Wireless Communications & Networking:

An overview

Ramiro Jordan and Chaouki T. Abdallah

Electrical & Computer Engineering Department

The University of New Mexico

Albuquerque, New Mexico 87131

{rjordan,chaouki}@eece.unm.edu

Contents

Abstract

This paper presents an overview of wireless local area networks (LANs) and wireless personal area networks (PANs), with emphasis on the two most popular standards: IEEE 802.11, and Bluetooth. While there are many such surveys in the current literature and online, we attempt here to present wireless LANs and PANS in a unified fashion as a viable alternative to wired LANs, while stressing the remaining challenges and limitations.

I. Introduction

Wireless communications continue to enjoy exponential growth in the cellular telephony, wireless Internet, and wireless home networking arenas. The wireless networks reviewed in this paper include wireless local area networks (WLANs) and wireless personal area networks (WPANs). WPANs are differentiated from the WLANs with their smaller area of coverage, and their ad-hoc only topology. The very first WPAN was probably the BodyLAN resulting from a DARPA project in the mid-1990s. It was a small-size, low-power, inexpensive network with modest bandwidth that connected personal devices within a range of 2 meters. Motivated by this project, a WPAN group started in 1997 as a part of the IEEE 802 standardization group [11]. The IEEE 802.11 [12] group has been responsible for setting the standards in wireless LANs focusing on the bottom two layers of the Open System Interconnect (OSI) model (see Table I). A similar effort is being conducted by IEEE 802.15 [13] for the wireless PANs.

This paper attempts to survey and compare the state of wireless networking (both WLANs and WPANs) and is organized as follows. Section II presents a history of wireless communications and data. In section III we discuss the challenges of mobility in communications systems, while section IV discusses various network concepts and technologies. Section V presents various acronyms, standards and a list of wireless vendors, while section VI presents our conclusions.

II. History & General Concepts

In this section, we present a brief overview of the history of wireless communication, and describe the development of wireless local area networks, and wide area networks.

A. History of Wireless Transmission

The following history is based mainly on [9]. The history of modern wireless communications starts in 1896 with Marconi who demonstrated wireless telegraphy by sending and receiving Morse code based on long wave ($>> 1km$), using high power transmitters. In 1907 the first commercial Trans-Atlantic wireless service was initiated using huge ground stations and 30×100 m antenna masts. World war I saw the rapid development of communications intelligence, intercept technology, cryptography, and other technologies which became later critical to the advent of a modern wireless system.

In 1920 Marconi discovered shortwave ($< 100m$) transmission. Such waves undergo reflections, refractions, absorptions, and bounce off the ionosphere, making for much more efficient transmission. The higher frequencies needed were made possible by vacuum tubes which became available around 1906. In addition, cheaper, smaller, and better quality transmitters became available. In 1915, a wireless voice transmission between New York and San Francisco was achieved, and in 1920 the first commercial radio broadcast took place in Pittsburgh, PA. In 1921 police cars in Detroit, MI, were equipped with wireless dispatch radios. In 1935 the first telephone call around the world was made and during the World War II years, radio technology developed rapidly to assist with the war effort.

In 1946 the first public telephone service started in 25 major US cities. It used 120 kHz of RF bandwidth in half-duplex mode. Then, in 1950 the FCC doubled the number of mobile channels, and improved technology cut the RF bandwidth to 60 kHz. In 1960 the FM Bandwidth was again cut to 30 kHz. Also, trunking was introduced, and telephone companies could offer full-duplex, auto-dial systems. In 1968 AT&T proposed the cellular concept to the FCC. By 1976, 543 customers (12 channels) could be accommodated in the NY Bell mobile system. In 1982 the European Global System for Mobile Communications (GSM) was established, then in 1983 the FCC allocated 666 duplex channels Advanced Mobile Phone System (AMPS) (40 MHz in 800 MHz band, each channel with 1-way Bandwidth of 30 kHz). In 1984 AT&T was broken and the AMPS cellular system began deploying. In 1985 the FCC released the unlicensed ISM Bands, which were to become important in the development of wireless LANs. In 1989 the FCC granted additional 166 channels (10 MHz

worth) to AMPS. In 1991 the US digital Cellular (USDC) or IS-54 which supports 3 users in each 30 kHz channel was released. This was later improved to accommodate 6 users per channel. In1993, 1.8 GHz was released for data Personal Communications System (PCS), followed in 1994 by the introduction of IS-95 Code Division Multiple Access (CDMA) [10]. During that year, approximately 16 million cellular phones were in use.

With the advent of new digital standards, wireless data communication became more prevalent [8]. In fact, the GSM and IS-95 standards have evolved in the 1990s to include wireless data transmission as an integral part of their service. Finally, the third generation (3G) wireless systems, based on CDMA technologies are being developed and deployed with data and voice communications in tight integration. It is now projected that wireless data traffic will actually surpass that of voice traffic. Moreover, the cost of wireless data devices is now low enough to allow wide penetration in the home and office markets. Many universities (Carnegie Mellon, Georgia Tech, University of Tennessee, etc) are currently operating a high-speed (11 Mbps) wireless network across their campuses.

B. Wireless Data

The original wireless networks were meant for voice traffic and as such as are not particularly suitable for data traffic. As an example, delays of less than 100 ms are required for voice traffic in order to avoid undesirable echoing effects but more delays may be tolerated for most if not all data. On the other hand, Packetized speech can tolerate some packet loss and Bit Error Rates (BER) of 0.001. This may result in a slight quality loss but no major aftermath. A BER of < 0.00001 is required for data transmission and no packet loss is allowed. Finally, telephone conversations last on the average between 3 and 20 minutes, so a set-up time of few seconds is acceptable. Data transmissions could vary from few seconds for a short e-mail, to minutes for a large data transfer, so the set-up time should be very small. These differences greatly affect wireless LANs and PANs, as they are designed to accommodate both data and voice traffics.

B.1 WLANs

Wireless local area networks use high-frequency electromagnetic waves, either infrared (IR) or radio frequency (RF), to transmit information from one point to another. It is generally agreed that RF will be more practical than IR in home and office networking, since it can propagate through solid obstacles. Multiple users traffic is modulated onto the radio waves at the transmitter, and extracted at the receiver. Multiple radio carriers can co-exist in the same physical space, and at the same time without interfering with each other by transmitting at different frequencies (Frequency-Division Multiple Access or FDMA, see Figure 1), in different time-slots, (Time-Division Multiple Access or TDMA, see Figure 2), or using specific codes for each message (Code-Division Multiple Access or CDMA, see Figure 3).

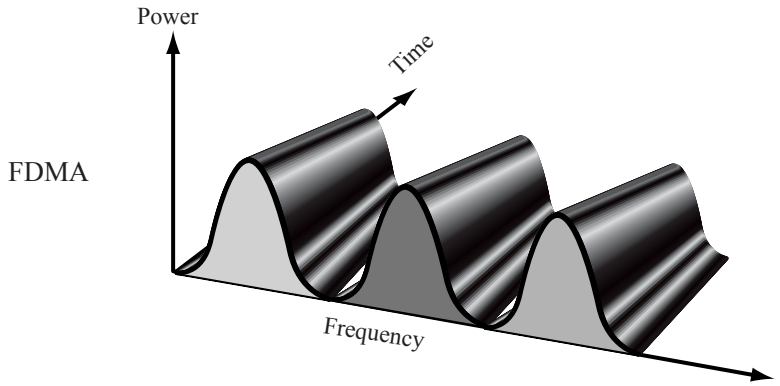

Fig. 1. Frequency Division Multiple Access

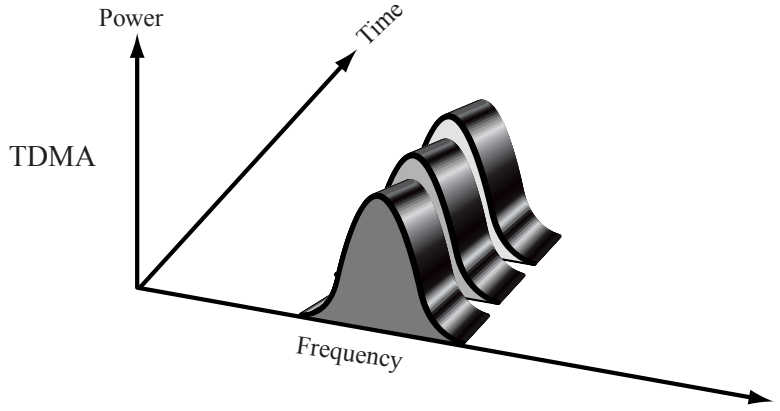

Fig. 2. Time Division Multiple Access

The wireless RF networks can feature an independent, peer-to-peer network, or an ad-hoc network that

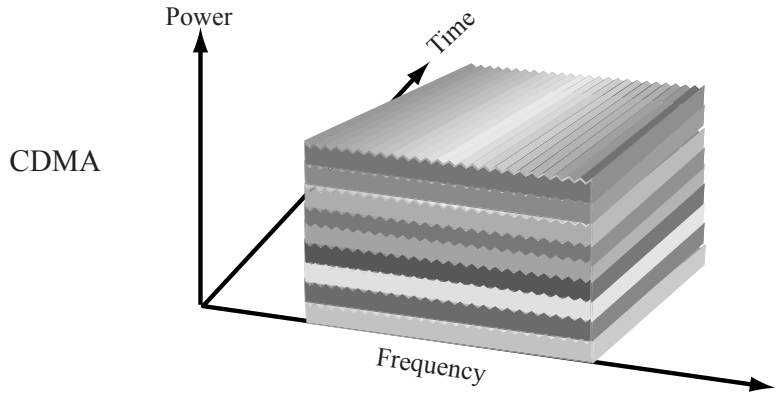

Fig. 3. Code Division Multiple Access

connects communications devices with wireless adapters operating within a given frequency range (such as the ISM bands). Wireless LANs have been standardized by the IEEE 802.11 standards subgroup.

B.2 WPANs

WPANs use RF technologies similar to those of the WLANs but are meant for smaller communication coverage areas (10's of meters versus 100's). In 1998, the WPAN group published the original functionality requirement. Also in 1998, the same group invited participation from several organizations such as Bluetooth [1], HiperLAN [3], HomeRF [2], and others. Only the HomeRF and Bluetooth groups responded. In March 1998, the Home RF group was formed. In May 1998, the Bluetooth development was announced, and a Bluetooth special interests group (SIG) was formed within the WPAN group. Bluetooth has since been selected as the base specification for IEEE 802.15 [13]. In March 1999, the IEEE 802.15 was approved as a separate subgroup within the IEEE 802 group to handle WPAN standardization. The IEEE 802.15 WPAN group focuses on developing standards for short distance wireless networks. The resulting standard is intended to coexist with other wireless and wired networks within the ISM band.

III. Challenges of Mobility in Communications Systems

The main desirable characteristic of wireless networks is their mobility. This desirable characteristic results in, and is influenced by the many challenges encountered in a wireless medium. These challenges take place at various layers of the theoretical OSI communications model. The goal of reliable communication is of course to

Application Layer
Presentation Layer
Session layer
Transport Layer
Network Layer
Data Link Layer Logical Control Sublayer Media Access Control Sublayer
Physical Layer

TABLE I

OSI Seven-Layer Model

guarantee a certain Quality of Service (QoS) as measured for example by speedy and error-free transmission. This places various requirements at the various layers of the theoretical OSI communications model shown in Table I.

In particular, at the physical layer (PHY), a choice needs to be made regarding the transmitting technology (RF or IR). At the Data Link layer, we have to account for the fading radio channels, characterized by burst errors. This makes reliable communications difficult as it becomes affected by short and long term fades [17], [15], [9]. At the Network layer, and due to the movement of the communication unit, constant re-routing may be needed. Due to the limited bandwidth available in a wireless channel, efficient source coding is needed at the Presentation layer. Finally, at the application layer, one has to be conscious about the location-dependence of a particular application. Most importantly however, the physical layer, and the medium access control (MAC) sublayer of the Data Link Layer need to be carefully designed, a job that has fallen on the IEEE 802.11 [14] and 802.15 [13] subgroups. As a specific example wireless devices need to solve a dynamic power control problem so that a particular device is transmitting at the right power level, high

enough for reliable transmission, but not too high as to interfere with nearby devices (see for example [4], [10] for a detailed discussion of this problem). In addition, the various devices need to cooperate in order to provide a system-wide connectivity [5]. Finally, ideas from game theory have recently been introduced to solve the power control problem in wireless networks [7].

IV. Networks Concepts & Technologies

Today, two major technologies are used for wireless LANs and PANs. The first technology exists in the Industrial ISM bands: 2.4–2.4835 GHz, 5.15–5.35 GHz, and 5.725–5.825 GHz. The other technology available in Europe is the Digital European Cordless Telecommunications (DECT) standard, ETS 300 175. We will focus in this paper on the ISM band technologies.

To use the ISM frequency band, equipment must also be compliant to the European Telecommunication Standard ETS 300 328 & FCC 15.247. Since the ISM band is used by other equipment (such as garage door openers and microwave ovens), avoiding interference from such equipment is important. The different standards stipulates that spread spectrum must be used [16]. In a spread-spectrum system, users are multiplexed by assigning them different spreading keys. Such a system is called a Code Division Multiple Access (CDMA) system. However, most wireless LAN and PAN products are not technically CDMA systems since users belonging to the same wireless network utilize the same spreading key. Instead, users are separated in time using a similar Carrier Sense Multiple Access (CSMA) protocol to that used in the Ethernet.

The spreading techniques normally used in wireless LAN products can be divided into two families: Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS). FHSS resists interference by jumping from frequency to frequency in a pseudo-random way. The receiving system jumps synchronously using the same pseudo-random sequence as the sender. DSSS resists interference by multiplying fast pseudo-random bits with the actual data. The receiver, multiplies the same pseudo-random sequence (synchronized) by the received data which generates the original data.

A. IEEE 802.11

The IEEE 802 standards committee formed the 802.11 Wireless Local Area Networks Standards Working Group in 1987. The 802.11-working group which contains members from international companies, universities and organizations, first took on the task of developing a global standard for radio equipment and networks operating in the 2.4GHz unlicensed frequency band for data rates of 1 and 2Mbps. The 802.11 final approval was obtained in 1997. The standard does not specify technology or implementation but simply specifications for the physical (PHY) layer and Media Access Control (MAC) layer (see Table I). The original standard called for 2 Mbps data rate using DSSS or FHSS. In 1999, IEEE 802.11b or the high rate standard with data rates of up to 11 Mbps using DSSS was adopted. Currently, IEEE 802.11a is looking into even faster rates (25 Mbps) in the 5 GHz band. The following discussion is taken mainly from [14].

A.1 Architecture

The IEEE 802.11 standard defines the protocol for two types of networks; Ad-hoc and client/server networks. An Ad-hoc network is a network where communications are established between multiple nodes without the need of an access point or server. The client/server network on the other hand, uses an access point that controls the wireless resources allocation for all nodes and allows mobile stations to roam from cell to cell. The access point is also used to interface the mobile radio to the wired or wireless backbone of the client/server network.

A.2 Media Access Control (MAC)

The access algorithm is based on Carrier Sense Multiple Access (CSMA) with collision avoidance, or CSMA/CA. The MAC supports a variety of physical layers, data rates and propagation characteristics, including infrared (IR) and radio frequency (RF). The MAC layer specification for 802.11 has similarities to the 802.3 Ethernet wired line standard. The protocol for 802.11 uses carrier-sense, multiple access, collision avoidance (CSMA/CA). This protocol prevents collisions instead of detecting them since collisions are bound to happen in a wireless network, unless the protocol attempts to avoid them a priori. The MAC layer, together

with the physical layer samples the energy over the wireless medium. The physical layer uses a clear channel assessment (CCA) algorithm to determine if the channel is clear. This is accomplished by measuring the RF energy at the antenna and determining the strength of the received signal. This measured signal is commonly known as RSSI. If the received signal strength is below a specified threshold the channel is declared clear and the MAC layer is given a green light for data transmission. If the RF energy is above the threshold, data transmissions are deferred in accordance with the protocol rules. The standard provides another option for CCA: Carrier sense can be used to determine if the channel is available by verifying that the channel contains a signal of the same carrier type as 802.11 transmitters, as opposed to simply being corrupted by other RF transmitters.

The CSMA/CA protocol also has options to minimize collisions by using request to send (RTS), clear-to-send (CTS), data and acknowledge (ACK) transmission frames, as described next. Communications is established when one of the wireless nodes sends a short message RTS frame. The RTS frame includes the destination and the length of message. The message duration is termed the network allocation vector (NAV). The NAV alerts all other nodes in the cell to back off for the duration of the transmission. The receiving station issues a CTS frame that echoes the sender's address and the NAV. If the CTS frame is not received by the original sender, it is assumed that a collision occurred and the RTS process starts over. After the data frame is received by the receiver node, an ACK frame is sent back to the sender verifying successful data transmission.

A common limitation with wireless LAN systems is the hidden node problem. This can disrupt communication in a busy wireless environment. This problem occurs when there is a station that can not detect the transmission of another station and thus assumes it is OK to transmit. As an example assume that stations A and B are within a communication range. Station C is also within a communication range of station B but not of A. Therefore both stations A and C could try to transmit at the same time to station B. The use of RTS, CTS, Data and ACK sequences helps to prevent the disruptions caused by this problem.

The IEEE 802.11 standard uses Inter Frame Spaces (IFS) to provide 4 types of priorities. The IFSs define minimum time a station need to wait after it senses that the medium is free. The smaller the IFS, the higher

the priority. If a collision occurs, an exponential backoff algorithm is used to compete for the medium.

Security provisions are addressed in 802.11 as an optional feature. Data security is accomplished by the Wired Equivalent Privacy Algorithm (WEP). WEP is based on protecting the transmitted data over the RF medium using a 64-bit seed key and the RC4 encryption algorithm. WEP only protects the data packet information and not the physical layer header so that other stations on the network can listen to the control data needed to manage the network. Finally, power management is supported at the MAC level for those applications requiring mobility under battery operation. Provisions are made in the protocol for the portable stations to go to low power "sleep" mode during a time interval defined by the base station.

A.3 IEEE 802.11 Physical Layer

Standard IEEE 802.11 provides data rates of 1 Mbit/s with Binary Phase Shift Keying (BPSK) modulation [18] or 2 Mbit/s with Quadrature Phase Shift Keying (QPSK) modulation [18], for DSSS. To mitigate interference and selective fading, five 26 MHz overlapping sub-bands are defined. Center frequencies are 2.412, 2.427, 2.442, 2.457, and 2.470 GHz. For FHSS, data rates of 1 Mbps and 2 Mbps are also defined. The band is divided into 79 sub-bands each with a bandwidth of 1 MHz. Each sub-band hops at a rate of 2.5 hops/sec. Unfortunately, BPSK and QPSK schemes do not meet the demands of higher data rate transmission schemes. To achieve the higher speeds, different modulation techniques should be implemented. The possible techniques considered by the IEEE 802.11 committee are : 1) M-ary Orthogonal Keying (MOK), 2) Complementary Code Keying (CCK), 3) Complementary Code Shift Keying (CCSK), 4) Pulse-Position Modulation (PPM), 5) Quadrature Amplitude Modulation (QAM), 6) Orthogonal Code Division Multiplexing (OCDM), and 7) Orthogonal Frequency Division Multiplexing (OFDM).

IEEE 802.11b selected the CCK scheme due to its resistance to multi-path fading [17], [15] for high data rate at 2.4 GHz band. CCK supports both 5.5 Mbps and 11 Mbps modulation, and it is backward compatible with the 1-2 Mbps scheme. For 5 GHz band, the IEEE 802.11a task group calls for a specification based on OFDM modulation scheme. The RF system operates at 5.15-5.25, 5.25-5.35 and 5.725-5.825 GHz bands. The OFDM system provides a data rate of 6-54 Mbit/s. IEEE 802.11a and HiperLAN2 [3] Physical Layer will

feature essentially the same Physical Layer.

In the DSSS systems, Differential BPSK (DBPSK) and Differential QPSK (DQPSK) [18] are used. FHSS uses 2-4 level Gaussian Frequency Shift keying (FSK) as the modulation signaling method. The radiated RF power is set by the rules governed by FCC part 15 for operation in the United States. Antenna gain is also limited to 6 dBi maximum. The radiated power is limited to 1W for the United States, 10mW per 1Mhz in Europe and 10mW for Japan.

The physical layer data rate for FHSS and DSSS systems is 1 Mbps and 2 Mbps as stated before. The choice between FHSS and DSSS will depend on a number of factors related to the user application and the environment that the system will be operating in. The DSSS physical layer uses an 11-bit Barker Sequence to spread the data before it is transmitted. Each bit transmitted is modulated by the 11-bit sequence. The processing gain of the system is defined as 10 times the log of the ratio of spreading rate (also known as the chip rate) to the data. The receiver de-spreads the RF input to recover the original data. This provides 10.4dB of processing gain, which meets the minimum requirements for the FCC rules. The spreading architecture used in the direct sequence physical layer is not to be confused with CDMA. All 802.11 compliant products utilize the same Pseudo random code and therefore do not have a set of codes available as is required for CDMA operation.

The frequency hop physical layer has 22 hop patterns to choose from. The FHSS physical layer is required to hop across the 2.4GHz ISM band covering 79 channels. Each channel occupies 1MHz of bandwidth and must hop at the minimum rate specified by the regulatory bodies of the intended country. A minimum hop rate of 2.5 hops per second is specified for the United States.

B. Bluetooth or IEEE 802.15

Bluetooth (named after the Viking king who unified Denmark and Norway in the 10th century) is an open standard for short range ad-hoc wireless voice and data networks operating in the unlicensed ISM 2.4 GHz frequency band. Bluetooth was originally conceived by ERICSSION in 1994. In 1998, ERICSSION, Nokia, IBM, INTEL and TOSHIBA formed a special interest group (SIG) to expand the concept and develop a

standard under IEEE 802.15. Currently, over 2000 companies are participating in the Bluetooth SIG, and many are developing Bluetooth products. Bluetooth SIG considers three application scenarios. The first is the wire replacement to connect a PC or laptop to its peripherals. The second is the ad-hoc networking of several different users at short ranges in a small area, forming a "piconet" similar to but smaller than an IEEE 802.11 cell. The third is to use Bluetooth as an access point to wide area voice and data services provided by a wired network or cellular system. The last two application scenarios are in direct competition with the intended use of IEEE 802.11.

Bluetooth transmits at 1 milliwatt (0 dBm), using a hybrid DSSS and FHSS technologies. It can accommodate up to 3 voice channels or 7 data channels per piconet, and a data speed of 721 Kbps per piconet. Its expected system range is around 10 meters. It can support up to 8 devices per piconet, and 10 piconets in a given coverage area. It can provide some security at the Link Layer and requires 2.7 volts as a power source. Finally, a Bluetooth device consumes 30 μA in sleep mode, 60 μA in hold mode, 300 μA in the standby mode and 8-30 mA while transmitting.

B.1 Architecture

The topology of Bluetooth is referred to as scattered ad-hoc network. The network has to be self-reconfigurable so it can adapt to constantly changing users and resources. To implement this, Bluetooth system provides different states for connecting/disconnecting to the network. In addition, the Bluetooth stations have the capability of co-existing in multiple networks. The underlying access method allows the formation of small, independent ad-hoc cells, as well as the capability of connecting to existing large voice and data networks. Bluetooth also requires the interoperability of protocols (to accommodate heterogeneous equipment) and their re-use.

The Bluetooth architecture defines a small cell called a piconet and identifies four states for the stations; Master (M), Slave (S), Stand By (SB), and parked or Hold (P). Each station can be in the M or S states. S stations can participate in one or more piconets. An M station can handle seven simultaneous links and up to 200 active slaves in a piconet. If access is not possible a station enters the SB mode waiting to join a piconet

but keeping its MAC address. A station can be in the P mode, that is in a low power connection, but in this case it must release its MAC address. Up to 10 piconets can operate in one area.

The Bluetooth protocol stack for voice, data and control signaling consist of the following pieces: An RF layer, a Baseband layer, a link Management Protocol (LMP) layer, a Logical Link Control and Adaptation Protocol (L2CAP) Layer, a Service Discovery Protocol (SDP) layer, a Telephony Control Protocol (TCS) layer, an RFCOMM layer, and the application layer. The overall structure of the protocol stack in Bluetooth does not completely match the OSI model (which is after all theoretical) and acronyms. The RF Layer specifies the radio modem. The Baseband Layer specifies the link control at bit and packet levels. It also specifies coding and encryption for packet assembly and frequency hopping operation. The Link Management Protocol (LMP) Layer configures the links by providing encryption and authentication, state of stations in the piconet, power modes, traffic scheduling, and packet format. The Logical Link Control and Adaptation Protocol (L2CAP) Layer provide connection oriented or connectionless services to upper layer protocols, services such as multiplexing, segmentation and re-assembly of packets, and group abstractions for data packets up to 64 kB in size. The audio signal is directly transferred from and application to the Baseband layer. Also, applications and the LMP Layer exchange control messages to prepare the physical transport to a particular application. Different applications may use different protocol stacks but all of them share the same physical and data link control mechanisms. There are three other protocols above L2CAP. The Service Discovery Protocol (SDP) Layer finds the characteristics of the services and connects two or more Bluetooth devices to support a service such as faxing, teleconferencing, or e-business transactions. The Telephony Control Protocol (TCS) Layer defines the call control signaling and mobility management for the establishment of cordless applications. With these protocols legacy telecommunication applications can be supported and developed. The RFCOMM Layer is a “cable replacement” protocol that emulates standard RS-232 control and data signaling over Bluetooth baseband. Using RFCOMM legacy applications can be supported.

The overall Bluetooth protocols can be divided into three groups. The core, exclusively Bluetooth-specific protocols are Baseband, LMP, L2CAP, and SDP. Protocols developed based on existing protocols include RFCOMM and TCS Binary and AT Commands. And the third group consist on protocols adopted by

Bluetooth SIG [1]. The Bluetooth specification is open, and other legacy protocols such as HTTP, FTP can be accommodated on top of the existing Bluetooth stack.

B.2 Media Access Control

The medium access mechanism in Bluetooth is a fast FHSS-CDMA/TDD system that employs system polling to establish a link. The 1,600 hops per second allow short time slots of 625 μ seconds (625 bits at 1 Mbps) for one packet of transmission that allows good performance in the presence of interference. FH-CDMA allows tens of piconets to overlap in the same area providing an effective throughput that is greater then 1 Mbps. The access method in each piconet is TDMA/TDD. TDMA allows multiple voice and data stations to participate in a a piconet. Time division duplexing (TDD) eliminates crosstalk between the transmitter and receiver, allowing a single chip implementation in which the radio alternates between transmitter and receiver modes. To share the medium among a large number of stations, at each slot the Master station decides and polls a Slave station. Polling is using instead of contention methods because contention requires more overhead for the short packets (625 bits) that were selected for implementation of a fast FHSS system.

Audio data can be transferred between one or more Bluetooth devices. Various usage models are possible and audio data in SCO packets is routed directly to and from the Baseband Layer and it does not go through L2CAP. The Audio model is relatively simple within Bluetooth; any two Bluetooth devices can send and receive audio data between each other just by opening an audio link. The Bluetooth air-interface, is either a 64 kb/s log Pulse Code Modulated (PCM) format (A-law or μ-law [9]) is used, or a 64 kb/s Continuous Variable Slope Delta Modulation (CVSDM) is used. The latter format applies an adaptive delta modulation algorithm with syllabic companding. The voice coding on the line interface should have a quality equal to or better than the quality of 64 kb/s log PCM.

The Bluetooth specifications provide for user protection and information confidentiality. There are three methods of operation: non-secure, service-level, and link-level security. Devices can also be classified into trusted and distrusted. Bluetooth security makes use of two secret keys, it uses 128 bits for user authentication and 8 to 128 bits for data encryption. It also uses 128 bits for random number generation and the 48-bit

MAC address of devices. Any pair of stations will create a session or link key using an initialization key, the device MAC address, and a PIN number.

B.3 Physical or Baseband and RF Layers

In the OSI Physical (PHY) Layer the RF and Baseband layers of Bluetooth are located. The Baseband layer contains the hardware that turns received radio signals into a digital form, which can be processed by the host application. It also converts digital or voice data into a form that can be transmitted using a radio signal. Each packet contains information about where it is coming from, what frequency it is using, and where it is going. Packets also contain information on how the data was compressed, the order in which the packets were transmitted, and information used to verify the effectiveness of the transmission. When the data is received it is checked for accuracy, extracted from the packet, reassembled, decompressed, and possibly filtered. The Baseband processor handles all the tasks just described. It takes care of converting data from one form to another (such as from voice to digital data), compressing it, putting it into packets, taking it out of packets, assigning identifiers and error correction information, and then reversing the entire process for data that is received. In Bluetooth, the Baseband function is called the link controller.

As mentioned earlier, the Bluetooth radio is a short-distance, low-power radio that operates in the unlicensed ISM spectrum of 2.4 GHz, using a nominal antenna power of 0 dBm. At 0 dBm, the range is 10 meters, meaning equipment must be within 10 meters of each other (about 33 feet) to communicate using the Bluetooth standard. Optionally, a range of 100 meters (about 328 feet) may be achieved by using an antenna power of 20 dBm. Data is transmitted at a maximum gross rate of up to 1 Mbps. Communication protocol overhead limits the practical data rate to a little over 721 kbps. Interference or being out of range may increase the bit error rate (BER) and require packets to be re-sent, further decreasing the achievable data rate. The 2.4-GHz frequency is shared by other types of equipment not the least being the IEEE 802.11 equipment. As a result, interference with Bluetooth devices is inevitable. The Bluetooth specification addresses this issue by using a two-level GFSK modem employing Frequency-Hopping Spread-Spectrum (FHSS) techniques. The two-level GFSK modem allows simple non-coherent detection implementation using FM demodulators. Bluetooth uses

seventy-nine hop frequencies spaced 1 MHz apart in the frequency range of 2.402 to 2.480 GHz. The hop rate is 1,600 hops per second (625-s dwell time, at each frequency). If the transmission encounters interference, it waits for the next frequency hop and re-transmits on a new frequency. Each piconet is assigned a specific frequency-hopping pattern. The pattern is determined by the piconet identity and master clock of the master station. The overall hopping pattern is divided into two 32 hop segments, odd and even. Each 32 hop pattern starts at a point in the spectrum and hops over a pattern that covers 64 MHz. After completion of each segment, the sequence is altered, and the pattern is shifted 16 frequencies in the forward direction. The 32 hops are concatenated, and the random selection of the index is changed for each new segment. The Baseband layer uses inquiry and paging procedures to synchronize the transmission hopping frequency and clock of different Bluetooth devices. It provides 2 different kinds of physical links with their corresponding baseband packets, Synchronous Connection-Oriented (SCO) and Asynchronous Connectionless (ACL) which can be transmitted in a multiplexing manner on the same RF link. ACL packets are used for data only, while the SCO packet can contain audio only or a combination of audio and data. All audio and data packets can be provided with different levels of FEC or CRC error correction and can be encrypted. Furthermore, the different data types, including link management and control messages, are each allocated a special channel. All audio and data packets can be provided with different levels of FEC or CRC error correction and can be encrypted. Furthermore, the different data types, including link management and control messages, are each allocated a special channel. The Bluetooth system provides a point-to-point connection (only two Bluetooth units involved), or a point-to-multipoint connection. In the point-to-multipoint connection, the channel is shared among several Bluetooth units. Two or more units sharing the same channel form a piconet. One Bluetooth unit acts as the master of the piconet, whereas the other unit(s) acts as slave(s). Up to seven slaves can be active in the piconet. In addition, many more slaves can remain locked to the master in a so-called parked state. These parked slaves cannot be active on the channel, but remain synchronized to the master. Both for active and parked slaves, the channel access is controlled by the master. Multiple piconets with overlapping coverage areas form a scatternet. Each piconet can only have a single master. However, slaves can participate in different piconets on a time-division multiplex basis. In addition, a master in one piconet

can be a slave in another piconet. The piconets shall not be time or frequency synchronized. Each piconet has its own hopping channel. Two link types may be defined between a master and slave(s): 1) Synchronous Connection-Oriented (SCO) link, and 2) Asynchronous Connection-Less (ACL) link. The SCO link is a point-to-point link between a master and a single slave in the piconet. The master maintains the SCO link by using reserved slots at regular intervals. The ACL link is a point-to-multipoint link between the master and all the slaves participating on the piconet. In the slots not reserved for the SCO link(s), the master can establish an ACL link on a per-slot basis to any slave, including the slave(s) already engaged in an SCO link.

C. Convergence Scenario

The application spaces of Bluetooth and IEEE 802.11 overlap. Many of the applications envisioned for IEEE 802.11 are also defined for Bluetooth. Yet, there are situations and conditions where IEEE 802.11 is better suited for transmitting data than Bluetooth and vice versa. Both IEEE 802.11 and Bluetooth consider data exchange as a primary function. Bluetooth and IEEE 802.11 Both use the same upper layer protocol to implement these data transfer applications, which allows Bluetooth and IEEE802.11 devices to co-exist.

Bluetooth's maximum mobility within the piconet allows for data exchange applications that may be difficult with IEEE 802.11. For example, with Bluetooth a person could synchronize their phone with a PC without taking the phone out of their pocket. An important feature of both Bluetooth and IEEE 802.11 is the ability to wirelessly connect to a wired network. Bluetooth's multipoint capability allows multiple devices to efficiently share the media. The one potential area of weakness for Bluetooth, when compared to IEEE 802.11, is performance. Bluetooth's aggregate bandwidth is limited to 1 Mbps, while IEEE 802.11 supports 11 Mbps with 25 Mbps under development. Moreover, Bluetooth coverage area is much smaller than that of IEEE 802.11.

A native feature of the Bluetooth specification is synchronous voice channels. Bluetooth has the ability to reserve bandwidth for carrying digital voice data. Finally, note that IEEE 802.11 devices are currently widely available and cost effective. Some manufacturers have completely integrated IEEE 802.11 solutions into their computers. Bluetooth's promise however remains unfulfilled as of today, although Bluetooth gadgets

are beginning to appear (see Table V).

Note that recent work is also being done on marrying IEEE 802.11 to the Telecommunications Industry Association/Electronics Industry Alliance (TIA/EIA) IS-856 standard [6]. While IEEE 802.11 focuses on WLANs, IS-856 deals with wireless wide area networks ranging in the tens of kilometers.

V. Acronyms, Standards Bodies, and Vendors

In this section, we provide for the reader's benefit a collection of acronyms, organizations and wireless vendors.

ACRONYMS	**DETAILS**
FCC	Federal Communications Commission
CDMA	Code division multiple access
FDMA	Frequency division multiple access
GSM	Global system for mobile communications
IEEE	Institute of Electrical & Electronics Engineers
IMTS	Improved Mobile telephone service
ISM	International, Scientific, Medical
ISO	International standards organization
ITU	International telecommunications Union
OSI	Open System Interconnect
TDMA	Time division multiple access
USDC	US digital cellular

TABLE II

List of Communications Acronyms

ORGANIZATION	FUNCTION	ADDRESS
FCC	Allocates spectrum in US	www.fcc.gov
IEEE	Technical standards body	www.ieee.org
ITU	Global markets and standards	www.itu.int
ISO	International standards organization	www.iso.org
WLANA	Education	www.wlana.org
Bluetooth SIG	Promote Bluetooth	www.bluetooth.com
HomeRF	Technology alliance	www.homerf.org
University of New Hampshire	Education	www.iol.unh.edu
GWEC	Education	www.gwec.org

TABLE III

List of Some Communications Organizations

VI. Conclusions

We have presented in this paper an overview of wireless LANs and PANs stressing the two most common standards, IEEE 802.11 and Bluetooth. While limited in scope, we have attempted to give the reader a quick comparison between the two technologies stressing various problems an solutions to the wireless networking problems.

IEEE WORKING GROUPS	TASK
802.0	Sponsor executive committee (SEC)
802.3	CSMA/CD working group
802.6	Metropolitan Area Network (MAN) working group
802.11	Wireless LAN (WLAN) working group
802.11 MAC	MAC for WLANs
802.11 PHY	Three PHY's: IR, 2.4 GHz FHSS & 2.4 GHz DSSS
802.11a	2 Mbps PHY
802.11b	Higher rate (11 Mbps) PHY
802.11c	Collaborate with 802.1 group
802.11d	Physical layer in new markets
802.11e	MAC enhancements
802.11f	Access points interoperability
802.11g	Higher 802.11b speeds
802.11h	Enhance 802.11 MAC and 802.11a PHY
802.11i	Enhance 802.11 MAC security
802.11 SG	Placement in Standards
802.11 5GSG	Globalization of 5GHz
802.11 PC	Publicity
802.11 R-REG	Regulatory issues
802.15	Wireless Personal Area network (WPAN) working group

TABLE IV

SOME IEEE 802 WORKING GROUPS

VENDOR	PRODUCT	ADDRESS
3COM	Bluetooth/802.11 Access points, PC cards	www.3com.com
Acer NeWeb	802.11 Access points, PC cards	www.acerneweb.com
Agere (ORiNOCO,Lucent)	802.11 Access points, PC cards, Bridges	www.agere.com
AmbiCom	802.11 Access points, PC cards	www.ambicom.com
Apple	802.11 Access points, PC cards	www.apple.com
Buffalo Technology	802.11 Access points, PC cards	www.buffalotech.com
Cisco (Aironet)	802.11 Access points, PC cards	www.cisco.com
D-Link Systems	802.11 Access points, PC cards	www.dlink.com
Linksys	802.11 Access points, PC cards	www.linksys.com
NETGEAR	802.11 Access points, PC cards	www.netgear.com
Proxim	HomeRF/802.11 Access points, PC cards	www.proxim.com
SOHOware	802.11 Access points, PC cards	www.sohoware.com
U.S. Robotics	802.11 Access points, PC cards	www.usrobotics.com
Xircom (Intel Company)	802.11 Access points, PC cards	www.xircom.com
Zoom Telephonics	802.11 Access points, PC cards	www.zoom.com

TABLE V

List of Some Wireless Vendors

References

[1] Bluetooth SIG. Website: www.bluetooth.org.

[2] HomeRF. Website: www.homerf.org.

[3] HiperLAN 2 Global Forum. Website: www.hiperlan2.com.

[4] Aly ElOsery. Autonomous Power Control in CDMA Cellular Systems Ph.D. Dissertation, EECE Department, University of New Mexico, 2001.

[5] P. Gupta and P. Kumar. The Capacity of Wireless Networks. *IEEE Trans. Inform. Theory*, 46, May 2000.

[6] J.W. Noerenberg II. Bridging Wireless Protocols. *IEEE Communications Magazine*, Vol. 39, No. 11, pp. 90–97, November 2001.

[7] A.B. MacKenzie and S.B. Wicker. Game Theory and the Design of Self-Configuring, Adaptive Wireless Newtorks. *IEEE Communications Magazine*, Vol. 39, No. 11, pp. 126–131, November 2001.

[8] V.K. Garg. *Wireless Network Evolution: 2G to 3G.* Prentice Hall PTR, New Jersey, 2002.

[9] T. S. Rappaport. *Wireless Communications: Principles and Practice.* Prentice Hall PTR, New Jersey, 2002.

[10] A.J. Viterbi. *CDMA principles of Spread Spectrum Communication.* Addison-Wesley, Reading, MA, 1995.

[11] IEEE 802 group. Website: grouper.ieee.org/groups/802.

[12] IEEE 802.11 group. Website: grouper.ieee.org/groups/802/11.

[13] IEEE 802.15 group. Website: grouper.ieee.org/groups/802/15.

[14] IEEE. Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specification. P802.11D6.2, July 1998.

[15] M. Yacoub. *Foundations of Mobile Radio Engineering.* CRC Press, 1993.

[16] R. Ziemer, R. Peterson, and D. Borth. *Introduction to Spread Spectrum Communications* Prentice-Hall, Upper Saddle River, NJ, 1995.

[17] W.C.Y. Lee. *Mobile Cellular Telecommunications Systems.* McGraw Publications, New York, 1989.

[18] W.C.Y. Lee. *Digital Communications, 4th Ed..* McGraw-Hill, New York, 2000.