc networks. We will look at sensor networks and MANIS in Section 10.6.

10.5.3 Key Characteristics of a MANET

It should be evident by now that MANETs are quite different from the traditional networks, wired or wireless. Figure 10-5 shows a typical MANET configuration where the mobile nodes A, B, C, D, and E form the ad hoc network. An Internet router can also participate in this network to pass information to a corporate site or a control center. The key characteristics of a MANET are:

- It does not require fixed infrastructure components such as access points or base stations. In a MANET, two or more devices are equipped with wireless communications and networking capability. Such devices can communicate with another node that is immediately within their radio range (peer-to-peer communication) or one that is outside their radio range by using intermediate node(s) to relay the packets from the source to the destination.
- It causes route changes, and sources may need to traverse multiple and different links to reach the destinations every time because all nodes may be moving. Due to this, the traditional routing protocols fail because they assume fixed network topology.
- It is self-organizing and adaptive. This means that a formed network can be formed on-the-fly without the need for any system administration. This allows rapid deployment of networks when needed and a quick teardown when not needed.
- It can consist of heterogeneous devices; i.e., the nodes can be of different types (PDAs, laptops, mobile phones, routers, printers, etc.) with different computation, storage and communication capabilities. The only requirement is that the basic MANET software has to be able to run in the devices.
- Power consumption can be high because nodes have to be kept alive to forward data packets sent by other nodes who just happen to be in the neighborhood. This especially presents a challenge to the tiny sensors that participate in MANETs.

There are several implications of these characteristics. First, the traditional Internet protocols do not work very well because the Internet assumes that its connectivity and topology would change only slowly over time. This is why Internet protocols are optimized for networks with reliable connectivity between nodes. In a MANET environment, the Internet protocols fail because they cannot handle the rapid fluctuations in connectivity among nodes. New routing protocols are needed for MANETs that can handle topology changes.

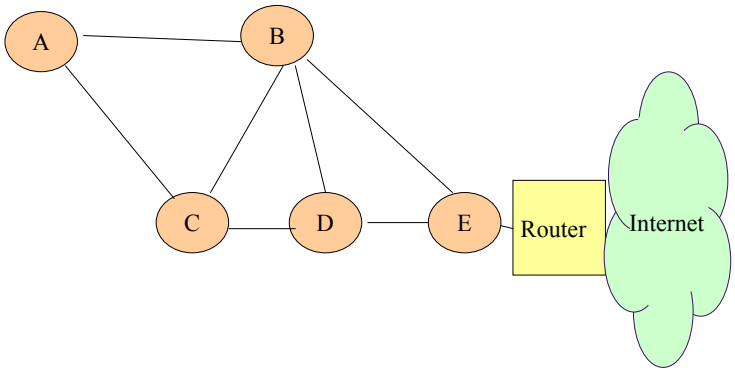


Figure 10-5: A Sample MANET Configuration

10.5.4 Advantages and Challenges of MANETs

A mobile ad hoc network has advantages over traditional wireless networks, including:

- Ease and speed of deployment – you can build a small, all-wireless LAN quickly.
- Minimum expenses because no expensive infrastructure is needed.
- A temporary fallback mechanism is there if normally-available infrastructure devices (access points or routers) stop functioning.

With these advantages, MANETs can support applications mentioned previously (military, emergency, discovery, group meetings, exhibitions, conferences, presentations, meetings, and lectures). However, MANETs present several challenges such as the following:

- Routing: As mentioned previously, the network topology changes randomly with time. Thus the routing protocol needs to update the routes and links frequently. Routing may also have to be adjusted to handle loss of radio links and mobile devices.
- Security: MANETs do not employ any centralized administration entity to enforce security and authenticate users. This means that any station within range can connect to other stations configured to allow ad hoc networking. If a station is connected to the corporate network and is configured to allow ad hoc networking, a hacker can attack the station and gain access to the network. All traffic from the hacker appears on the wired network as originating from the authorized station.
- Power Management: MANET nodes are powered with lightweight batteries. These batteries have limited battery life and thus impose restrictions on transmission range, communication activity and computational capabilities of these nodes.
- Selfish Nodes: Since power is at a premium, some nodes may become selfish and refuse to route packets of other nodes. Sophisticated measures are needed to detect and correct such situations. For example, selfish nodes may be "starved" by other nodes by refusing to route packets of the selfish nodes.
- Fault Tolerance and QoS: MANET has to provide fault tolerance and QoS guarantees under very trying situations. For example, varying physical link properties make it difficult to ensure that a minimum level of service is satisfied.

10.5.5 Protocols and Algorithms for Dynamics and Access Controls

MANETs must address issues of dynamic allocations and medium access control (MAC). MAC is common to all networks because all communications devices have to know who has access to the communications medium at any given time. Handling dynamics due to changing

associations and faults, however, is a key distinguishing feature between MANETs and other wireless networks.

10.5.5.1 Handling Dynamics in MANETs

Some of the key approaches used to support dynamic behavior in MANET (Gupta [1997], McDonald [1999], Pegani [1999]) include:

- **Dynamic Address Assignment**: This allows a node to recover from many faults by creating a new address that it can use to send or receive information. Thus a node assumes a new IP address if its current address is not operational or claimed by someone else, accidentally or maliciously. This, however, creates a possible denial-of-service vulnerability where a malicious node may claim to use all available IP addresses and thus stop traffic on a link.
- **On-Demand Routing:** Dynamic address assignment only deals with part of the communication problem. On-demand routing is needed in large ad hoc networks because they are typically created through a number of nodes acting as routers between the other nodes. In order to create connections through such a network, the network needs to construct routing tables dynamically, allowing nodes to initiate communication with nodes located in other subnets or to continue communication when a previously local node moves beyond local radio coverage. Due to the highly dynamic nature of ad hoc networks, it is not useful to maintain full up-to-date connectivity data in routing tables. Instead, new routes are acquired on demand – hence the name on-demand routing.
- **Dynamic Service Discovery**: This is similar to dynamic address assignment or dynamic route discovery but acts on a higher protocol. For example, new services become available as a new node with an extensive directory or a map moves into the neighborhood. The main benefits of dynamic service discovery is the ability to detect any new services as they become available and to utilize them effectively.
- **Behavior Adaptation:** This allows nodes to dynamically adapt their behavior by using patterns. These patterns represent certain behavioral roles (e.g., user, commander, network manager) by combining a small number of objects. Thus as a node detects a new situation calling for a new role, it can dynamically change its behavior by invoking objects that represent the new usage pattern.
- **Lease-Based Resource Management:** This approach allows a node to lease services on an as-needed basis. Once the lease expires, the node has to renew. Different leases can be used with different lease periods (ranging from a few minutes to days or months) for different situations. For example, a user's home directory may be on a longer lease than a map service that may be needed only for a certain period. Lease-based resource management allows the nodes to be more dynamic and efficient.

10.5.5.2 MAC (Medium Access Control) Protocols

MAC (Medium Access Control) schemes can be divided into two categories: scheduled (also called time-based) access and random (also called contention-based) access. Schedule-based algorithms reserve bandwidth for a node regardless of whether or not it has anything to send. This is well suited for periodic traffic (e.g., voice or video packets, which tend to be generated at regular intervals) but is inefficient for asynchronous traffic (when packets arrive at random). Random-access algorithms make no assignment of bandwidth, and each node seeks access only if it has something to send. These protocols tend to be better suited for asynchronous traffic, but cannot guarantee QoS agreements.

As we discussed in a previous chapter, the IEEE 802.11 working group has developed a MAC protocol that includes both scheduled and random components to accommodate asynchronous as well as periodic traffic. But it requires a central controlling authority to

allocate bandwidth. This central functionality is incompatible with the peer-to-peer model of a MANET. MAC protocols for a MANET should support scheduled as well as random access schemes but without any centralized control. This is currently work under progress.

10.5.6 Routing Protocols and Algorithms

10.5.6.1 Routing Principles

Routing algorithms, it is well known, determine the optimum path between senders and receivers based on specific metrics, such as shortest time delay or minimum cost (see Figure 10-6). Determination of optimal paths in large networks has been an area of active research for many years, with applications for travelling salesmen, school bus routing, flight routings and others. An important factor in routing algorithm design is the time T it takes to develop a solution. If T is more than the average time between topology changes, then the algorithm cannot update the routing table fast enough. For example, if the topology changes every 20 seconds but it takes a minute to find a route, then the routing tables will not have correct routing information and the whole routing system will collapse. This is the main challenge in MANET routing. In MANET, the Internet routing algorithms do not work well because they assume that the topology will change very infrequently, thus an optimal path can be found almost at leisure.

For mobile ad hoc networks, the core routing functionalities include:

- Path generation to generate possible paths between the senders and receivers
- Path selection to determine the appropriate paths based on a selection criterion (e.g., minimal time)
- Data forwarding to transmit user traffic along the selected paths
- Path maintenance to make sure that the selected route is maintained and to find alternates in case of problems

Due to the nature of MANETs, the routing protocols should be highly adaptive, fast, and energy/bandwidth efficient.

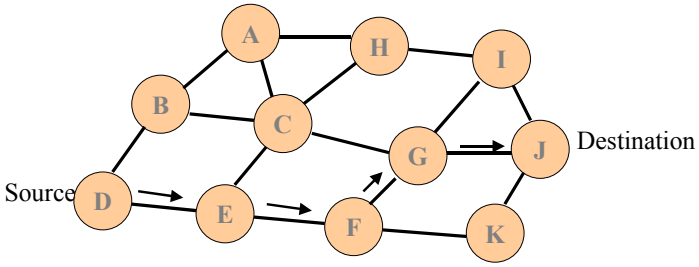


Figure 10-6: A Typical Routing Algorithm

10.5.6.2 MANET Routing Algorithms at a Glance

Many routing protocols for MANET have been published. Although there are different ways of classifying them, a convenient approach is to view them in terms of small or large networks. Let us mention a few.

For smaller networks, the following are well known:

- Dynamic Source Routing (DSR) uses a source (versus hop-by-hop) algorithm. Thus there is no need for intermediate nodes to maintain routing information. See Section 10.5.6.3 for additional discussion.
- Ad hoc On-Demand Distance Vector (AODV) combines DSR with sequence numbering and other features to make it more efficient.

- Optimized Link State Routing (OLSR) performs numerous optimizations on the AODV algorithm, including using subsets of the network instead of the entire network for many parts of the implementation.
- Topology-Based Reverse Path Forwarding (TBRPF) performs more optimizations in addition to OLSR, such as only reporting updates in the network state instead of all available nodes with every request.

For larger networks, the following algorithms are well known:

- Temporally-Ordered Routing Algorithm (TORA) uses routing on demand and reacts locally to topological changes to make it more suitable for larger networks. See Section 10.5.6.4 for additional information.
- Zone Routing Protocol (ZRP) gains efficiency by using the concept of a minimum spanning tree – the shortest connections between nodes in the network that still are able to cover the entire network.
- Landmark Router (LANMAR) uses a hierarchical structure in the layout of the MANET in order to transfer data between nodes more efficiently.

Additional information about these algorithms can be found at the following sources:

- http://www.ics.uci.edu/~atm/adhoc/paper-collection/papers.html
- http://www.ics.uci.edu/~atm/adhoc/paper-collection/johnson-dsr.pdf
- http://www.ee.iastate.edu/~russell/cpre537xf00/Projects/binlin.pdf

10.5.6.3 Dynamic Source Routing (DSR) – a Routing Algorithm for Smaller Networks

In this algorithm, packet headers include every node in the path. Thus when a node receives the packet, it checks if it is the final destination. If not, then it examines the next hop location and transmits the packet to that location. For efficiency, each node maintains a *route cache*, in which it caches the source routes it has learned. If routes are unknown or unavailable, then a *route discovery* algorithm is run to determine where the packet should go next. The packet is buffered until the next hop location is found.

10.5.6.4 Temporally-Ordered Routing Algorithm (TORA) for Larger Networks

DSR and its variants do not work well in large-scale networks because packet headers that include every node in the path become simply too large. TORA is designed to work with large-scale networks by using a totally different approach. Instead of carrying large packet headers, routes within the network are established by a series of query/reply messages that are sent across the network. The main feature of TORA is that when a link fails, the control messages are only propagated around the point of failure. Thus TORA can recover quickly by looking around the point of failure. In contrast, other protocols re-initiate a complete route discovery when a single link fails. This distinguishing feature allows TORA to scale up to larger networks. But TORA has higher overhead for smaller networks.

10.5.6.5 Approaches to Analyze MANET Algorithms

MANET algorithms can be analyzed by using a variety of factors. One approach concerns whether nodes should keep track of routes to all possible destinations, or instead keep track of only those destinations that are of immediate interest. As suggested by Eurocom, MANET routing algorithms fall into the following broad classes:[3]

[3] "Mobile Ad Hoc Networking & Computing at Eurecom," http://www.eurecom.fr/~nikaeinn/adhocNetworks/routing.htm

Flooding: A sender broadcasts data packets to all its neighbors. Then, each node receiving the data packets forwards this data packets to its neighbors, etc.

Proactive (Table Driven): These algorithms keep track of routes for all destinations in routing tables. Many Internet protocols use this approach because it is quite appropriate for a network with low mobility. Table-driven approaches are the first generation of routing in mobile ad hoc networks.

Reactive: These protocols acquire the routing information only when it is actually needed. These protocols save the overhead of maintaining route tables but suffer long operational delays because routes have to be determined frequently. Several MANET algorithms such as Dynamic Source Routing (DSR) and Temporally Ordered Routing Algorithm (TORA) use this approach. These are the second generation of MANET routing algorithms.

Hybrid. These algorithms partition the network into zones. The proactive approach is used within each zone to maintain routing information, and the reactive approach is used to route packets between different zones. These are the third generation of MANET routing protocols.

The following table highlights the plusses and minuses of these different approaches.

Table 10-6: Classes of MANET Routing Protocols (Source: Eurocom[4])

FLOODING	TABLE-DRIVEN	ON-DEMAND	HYBRID
+ Simplicity + Multiple path to the destination - High Overhead - Lower reliability of data delivery : Because of broadcast behavior of flooding ? Network properties : + Rate of topology changes increase - Number of communications increases - Number of nodes in the network increases	+ Delay of route determination decreases -Communication overhead increases -Storage requirements increases ? Network properties : + Number of communication increases - Rate of topology changes increases - Number of nodes in the network increases	+ Communication overhead decreases but it is subject to number of communications in the network - Not optimal bandwidth utilization - Delay of route determination increases ? Network properties : + Rate of topology changes increases - Number of communications increases - Number of nodes in the network increases	o Better trade-off between communication overhead and delay ? Network properties : o Rate of topology changes increases o Number of communications increases o Number of nodes in the network increases

10.5.7 Standardizing MANET

The Internet Engineering Task Force (IETF) established a Mobile Ad Hoc Networking (MANET) working group in June 1997. The primary focus of the working group is to develop MANET routing specifications and submit them to the Internet standards track. This working group is choosing and standardizing IP routing protocols suitable for MANET. The

[4] "Mobile Ad Hoc Networking & Computing at Eurecom," http://www.eurecom.fr/~nikaeinn/adhocNetworks/routing.htm

issues being considered in developing the routing protocols include the network size (the number of nodes connected), network connectivity (the average number of neighbors of a node), traffic patterns, link capacity, and performance characteristics. More information can be obtained from the IETF Website (http://www.ietf.org/html.charters/manet-charter.html).

Selected MANET References

Basagni S., Chlamtac, I., and Syrotiuk, V. R. "Dynamic Source Routing for Ad Hoc Networks Using the Global Positioning System." In *Proceedings of the IEEE Wireless Communications and Networking Conference 1999* (WCNC'99), New Orleans, LA, September 21-24, 1999.

Basagni S., Myers, A. D., and Syrotiuk, V. R. "Mobility-Independent Flooding for Real-Time, Multimedia Applications in Ad Hoc Networks." In *Proceedings of 1999 IEEE Emerging Technologies Symposium on Wireless Communications & Systems*, Richardson, TX, April 12-13, 1999.

Gupta, P. and Kumar, P. "A system and traffic dependent adaptive routing algorithm for ad hoc networks." In *Proceedings of the 36th IEEE Conference on Decision and Control*, San Diego, Dec. 1997, pp. 2375–2380.

McDonald, A. and Znati, T. "A Mobility-Based Framework for Adaptive Clustering in Wireless Ad-Hoc Networks." *IEEE Journal on Selected Areas in Communication* 17, no. 8 (August 1999).

Royer, E. and Toh, C. "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks" *IEEE Personal Communications Magazine*, April 1999, pp. 46-55.

10.6 Wireless Sensor Networks (WSNs) – A Closer Look[5]

10.6.1 A Quick Revisit

As stated in Chapter 7, WSNs typically consist of thousands of sensor motes interacting with each other in an ad hoc structure. If a sensor node, called a mote, captures some information, it will transfer this information to a chosen neighboring node until it gets to a node that is in the range of an access point (node E in Figure 10-7). The access point can then transfer this information to other interested parties through a corporate LAN, public Internet or any other network. This shuffling of messages does not have to involve and *should not* involve all nodes on the network, as shown in the diagram. This approach of involving only a few nodes in routing conserves energy of the individual motes (one of the major design considerations). In addition, transferring information to the access point can use shortest distance algorithms and shortest node-to-node distances to further conserve the energy of the communication system.

[5] This discussion is based on the presentation by M. Haq, B. Saleh, H. Abdullah, and G. Nandipati.

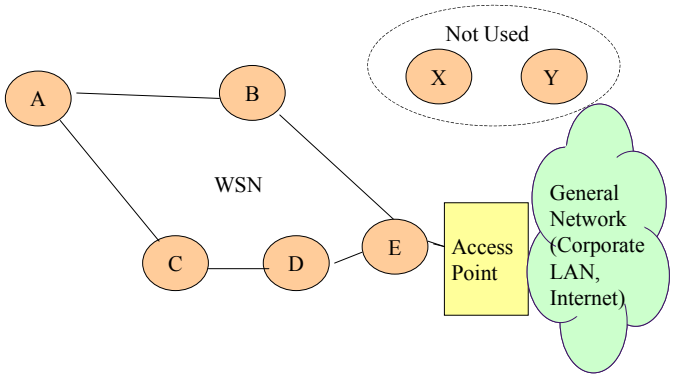


Figure 10-7: A Sample Wireless Sensor Network

The MANET (Mobile Ad hoc Network) model, discussed previously in this chapter, is a natural for WSNs because sensors tend to speak to each other directly without an access point. Although not all WSNs are MANETs, most are. In fact, MANIS (mobile ad hoc network of intelligent sensors) is an active area of work in sensors and ad hoc networks. Due to this large overlap, the concepts and algorithms developed for MANETs apply to WSNs. Thus many ideas presented in Section 10.5 are of value in the discussion that follows.

Major design considerations for WSN include minimizing power consumption to extend the useful life of the network, and working within the hardware/software constraints of the sensor nodes, such as CPU, RAM, operating system, location-finding system, antenna, power amplifier, modulation, etc. Environmental (e.g., in the battlefield, at home, in space, on the roads), and deployment (e.g., node replacement and/or maintenance) factors should also be considered. In addition, the typical goals of fault tolerance (failures should not severely degrade the overall performance of the network) and scalability (more nodes should be easy to add) need to be met. These design decisions have to be made at almost every layer of the protocol stack (from physical layer to application layer) shown in Figure 10-8. The major considerations and decisions at each layer of WSNs are discussed next.

10.6.2 Physical Layer Considerations

Frequency selection in WSN presents special issues. It is naturally desirable to operate in unregulated bands in the 900 MHz, 2.4 GHz, and 5.8 GHz ranges. Since many of the lower frequency ranges are highly congested, WSNs may have to operate at higher frequencies. But to operate at higher frequencies, the circuitry becomes more complex to handle higher bandwidths and perform intricate filtering. This is usually beyond the capability of motes. Operating at higher frequencies also requires the usage of more power.

For error detection and correction, sensor networks suffer from the same signal impairments as other wireless networks. In particular, scattering, reflection, diffraction and fading (discussed in Chapter 5) in WSNs are not dramatically different than other networks. The only difference is environmental, especially if a WSN is to operate in a battlefield or other harsh environment. In such environments, the errors and impairments are naturally amplified. In addition, modulation for signal encoding should also be simple for WSNs.

Many technologies for WSNs are being considered, but Bluetooth and UWB are the two prime contenders. Although Bluetooth can do the job, UWB appears to be more suited. As discussed previously, UWB technology provides high data rates for distances less than 10

meters. It is also attractive because of low power consumption and resistance to multipath propagation errors.

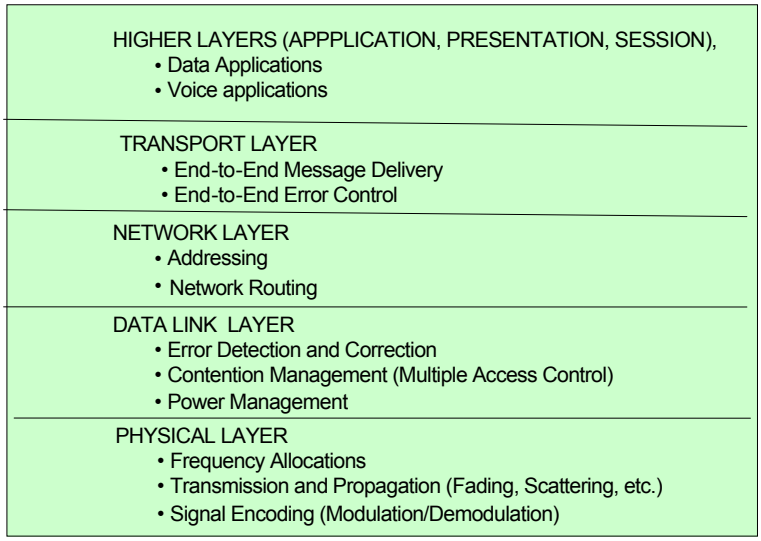


Figure 10-8: WSN Protocol Stack

10.6.3 Data Link Layer Considerations

The Data Link Layer is responsible for a variety of activities such as controlling access to the medium for all users, setting up a reliable system for transmission without collisions, and error control. This layer is actually further subdivided into two sub-layers: the Medium Access Control (MAC) and the Logical Link Control (LLC) Layer. In sensor networks, local network initiation and management are the main considerations for MAC. Because WSNs are based on mobile ad hoc networks, the individual sensors attempt to discover their neighbors and the "neighborhood topology" so that the neighbors can communicate with each other. However, keep in mind that the neighborhood could change, thus an efficient discovery/rediscovery process frequently takes place. Naturally efficient but simple algorithms are needed.

For power savings, it is a good idea to keep only two states: on (transmitting/receiving) and off (not transmitting/receiving). But what exactly is "off"? It is not a good idea, in fact, to turn off each device because to turn the device back on takes considerable power. It is better to put the device in sleep mode, so that at can be "woken up" when needed. This implies that the data link layer broadcasts a "wake up" signal to all sleeping nodes. Once awake, the nodes enter the communication mode (on) and can discover the neighbors and send/receive data. Thus most motes have three states: on, off, and sleep.

To handle errors, the messages can be retransmitted using an ARQ (Automated Repeat Request) protocol and corrected by using an FEC (Forward Error Correction) Algorithm. ARQ is simple to implement but is not desirable in WSNs because it can waste time re-transmitting the same message again and again. FEC is desirable but in FEC, as discussed in Chapter 5, redundancy bits are added to improve recovery, and sophisticated algorithms are used for recovery. For sensor networks, it is best to first look at the channel conditions and then make the best decision on whether to use FEC, ARQ, or a combination. For example, in

a highly error-prone environment, the mote could rely heavily on FEC and minimize the use of ARQ.

10.6.4 Network Layer Considerations

The network layer deals with addressing and routing of packets. Although IP-based routing is used commonly in most networks, it is not used in WSNs for two reasons: a) motes are not IP addressable because they do not have IP addresses, and b) MANETs require different protocols than IP. In WSNs, a sending node has to know who to send the packet to so that ultimately it reaches its destination. The routing algorithms and protocols discussed in MANETs can be used in WSNs. The main consideration is that WSNs have many nodes, thus algorithms designed for large MANETs are more suitable. In particular, algorithms such as TORA (Temporally-Ordered Routing Algorithm) are valuable for MANETs because they react locally to topological changes. In addition, Delayed Tolerant Networking (DTN), discussed as part of Deep Space Communications (Chapter 9) has some applications in WSNs (see the sidebar, "Using Delayed Tolerant Networking in Wireless Sensor Networks").

A specific method for routing information is SPIN (Sensor Protocol for Information via Negotiation). In this system, the sensor nodes minimize traffic by sending a small packet which advertises about the nature of the data. If the destination node is interested, it sends back a request for the specific data that it wants. The sensor node then sends the requested data.

Using Delayed Tolerant Networking (DTN) in Wireless Sensor Networks

WSNs typically comprise a large collection of primitive sensor devices interspersed with a smaller collection of more capable nodes, all interconnected by some form of wireless communications. Such devices benefit directly from the ability to offload their end-to-end communications to more capable partners and thus extend their operational lifetime by minimizing their interactions. The DTN architecture and protocols, developed as part of the Deep Space Communications (see Chapter 9), are well suited to these kinds of communication restrictions. In particular, by using a store-forward model, data can incrementally move towards the destination, with custody progressing forward along a series of relay hops. This avoids the need to establish an end-to-end path for reliable transmission and consequently saves the power resources of the network.

10.6.5 Transport Layer Considerations

The Transport Layer is responsible for end-to-end error recovery and control flow and makes sure that the packets arrive in the correct order and error-free. Traditional TCP does not work very well for WSNs because the same level of reliability is not needed in a network consisting of many sensor nodes when many of the nodes are sending the same information. In addition, there are many more senders (sensors) and fewer receivers (sinks such as access points) as compared to the typical TCP/IP networks. Once again, WSN transport layer protocol should take into consideration energy constraints and transmission times.

A few specialized transport layer protocols are suitable in this area. For example, according to the PSFQ (pump slowly, fetch quickly) protocol, the sensor nodes send (pump) packets

slowly to other nodes. If a receiver detects packet loss, it quickly "fetches" data from neighboring nodes. This protocol works well for sensor-to-sensor delivery and end-to-end reliability but is weak in terms of congestion control. Another example is the Event-to-Sink Reliable Transport (ESRT) protocol, that has many features including self-configuration, congestion control and collective identification. It takes into account energy usage optimization and operates more from the sink than the sensor side.

10.6.6 Application Layer Considerations

Many factors have to be considered at the application layer. The main consideration is that since sensors cannot store large programs, simple applications have to be used. Thus sophisticated applications cannot be used. A specialized application layer protocol is SMP (Sensor Management Protocol) that controls the various modes such as ON, OFF, and SLEEP. It also controls the movement of the sensor if it has those capabilities. The location-finding algorithms, compression, and security features are also controlled by this sensor management protocol.

The application layer also includes the advertisements and the algorithms used to extract important information from the sensors, because such information is application-dependent. For example, a temperature control application would only advertise and extract temperature fluctuations and ignore everything else. This is important, because one sensor node may collect data that may be of value to multiple applications.

10.6.7 Location Services in WSNs

Sensors are deployed at different locations to measure characteristics of the environment, so each sensor's position is crucial in making sense of the data being collected. The location of a sensor in a sensor network acts as an identity because the best way to identify an object is its location. This property becomes especially useful when the number of networked nodes is extremely high, which is often the case in sensor networks. With knowledge of each other's positions, and the ability to communicate with each other, a coherent picture of the information collected can be made. With all the nodes of the network knowing where they are, efficient and reliable data collecting can be done. Location services are essential in developing efficient routing algorithms. Due to the limited processing power available, designers must ensure that nodes only perform computation that is essential. Often, the low power nodes of sensor networks have limited range in communication. This can be solved through efficient routing algorithms that take advantage of the knowledge of each node's position.

We have discussed various location techniques (Cell ID-based, assisted GPS, angle of arrival, time of arrival, estimated signal strength, etc.) in Chapter 5. Many of these techniques, especially the ones that need added capabilities at the mobile devices, are not suitable for WSNs. Thus, AGPS is not adequate. The following are specialized considerations for location-based services for WSNs:

- The ability of the sensor nodes to perform complicated position location computation is limited. The primary purpose of the nodes is to collect the data that it was set out to collect; thus most of the power of a device should not be directed towards finding its position. Enough energy must remain in order for the sensor to perform its task. The hardware attached to sensors for position determination must be small because the sensors that collect data describing their environment are small. The sensor network has

to be tolerant to node failure and be able to still determine position in case of node failures.

- UWB signals can be used for time of arrival (TOA) purposes and can be highly reliable. However, UWB hardware is very expensive; but the field is still evolving. Infrared sensing is another possibility for sensor location services. The system locates users who each wear a badge that emits a globally unique identifier approximately every 10 seconds or on demand. Infrared sensors receive the data and send it to a central server that aggregates and calculates the position of the sensor. This system can only determine a position of a person within rooms and also has difficulty in environments with fluorescent light or sunlight because of the infrared signals that these sources create. Ultrasonic positioning techniques also offer some promise in short distance environments. These systems use time-of-flight measurements from various ultrasonic sensors to ultrasonic receivers. An accuracy of approximately 9 centimeters has been achieved, which is accurate enough for most location awareness in sensor networks.
- The Long Range Navigation Position Location (LORAN) system uses terrestrial pulses from up to five ground stations to send pulses to a user. The system then determines the time difference of arrival to compute position. The system emits a pulse with a carrier frequency of 100 kHz to transmit the ground signal. The accuracy is 100 feet.

10.6.8 Data Management in WSNs

Data management is important because the goal of sensor networks is to gather data and transfer it to each other or some central identity that will actually use this data. It is difficult for sensor nodes to store the data they collect. Hence they try to distribute the work among the nodes. However, distributed computing with data synchronization among many nodes is a non-trivial task. For practical reasons, the nodes are subdivided into a hierarchy – nodes that mainly collect data, nodes that that route network traffic, and nodes whose locations are used as reference for the rest of the network nodes. Different schemes can be used:

- Local storage schemes which use the data storage capacity of each node. The nodes capture information as it becomes available, store it temporarily, and then transmit it when the communication data links are relatively free. This schemes requires more storage capacity at each node but is efficient in terms of communication because it is needed only when sufficient data has been accumulated.
- External storage schemes which use a computer outside of the sensor network to store all the relevant data. The advantage of such a scheme is that sensors do not need great capacity for data storage. However, the disadvantage is intense communication burden on nodes handling communication to and from the data server. Since the nodes are not assumed to have adequate storage capacity, all the data must be transmitted as soon as it is collected. This is inefficient, slow, and leads to loss of data that could not be transmitted.
- Data-centric schemes solve some of the problems associated with the previous two schemes. Nodes are grouped together based on the events and type of data they are supposed to record. Each group of nodes has an elected home node that handles communication with other groups of nodes. With home nodes gathering data from neighboring nodes, the home nodes can gather the important data and eliminate the redundant data that may exist. Also, the communication burden of the nodes is less than with the previous schemes. Only relevant and non-redundant data is transmitted over long distances, easing the communication burden of all nodes, especially those topologically close to the system that is polling the network for data.

In all these schemes, reduction of communication traffic is a common issue. One way to reduce the communication burden of the network is through data compression. Efficient routing algorithms to take advantage of the location services that are built into the sensors can also make the process computationally less intense. More efficient storage methods would allow more data to be stored on the individual sensors to allow them to transmit data less frequently. Finally, in order to make the data collected accessible to outside parties, an SQL database interface allows a variety of applications to have quick and straightforward access.

10.6.9 WSN Security

Security of wireless sensor networks is important for several reasons. First, many sensor applications record and report sensitive data, especially in military and surveillance applications. Secondly, wireless sensor networks broadcast the information that is not encrypted. Thus others can possibly listen to data by using antennas. Finally, the WSNs are vulnerable to active attacks which include replay attacks and denial of service.

We will discuss wireless security extensively in a later chapter. Security of a system, WSN or any other, needs to support the following main requirements:

- Privacy: Allows communicating parties to ensure confidentiality. Privacy is obtained through symmetric and asymmetric cryptographic techniques.
- Integrity: Ensures that messages have not been altered (intentionally or unintentionally) in transit. Integrity is implemented by using hashes such as MD5 or SHA.
- Authentication: Assures that the users are who they say they are. This is typically enforced through ID and password or other identification schemes such as fingertips.
- Authorization: Allows only authorized and authenticated entities to perform certain operations. This is usually accomplished through ACLs (authorization control lists).

A secure system with proper inclusion of privacy, integrity, authentication, and authorization controls can withstand attacks that may range from snooping to complete destruction, especially in the battlefield situations. Existing security solutions such as cryptography and key management were designed for relatively powerful machines with enough resources for intensive calculations. These solutions do not work well in WSN environments and, once again, it is difficult to build a sophisticated security system around WSNs due to the limitations of battery power, computational capabilities, and communication aspects of WSNs. In addition, the mobility of nodes adds another constraint for wireless sensor networks due to their dynamic nature.

Extensive work has not been done in this area. One of the available solutions is SNEP (Sensor Network Encryption Protocol) that provides data confidentiality, two-party data authentication, integrity, and freshness. SNEP has low communication overheard, has a counter value that is kept at communicating parties, and also provides data authentication. Another scheme, called μTESLA, provides authentication for data broadcast. μTESLA overcomes the problem of needing asymmetric encryption (which requires a large computational overhead) by introducing asymmetry through a delayed disclosure of symmetric keys, which results in an efficient broadcast authentication scheme.

We will revisit WSN security in Chapter 12 when we discuss the general wireless security issues.

WSN Sources of Information

Akyildiz, I., et al. "A Survey of Sensor Networks." *IEEE Communication Magazine*, August,

2002.

Callaway, E. *Wireless Sensor Networks: Architectures and Protocols*. CRC Press, August 2003.

Communications of the ACM (CACM), June 2004, Special Issue on Wireless Sensor Networks.

Kahn, J., et al. "Next Century Challenges: Mobile Networking for "Smart Dust." In *International Conference on Mobile Computing and Networks* (MOBICOM), 1999.

Krishnamachari, K. "A Wireless Sensor Networks Bibliography." *Autonomous Networks Research Group*, Univ. of Southern California, Spring 2004, http://ceng.usc.edu/~bkrishna/teaching/SensorNetBib.html

Li, X., Wan, P. and Frieder, O. "Coverage in wireless ad hoc sensor networks." *IEEE Transactions on Computers* 52 , Issue 6, (June 2003).

Mainwaring, A., et al. "Wireless Sensor Networks for Habitat Monitoring," *WSNA'02,* Atlanta, Georgia, September 28, 2002.

Meguerdichian, S., et al. "Localized Algorithms In Wireless Ad-Hoc Networks: Location Discovery and Sensor Exposure." *MobiHOC'01*, Long Beach, CA, USA. October 04 – 05, 2001.

Perrig, A., Stankovic, J., and Wagner, D., "Security in Wireless Sensor Networks", Comm. ACM, June 2004, pp. 53-57.

Pottie, G. and Kaiser, W. "Wireless Integrated Network Sensors." *Comm. of the ACM* 43, no. 5, (May 2000), pp. 51-58.

Savarese, C., et al. "Locationing in Distributed Ad-Hoc Wireless Sensor Networks." ICASSP, May 2001.

Slijepcevic, S., et al. "On Communication Security in Wireless Ad-Hoc Sensor Networks." IEEE Eleventh International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE-2002), Pittsburgh, Pennsylvania, USA. June 10-12, 2002.

Sohrabi, K., et al. "Protocols for Self-Organization of a Wireless Sensor Network." *IEEE Personal Communications* 7, no. 5 (Oct. 2000).

Zhao, F. and Guibas, L. *Wireless Sensor Networks : An Information Processing Approach.* Morgan Kaufmann, May 2004.

Zhou, L. and Haas, Z. "Securing Ad Hoc Networks." *IEEE Networks* Special Issue on Network Security, November/December, 1999.

Time to Take a Break
- ✓ Powerline Networks, UWB, and FSO
- ✓ MANETs and Wireless Sensor Networks
- Flash OFDM and Synthesis

10.7 Flash OFDM

10.7.1 Overview

There is a great deal of debate about the future of 3G cellular networks. As discussed in a previous chapter, many existing wireless operators are investing in 3G cellular networks, while other operators appear to be content with 2.5G technologies. Some feel that 3G by itself is not enough. The main problem with 3G cellular technologies is that the longer it takes to actually offer these services to consumers, the more potential 3G users are looking elsewhere for broadband wireless network access.

One of the most attractive alternatives to 3G cellular is Flash OFDM (Orthogonal Frequency Division Multiplexing), also known as radio-router technology. Flash OFDM is a packet-switched radio access network that seamlessly transports IP services over the air from an IP network to a mobile user device. Currently being developed by Flarion Technologies (http://www.flarion.com) Flash OFDM provides an IP-based architecture that is designed to deliver around 1.5 Mbps link layer for wide-area mobile data traffic. It comprises an air interface design that integrates layers one through three of the OSI model.

The foundation of this technology is OFDM, an improvement over the classical FDM technology. In OFDM, a single channel is divided into multiple sub-channels, each having a different frequency. This allows multiple simultaneous transmissions, effectively increasing the bandwidth of the system (we discussed OFDM in Chapter 6). The Flash OFDM scheme builds on top of OFDM lower-layer implementation. The layers three and above of the OSI model are entirely IP-based in Flash OFDM.

The main advantage of Flash OFDM is that common commercially available IP infrastructure equipment may be used to connect the network directly into the Internet. This reduces the technology risk and total cost of deployment. The key ideas are summarized here.

10.7.2 OFDM Technology

Due to its overall approach, flash OFDM technology provides the user with broadband data rates of 1.5 Mbps (with peak data rates of 3 Mbps) and the mobility of a traditional cellular network. Figure 10-9 shows the overall architecture of flash OFDM. It can be seen that the architecture is quite simple. The Radio Router base stations provided by flash OFDM connect to the edge routers in the managed IP network through any standard IP technology. These routers are then connected to the public Internet and also to the back-end systems. The physical data stream is secured using a 128-bit encryption scheme before transmission at the air interface. The flash OFDM network also provides an interface to the authentication,

authorization, and accounting (AAA) system that enables many key revenue streams and business models for wireless network operators.

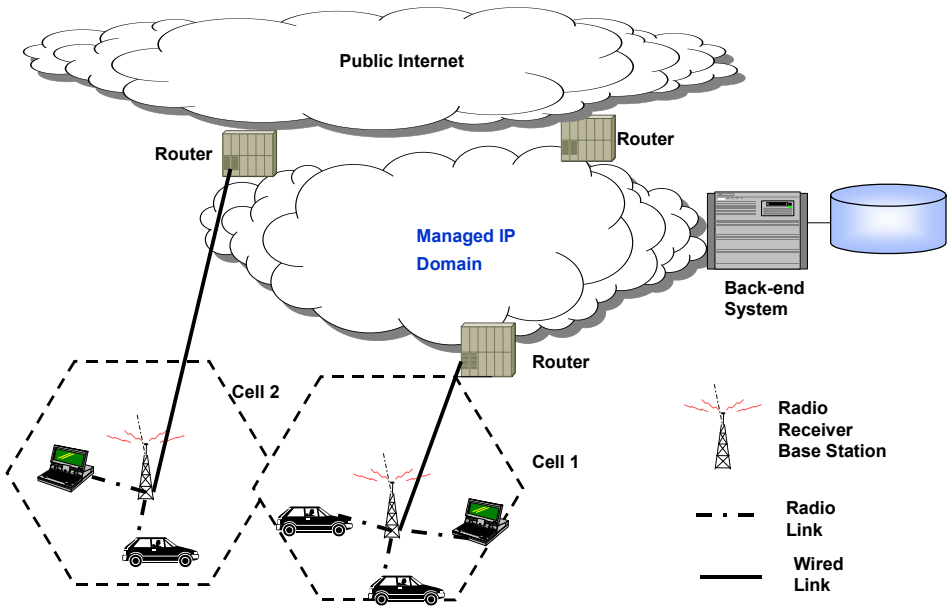


Figure 10-9: Flash OFDM Architecture

At the physical layer level, the key to the Flash OFDM design lies in its ability to reliably support data traffic with low delays over native IP networks. Basically, OFDM allows a mobile device to power up, transmit a single bit (such as a NAK or ACK), and quickly power down. This is possible because, in OFDM, a single channel is divided into multiple sub-channels, each having a different frequency. Thus each bit can be sent on a different channel. This is a major improvement over alternative networks that must wait to accumulate many control bits or until a control signal can be piggybacked with a data signal, due to the large overhead associated with transmitting a single bit. For example, in a typical TDMA link, the transmission of a single bit of data requires a minimum frame size of a few hundred bits to be transmitted. In 3G cellular systems, significant resources are wasted when merely initiating a data transmission. With flash OFDM, typical delays of between 5 and 15 ms are possible. This avoids the TCP timeout problem in 3G cellular networks because in many cases, the *latency in a Flash OFDM system is so small that TCP thinks it is operating over a wired network*. Flarion has also developed a proprietary forward error correction (FEC) scheme to maximize the reliability of the wireless broadband network.

At the Media Access Control (MAC) layer level, the Flash OFDM MAC layer supports varied QoS and SLA (service layer agreement) performance criteria. Basically, the Flash OFDM MAC layer retains the knowledge of IP packet boundaries and uses this knowledge so resource allocation decisions are made quickly and efficiently. Delays are kept to a minimum to allow Flash OFDM to seamlessly interact with existing TCP/IP networks and to support interactive services such as VoIP. In 3G cellular systems the latency is so large that the base station may get only one opportunity to transmit a given frame of data within a usable delay. The flash OFDM system takes advantage of the low-latency MAC layer and uses an aggressive FEC, knowing that there will be several opportunities for the base station to re-transmit the frame within the bounds of the same usable delay.

At the network layer level, Flash OFDM networks support statistical multiplexing of users through an IP-based, packet-switched broadband wireless network. The Flash OFDM network architecture utilizes standard devices (routers, switches, firewalls, gateways, and billing and provisioning servers) that may be found in any wired IP network. This provides a seamless transition between wireless air interface and existing IP networks. As was shown in Figure 10-9, the Flash OFDM Radio Router base stations connect to the edge routers in the core IP network through any standard IP backhaul technology. A benefit of flash OFDM network implementation is that autonomous Radio Router base stations can easily overlay existing cell sites and spectrum [Kennedy 2002]. The network also supports mobility and QoS.

10.7.3 Flash OFDM Technology – A Closer Look

Figure 10-10 shows a more detailed view of the flash OFDM architecture. The key architectural players are the Radio Routers that act as base stations in the flash OFDM architecture, the IP routers that move the IP traffic, and the media gateways that convert IP to PSTN traffic.

Flash OFDM architecture uses Mobile IPv6 to control handoffs. During handoffs, Radio Routers are used to maintain continuous connections with a mobile user. Handoffs between a public and private network are also handled at the IP level. As discussed in a previous chapter, Mobile IP uses home agents and foreign agents to move traffic to a mobile device. Figure 10-10 shows a sample situation where a Mobile unit A moves from a home network to a foreign network. Suppose a user in cell1 wants to send a message to Node A. In this case, the home agent intercepts packets sent to the mobile node A's home address and redirects them to the care-of address of the foreign agent, from where it is sent to the mobile node A. The mobile node always transmits packets directly to the origin node in cell 1. A performance improvement has been made in this system – once the node in cell 1 learns the mobile node's care-of address, it sends packets directly to the mobile node rather than going through the mobile node's home agent.

In addition to handoffs, the Radio Routers enforce authentication, authorization, and accounting (AAA) at the IP level. VoIP between the mobile device and the PSTN is also supported through the Radio Routers. Flash OFDM also supports mobility between different types of wireless technologies (cellular networks to IEEE 802.11 LANs, for example) at the IP level. The Flash OFDM link layer is designed to enforce QoS agreements.

10.7.4 Concluding Comments about Flash OFDM

Flash-OFDM provides high-speed mobile user access over the Internet. Mobile IP is used for handoffs between various types of technologies and users. The delay performance of the underlying Flash OFDM network has been optimized through several improvements to offer more users higher data rates with less latency than competing 3G cellular systems. Additional details can be found at the Flarion Technologies website – http://www.flarion.com.

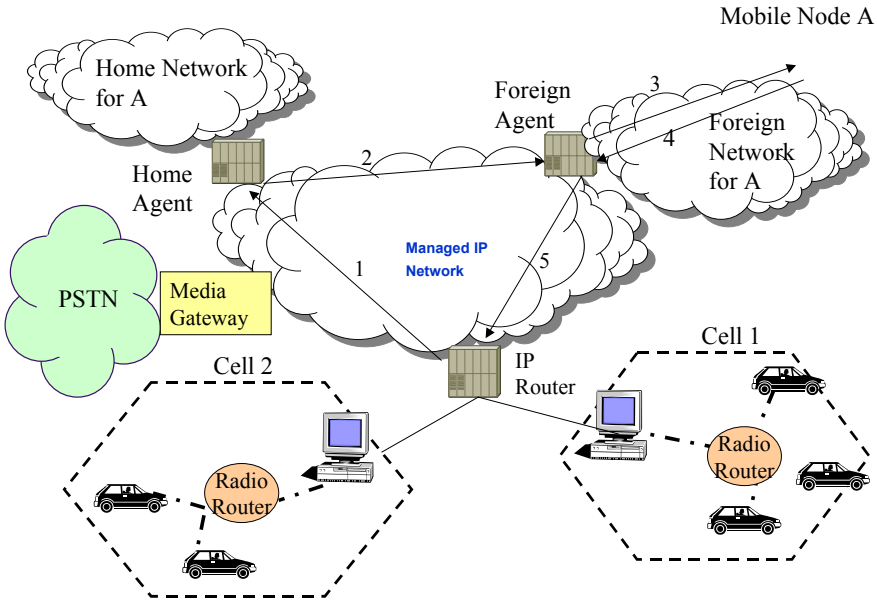


Figure 10-10: Flash OFDM Architecture

References for Flarion Flash OFDM

Flarion Technologies website – http://www.flarion.com

Bae, K., Alam, F., and Mostafa, R. "3G – Around the World and Back Again." *RF Design*, Feburary 2002, pp 52-66.

Corson, M. Scott, Laroia, R., O'Neill, A., et al. "A New Paradigm for IP-Based Cellular Networks." *IT Professional*, November-December 2001, pp 20-29.

The International Engineering Consortium website – http://www.iec.org

Dornan, A. "Mobile Broadband for the Masses?" *Network Magazine*, Jan 7, 2002.

Kennedy, C.J. "The Truth About 3G." *Unstrung*, Feburary 8, 2002.

Corson, M. Scott, Macker, Joseph P., and Park, Vincent D. "Mobile and Wireless Internet Services: Putting the Pieces Together." *IEEE Communications Magazine*. June 2001, pp 148-155.

Additional Reference Websites

http://nms.lcs.mit.edu/~haril/papers/CS294/paper/paper.html
http://www.redherring.com/mag/issue/issue101/1430019743.html
http://www-106.ibm.com/developerworks/library/wi-what2/?dwzone=wireless
http://www.shortcliffcommunications.com/magazine/volume.asp?vol=8&story=42

10.8 Synthesis of Wireless Network Alternatives

Let us conclude this chapter by considering the general problems faced by wireless communications, and the current trends in wireless communications. Suppose you wanted to send large volumes of data, very far and very fast, to highly mobile users. It is virtually impossible to find such solutions – you have to give up one or more attributes for the others to improve. Improvements in one aspect of wireless communications (such as data rates) come with a tradeoff in some other aspect (such as distance and user mobility). A good example is cellular technology. In cellular networks, higher data rates can be obtained if the users are not very mobile. For example, 3G cellular networks can deliver up to 2 Mbps for a user who is not moving, but can only promise around 200 Kbps for users driving around at 100 kilometers per hour. Similarly, cells cover distances of 100 to 10,000 meters. As discussed previously, cell sizes are reduced to allow spectrum reuse and to increase the number of users served. But as the cell size is reduced, the number of handoffs between cells go up, thus slowing down the data rates. Similarly, data can be transferred at high data rates in WLLs, but then the subscriber is assumed to be stationary. However, if the subscriber is stationary, then fiber optic cables provide much higher data rates than WLLs. Thus the tradeoffs go on.

We have discussed a wide range of wireless network technologies, ranging from short range networks such as Bluetooth and UWB to deep space satellites that communicate over more than a million miles. New technologies are also being introduced and the existing technologies are being refined and improved on an ongoing basis. Although these developments can be compared and contrasted in a variety of ways, data rates and the distance covered are the two main evaluating factors. Another factor is the level of user mobility needed (e.g., no mobility, low mobility such as walking speed, or high mobility such as driving in a car). The radio frequency in which a particular wireless network operates is another important factor. We have used these factors throughout this part of the book to capture the highlights of available wireless network technologies.

Table 10-7 summarizes the characteristics of the available wireless network solutions in terms of the four factors: data rates, distance covered, user mobility, and frequency used. It can be seen from this table that several technologies compete with each other directly or indirectly. This table can be used to decide what technology to use under what situation.

Table 10-7: Wireless Technologies Alternatives

	Data Rate (Mbps)	Approximate Range (meters)	User Mobility	Radio Frequency (GHz)
Bluetooth	1 Mbps	10 meters	Very Low (moving within a room)	2.4 GHz
UWB	50 Mbps	<10 meters	Very Low (moving within a room)	7.5 GHz
IEEE 802.11a	Up to 54 Mbps	<50 meters	Low (walking speed within a building)	5 GHz (802.11a)
IEEE 802.11b	11 Mbps	100 meters	Low (walking speed within a building)	2.4 GHz
IEEE 802.11g	Up to 54 Mbps	100 meters	Low (walking speed within a building)	2.4 GHz
HiperLAN/2	Up to, 54	30 meters	Low (walking speed within a building)	5 GHz
GSM	9.6 Kbps	Cell sizes 10 to 20	Medium to High (driving	Around 900 MHz

		km	speed within a building)	
3G Cellular	Up to 2 Mbps	Cell sizes 5 to 10 km	High (driving speed within a building)	Between 1 GHz and 2 GHz
WLL (LMDS)	up to 37 Mbps	2 to 4 KM	None (fixed wireless, receivers are houses/buildings)	Between 10 GHz and 100 GHz
FSO	100 Mbps to 2.5 Gbps	1 to 2 kilometers	None (fixed wireless, receivers are houses/buildings)	terahertz spectrum
Satellites	64 Kbps	thousands of miles	None (the dishes do not track the highly mobile satellites)	3 to 30 GHz

10.9 Review Questions and Exercises

1) What are powerline communication (PLC) networks and why are they considered as wireless networks? What are the main competitors to PLCs?

2) What are the unique features of Ultra Wideband (UWB) networks and what are their main competitors?

3) What are the unique features of Free Space Optics (FSO) and what are their main competitors?

4) What are MANETs and what are the main algorithms used in MANETs? In what situations would MANETs be used?

5) What is Flash OFDM and how does it compare and contrast with the 3G cellular networks?

6) Expand Table 10-7 to include two more columns: typical applications and standards.

10.10 References

Aiello, R., et al. "Understanding UWB – Principles and Implications for Low-Power Communications – A Tutorial." Available at: http://www.discretetime.com/papers/03157r0P802-15_WG-Understanding_UWB_For_Low-Power_Communications-A_Tutorial.pdf

Bae, K.K., Alam, F., and Mostafa, R. "3G – Around the World and Back Again." *RF Design,* 2002 Feburary, pp 52-66.

Basagni S. "Distributed and Mobility-Adaptive Clustering for Multimedia Support in Multi-Hop Wireless Networks." In *Proceedings of the IEEE Vehicular Technology Conference (VTC),* 1999. Amsterdam, The Netherlands, September 19-22, 1999.

Blankenhorn, D. "Ultra Wideband." *Mobile Radio Technology*, 1 January 2003. Available at http://iwce-mrt.com/ar/radio_ultra_wideband/

Callaway, E. *Wireless Sensor Networks: Architectures and Protocols*. CRC Press, August 2003.

Corson, M., Laroia, R., O'Neill, A., et al. "A New Paradigm for IP-Based Cellular Networks." *IT Professional*, November-December 2001, pp 20-29.

Corson, M., Macker, J., and Park, V. "Mobile and Wireless Internet Services: Putting the Pieces Together." *IEEE Communications Magazine,* 2001 June, pp 148-155.

Dornan, A. "Mobile Broadband for the Masses?" *Network Magazine*, January, 7, 2002.

Gupta, P., and Kumar, P.R. "A system and traffic dependent adaptive routing algorithm for ad hoc networks." In *Proceedings of the 36th IEEE Conference on Decision and Control*, San Diego, Dec. 1997, pp. 2375–2380.

Haas, Z.J. and Liang, B. "Ad-Hoc Mobility Management with Randomized Database Groups." *IEEE ICC'99*, Vancouver, BC, Canada, June 6-10, 1999.

Haas, Z.J. and Liang, B. "Ad Hoc Location Management Using Quorum Systems." *ACM/IEEE Transactions on Networking*, April 1999.

Kennedy, C.J. "The Truth About 3G." *Unstrung*, Feburary 8, 2002.

McDonald, B., and Znati, T. "A Mobility-Based Framework for Adaptive Clustering in Wireless Ad-Hoc Networks." *IEEE Journal on Selected Areas in Communication* 17, no. 8 (August 1999).

Pagani, E. *Providing Reliable and Fault Tolerant Broadcast Delivery in Mobile Ad-Hoc Networks*. Kluwer, 1999

Perkins, C. and Royer, E. "Ad-hoc On-Demand Distance Vector Routing." In *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications,* New Orleans, LA, February 1999, pp. 90-100.

Rappaport, T. *Wireless Communications: Principles & Practice*. Prentice Hall, 1996, pp. 139-192.

Zhao, F. and Guibas, L. *Wireless Sensor Networks : An Information Processing Approach*. Morgan Kaufmann, May 2004.