CHAPTER 2

OFF-THE-SHELF ENABLERS OF AD HOC NETWORKS

GERGELY V. ZÁRUBA and SAJAL K. DAS

2.1 INTRODUCTION

Today, when ad hoc networking professionals or would-be professional talk about ad hoc networks, they almost always implicitly assume that these networks are based on one of the wireless local area network (WLAN) technologies. The majority of research papers published on simulation-based performance evaluation of proposed ad hoc routing protocols assume underlying WLAN medium access control (MAC) and physical (PHY) layers. Most recently, with the appearance of short-range wireless personal area networking (WPAN) technologies, researchers also started to use the characteristics of these technologies as a basis for underlying transport assumptions to evaluate their novel network (or higher-) layer protocols.

It is extremely important to point out, that WLANs and WPANs are significantly different from ad hoc networks. Ad hoc networks have received their name due to the fact that there is no predefined structure or infrastructure of communication over which they should be established, but they consist of nodes that relay information to their neighbors possibly on behalf of other neighbors. Ad hoc networks are often called wireless multihop networks due to the fact that most packets will have to be relayed by several nodes before they reach their destinations. WLANs, on the other hand, are based on infrastructure—just like cellular networks—where there are dedicated access points (likely connected to the wired infrastructure) controlling their entire transmission range, namely their wireless domain. WLANs are considered single-hop networks, since all nodes attached to the access point talk to only the access point, which is the only entity equipped with a routing function. Fortunately, as outlined in the next subsection, the histories and requirements for ad hoc and

Ad Hoc Networking. Edited by Basagni, Conti, Giordano, and Stojmenovic.
ISBN 0-471-373133 © 2004 Institute of Electrical and Electronics Engineers

WLAN/WPAN technologies are converging, and most (if not all) technologies defined for WLANs/WPANs are extended to be employable as the basis for ad hoc networking.

2.1.1 The Converging History of Ad Hoc Networks and WLANs

The idea of both WLANs and ad hoc networks date back to approximately the same time, the early 1970s. Although the main driving force behind ad hoc networks was the need for survivable, infrastructureless and hard-to-detect military applications, WLANs received a lot of attention from academia and companies interested in commercial deployment.

In 1972, the Department of Defense (DoD) initiated a new program on Packet Radio Networks (PRNET) with the intention to create technologies for the battlefield that do not need a previously deployed infrastructure but are highly survivable even when some of the radios fail or are destroyed. The medium-access technology employed was a slightly modified version of the ALOHA protocol developed two years earlier in academia to interconnect the computing infrastructure over four Hawaiian islands with eight transceivers. Thus, the first ad hoc network was already using wireless LAN technology as the underlying MAC and PHY layers. Later on, in the early 1980s, the PRNET program was replaced by the Survivable Adaptive Radio Networks (SURAN) program, improving upon the physical properties and routing of PRNET. Technologies to create moderate-cost ad hoc networks outside of the DoD were not present, and since there were very few mobile devices with any computing power, there was no need for commercial deployment either.

In the early 1990s, mobile computing power became affordable for the masses in the forms of laptops, notebooks, and personal digital assistants (PDAs). At the same time, hardware and software, especially open-source software, became widely available for trivial interconnection of computers and maybe connection to the emerging global network, the Internet. It was just a question of time of when the need for mobile connectivity would reach a critical mass to be worthy for commercial companies to look into developing standards, technologies, and products to enable mobile, i.e., wireless interconnection of devices. The early 1990s was also the time of the renaissance of ad hoc networking research, wherein packet radio networks were renamed ad hoc networks [23, 36], and old ad hoc networking problems became important research topics again. There was a commercial need for mobile interconnection, leading toward a push for wireless infrastructure based standards as well as a strong lobbying from research organizations to develop technologies that could be used as the basis of ad hoc networking (with more stress on the former). Due to the major interest from several companies, the Institute of Electrical and Electronics Engineers (IEEE) 802 Group in charge of computer communication networks established a subcommittee, IEEE802.11, to standardize and unify techniques and technologies to be used for wireless LANs. Since the subcommittee was established involving experts from companies and academia, it was also aware of the need for infrastructureless communications and was working in parallel to address both infrastructure-based and infrastructureless needs.

The DoD never lost interest in ad hoc networking, and funded programs such as the Global Mobile Information Systems (GloMo) and Near-term Digital Radio (NTDR), the former addressing Ethernet-type connectivity, and the latter focusing on military applications (NTDR also became the first nonprototype, real ad hoc network in the world). By 1997, the IEEE802.11 subcommittee had approved its first WLAN standard, defining the physical layer as well as the MAC and logical-link control layers for infrastructured and infrastructureless communication.

Today, the prices for IEEE802.11-based technologies are within everybody's reach and since an infrastructureless mode is defined, it has become the premier choice for the underlying bottom two layers (PHY and MAC) for most simulation, test-bedding, and even commercial ad hoc networks and applications. Yet, one should not forget that it is the infrastructureless part of the specification that permits the ad hoc mode, not the WLAN technology, which provides for ad hoc networks. Another factor to keep in mind is that most of the revenues are generated from the technology being deployed in WLANs and, thus, some protocol issues significantly different in WLAN and ad hoc scenarios will show a strong bias toward a primary WLAN behavior.

2.1.2 Wireless LANs

In the strict sense of the word, WLANs are infrastructure-based wireless networks, in which there is a need to deploy wireless access points ahead of time; these access points control network usage in their respective transmission range or domain. A local area network's spatial span is usually between 10 meters to a few hundred meters; thus, the same coverage range is demanded from a wireless LAN. A node that wants to connect wirelessly to a WLAN, should (i) be in the transmission range of the access point, (ii) obtain or carry an IP address from the same IP domain (assuming IP communication) that the access point is in, and (iii) use the access point as a bridge or router for every packet it sends or receives.

Wireless bandwidth is one of the most important natural resources of countries; thus, its usage is regulated by national regulation bodies. In the United States, the regulatory body in charge of the national radio frequency resources is the Federal Communications Commission (FCC). In order for a frequency band to be used, the FCC has to issue licenses to devices using that band as well as a license to operate devices in that band. The FCC has designated several frequency bands, commonly known as the ISM (Industrial, Scientific, and Medical) and/or U-NII (Unlicensed-National Information Infrastructure) bands, for which an FCC license is only needed for the device and not for the usage of the band. WLANs take advantage of these ISM bands, so the operators do not have to request permits from the regulatory bodies. The most common ISM bands for WLANs in order of their importance are: 2.4 GHz–2.483 GHz, 5.15 GHz–5.35 GHz, 5.725 GHz–5.825 GHz (United States) and 5.47 GHz–5.725 GHz (European Union), and 902 MHz–928 MHz (not relevant).

Since WLANs rely on a centrally controlled structure, just like cells of cellular networks, several access points can be used to create cellular-like WLAN structures. Some WLAN technologies are more suited for such large-coverage, cellular-like WLANs, whereas others may not perform well in such scenarios, will be pointed out later in this chapter. The term *hot-spot* recently became a frequently used term, referring to an area covered by one or more WLAN access points to provide Internet connectivity at a fraction of the cost of a cellular data connection, to users whose terminals are equipped with wireless network interface cards. Providing hotspots is an extremely controversial issue; current cellular providers are likely to loose revenue unless they are the ones providing the service.

2.1.3 Wireless PANs

The term wireless personal area networks came along with the appearance of its first representative technology: Bluetooth. WPANs (or, in short, PANs) are very short range wireless networks with a coverage radius of a few centimeters to about 10 meters, connecting devices in the reach of individuals, thus receiving the name. WPANs do not necessarily require an infrastructure; they imply single-hop networks in which two or more devices are connected in a point-to-multipont "star" fashion. Although the communication distance is shorter, so that the power requirements are lessened, Bluetooth provides a significantly lower symbol rate than WLANs. Fortunately, this contradicting "feature" is currently being addressed and it is likely that future WPAN technologies will provide users with options of significantly higher transmission speeds.

2.1.4 Digital Radio Properties

In order to fully comprehend the different aspects of medium-access control in WLAN and WPAN standards and specifications, it is necessary to possess basic knowledge on the behavior/terminology of digital radio transmissions. If using radio as the medium for communication, the bit error rate (BER) due to undesired interfering sources could become 8–10 orders of magnitude higher than in an optical or wired medium. The attenuation of radio signals is proportional to at least the square of the distance and the square of the carrier frequency in open propagation environments, in which there are no obstacles (not even the earth's surface) reflecting the radio signal, and the receiver and transceiver are in the line of sight. In real environments, statistically, the received signal strength can be decaying with as much as the fourth power of the transmitter–receiver distance, due to obstacles absorbing and reflecting the radio signal. Additionally, in a mobile environment, reflection and absorption of signals from obstacles causes fading effects that can be classified into short- and large-scale fadings depending on how far the transmitter moves away from the transmitter.

Rayleigh fading describes the fading of the signal when the transmitter–receiver distance varies around the wavelength of the carrier signal (about 12 cm at 2.4 GHz). With Rayleigh fading, one has to consider that a radio signal can be received through different paths via obstacles reflecting the signal. Signals received from multiple paths travel different distances; thus, their phases can vary significantly at the receiver, causing amplification and attenuation of each other, Rayleigh fading causes local signal strength minima, or *fading dips,* that are about half a wavelength (about 6.25 cm at 2.4 GHz) away from each other, strongly depending on the carrier frequency.

Log-normal fading describes the fading effect when the signal strength's variation is measured on a large-scale (much greater than the wavelength of the carrier) movement. With log-normal fading, different reflecting and line-of-sight components' strengths can vary with the order of the sizes of obstacles (buildings, etc.) absorbing the energy of the signal; log-normal fading dips are thus 2–3 orders of magnitude farther away than those of Rayleigh fading.

Thus, the received signal strength does not only depend on the approximate distance from the transmitter, but strongly depends on the exact distance (see Figure 2.1) and location, and on the exact frequency carrier used; that is, it is possible to produce a significant change in the received signal strength just by moving the receiver a few centimeters or by changing the carrier frequency by a few kilohertz.

Time dispersion is yet another problem to address—signals bouncing back from obstacles have a time shift comparable to the duration of bit times. Time dispersion could cause the reception of contradicting information, called *intersymbol interference* (ISI).

Since transmission and reception cannot occur at the same time on the same frequency at a single node, and because most building blocks of receivers and transmitters

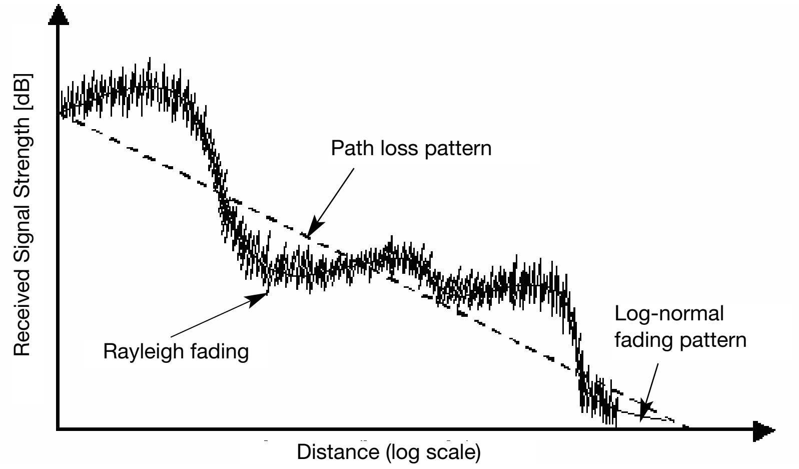

Figure 2.1. Received signal strength.

are the same, it makes economic sense to use time-division duplexing to provide only a single radio unit per device that can be switched between reception and transmission modes. Additionally, the consecutive reception and transmission events of the radio do not necessarily have to take place at the same frequency carrier in order to reduce the risk of being in a fading dip. Unfortunately, it takes significant time (up to a few hundred microseconds) to switch radios between transmission and reception modes (with or without changing the frequency), waiting for all the transients to settle. This time is sometimes referred to as *radio switch-over* or *radio turn-over time,* during which the radio is useless.

Since radio frequency is a scarce resource, it needs to be used wisely. In order to increase the capacity of a system, the same frequency (band) may be reused at some distance where the other signal becomes low. In order to reduce the reuse distance, thus reducing the interference, systems are sometimes required to implement radio-power control, with which the transmission power to different clients can be dynamically adjusted depending on the reading of the received signal strength.

To reduce the average transmission energy over small frequency bands and to provide better protection against fading dips, *spread-spectrum* (SS) technologies are employed (in fact, the FCC requires SS to be used in the ISM bands). The most well known and widely used SS technologies are (Fast) Frequency Hopping (FH or FFH), Direct Sequence Spreading (DSS), and the novel Orthogonal Frequency Division Multiplexing (OFDM) and Ultra Wide Band (UWB). With FFH, the frequency band is divided up into several narrower bands (using a central carrier frequency in each of these narrow bands). An FFH transmission will use one of the narrow bands for a short period of time, then switch to another, and, again, another, cyclically. The time spent at each carrier frequency is called the *dwell time*. In DSS, the signal to be transmitted is multiplied by a high-speed chip-code or pseudorandom noise (PN) sequence, essentially spreading the energy of the signal over a larger band (resulting in less spectral efficiency). With OFDM, just like with FFH, several frequency carriers are defined, but, unlike FFH, more than one carrier may be used at the same time to transmit different segments of the data. As will be shown, Bluetooth employs FFH, whereas IEEE802.11b and IEEE802.11a employ DSS and OFDM, respectively, and UWB is in its infancy.

The reader interested in more details of digital radio signal propagation and fading effects and their mitigation is referred to [39, 40]. Additionally, [44] provides a good overview of differences in propagation for TDMA/FDMA and CDMA systems.

The rest of this chapter is organized as follows: Section 2.2 introduces WLAN technologies and outlines why they can/cannot be used for ad hoc networking. Section 2.3 deals with WPAN technologies, focusing mostly on Bluetooth, and outlines the problems researchers are facing before Bluetooth can be used for ad hoc networking. Section 2.4 concludes the chapter.

2.2 WIRELESS LAN TECHNOLOGIES

As described in the previous section, the history of WLANs starts with the ALOHA system. In the early 1990s, radio technologies became mature enough to enable the production of relatively inexpensive digital wireless communication interfaces. The first generation of WLANs operated in the 900 MHz ISM band, with symbol rates of around 500 kbps, but they were exclusively proprietary, nonstandard systems, developed to provide wireless connectivity for specific niche markets (e.g., military or inventorying). The second-generation systems came along around 1997, enjoying a strong standardization effort. They operated in the 2.4 GHz range and provided symbol rates of around 2 Mbps. The IEEE802.11 Working Group (WG) and its similarly named standard were the most successful of the standardization efforts. People did not have to wait long for an inexpensive third-generation (2.4 GHz band, 11 Mbps symbol rate) WLAN standard and equipment, as the IEEE802.11b Task Group (TG) was quick in standardizing it, and, due to increased need, products rolled out extremely quickly. Although the IEEE802.11a TG was formed at the same time as IEEE802.11b TG and its standard was available at approximately the same time, it took longer for the first IEEE802.11a products to appear. IEEE802.11a operates in the 5.2 GHz band with speeds up top 54 Mbps (or 108 Mbps in a non-standardized “turbo” or dual mode) and represents the fourth generation of WLANs. The Wireless Ethernet Compatibility Alliance (WECA) was established by companies interested in manufacturing IEE802.11b and IEEE802.11a products. WECA forged the by now widely accepted term Wi-Fi (Wireless Fidelity) to replace the user-unfriendly IEEE802.11 name. WECA is known today as the Wi-Fi Alliance and provides certification for 2.4 GHZ and 5.2 GHz products based on the IEEE802.11b and IEE802.11a standards, respectively.

While the IEEE802.11 WG was working on IEEE’s WLAN standard, the European Telecommunication Standards Institute (ETSI) was working on another standard known as HiperLAN (High Performance Radio LAN). HiperLAN was released at about the same time as the first IEEE802.11 standard in 1998 but has received less attention due to its more stringent manufacturing requirements (representing better qualities, too). HiperLAN operates in the 5.2 GHz band with data rates up to 20 Mbps. The ETSI updated the HiperLAN standard in 2000, releasing HiperLAN 2, which provides similar data rates as IEEE802.11a while enabling easy architectural integration into 3G wireless networks (UMTS) and providing quality of service (QoS) provisioning.

In this section the readers will be introduced to the standardization efforts of the different IEEE802.11 Task Groups as well as to the technology of HiperLAN 1 and 2. It will be shown how these standards provide for not only WLAN usage scenarios but also for ad hoc networking.

2.2.1 IEEE802.11 Technological Overview

The IEEE802.11 Working Group was formed in 1990 to define standard physical (PHY) and medium-access control (MAC) layers for WLANs in the publicly available ISM bands. The original goal was to have data rates of 2 Mbps, falling back to 1 Mbps in the presence of interference or if the signal became too weak. Originally, three different physical layer options were provided: (i) infrared, (ii) frequency hopping spread spectrum (FHSS) at 2.4 GHz, and (iii) direct sequence spread spectrum (DSSS) at 2.4 GHz. Due to the possible need, two kinds of operation modes were also defined: a client-server, regular WLAN mode that received the name IM-BSS (Infrastructure Mode Basic Service Set), and an ad hoc operational mode called IBSS (Independent Basic Service Set). A Basic Service Set (BSS) is nothing but a group of at least two nodes or *stations* (STA) cooperating via the wireless interface.

The infrared PHY layer did not catch up and has been neglected subsequently. The FHSS PHY used 79 different carrier frequencies with 22 different hopping patterns, defining 22 virtual channels with a dwell time of 20 ms (50 hops/s). Although most of the research comparing the DSSS PHY and the FHSS PHY showed that the interference resistance and resilience of the FHSS PHY layer was superior, the FHSS PHY slowly lost the interest of the IEEE80.11 group and more emphasis was put on the DSSS PHY, mainly due to the fact that increasing the rate was hardly possible using the FHSS PHY. The DSSS PHY divided up the available 80 MHz band at the 2.4 GHz range into three nonoverlapping channels, each of them having around 20 MHz of bandwidth, thus enabling interinterferenceless operation of three different networks in the same spatial area. The 1 or 2 Mbps stream was used to modulate a so-called Baker sequence—a well-defined PN (pseudo random noise) sequence to spread the information over the respective 20 MHz band. The original MAC and PHY specifications of the IEEE802.11 were released in 1997.

Two different MAC channel access methods were defined. The first method, Distributed Coordination Function (DCF) to be used ether in the Infrastructure Mode or in the IBSS ad hoc mode employing the Carrier Sense Multiple Access–Collision Avoidance (CSMA/CA) MAC protocol, was first proposed in [25]. The second (optional) access method is the Point Coordination Function (PCF), to be solely used in the Infrastructure Mode, based on a MAC polling scheme. Only a few products have the capability to work with a PCF method and since the PCF is not defined for the ad hoc mode, further description of it is omitted in this chapter.

According to the IEEE802.11 standard, all stations (STA) have to be able to work with the DCF. The goals of the 802.11 group were to provide a similar service on the radio interface as the interface defined for wired LANs in the IEEE802.3 standard or Ethernet; that is, best effort with high probability access but no QoS guarantees. The IEEE802.11 MAC protocol is described in Chapter 3 of this book together with analyses of its performance in ad hoc environments.

Providing security was a major concern of the IEEE802.11 group, whose goal was to provide at least the same level of security as the wired Ethernet. IEEE802.11 defines its own privacy protocol called WEP—Wired Equivalent Privacy. Since in IEEE802.11 packets are broadcast over radio, it is relatively easy to intercept messages and to get attached to a network. Detecting access points is relatively easy even when they do not broadcast their so-called SSID periodically (which they do more often than not), and since most of the access points provide access to a network with a DHCP server, attaching to foreign networks is a relatively easy process for hackers. WEP was supposed to provide an optional encryption service in the MAC layer to enable the communication between access points and clients that share the same secret key. With WEP enabled, the MAC layers will encode each IEEE802.11 frame before transmission with an RC4 cipher (by RSA Security) using a 40, 64, or 128 (WEP-2) bit key and a pseudorandom 24 bit number, whereas the other side will decode the same stream using the same key and random number. The random number is used to increase the lifetime of the key, yet it has been shown that in a busy network, just by listening to the channel for a while, keys can be easily decoded if the original shared key remains the same [6, 9].

In the rest of this section, readers will be introduced to the IEEE802.11 variants (Task Groups), starting with the most popular IEEE802.11b or Wi-Fi 2.4 GHz, and continuing with the strongly emerging IEEE802.11a or Wi-Fi 5.2 GHz. Some insight will be provided into the soon-to-be approved IEE802.11g and the other Task Groups' work (e.g., TGs c, d, e, f, g, and h).

2.2.1.1 IEEE802.11b (Wi-Fi 2.4 GHz). The goal of Task Group b was to increase the maximum bit rate in the 2.4 GHz frequency range while maintaining interoperability with the original standard. The standard was released in 1999, keeping the original MAC layer but redefining the PHY layer to only work with DSSS, thus increasing the spectral efficiency of the three channels with bit rates of up to 11 Mbps each (with fall-back rates of 5.5, 2, and 1 Mbps). It did not take long for Wi-Fi to became widely accepted throughout the world for corporate WLANs, wireless home networks, and so-called hotspots at airports and cafés, as well as by the ad hoc networking community as an easy-to-set up basis for ad hoc testbeds.

2.2.1.2 IEEE802.11a (Wi-Fi 5.2 GHz). Although Task Groups a and b were established at the same time and the standards were accepted at the same time, IEEE802.11a products did not arrived on the market until late 2001 due to technological difficulties. The goal of Task Group a was to port IEEE802.11 to the newly available U-NII at 5.2 GHz and to provide higher bit rates. Thus, the original MAC layer was kept and the PHY was reworked to provide rates of up to 54 Mbps (with fall-back rates of 48, 36, 24, 18, 12, 9, and 6 Mbps). Since the available band at U-NII is about 300 MHz, eight nonoverlapping bands were defined; thus, eight different IEEE802.11a-based WLAN networks can operate in the same space without interference. This is essential to build cellular kinds of structures, in which neighboring cells should not use the same frequency (to reduce interference). With eight different bands (compared to three with IEE802.11b), it becomes relatively easy to establish noninterfering cellular structures. DSSS was not efficient at working with these high bit rates while satisfying frequency regulatory specifications, so a new spectrum spreading technology called OFDM (Orthogonal Frequency Division Multiplexing) or COFDM (Code OFDM) was accepted. OFDM was specifically developed for indoor environments, addressing indoor-specific fading effects.

With OFDM, the signal to be transmitted is modulated over several frequency carriers. In IEEE802.11a, a 20 MHz bandwidth channel is divided into 52 subcarriers, each about 300 kHz wide; 48 of these subcarriers are used as carriers for the data, whereas the remaining four are employed for forward-error correction. Modulation is performed by changing the phase and amplitude of each of the subcarriers. To provide different symbol rates, different levels of amplitudes and phase shift keying are employed (e.g., binary phase shift keying, 16-level shift keying, etc.).

Although the power attenuation due to distance is at least four times as much at the 5.2 GHz range than at the 2.4 GHz range, and signal energy is more likely to be absorbed by obstacles, it has been shown by researchers at Atheros Communications [13]—a pioneer of IEE802.11a products—that the performance of IEEE802.11a is superior to the performance of IEEE802.11b at distances less than 70 meters, by at least a factor of two (see Figure 2.2). Due to this fact and due to the availability of eight channels, IEEE802.11a is likely going to have a prosperous future. Equipment manufactured by some companies extends the standard by introducing even higher-rate modes capable of transmitting with a 108 Mbps symbol rate.

2.2.1.3 IEEE802.11g. Task Group g is working on an extension to IEEE802.11b at 2.4 GHz, enabling transmission at symbol rates of 54 Mbps while retaining the fall-back speeds of IEEE802.11b, thus ensuring interoperability. After a long and rough debate, Task Group g has agreed to the adoption of OFDM technology (while keeping DSS for the interoperability mode); the standard is expected to be finalized at the end of 2002. Although IEEE802.11g-based equipment will provide the same symbol rate as IEEE802.11a, it will still have the same three-channel restriction of the original standard as well as it will operate in the crowded 2.4 GHz range.

All of the previously outlined IEEE802.11-based technologies can be used and deployed as the PHY and MAC layers of ad hoc networks.

2.2.1.4 Other IEEE802.11 Task Groups. **IEEE802.11h.** There were strong European concerns that 802.11a could interfere with NATO satellites and microwave radar sys-

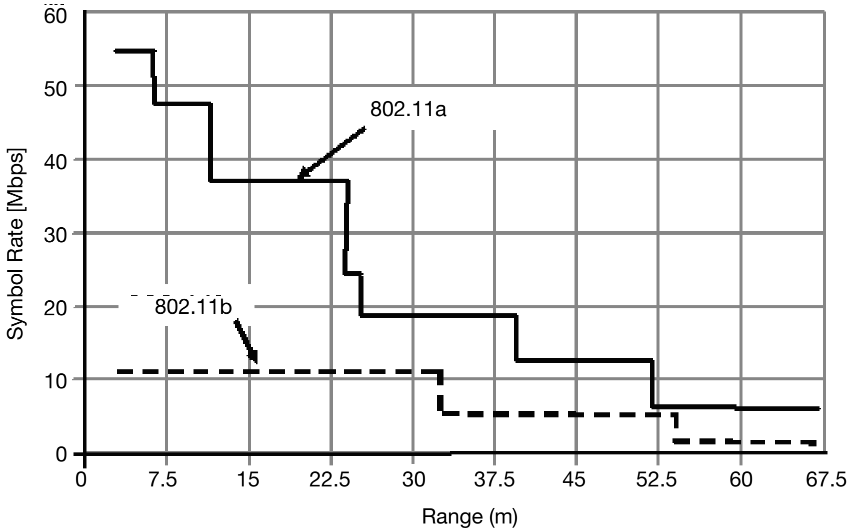

Figure 2.2. Symbol rates of IEEE802.11b versus IEEE802.11a [13].

tems. To avoid such interference, two extensions to the PHY of 802.11a were added in 802.11h, one of them being the capability to select the employed channel automatically based upon observations (DFS—Dynamic Frequency Selection), the other ensuring the enforcement of strict radio power control (TPC—Transmit Power Control).

IEEE802.11e. Task Group e is addressing the flaw of IEEE802.11, working in a best-effort mode but not being able to provide with any QoS provisioning. This Task Group is redefining both the centrally controlled channel access as well as redefining the contention-based channel access of CSMA/CA, including priorities to ensure that packets with higher priorities enjoy access benefits comparable to lower-priority packets in a Differentiated Services manner. This later function is called the *Enhanced Distributed Coordination Function* (EDCF).

IEEE802.11c is a wireless extension to IEEE802.1D, enabling bridging using IEEE802.11 (irrelevant to ad hoc networking).

IEEE802.11d deals with including country-specific information into the beacon transmissions, so STAs are informed of what part of the spectrum is available and what radio constraints they have to obey to (e.g., maximum transmission power).

IEEE802.11f is defining a standard interaccess-point communication protocol for users roaming between access points (irrelevant to ad hoc networks).

IEEE802.11i addresses the flaws of WEP, improving the wireless security at the MAC layer.

2.2.1.5 Further Reading. The reader interested in more high-level details is referred to the 802.11-Planet [3], an online resource on IEEE802.11-related information and news. Readers looking for a more detailed description can obtain the freely available IEEE 802 standards [1, 2] as a result of a new initiative of IEEE 802 to increase interoperability of devices. For a brief online explanation of the OFDM principles, the reader is referred to McCormick's tutorial [26] or to the online white papers and materials of the OFDM Forum [34].

2.2.2 HiperLAN 1 and 2

HiperLAN [16] is the well-known name of the WLAN standardization efforts of the European Telecommunications Standards Institute (ETSI); more precisely, it is being developed by the BRAN (Broadband Radio Access Networks) project of ETSI. HiperLAN 2 [17] is the new version of the standard, providing more bandwidth and interoperability considerations with third-generation wireless networks (e.g., Universal Mobile Telecommunication System or UMTS).

HiperLAN 1 is defined to work in the 5.2 GHz U-NII band, providing symbol rates of up to 23.5 Mbps. Unfortunately, HiperLAN was not picked up by any companies to manufacture products—it quickly became obsolete. ETSI-BRAN has proposed HiperLAN 2, hoping for better acceptance.

The PHY layer of HiperLAN 2 is nearly identical to that of IEEE802.11h (which is a European-initiated extension to IEEE802.11a), using OFDM as the basis. The main difference between HiperLAN2 and IEEE802.11a lies in the definition of the MAC layer. As IEEE802.11a relies on a CSMA/CA-based channel access related to Ethernet, HiperLAN 2 is based on a TDMA approach, with scheduling principles taken from Wireless ATM. HiperLAN 2 thus is able to provide QoS provisioning and can be used for guaranteed real-time data delivery. The MAC layer of HiperLAN 2 defines both a centralized (infrastructure) mode and an ad hoc mode, similarly to IEEE802.11.

Since no company has yet manufactured inexpensive, commercially available HiperLAN products, there are no ad hoc network testbeds based on HiperLAN. The 802.11 standards seem to be more widely accepted than HiperLAN 1 or 2, despite the advertised superiority of HiperLAN 2. Just as with HiperLAN 1, there are no products currently available in large quantities for HiperLAN 2 hindering its deployment as the basis for ad hoc networks. Ad hoc routing protocols (and their simulation) relying on HiperLAN have been proposed [14, 19] but not as widely as protocols relying on IEEE802.11 standards. Optimized Link State Routing (OLSR) [14] is specifically tailored toward HiperLAN. The reader interested in more details is referred to the standards [16, 17] or the excellent white papers provided at the HiperLAN2 Global forum [24].

2.2.3 Infrared WLANs

Although not mentioned yet, the commercial history of WLANs began in 1979 with the Diffused Infrared WLAN project of IBM in Switzerland. The main disadvantage of using photonic electromagnetic waves is that light requires line-of-sight transmission—the receiver and transmitter have to be physically visible to each other. Although fixed environments can be engineered to abide by the line-of-sight rules, mobility can render an infrared WLAN useless. Omnidirectionality of transmissions is not achievable since light is absorbed by most conventional obstacles (such as furniture, the computing unit itself, or people). Due to these major disadvantages, infrared transmission has never taken off as a WLAN competitor (e.g., the original 802.11 defines the operation on an infrared medium as well). It is rarely even used for short-range wireless connections, despite the fact that many portables are equipped with an IrDA (Infrared Data Association) port.

Using infrared transmission in ad hoc networks would defeat the purpose of the ad hoc requirements—networks have to work in all kinds of (mostly hostile) environments. Yet there are projects (such as [12, 22]) exploiting the inexpensive infrared technology for a limited population of ad hoc nodes in indoor environments where the diffusion of the signal can be used as a benefit to somewhat overcome the problem of obstacles.

2.2.4 UWB

Ultra Wide Band (UWB) [39] is a novel spread-spectrum technique acknowledged by the FCC in Spring 2002. UWB can be used for communication as well as to "see through walls," thus its commercial usage is strongly restricted by the FCC, making it a short-to-medium range wireless communication technology. UWB does not use conventional frequency carriers but generates very short duration rectangular pulses (close to that of Dirac pulses), thus spreading the energy of the transmission over an extremely wide spectrum. Due to this extreme spreading of the energy, UWB does not pose a significant interfering source at any band, and it does not require line of sight.

The first UWB chips have just appeared on the market but it will take a tremendous amount of additional research and standardization effort until UWB-based network adapters become commercially available. UWB has all the properties needed to be the next most popular PHY layer for ad hoc networks. The 802.15.3 Group is also considering UWB as the basis for a high-speed WPAN standard.

2.2.5 Using IEEE802.11 for Ad Hoc Networking

As mentioned earlier, Wi-Fi is extremely popular among ad hoc network researchers as an off-the-shelf support for their simulation or testbedding efforts. In this subsection, some Wi-Fi-based simulation libraries and testbeds will be outlined.

Most major network-simulation toolkits have either an integrated or a contributed IEEE802.11 library. The three most widely used simulators for ad hoc networks—NS2 [33], OPNET [35], and GloMoSim [18]—come with their own implementation of the MAC and PHY layers of IEEE802.11. By far the most simulation efforts of ad hoc routing protocols are carried out assuming (and employing) IEEE802.11-based MAC and PHY layers of one of the above simulation tools.

Due to the availability of inexpensive Wi-Fi products that can be used to establish ad hoc networks, it would be more of a challenge to list all projects that have established an ad hoc network testbed than to list those universities and research labs that do not have any. Here, some of the major projects are listed, starting with possibly the most well-known public license testbed. Uppsala University in Sweden provides everybody the opportunity to build their own Wi-Fi-based ad hoc testbed by providing a GNU Public License on their Ad Hoc Protocol Evaluation (APE) Testbed [5]. APE aims to make the establishment of ad hoc testbeds as easy as possible while providing all the functions required for customization. Project MART (Mobile Ad Hoc Routing Testbed) [30] at the Helsinki University of Technology is establishing a college-wide Wi-Fi-based ad hoc network to evaluate different proposed ad hoc routing protocols.

The MONARCH Project [32] uses a Wi-Fi-enabled ad hoc testbed to evaluate the Dynamic Source Routing (DSR) ad hoc routing approach proposed by them. They also provide the functionality to connect the ad hoc network to a traditional IP network using gateways. The MOMENT Lab at the University of California, Santa Barbara, has its own Wi-Fi-based testbed [31], running on pocket PCs, laptops, and desktops, to evaluate their proposed ad hoc routing protocol: AODV (Ad Hoc On Demand Distance Routing). A project in the R&D Group of Acticom [4] is focused on an ad hoc routing testbed to research multimedia-aware routing protocols for ad hoc networks. The testbed is based on the Wi-Fi 2.4 GHz technology (to be extended to Wi-Fi 5.2 GHz), using multimedia-enabled laptops and running video conferencing applications over their ad hoc network. The Wireless Network Testbed (WNT) [42] at the University of Surrey, United Kingdom, focuses on the evaluation of mobility management protocols, QoS provisioning techniques, routing, and reconfigurability with their Wi-Fi-based ad hoc network. Trinity College in Dublin, Ireland, envisions a Wi-Fi-based ad hoc network covering the entire city of Dublin, using their DAWN (Dublin Ad Hoc Wireless Network) testbed [15]. DAWN is not only envisioned as a testbed but also as the ad hoc medium for fourth-generation (4G) wireless systems, and is fully operational on the campus. Unfortunately, as pointed out in the next paragraph, Wi-Fi was not designed to serve multihop networks, and the community has yet to produce an inexpensive ad hoc tailored PHY and MAC standard.

An extensive analysis of the problems related to the use of IEE802.11 in ad hoc networks is presented in Chapter 3. Here, we would like to point out in advance that Wi-Fi has not been developed for ad hoc networking and, thus, it can exhibit undesired behavior when used for ad hoc networking. Although IEEE802.11 was developed keeping an ad hoc mode in mind, this ad hoc mode is tailored toward simple point-to-point connections; that is, to interconnect laptops for quick file transfers without the buffering and relaying requirement of access points. A recent article [43] in the *IEEE Communication Magazine* points out the shortcomings of the IEEE802.11 MAC layer in providing for ad hoc networks. In [43] the authors claim that the Wi-Fi MAC does not suit ad hoc networks well and that Wi-Fi-based ad hoc testbeds will not perform properly and may cause significant secondary problems (such as TCP instability and unfairness between nodes), reducing the effectiveness of the proposed routing protocols.

2.3 WIRELESS PAN TECHNOLOGIES

Wireless Personal Area Networks (WPANs) are short to very short range (less than 10 meters) wireless networks covering the immediate surroundings of individuals. WPAN technologies are not (and should not be) considered to be contenders of WLAN technologies, but are destined to complement WLANs. The market segment of WPANs is different from that of WLANs; not only is the required range shorter but the required service levels are also different. A PAN is the next wireless networking paradigm in the ordered list of WAN-MAN-LAN paradigms. To enable the embedding of WPAN technologies into general, low-cost devices, theses technologies have to have small footprints, very low costs, and relaxed power requirements. WPAN technology can be used, for example, to interconnect portable computers/digital assistants and their peripherals, to connect sensors/actuators, to connect devices worn by individuals establishing *personal operating spaces* (POS), or to connect devices in cars without the need for cabling. Cost effectiveness is the major keyword that one should associate with WPANs.

2.3.1 Short History

The term personal area network was forged and its standardization started by the establishment of an “Ad Hoc Group” within the IEEE Portable Applications Standards Committee (PASC). In 1998, a Study Group inside the 802.11 Working Group was formed to develop a project authorization request. In March 1999, the 802.15 Working Group was established. Meanwhile, industrial interest groups were formed throughout the world to address the same low-range, low-power, low-cost networking needs. The HomeRF working group/consortium was formed in March 1998, focusing on the home environment—a larger domain than personal area but smaller than local area, with needs similar to PANs. The Bluetooth Special Interest Group (SIG) was formed in May 1998 with the goal of defining an industry standard to replace short-range data cables. Bluetooth took the same route as the IEEE WPAN working group (strong overlap in interested parties), overtaking the IEEE efforts, whereas HomeRF was getting more and more away from WPAN.

The first publicly released version of the Bluetooth specification of the Bluetooth SIG became available in the fourth quarter of 1999 but, due to disturbing imperfections, a new version was released in February 2001. Meanwhile, the IEEE802.15 working group had formed four Task Groups and a Study Group for different WPAN requirements. Task Group 1 (805.15.1) adopted the bottom layers of the Bluetooth specification in June 2002, whereas Task Groups 2, 3, and 4 and the Study Group are concentrating on coexistence with WLANs, and high-rate, low-rate, and alternative-high-rate versions of the standard.

2.3.2 Bluetooth Technological Overview

The Bluetooth SIG was formed in May 1998 by the so-called promoter companies, consisting of Ericsson, IBM, Intel, Nokia, and Toshiba, and later on 3Com, Lucent, Microsoft, and Motorola. The SIG also contains associate members; participating entities pay membership fees and, in turn, can vote or propose modifications for the specifications to come. Adopter companies can join the SIG for free but can only access the oncoming specifications if these have reached a given evolutional level. The name Bluetooth supposedly comes from a Scandinavian history-enthusiast engineer involved in the early stages of developing and researching this short-range technology, and the name stuck; nobody being able to propose a better one. Bluetooth was the nickname for Harold Blåtand—“Bluetooth,”—King of Denmark (940–985 A.D.). Bluetooth conquered both Norway and Denmark, uniting the Danes and converting them to Christianity. One of the major goals of the Bluetooth standard is to unite the “communication worlds” of devices, computers, and peripherals and to convert “the wired” into wireless; thus, the analogy.

The Bluetooth specification defines functions for all the layers of the ISO-OSI 7-layer architecture; the protocol stack of Bluetooth is depicted in Figure 2.3. Bluetooth is designed so that a single chip can implement the bottom three layers with a serial (RS-232, USB, or similar) interface connecting the chip to the controller host through the so-called HCI (Host Controller Interface).

2.3.2.1 The RF Layer. The physical or RF Layer (Radio Frequency) of Bluetooth is built on a synchronous fast-frequency-hopping paradigm with a symbol rate of 1 Mbps operating in the publicly available 2.4 GHz ISM band. In a normal operation mode, Bluetooth units will change the carrier frequency (hop) 1600 times a second over 79 different carrier frequencies separated 1 MHz apart, starting with 2.402 GHz. (Since the 2.4 GHz ISM band is not equally available in all countries, e.g., France and Spain, Bluetooth enables the operation on a reduced band with only 23 different carrier frequencies.) The modulation scheme employed is similar to that of GSM, that is, GFSK (Gaussian Fre-

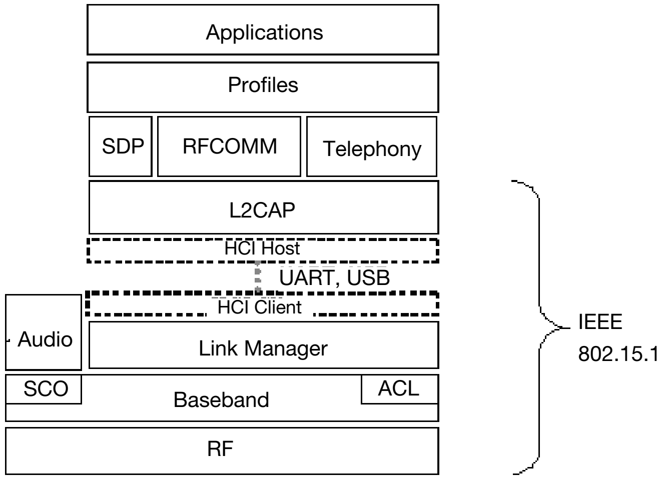

Figure 2.3. Simplified Bluetooth protocol stack.

quency Shit Keying). According to the transmitted power, Bluetooth devices can be classified into different power classes from 20 dBm to 0 dBm transmission power. Class-3 devices are the most common, transmitting with 0 dBm, and not requiring external power amplification or power control; thus, they can be integrated on a single chip.

2.3.2.2 The Baseband Layer. The Baseband layer is in charge of controlling the RF layer and providing the communications structure to the higher layers, thus taking on the functions of the MAC sublayer of the OSI-7. The basic communication structure provided by Bluetooth is a point-to-point link between two devices, each of them hopping along the same pseudorandom sequence of frequency carriers. In order for the two nodes to agree on the hopping sequence and on the control of the channel, one of the nodes will assume the role of master while the other becomes a slave. (Nodes do not have to be different in their capabilities, the master/slave roles are logical roles in the point-to-point communication link.) A point-to-multipoint *Piconet* can be established by a single master controlling the channel for several slaves (the point-to-point communication structure in general is also called a Piconet). A Piconet only has one master and can have several slaves hopping along the pseudorandom sequence of the master of the Piconet, with a maximum channel capacity of 1 Mbps shared by the members of the Piconet. As mentioned earlier, a functioning Piconet makes 1600 hops in a second, thus having 1600 slots, each 625 μs long in one second. In an odd-numbered slot, only the master of the Piconet is allowed access (with a few exemptions); whereas, in an even-numbered slot, a slave that was polled in the previous slot can gain access to the channel. To enable Bluetooth devices to tune to the new frequency carrier and change their mode from reception to transmission, a 220 μs *guard time* is set aside at the end of transmission slots, thus reducing the goodput. Nodes are also enabled to transmit during not only one but three and five slots, using different packet types (with no hopping while in transmission) to increase efficiency by reducing the "effective usage time–guard time" ratio. The effective data rate in a Piconet can be determined according to the packet types and lies anywhere between 216 kbps and 780 kbps per Piconet. Several Piconets can operate in the same space independently without causing a significant interference among each other, since all these Piconets will hop according to different hopping sequences. The probability of interference between independent Piconets grows by the number of Piconets covering the same area. It is also worth noting that the 2.4 GHz band is also utilized by other (interfering) technologies such as IEEE802.11b and microwave ovens.

There are two different types of classifications for the virtual links between nodes in a Piconet: a link can be Synchronous Connection Oriented (SCO) or Asynchronous Connectionless (ACL). If an SCO link is established between two nodes of a Piconet, then slots are reserved at fixed intervals for the master and one of its slaves in the Piconet, ensuring a deterministic assignment of slots to the traffic. SCO links provide a voice-type quality of service provisioning, indeed designed for voice transmissions. ACL links, on the other hand, are in sole control of the master polling the slaves in the order the master desires. Slots assigned to SCO links have priority over ACL links as well as priority over any other task a master may be performing (e.g., inquiring or paging).

As mentioned earlier, the basic communication structure of Bluetooth is a Piconet; thus, Piconets need to be established over Bluetooth devices before they can exchange data or communicate. The Piconet establishment process is a three-step process including device discovery (or inquiry, in Bluetooth terms), device attachment (or paging, in Bluetooth terms), and Piconet parameter negotiations.

During the *inquiry* process, the common objective of Bluetooth nodes is to discover each other's presence with some of the nodes listening or *scanning* the (reduced set) of hopping frequencies while other nodes constantly transmit very short so-called ID packets. Since inquiry ID packets are extremely short and represent a unique bit pattern, the number of hops can be increased to 3200 hops per second to reduce discovery times. If a scanning node overhears an ID packet for the first time, it will refrain from replying immediately but will wait a random (back-off) period of time to reduce the collision probability of scanning nodes replying to the same ID packet. When finished with the backlogging, nodes return to the inquiry scan state, and, if they overhear another ID, packet they will respond to the transmitter of that ID packet in exactly 625 μs. The inquiring nodes send two ID packets at two different frequencies and then listen to the corresponding reply frequencies for the next 625 μs if reply is received. The inquiring node will be aware of the proximity and the identity of the scanning node.

The *paging* process can start if there are devices that are aware of the identities other devices in their proximity, most likely after a successful inquiry. Just like with the inquiry process, the frequency of the hopping is increased to 3200 and devices can be either in a page scan or page mode. By definition, the node that initiates the paging (the node in the page mode) will become the master of the Piconet, whereas the node that was successfully paged will become the slave. The device in the paging mode will transmit an ID packet with the address of the device it has discovered before. If the device whose ID is transmitted is in the page scan mode and overhears the ID packet with its own address, then it will respond to this "page" with the same ID packet. Note that the paging node knows the identity of the paged device but not necessarily vice versa; thus, the paging node that received a reply from the paged node will send an identification packet with its own parameters to the paged node (the latter responding with another ID packet). By the time this four-way handshake is executed, the slave (paged node) has enough information to calculate the master node's pseudorandom hopping sequence so both the nodes can start using the hopping sequence of the master, establishing a *connection.*

Reaching the connection state, the master will poll the slave to verify that the slave has entered the Piconet. The third phase of the connection establishment is initiated by the Link Manager layer to set up a control ACL link.

A Piconet can consist of a maximum of eight active nodes: a master and seven active slaves. This is due to three-bit node addressing inside Piconets. Yet, a Piconet can consist of much more devices in an inactive mode; indeed, the number of nonactive slave devices in a Piconet is not constrained. Other than being actively participating in a Piconet, slaves can go or be put into three different power saving modes: Sniff, Hold, and Park. A slave in Sniff mode will not listen to the channel in every odd time slot, but will negotiate a parameter with the master for periodic small time windows during which it will wake up and check whether the master wants to transmit to it. The Sniff mode can be used to reduce power consumption of rarely active nodes. In the Hold mode (just like in the Sniff mode), a slave still does not give up its three-bit active-address but will not able to receive any ACL packets for a negotiated period of time. The Hold mode may be used to perform inquiry and scanning operations while being connected to a Piconet and to enable the participation of nodes in more than one Piconet, as outlined later. Finally, slaves in the Park mode take the three-bit active address but will remain synchronized to the master by listening to the channel during so-called Beacon intervals. If a master wants to wake up a parked slave, it will have to wait for the negotiated Beacon window and address the slave to be awaked with the device address or parked address. Parked slaves will also receive an opportunity during the Beacon window to inform the master that they need to be woken up.

Although the main communication unit in Bluetooth is a point-to-multipoint Piconet, the specification allows nodes to participate in more than one Piconet semisimultaneously (note that a node can be a master in only one Piconet), switching between its roles of the different Piconets acting as bridges between Piconets, likely using the Hold mode to schedule between the several Piconets. Two or more overlapping Piconets interconnected with bridges in such manner form a *Scatternet.* Although a Piconet's topology is a star-shaped point-to-multipoint structure with only a single link between a master and any of its slaves (single-hop), a Scatternet can represent any type of the possible topologies and, thus, can be used to establish a multihop or *ad hoc network* (a possible Scatternet is depicted in Figure 2.4). Other than describing the possibility of forming Scatternets, the Bluetooth specification does not address how Scatternets or ad hoc networks should be established; it solely provides the possibility to employ Bluetooth as the basis for ad hoc networking.

2.3.2.3 Link Manager. The Link Manager (LM) layer of Bluetooth fulfils part of the functionality of the Logical Link Control sublayer of the OSI-7 architecture. The main functions of the LM are: Piconet management, link configuration, and providing security, that is, authentication and encryption. Right after a slave has been put into a Connection mode, an ACL link is established between master and slave to manage the Piconet. Management functions include the attachment and detachment of slaves, negotiating piconet parameters, a possible change in the roles (when a slave becomes the new master of the Piconet), the establishment of SCO or ACL links, and the handling of the low-power modes. The management functions are based on a request–response communication scheme between the master and the slave, whereby the master requests some parameter to be changed and the slave either accepts it or challenges it.

The link configuration tasks consist of (i) quality of service negotiations, whereby the maximum polling time is negotiated in a request–response manner and broadcast parameters are set up; (ii) negotiation of power-control parameters; (iii) negotiation of accepted packet types at both sides, with determination of whether multislot packets will be allowed.

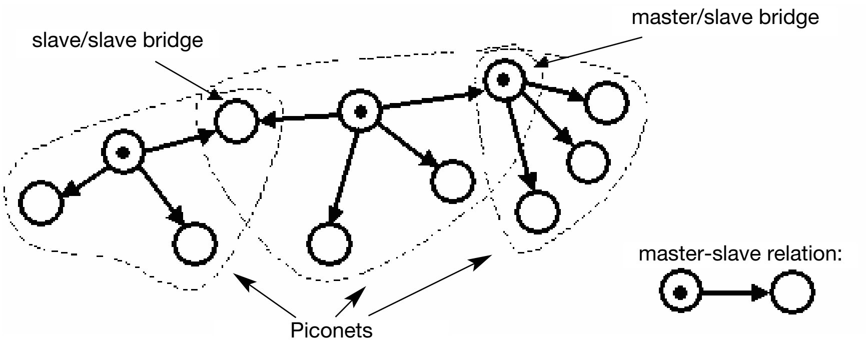

Figure 2.4. A Bluetooth Scatternet consisting of three Piconets.

The security goals include (i) optional authentication to only allow devices that are known or trusted to connect, and (ii) encryption to prevent eavesdropping by a third party on the channel. Authentication is based on a common link key, whereby the verifier challenges the claimant to compute an answer that can only be computed by knowing the link key. In order to distribute the link key, nodes go through a process called *pairing.* During pairing, a link key is formed from a PIN code, a random number, and the claimants address. For encryption of data, an encryption key length is negotiated between master and slave and an encryption key is created using the same algorithm at both sides and the link key.

2.3.2.4 Logical Link Control and Adaptation Protocol Layer. The Logical Link Control and Adaptation Protocol Layer (L2CAP) is the other subprotocol of the Logical Link Control sublayer of the OSI-7 protocol stack. The goals of L2CAP are to enable several higher-layer protocols to transmit their protocol data units (PDU) over ACL links (protocol multiplexing), segmentation and reassembly of higher layer PDUs into Baseband packets, and quality of service negotiations for individual ACL links for the higher-layer protocols. The L2CAP can provide both connection-oriented and connectionless communication to the higher layers. L2CAP is needed for protocol multiplexing, since the headers of Baseband packets does not include bits to specify what higher-layer protocol is encapsulated in the Baseband packet. The L2CAP protocol header contains logical channel identification bits with which connection-oriented protocol multiplexing can be done, whereas, for connection less services and control information fixed, special channel identifiers are used. Segmentation and reassembly takes care of using several of the small Baseband packets to transmit higher-layer packets of size of up to 64 kB. Once the transmission of a segmented packet starts on the ACL link, no other L2CAP ACL packets can be interleaved with the transmission; the transmitting of the whole higher-layer PDU has to be finished first. The L2CAP layer does not support SCO links nor does it perform integrity checks. It assumes that data integrity issues are taken care of at the Baseband layer with automatic retransmissions or forward-error corrections.

2.3.2.5 Higher Layers and Bluetooth Profiles. The Bluetooth specification defines higher-layer protocols, that is, protocols to emulate several serial connections over ACL links, such as the RFCOMM protocol, and a protocol that defines how devices can find out about what services other devices provide, such as the Service Discovery Protocol (SDP). In the second volume of the specification, called the *Profiles,* different services are standardized for Bluetooth links, such as headset profiles, serial port profiles, intercom profiles, LAN access profiles, file transfer profiles, and synchronization profiles. Bluetooth devices connected to each other can query the profiles the other device is offering and, if they implement the same profiles, they can establish connections for the given profiles, ensuring interoperability.

These protocols and profiles do not reside at the bottom two layers of the OSI-7 model and, thus, are not an integral part of IEEE802.15.1. Since they have little significance to ad hoc networks, their functional description is omitted in this chapter.

2.3.2.6 Further Reading. Readers interested in more details of the Bluetooth specification are referred to the freely available Bluetooth specifications [7, 8], to books summarizing the Bluetooth specifications, such as [10, 28], or to the many available white papers and general resources on Bluetooth on the World-Wide-Web.

2.3.3 Using Bluetooth for Ad Hoc Networking

Scatternet functionality is essential for Bluetooth to be used as an enabler for ad hoc networks; discussions on such possibilities were ongoing as early as the first appearance of the Bluetooth specification. Unfortunately, only few of the commercially available Bluetooth kits implement Scatternet functionality (most of them do not even implement the power saving modes or point-to-multipoint operations). In order to use Bluetooth as an ad hoc network enabler, several research problems have to be solved, including an efficient way to discover other devices (inquiry) [45], an efficient way to switch bridge nodes between Piconets (Scatternet scheduling) [29], efficient ways to schedule the polling in multislave Piconets (Piconet scheduling) [11], selecting the best links to be activated for a Piconet [27], and having distributed algorithms forming Scatterenets (Scatternet formation) [46]. An enormous amount of research is focused on each of these areas; the cited references to each of these research areas only show a single representative publication for the reader who wants to get more details.

Chapter 4 of this book presents, investigates, and compares proposed Bluetooth Scatternet formation algorithms in detail.

Although several research groups plan to establish Bluetooth-based ad hoc networks, currently, no working testbed is available for study, so Bluetooth ad hoc network study remains in the simulation domain. IBM research has made their Bluetooth NS-2 extension [21] open-source available and the next release is supposed to have Scatternet functionality for simulation evaluation of Bluetooth-based ad hoc networks.

2.3.4 HomeRF—SWAP

The HomeRF Working Group [20] was launched in 1998 by Compaq, Intel, Motorola, National Semiconductor, Proxim, and Siemens to establish an industry standard supporting wireless home networks. Although enjoying the support of several big industry players, HomeRF has never taken off due to the popularity of IEEE802.11b. HomeRF positioned itself in the niche market of domestic users, which is why it is listed in this chapter under WPANs. HomeRF provides QoS-provisioned services, for example, for voice calls, as well as packet-switched best-effort services at the 2.4 GHz ISM band, with rates similar to that of IEEE802.11b (from specification 2.0), using FH technology. HomeRF's FH PHY layer was designed to work around interfering sources in the home environment, such as microwave ovens, by monitoring the channels and banning those channels from its hopping scheme that have too much interference.

The MAC layer protocol of HomeRF is called SWAP (Shared Wireless Access Protocol), which provides TDMA services for isochronous data and two different priorities of IEEE802.11, like CSMA/CA service for asynchronous data.

Although HomeRF products are available in limited supply, and nothing contradicts using the technology for ad hoc networking, the popularity and inexpensiveness of Wi-Fi preempts HomeRF for use as an enabler for ad hoc networking testbeds. Additionally, HomeRF is not an open standard, making its acceptance even more difficult.

2.3.5 RFID

Radio Frequency Identification (RFID) is a technology for providing a low-bandwidth, extremely inexpensive scheme for small integrated devices to talk wirelessly to access points relaying their ID (along with some optional data). RFID is used mainly for inventory purposes to be able to automatically monitor large inventories that are individually tagged with RFID tags. RFID can use active or passive tags. Passive tags do not have an internal power source but need to be placed in an electromagnetic field to be activated and readable, whereas active tags are battery operated and have a longer range, but are more expensive. Unfortunately, RFID technology lacks strong standards; most of the products available represent someone's proprietary technology.

The authors of this chapter are unaware of any serious RFID-based ad hoc network proposals, testbeds, or simulations, although RFID can be an extremely inexpensive basis for large-scale, low-rate-sensor ad hoc networks. The reader interested in more details about RFID is referred to the online resources [37, 38].

2.4 CONCLUSION

This chapter introduced several WPAN and WLAN standards. In the WLAN are, the strongest competitor today is IEEE802.11b, also called Wi-Fi 2.4 GHz. Wi-Fi 5.2 GHz (IEEE802.11a) is quickly emerging, providing symbol rates comparable to that of Fast-Ethernet. Wi-Fi defines an ad hoc operational mode, which makes it the most common off-the-shelf enabler for ad hoc network testbeds.

Bluetooth is the strongest standard in the WPAN field. Although the Bluetooth specification allows for the establishment of ad hoc networks, referred to as Scatterenets, there are major challenges that need to be overcome for Bluetooth to be considered a strong contender as an off-the-shelf ad hoc networking enabler.

Although it has been shown that none of these technologies is perfect for ad hoc networks, they will remain the premier choices for establishing testbeds. Ad hoc research will have to wait for dedicated ad hoc PHY and MAC technology until a killer application is defined for wide, commercial use of ad hoc networks.

Chapters 3 and 4 further investigate the use of the IEEE802.11 and Bluetooth technologies, respectively, for ad hoc networking.

ACKNOWLEDGMENTS

Our sincere gratitude goes to Rózsa P. Záruba and Wook Choi, who helped in collecting and compiling the documents for this chapter.

REFERENCES

1. Official Homepage of The IEEE802.11 Working Group for Wireless LANs, http://grouper.ieee.org/groups/802/11/.
2. IEEE 802, "Get IEEE 802," http://standards.ieee.org/getieee802/.
3. 802–11 Planet Online Resource, http://www.80211-planet.com/.
4. Acticom R&D, http://www.acticom.de/1357.html.
5. Ad Hoc Protocol Evaluation Testbed, http://apetestbed.sourceforge.net/.
6. W. A. Arbaugh, "An Inductive Chosen Plaintext Attack Against WEP/WEP2," *IEEE Document 802.11-01/230,* May 2001.

7. Bluetooth SIG, "Specification of the Bluetooth System—Core," vol. 1, version 1.1, http://www.bluetooth.com/dev/specifications.asp, February 2001.
8. Bluetooth SIG, "Specification of the Bluetooth System—Profiles," vol. 2, version 1.1, http://www.bluetooth.com/dev/specifications.asp, February 2001.
9. N. Borisov, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11," in *Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking (MOBICOM2001),* pp. 180–189, Rome, Italy, July 2001.
10. J. Bray, C. F. Sturman, and J. Mendolia, *Bluetooth 1.1: Connect Without Cables,* 2nd ed., Prentice-Hall, 2001.
11. A. Capone, M. Gerla, and R. Kapoor, "Efficient Polling Schemes for Bluetooth Picocells," in *Proceeding of the IEEE International Conference on Communications (ICC2001),* vol. 7, pp. 1990–1994, Helsinki, Finland, June 2001.
12. I. Chen, "Wireless Ad Hoc Messenger," a Virginia Tech and Microsoft project, http://people.cs.vt.edu/~irchen/microsoft-grant/description.html.
13. J. C. Chen and J. M. Gilbert, "Measured Performance of 5GHz 802.11a Wireless LAN Systems," Atheros Communications White Paper, http://www.atheros.com/pt, 2001.
14. T. Clausen, P. Jacquet, A. Laouiti, P. Minet, P. Mulethaler, A. Qayyum, and L. Viennot, "Optimized Link State Routing Protocol," IETF DRAFT, draft-ietf-manet-olsr-02.txt, http://hipercom.inria.fr/olsr/, July 2002.
15. The DAWN project, http://ntrg.cs.tcd.ie/dawn.php.
16. ETSI—BRAN, "ETSI HIPERLAN 1 Standards," http://www.etsi.org/frameset/home.htm?/technicalactiv/Hiperlan/hiperlan1.htm.
17. ETSI—BRAN, "ETSI HiperLAN 2 Standards," http://www.etsi.org/frameset/home.htm?/technicalactiv/Hiperlan/hiperlan2.htm.
18. Global Mobile Information Systems Simulation Library (GloMoSim), http://pcl.cs.ucla.edu/projects/glomosim/.
19. J. Habetha and M. Nadler, "Concept of Wireless Centralized Multihop Ad Hoc Network," in *Proceedings of the European Wireless Conference,* Dresden, September 2002.
20. HomeRF Working Group, http://www.homerf.org.
21. IBM Research, BlueHoc: Open-Source Bluetooth Simulator, http://www–124.ibm.com/developerworks/opensource/bluehoc/.
22. IBM Zurich Research Laboratory, "Wireless Infrared Multipoint Network—Alr," http://www.zurich.ibm.com/cs/wireless/usermodel.html.
23. D. B. Johnson, "Routing in Ad Hoc Networks of Mobile Hosts," in *Proceedings of the. ACM MOBICOM '94,* December 1994.
24. M. Johnsson, "HiperLAN/2—The Broadband Radio Transmission Technology Operating in the 5GHz Frequency Band," White Paper in HiperLAN 2 Global Forum, http://www.hiperlan2.com/technology.asp, 1999.
25. P. Karn, "MACA—A New Channel Access Protocol for Wireless LANs," in *Proceedings of the ARRL/CRRL Amateur Radio 9th Computer Networking Conference,* pp.134–140, 1990.
26. A. McCormick, "OFDM Tutorial," http://oldeee.see.ed.ac.uk/~acmc/OFDMTut.html.
27. Gy. Miklós, A. Rácz, Z. Turányi, A. Valkó, and P. Johansson, "Performance Aspects of Bluetooth Scatternet Formation," in poster section of *MobiHoc 2000,* Boston, MA, August 2002.
28. B. A. Miller and C. Bisdikian, *Bluetooth Revealed: The Insider's Guide to an Open Specification for Global Wireless Communications,* Prentice-Hall, 2000.
29. V. B. Misic and J. Misic. "Performance of Bluetooth Bridges in Scatternets With Limited Service Scheduling", *ACM/Kluwer Journal of Mobile Networks and Applications (MONET),* special issue on Advances in Research of Wireless Personal Area Networking and Bluetooth Enabled Networks, to appear, 2002.

30. Mobile Ad Hoc Network Testbed (MART), http://www.cs.hut.fi/~mart/index.html.

31. The MOMENT Ad Hoc Network Testbed Project, http://moment.cs.ucsb.edu/projects.html.

32. The Monarch Project, http://www.monarch.cs.rice.edu/.

33. The Network Simulator—NS-2, http://www.isi.edu/nsnam/ns/.

34. The OFDM Forum, http://www.ofdm-forum.com.

35. OPNET modeler, http://www.opnet.com.

36. C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination Sequenced Distance Vector Routing (DSDV) for Mobile Computers," in *Proceeding of the ACM SIGCOMM '94,* vol. 24, no. 4, p. 234, October 1994.

37. RFID Technologies, http://www.aimglobal.org/technologies/rfid/.

38. *RFID Journal,* www.rfidjournal.com.

39. B. Sklar, "Rayleigh Fading Channels in Mobile Digital Communications Systems Part I: Characterization," *IEEE Communications Magazine,* pp. 90–100, July 1997.

40. B. Sklar, "Rayleigh Fading Channels in Mobile Digital Communications Systems Part II: Mitigation," *IEEE Communications Magazine,* 102–109, July 1997.

41. Ultra-wideband Networking Group, http://www.uwb.org.

42. The Wireless Network Testbed, http://www.ee.surrey.ac.uk/CCSR/Mobile/Projects/Testbed/.

43. S. Xu and T. Saadawi, "Does the IEEE802.11 MAC Protocol Work Well in Multihop Wireless Ad Hoc Networks?," *IEEE Communications Magazine, 39,* 6, 130–137, June 2001.

44. O-C. Yue, "Design Trade-Offs in Cellular/PCS Systems," *IEEE Communications Magazine,* 146–152, September 1996.

45. G. V. Záruba, "Accelerated Neighbor Discovery in Bluetooth Based Personal Area Networks," in *International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA'02),* Las Vegas, NV, June 2002.

46. G. V. Záruba, I. Chlamtac, and S. Basagni, "Bluetrees—Scatternet Formation to Enable Bluetooth-Based Ad Hoc Networks," in *Proceedings of the IEEE International Conference on Communications (ICC2001),* pp. 273–277, Helsinki, Finland, June, 2001.