NEAR EAST UNIVERSITY

Fac·ulty of Englneering

\

Department of Electrical & Electronic
Engineering

WIRELESS COMMUNICATION USING BLUETOOTH

Graduation Project
EE -400

Siudent: **Özer İngün (970916)**

Supervısôri: Prof.t.Or.<Fakhreddin Memedov

Lefkoşa - 2005

CONTENTS

ACKNOWLEDGEMENT

I am very thankful to my supervisor Prof. Dr. Fakhreddin Memedov who was generous with his help at every stage in preparation ofthis project.

Special thanks to Near East University education staff, especially to Electrical and Electronic Engineerinğ-staff for concem ofme.

Also my heartily gratitude goes to my friends Özgür İNGÜN, Barış TANYERİ for their help and suggestion during preparation ofmy project.

Finally, I want to thaıılcto my parents for their sacrificed, supported and encouraged me during my educatiorı.'Without their endless support and love for me, I would have never achieved my currenfpösition.

LIST OF ABBREVIATIONS

lG	First Generation
2G	Second Generation
2.5G	Twô--and-a-Half Generation
3G	Th:frd. Generation
AES	Advanced Encryption Standard
AP	Access Point
BSS	Basic Service Set
CDPD	Cellular Digital Packet Data
CVSD	Continuous Variable Slope Delta Modulation
DSSS	IDirect Sequence Spread Spectrum
EM	.Electromagnetic
ESS	Extended. Service Set
ETSI·	Eurôpean Telecommunications Standarda Institute
FH	Frequency Hopping
FHSS	Frequency Hopping Spread Spectrum
GAP	Generic Access Profile
GFSK	Gaussian Frequency Shift Keying
GSM	Global System for Mobile Communications
HC::I	HostController Interface
IBSS	Interdependent Basic Service Set
IEEE	Institute of Electronic and Electrical Engineering

IP	Internet Protocol
IR	Infrared
IrDA	Infra-red Data Association
IrOBEX	Infra-red OBject EXchange protocol
ISDN	I:fitegratedServices Digital Networks
ISM	Iıdustrial, Scientific, Medical
ITU-T	ınternational Telecommunications Union-Telecommunication
L2CAP	Logical Link Control and Adaption Protocol
LAN	Local Area Network
LCP	:Uirık ControLProtocol
LM	Link Manager
LMP	Link Manager Protocol
MAC	:MediumAccess Control
MMS	Multi-Media Messaging Service
NIC	Network Interface Card
OBEX	OBject EXchange protocol
OFDM	O:rtliogonalFrequency Division Multiplexing
OSI	Open Systems I:fiterconnection
P2P	Peerto Peer
PAN	Personal Area Network
PC	Personal Computer
PCM	Pulse Coded Modulation
PCMCIA	Personal ComputerMemory Card I:fiternationalAssociation
PDA	PersonalDigital Assistant
PHY	Physical Layer
PiN	Personal Identification Number
ppp	Point-to-Point Protocol

RF	Radio Frequency
RFCOMM	Serial cable emulation protocol based on ETSI TS 07.10
RS-232	A serial communications interface
SAP	Service. Access Points
SDP	Service Discovery Protocol
SIG	Special Interest Group
TCP	Transport Control Protocol
TCS	Telephony Control protocol Specification
TDD.	Ti:riie ..Division Duplex
UART	Universal Asynchronous Receiver Transmitter
UDP	User Datagram Protocol
USB	Universal Serial Bus
WAP	Wireless Application Protocol
WI-FI	Wireless Fidelity
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Networks
WWAN	Wireless Wide Area Network

INTRODUCTION

.~

~ortanı characteristicsand applicationsof Bluetoothwirelesscommunications are examined. The packet formats of the Bluetooth protocols are particularly studied in all ',layer parts. It also deals with marketing aspects. Furthermore, the reliablity of the Bluetooth, competing technologies, usage models, products and its effects on human health are the other examined topics.

The document begins with an technology overwiev part where the Wireless communication history, marketing aspects arid technology basics are described. in chapter 2 also includes the story of how this technology came to be named Bluetooth. in the technology basics subtopic, the basic of wireless communications and some necessary a priori knowledge about Bluetooth as master an slave roles, communication topologies, are explained. The Bluetooth protocol layers and their configuration is described in the section Bluetooth protocols, chapter 3. in this chapter, the packet formats and the links that the Bluetooth devices can communicate over, are especially examined.i'J'he main purpose of this section is to clearly understand and explain all time period passing bef'\\reenthe starting and end point of the communication between at least two Bluetooth device.Chapter 4 covers some ofthe usage models of Bluetooth and early products. A brief look at the near Bluetooth future is done in the last section in the concluding part and references are ordered from most used souce to least used one. in chapter 5, The competing technologies as .ItDA, UWB, IEEE 802.11 and HomeRF are explained shortly. Finally, The effects ofBluetooth systems on human health is presented in chapter 6.

ABSTRACT

The objective of this project is examining of important characteristic and applications Bluetooth wireless communication technologies. Bluetooth frequencies , security specifications and products will analyzed.

1. WIRELESS TECHNOLOGIES

1.1 Overview of Wireless Technology

Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections without requiring network or peripheral cabling. Wireless technologies use radio frequency transmissions as the means for transmitting <lata, whereas wired technologies use cables. Wireless technologies range from complex systems, such as Wireless Local Area Networks (WLAN) and cell phones to simple devices such as wireless headphones, microphones, and other devices that do not process or store information. They also include infrared (IR) devices such as remote controls, some cordless computer keyboards and mice, and wireless hi-fi stereo headsets, all of which require a direct line of sight between the transmitter and the receiver to close the link. A brief overview of wireless networks, devices, standards are presented in this section.

1.2 Wireless Networks

Wireless networks serve as the transport mechanism between devices and among devices and the traditional wired networks (enterprise networks and the Internet). Wireless networks are'many and diverse but are frequently categorized into three groups based on their coverage range: Wireless Wide Area Networks (WWAN), WLANs, and Wireless Personal Area Networks (WPAN). WWAN includes wide coverage area technologies such as 2G cellular, Cellular Digital Packet Data (CDPD), Global System for Mobile Communications (GSM), and Mobitex. WLAN, representing wireless local area networks, includes 802.11, HiperLAN, and several others. WPAN, represents wireless personal area network technologies such as Bluetooth and IR. All of these technologies are "tether less"-they receive and transmit information using electromagnetic (EM) waves. Wireless technologies use wavelengths ranging from the radio frequency (RF) band up to and above the IR band. The frequencies in the RF band cover a significant portion of the EM radiation spectrum, extending from 9 kilohertz (kHz), the lowest allocated wireless communications frequency, to thousands of gigahertz (GHz). As the frequency is increased beyond the RF spectrum, EM energy moves into the IR and then the visible spectrum. This document focuses on WLAN and WP AN technologies.

1.3 History ofWLAN

Motorola developed one ofthe first commercial WLAN systems with its Altair product. However, early WLAN technologies had several problems that prohibited its pervasive use. These LANs were expensive, provided low data rates, were prone to radio interference, and were designed mostly to proprietary RF technologies. The IEEE initiated the 802.11 projects in 1990 with a scope "to develop a Medium Access Control (MAC) and Physical Layer (PHY) specification for wireless connectivity for fixed, portable, and moving stations within an area." in 1997, IEEE first approved the 802.11 intemational interoperability standard. Then, in 1999, the IEEE ratified the 802.1la and the 802.11b wireless 'networking communication standards. The goal was to create a standards-based technology that could span multiple physical encoding types, frequencies, and applications, The 802.1la standard uses orthogonal frequency division multiplexing (OFDM) to reduce interference. This technology uses the 5 GHz frequency spectrums ari.d can process data at up to 54 Mbps.

1.3.1 FrequencyXatıd Data Rates

Ethemet that has been available for many years. The IEEE 802.1la standard is the most widely adopted IEEE developed the 802.11 standards to provide wireless networking technology like the wired tı:iember.ofthe 802.11 WLAN families. it operates in the licensed 5 GHz band using ÔFDM t~chııölogy. The popular 802.llb. standard operates in the unlicensed 2.4 GHz-2.5 GHz Iıądustrial, Scientific, and Medical (ISM) frequency band using a direct sequence spread-spectrum technology. The ISM band has become popular for wireless communications because it is available worldwide. The 802.11b WLAN technology permits transmission speeds of up to 11 Mbits per second. This makes it considerably faster than the original IEEE 802.11 standard (that sends data at up to 2 Mbps) and slightly faster than standard Ethemet.

Table 1.1 Key Characteristics of802.11 Wireless LANs

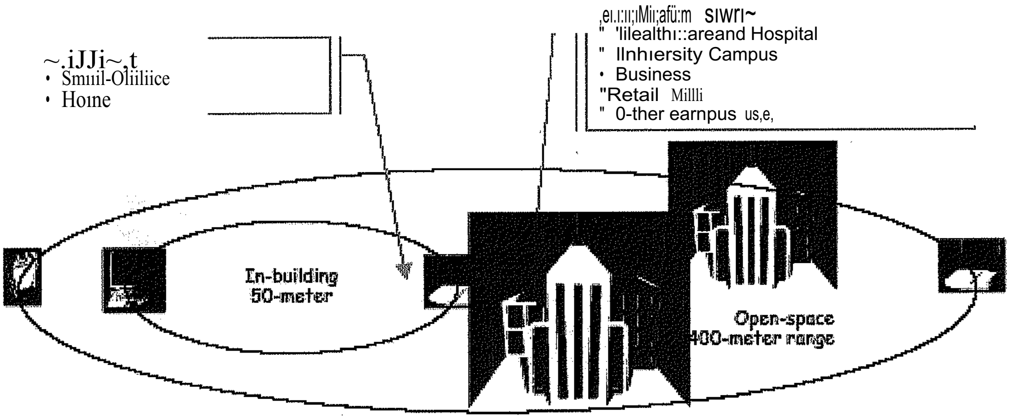
Characteristic	Description
Physical Layer	Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), Orthogonal Frequency Division Multiplexing (OFDM), infrared (IR).
Frequency Band	2.4 GHz (ISM band) and 5 GHz.
Data and Network Security	RC4-based stream encryption algorithm for confidentiality, authentication, and integrity. Limited key management. (AES is being considered for 802.1 li.)
Operating Range	Up to 150 feet indoor and 1500 feet outdoors.
Positive Aspects	Ethemet speeds without wires; many different products from many different companies. Wireless client cards and access point costs are decreasing.
Negative Aspects	Poor security in native mode; throughput decrease with distance and load.

1.3.2 WirelessLAN Components

A WLAN comprises two types of equipment: a wireless station and an access point. A station, or client, is typically a laptop or notebook personal computer (PC) with a wireless NIC. A WLAN client may also be a desktop or handheld device (e.g., PDA, or custom device such as a barcode scanner) or equipment within a kiosk on a manufacturing floor or other>publicly. .accessed area. Wireless laptops and notebooks "wireless enabled" are identical to Iaptops and notebooks except that they use wireless NICs to connect to access points in the network. The wireless NIC is commonly inserted in the client's Personal Computer Memory Card Intemational Association (PCMCIA) slot or Universal Serial Bus (USB) port. The NICs use radio signals to establish connections to the WLAN. The AP, which acts as a bridge between the wireless and wired networks, typically comprises a radio, a wired network interface such as 802.3, and bridging software. The AP functions asa base station for the wireless network, aggregating multiple wireless stations onto the wired network.

1.3.3 Range

The reliable coverage range for 802.11 WLAN's depends on several factors, including data rate required and capacity, sources of RF interference, physical area and characteristics, power, connectivity, and antenna usage. Theoretical ranges are from 29 meters (for 11 Mbps) in a closed office area to 485 meters (for 1 Mbps) in an open area. However, through empirical analysis, the typical range for connectivity of 802.11 equipment is approximately 50 meters (about 163 ft.) indoors. A range of 400 meters, nearly V,ı mile, makes WLAN the ideal technology for many campus applications. It is important to recognize that special high-gain antennas can increase the range to several miles.



Figurel.1 Typical Range of802.11 WLAN

AP's may also provide a "bridginğ" function. Bridging connects two or more networks together and allows them to coınmunicate to exchange network traffic. Bridging involves either a point-to-point or a multipoint configuration. In a point-to-point architecture, two LANs are connected to each other via the LAN's respective AP's. In multipoint bridging, one subnet on a LAN is connected to several other subnets on another LAN via each subnet AP. For example, ifa computer on Subnet A needed to connect to computers on Subnets B, C, and D, Subnet A's AP would connect to B's, C's, and D's respective AP's. Enterprises may use bridging to connect LANs between different buildings on corporate campuses. Bridging AP devices are typically placed on top of buildings to achieve greater antenna reception. The typical distance over which one AP can be connected wirelessly to another by means of bridging is approximately 2 miles. This distance may vary depending on several factors including the specific receiver or transceiver being used. Figure 1.2 illustrates point-to-point bridging between two LANs. In the example, wireless data is being transmitted from Laptop A to Laptop B, from one building to the next, using each building's appropriately positioned AP. Laptop A connects to the closest AP within the building A. The receiving AP in building A then transmits the data (over the wired LAN) to the AP bridge located on the building' s roof. That AP bridge then transmits the data to the bridge on nearby building B. The building's APbridge then sends the data over its wired LAN to Laptop B.

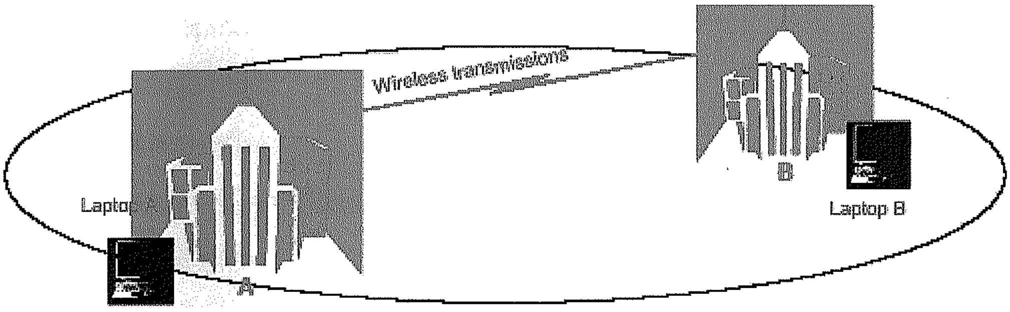


Figure 1.2 Access Point Bridging

1.3.4 Benefits

WLAN s offer four prii.nacyibeiiefits:

- User Mobility-----'-Ustfrs>can access files, network resources, and the Intemet without having to physically connect to the network with wires. Users can be mobile yet retain high-speed, real-time access to the enterprise LAN.
- Rapid Installation=-The time required for installation is reduced because network connections can be made without moving or adding wires, or pulling them through walls or ceilings, or making modifications to the infrastructure cable plant. For example, WLANs are often cited as making tAN installations possible in buildings that are subject to historic preservation rules.
- Flexibility-Enterprises can also enjoy the flexibility of installing and taking down WLANs in locations as necessary. Users can quickly install a small

WLAN for temporaty needs such as a conference, trade show, or standards meeting.

- Scalability-WLAN network topologies can easily be con:figured to meet specific application and installation needs and to scale from small peer-to-peer networks to very large enterprise networks that enable roaming over a broad area.

Because of these fundamental benefits, the WLAN market has been increasing steadily over the past several years, and WLANs are still gaining in popularity. WLANs are now becoming a viable alternative to traditional wired solutions. For example, hospitals, universities, airports, hotels, and retail shops are already using wireless technologies to conduct their daily business operations.

1.4 Ad Hoc Networks

Ad hoc networks such as Bluetooth are networks designed to dynamically connect remote devices such as cell phones, laptops, and PDAs. These networks are termed "ad hoc" because of their shifting network topologies. Whereas WLANs use a fixed network infrastructure, ad hoc networks maintain random network con:figurations, relying on a master-slave system connected by wireless links to enable devices to communicate. in a Bluetooth network, the master of the piconet controls the changing network topologies of these uetworks. It also controls the flow of <lata between devices that are capable of supporting direct links to each other. As devices move about in an unpredictable fashion, these networks must be reconfigured. on the fly to handle the dynamic topology. The routing that protocol Bluetooth employs allows the master to establish and maintain these shifting networks.

Figure 1.5 illustrates an example ofa Bluetooth-enabled mobile phone connecting to a mobile phone network, synchronizing with a PDA address book, and downloading e-mail on an IEEE 802.11 WLAN.

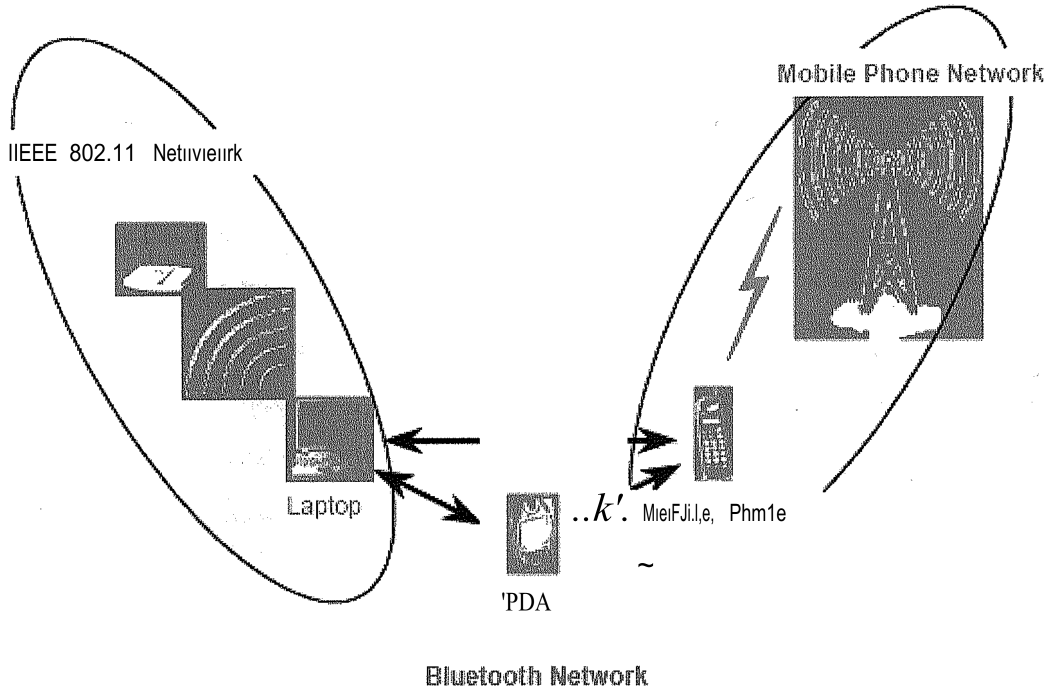


Figure 1.5 Notional Ad Hoc Network

1.5 Wireless Devices

A wide range of·devföesuse wireless technologies, with handheld devices being the most prevalent form.today. This document discusses the most commonly used wireless handheld devices such;:ı.stextmessaging devices, PDAs, and smart phones.

1.5.1 PersonalDiğifal Assistants

PDAs are data organize:rstha.fare small enough to fit into a shirt pocket or a purse. PDAs offer applications such as office' pröductivity, database applications, address books, schedulers, and to-do lists, a.ı:ıd they a.llôwusers to synchronize data between two PDAs and between a PDA and a personal computer. Newer versions allow users to download their e-mail and to connect to the Intemet. Security administrators may also encounter one-way and two-way text-messaging devices. These devices operate on a proprietary networking standard that disseminates e-mail to remote devices by accessing the corporate network. Text-messaging technology is designed to monitor a user's inbox for new e-mail and relay the mail to the user's wireless handheld device via the Intemet and wireless network.

1.5.2 Smart Phones

Mobile wireless telephones, or cell phones, are telephones that have short wave analog or digital transmission capabilities that allow users to establish wireless connections to nearby transmitters. As with WLANs, the transmitter's span of coverage is called a "cell." As the cell phone user moves from one cell to the next, the telephone connection is effectively passed from one local cell transmitter to the next. Today's cell phone is rapidly evolving to integration with PDAs, thus providing users with increased wireless e-mail and Intemet access. Mobile phones with information processing and <lata networking capabilities are called "smart phones." This document addresses the risks introduced by the information processing and networking capabilities of smart phones.

1.6 Wireless Stanclards

Wireless technologies"conform to a variety of standards and offer varying levels of security features. /The principal advantages of standards are to encourage mass production and tôVallow products from multiple vendors to interoperate. For this document, the disctissiôn of wireless standards is limited to the IEEE 802.11 and the Bluetooth standard.. WLANs follow the IEEE 802.11 standards. Ad hoc networks follow proprietary techı::ıiqtiesor are based on the Bluetooth standard, which was developed by a consô:rtiumôf commercial companies making up the Bluetooth Special Interest Group (SIG)?Theseistandards are described below.

1.6.1 IEEE 802~11

WLANs are based on the IEEE 802(11 standard, which the IEEE first developed in 1997. The IEEE designed' 802.1l tö support medium-range, higher <lata rate applications, such as Ethemet networks, and to address mobile and portable stations. 802.11 are the original WLAN standard, designed for 1 Mbps to 2 Mbps wireless transmissions. It was followed in 1999 by 802.1la, which established a high-speed WLAN standard for the 5 GHz band and supported 54 Mbps. Also completed in 1999 was the 802.11b standard, which operates in the 2.4 - 2.48 GHz band and supports 11 Mbps. The 802.11b standard is currently the dominant standard for WLANs, providing sufficient speeds for most of today's applications. Because the 802.llb standard has been so widely adopted, the security weaknesses in the standard have been exposed. Another standard, 802.llg, still in draft, operates in the 2.4 GHz waveband, where

current WLAN products based on the 802.11 b standard operate. Two other important and related standards for WLANs are 802. lX and 802.lli. The 802.lX, a port-level access control protocol, provides a security framework for IEEE networks, including Ethemet and wireless networks. The 802. I li standard, also still in draft, was created for wireless-specific security functions that operate with IEEE 802. lX.

1.6.2 IEEE 802.11 Arehttecnıre

The IEEE 802.11 standard permits devices to establish either peer-to-peer (P2P) networks or networks based on fixed access points (AP) with which mobile nodes can communicate. Hence, the standard defines two basic network topologies: the infrastructure network: arid the ad hoc network. The infrastructure network is meant to extend the range ofthe wired LAN to wireless cells. A laptop or other mobile device may move from celltö cell (from AP to AP) while maintaining access to the resources of the LAN. A cell is the area covered by an AP and is called a "basic service set" (BSS). The collection of all cells of an infrastructure network is called an extended service set (ESS). This first topology is useful for providing wireless coverage of building or campusjareas. By deploying multiple APs with overlapping coverage areas, organizations can achieve broad network coverage. WLAN technology can be used to replace wired LANstotally and to extend LAN infrastructure. A WLAN environment has wireless client stations that use radio modems to communicate to an AP. The client stations are generallyfequipped with a wireless network interface card (NIC) that consists of the radio tran.scc:iver..and the logic to interact with the client machine and software. An AP comprises essentially a radio transceiver on one side and a bridge to the wired backbone on the other. The AP, .a stationary device that is part of the wired infrastructure, is analogous to a cell-site (base station) in cellular communications. All communications between the client stations and between clients and the wired network go through the AP. The basic topology of aWLAN is depicted in Figure 1.3

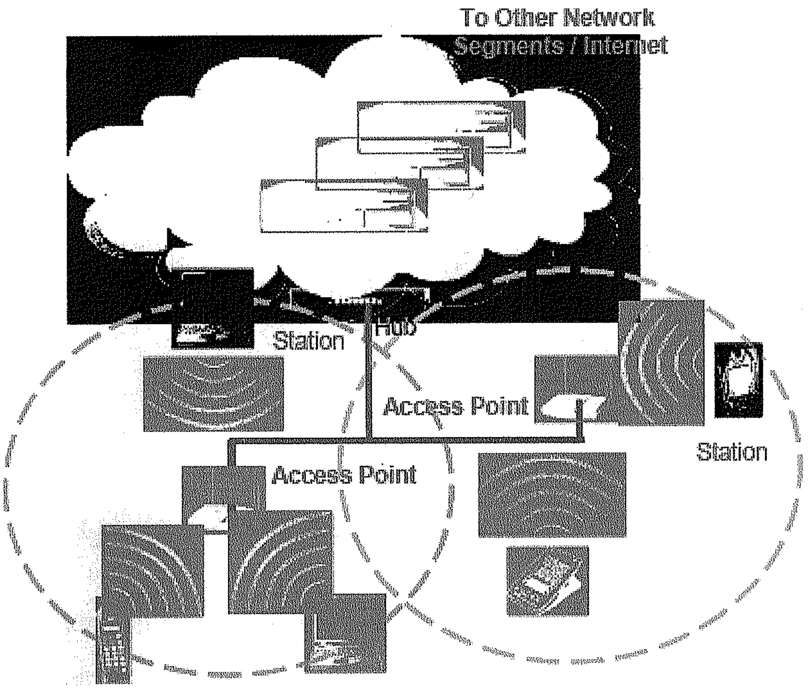
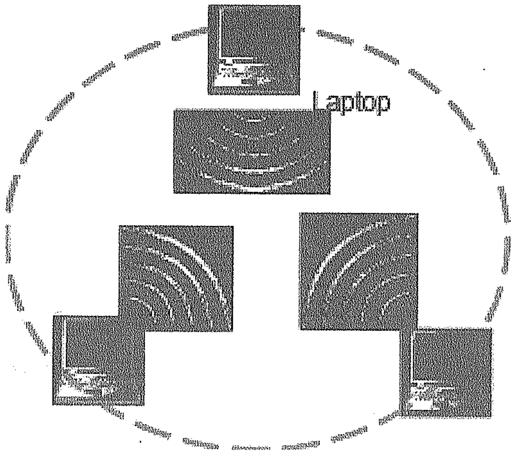


Figure 1.3 Fundamental 802.11 Wireless LAN Topology

Although most WLANs operate in the "infrastructure" mode and architecture described above, another topolögy is also possible. This second topology, the ad hoc network, is meant to easily intercorinect mobile devices that are in the same area (e.g., in the same room). in this architecture, client stations are grouped into a single geographic area and can be Internet-worked without access to the wired LAN (infrastructure network). The interconnected devices in the ad hoc mode are referred to as an independent basic service set (IBSS). The ad hoc topology is depicted in Figure 1.4 below.



Figu.re 1.4 802.11 Wireless LAN Ad Hoc Topology

The ad hoc configuration is similar to a peer-to-peer office network in which no node is required to function as a server. As an ad hoc WLAN, laptops, desktops and other 802.11 devices can share files without the use of an AP.

1.6.3 Bluetoôth

Bluetooth has emerğed as a very popular ad hoc network standard today. The Bluetooth standard is a computirı.ğand telecommunications industry specification that describes how mobile phones, coınputers, and PDAs should interconnect with each other, with home and business phôrtes, and with coınputers using short-range wireless connections. Bluetooth network applications include wireless synchronization, e-mail/Intemet/intranet access using local personal computer connections, hidden computing through aııtomated a.pplicationsand networking, and applications that can be used for such devices as haııds--freeheadsets and car kits, The Bluetooth standard specifies wireless operation in the 2.45 GHz .radio band and supports <lata rates up to 720 kbps. (Next generation of Bluetooth will have a theoretical throughput of up to 2 Mbps.) it further supports up to three simultaneous voice channels and employs frequency-hopping schemes and power reduction to reduce interference with other devices operating in the same frequency band. The IEEE 802.15 organization has derived a wireless personal area networking technology based on Bluetooth specifications v1.1.

2. INTRODUCTION TO BLUETOOTH

2.1 Bluetooth History

Bluetooth is a notable technology among the other high technologies in several respects, but its name garners much attention. Most new industry enterprises are known by a name that describes their associated technology or its applications and often they quickly become known by an acronym describing the full name. So why the name of the technology is "Bluetooth"? And why an acronym has not been considered for Bluetooth? The answer lies in the heritage ofthe original inventors. There are numerous histories and accounts of the Bluetooth namesake and how that name came to be chosen. Harald Bluetooth was a Viking and King of Denmark between 940 and 981. In fact, his name was Harald Blatand, but by the time "Blatand" became "Bluetooth" and it has probably tak.en from two Old Danish words, 'ble' (blue) meaning dark skinned and 'tan' meaning great man. üne of King Harald's skills was getting people to talk to each other, and during his rule Denmark and Norway were Christianized and united. Today Bluetooth wireless technology enables devices to talk to each other, but this time by means of a low-cost short-range radio link. In the Danish town of Jelling, Harald Bluetooth raised an enormous rune stone that still stands in its original position. It has the following runic inscription, adomed with an image of Christ: King Harald raised this monument to the memory of Gorm his father and They're his mother, that Harald which won all Denmark'aııd Norway and made the Danes Christian. Originally, the stone was painted. In Septerrıöe:r 1999, a new stone was raised outside of Ericsson Mobile Communications in Ltınd., this time 'to the memory of Harald Bluetooth. In 1998, IBM, Intel, Nokia, and Toshiba formed the Bluetooth SIG, which serves as the governing body of the specification. The SIG began as a means to monitor the development of the radio technology and the creation of a global and open standard. Today more than 2,000 organizations are part of the Bluetooth SIG, comprising leaders in the telecommunications and computing industries that are driving development and promotion of Bluetooth technology. Bluetooth was originally designed primarily as a cable replacement protocol for wireless communications. However, SIG members plan to develop a broad range of Bluetooth-enabled consumer devices to enhance wireless connectivity. Among the array of devices that are anticipated are cellular phones, PDAs, notebook computers, modems, cordless phones, pagers, laptop computers, cameras, PC cards, fax machines, and printers. Bluetooth is now standardized within the IEEE 802.15 Personal Area Network (PAN) Working Group that formed in early 1999. The Bluetooth SIG Web site provides numerous links to other Web sites with additional information. The IEEE Web site provides updates on the IEEE 802.15 Working Group. This is the Working Group that develops Personal Area Networking consensus standards for short distance wireless networks, or WPANs.

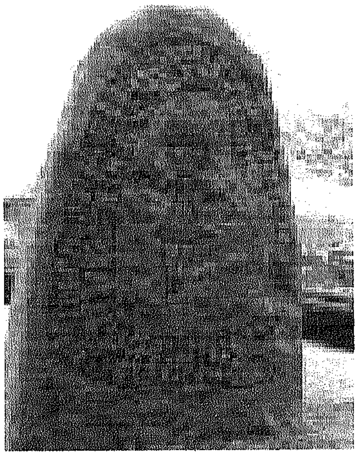


Figure 2.1 Harald Bluetoooth

2.2 Blnetooth Overview

Ad hoc networks today are based primarily on Bluetooth technology. Bluetooth is. an open standard for short-range digital radio. it is touted as a low-cost, low power, and low profile technology that provides a mechanism for creating small wireless networks on an ad hoc hasis. Bluetooth is considered a wireless PAN technology that offers fast and reliable transmission for both voice and data. Untethered Bluetooth devices will eliminate the need for cables and provide a bridge to existing networks. Bluetooth can be used to connect almost any device to any other device. An example is the connection between a PDA and a mobile phone. The goal of Bluetooth is to connect disparate devices (PDAs, cell phones, printers, faxes, ete.) together wirelessly in a small environment such as an office or home. According to the leading proponents of the technology, Bluetooth is a standard that will ultimately:

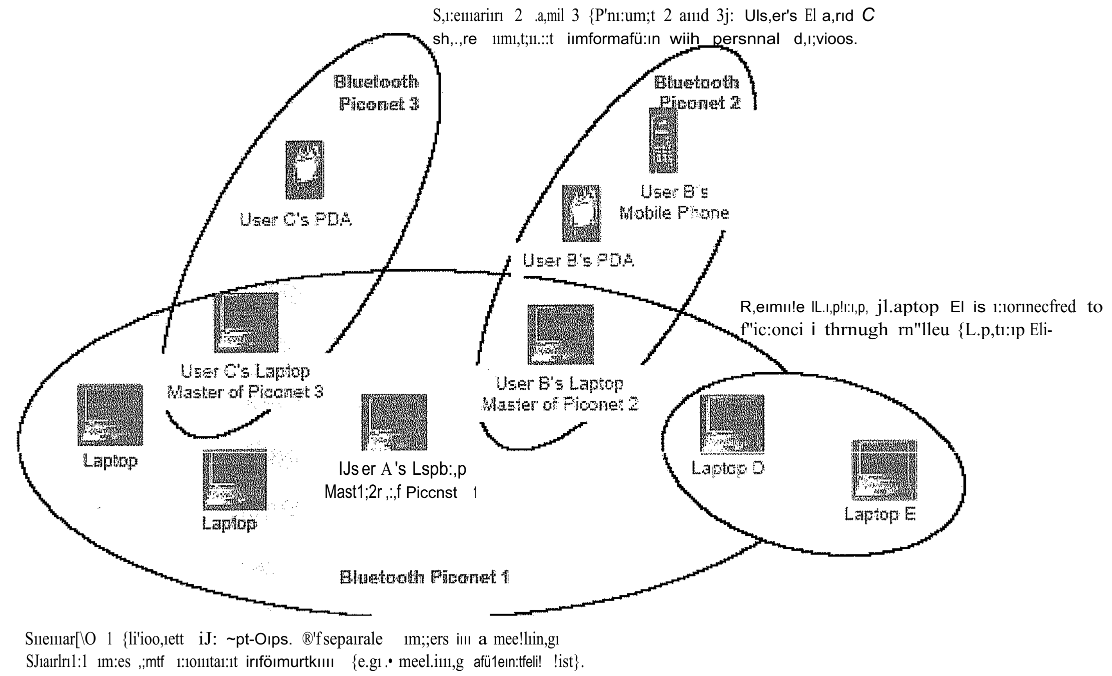
- Eliminate wires and cables between both stationary and mobile devices

- Facilitate both data and voice communications
- Offer the possibility of ad hoc networks and deliver synchronicity between personal devices.

Bluetooth is designed to operate in the unlicensed ISM (industrial, scientific, medical applications) band that is available in most parts of the world, with variation in some Iocations, The characteristics of Bluetooth are summarized in Table 2.1 Bluetooth-enabled devices will automatically locate each other, but making connections with other devices and forming networks requires user action. As with all ad hoc networks, Bluetooth network topologies are established on a temporary and random hasis. A distinguishing feature of Bluetooth networks is the master-slave relationship maintained between the network devices. Up to eight Bluetooth devices may be networked together in a master-slave relationship, called a "piconet." In a piconet, one device is designated as the master of the network with up to seven slaves connected directly to that network. The master device controls and sets up the network (including defining the network' s hopping scheme).. Devices in a Bluetooth piconet operate on the same channel and follow the same frequency hopping sequence. Although only one device may perform as the master for each network, a slave in one network can act as the master for other networks, thus creating a chain of networks. This series of piconets, often referred to as scatter-nets, allows several devices to be Intemet worked over an extended distance. This relationship also allows for a dynamic topology that may change during any given session: as a device moves toward or away from the master device in the network, the topology and therefore the relationships of the devices in the immediate network change.

Table 2.1 Key Characteristics ofBluetooth Technology

Charaeteristlc	Description
Physical Layer	Frequency Hopping Spread Spectrum (FHSS).
Frequency Band	2.4 - 2.4835 GHz (ISM band).
Hop Frequency	1,600 hops/sec.
DataRate	1 Mbps (raw). Higher bit rates are anticipated.
Data and Network Security	Three modes of security (none, link-level, and service level), two levels of device trust, and three levels of service security. Stream encryption for confidentiality, challenge-response for authentication. PIN-derived keys and limited management.
Operating Ran.ğe	About 10 meters (30 feet); can be extended to 100 meters.
Throughput	Up to approximately 720 kbps.
Positive Aspects	No wires and cables for many interfaces. Ability to penetrate walls and other obstacles. Costs are decreasing with a $5 cost projected. Low power and minimal hardware.
Negative Aspects	Possibility for interference with other ISM band technQlôgies. Relatively Iow datarates. Signals leak outside desired houndari.es.


S,ı:eııariırı 2 .a,mil 3 {P'nı:um;t 2 aııd 3j: Uls,er's El a,rıd C
sh,.,re ıımı,t;ıı.::t iımformafü:ın wiih persnnal d,ı;vioos.
Bluetooth Piconet 3
User C's PDA
Bluetooth Piconet 2
User B's Mobile Phone
User B's PDA
R,eımıı!e lL.ı,p!ı:ı,p, jl.aptop El is ı:ıorıııecfred to
f''ic:onci i thrnugh rn''lleu {L.p,tı:ıp Eli-
User C's Laptop Master of Piconet 3
User B's Laptop Master of Piconet 2
Laptop
Laptop
IJs er A's Lspb:,p Mast1;2r ,:,f Piccnst 1
Laptop D
Laptop E
Bluetooth Piconet 1
Sııeııar[\O 1 {li'ioo,ıett iJ: ~pt-Oıps. ®'fsepaırale ım;;ers iıı a mee!lıin,gı
SJıaırlrı1:1 ım:es ,;mtf ı:ıoııtaı:ıt irıföımurtkııı {e.gı.• meel.iıı,g afü1eın:tfeli! !ist}.

Figun~2.2 Typical Bluetooth Network - A Scaternet-Net

Mobile routers in a.Bliıetooth network control the changing network topologies of these networks. The routers.a.lso control the flow of <lata between devices that are capable of supporting a direct linkto each other. As devices move about in a random fashion, these networks must be reconfigured on the fly to handle the dynamic topology. The routing protocols it employs allowBluetooth to establish and maintain these shifting networks. Bluetooth transceivers operate in the 2.4 GHz, ISM band, which is similar to the band WLAN devices and other <IEEE, 802.11 compliant devices occupy. Bluetooth transceivers, which use Gaıssian Freqtiency ShiftKeying (GFSK) modulation, employ a frequency hopping (FH) spread spectrum system with a hopping pattern of 1,600 times per second over 79 frequencies in a quasi-random fashion. The theoretical maxımum bandwidth of a Bluetooth network is 1 Mbps. However, in reality the networks cannot support such <lata rates because of communication overhead. The second generation of Bluetooth technology is expected to provide a maximum bandwidth of 2 Mbps. Bluetooth networks can support either one asynchronous <lata channel with up to three simultaneous synchronous speech channels or one channel that transfers asynchronous <lata and synchronous speech simultaneously. Bluetooth uses a combination of packet-switching technology and circuit-switching technology. The

advantage of using packet switching in Bluetootlı is tlıat it allows devices to route multiple packets of information by tlıe same data patlı. Since tlıis metlıod does not consume all tlıe resources on a data patlı, it becomes easier for remote devices to maintain data flow throughout a scatter-net.

2.2.1 Frequency and Data Rates

The designers ofBluetooth like those oftlıe 802.11 WLAN standard designed Bluetooth to operate in theunlicensed 2.4 GHz-2.4835 GHz ISM frequency band. Because numerous other technologies also operate in this band, Bluetooth uses a frequency-hopping spread-spectrum (FHSS) technology to solve interference problems. The FHSS scheme uses 79 different radio channels by changing frequency about 1,600 times per second. üne channel is used in 625 microseconds followed by a hop in a pseudo-random order to another channel for anotlıer 625-microsecond transmission; this process is repeated continuously. As stated previously, the ISM band has become popular for wireless communications because it is available worldwide and does not require a license. In the ISM band, Bluetooth technology permits transmission speeds of up to 1 Mbps and achieves a throughput of approximately 720 kbps. Although tlıe data rates are low compared to tlıose of 802.11 wireless LANs, it is still three to eight times the average speed of parallel and serial ports, respectively. This rate is adequately fast for many of the applications for which Bluetooth was conceived. Moreover, it is anticipated that even faster data rates will be available in the future.

2.2.2 Frequeney Hoppmg Spread Spectrum

the RF communications, spread spectrum refers to dividing the available spectrum based upon frequency, time, a coding scheme or some other method. Messages to be sent are then divided into various packets that are transmitted across the divided spectrum (or frequency hopping). The method is employed with Bluetooth wireless cömmunication, divides the spectrum into different frequencies, or channels. A single message packet is transmitted on a selected channel, tlıen the radio selects a new channel (this process is called hopping to a new frequency) to transmit the next packet, and<the process repeats, by that means spreading the message across the available frequency spectrum. Obviously the receiver of the message must know the hopping patt:em to tune to the correct channels successfully to receive each packet and assemble

the complete message. This process is called *frequency hopping spread spectrum,* or FHSS. The devices thaı communicate with each other must transnıit and receive on the same frequency at the same time. The frequency-selection module (FSM) contains the procedure for selecting the next frequency to be used under various operating conditions.

2.2.3 Bluetooth Architecture and Components

As with the IEEE 802.11 standard, Bluetooth permits devices to establish either P2P networks or networks based on fixed access points with which mobile nodes can communicate. In this document, however, we only discuss the ad hoc network topology. This topology is meant to easily interconnect mobile devices that are in the same area (e.g., in the same room). In this architecture, client stations are grouped into a single geographic area and can be inter-networked without access to the wired LAN (infrastructure network). The basic Bluetooth topology is depicted in Figure 2.2. As shown in this piconet, one of the devices would be a master, and the other two devices would be slaves,

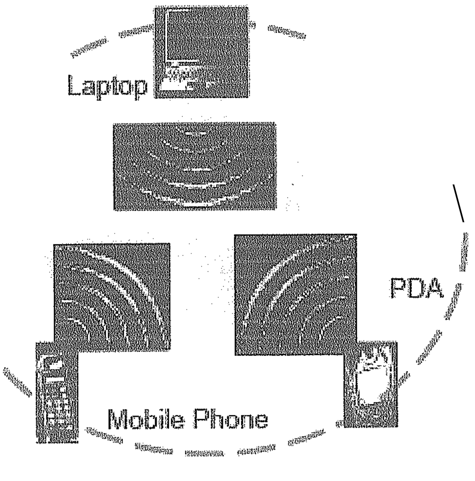


Figure 2.3 Bluetooth Ad Hoc Topology

Unlike a WLAN that comprises both a wireless station and an access point, with Bluetooth, there are only wireless stations or clients. A Bluetooth client is simply a device with a Bluetooth radio and Bluetooth software module incorporating the Bluetooth protocol stack and interfaces.

2.2.4 Range

Bluetooth provides three different classes of power management, Class 1 devices, the highest power devices, operate at 100 milliwatt (mW) and have an operating range of up to 100 meters (m). Class 2 devices operate at 2.5 mW and have an operating range ofup to 10 m. Class 3, the lowest power devices, operate at 1 mW and have an operating range of :from 1/1 0 meter to 10 meters. These three levels of operating power are summarized in Table 2.2

Table 2.2 Device Classes of Power Management

Type	Power	Power Level	Operating Level
Class 1 Devices	High	100 mW (20 dBm)	Up to 100 meters (300 feet)
Class 2 Devices	Medium	2.5 mW (4 dBm)	Up to 10 meters (30 feet)
Class 3 Devices	.Low	1 mW(OdBm)	0.1-10 meters (less than 30 feet)

The three ranges for Bluetooth are depicted in Figure 2-4. As shown, the shortest range may be good for applications such as cable replacement (e.g., mouse or keyboard), file synchronization, or business card exchange, The high-powered range can reach distances of 100 m, or.aboüt300 ft. Additionally, aswiththeidata rates,it is anticipated that even greater distances wiUbe achievedinthe future.

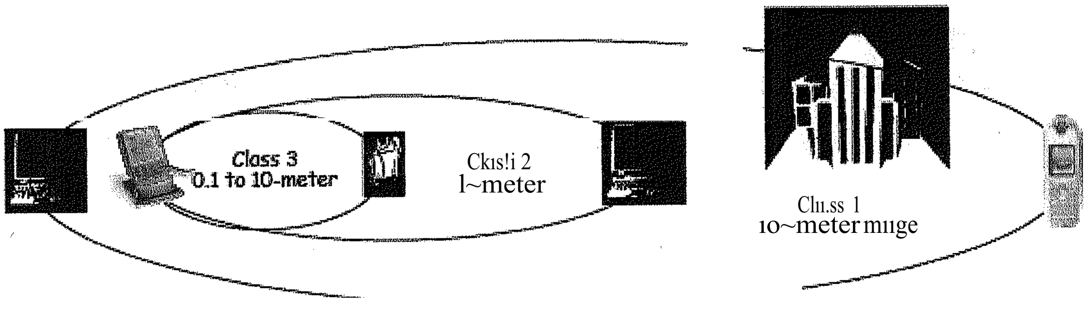


Figure 2.4 Bluetooth Operating Range

293 Benefits

Bluetooth offers five primary benefits to users. This ad hoc method of untethered communication mak:es Bluetooth very attractive today and can result in increased efficiency and reduced costs. The efficiencies and cost savings are attractive for the home user and the enterprise business user.

Benefiıs of Bluetoothinclııde:

- Cable replaeement: Bluetooth technology replaces cables for a variety of interconnections. These include those of peripheral devices (i.e., mouse and keyboard computer connections), USB at 12 Mbps (USB 1.1) up to 480 Mbps (USB 2.0); prirtters and modems, usually at 4 Mbps; and wireless headsets and microphones that interface with PCs or mobile phones.
- Ease of file sharing: Bluetooth enables file sharing between Bluetooth-enabled devices. For example, participants of a meeting with Bluetooth-compatible laptops can share files with each other. In another example, a Bluetooth-compatiblestiöbile phone acts asa wireless modem for laptops. Using Bluetooth, the laptop interfaces with the cell phone, which in turn connects to a network, thus giving thelaptop a full range of networking capabilities without the need of an electricalinterface for the laptop-to-mobile phone connection.
- Wireless synehtôıııization: Bluetooth provides automatic wireless synchronization with other Bluetooth-enabled devices. For example, personal information corıtainedXirı. address books and date books can be synchronized between PDAs, laptôpsÇimobilephoııes,and other devices.
- Automated wireless appliea.tiô:n.s: >Bfüetôoth supports autômatic wireless application functions. Un.like synch:förı.ization,which typically occurs locally, automatic wireless applications interface with the LAN and Intemet. For example, an individual working offline on e-mails might be outside of their regular service area on a flight, for instance. To e-mail the files queued in the inbox of the laptop, the individual, once back in a service area (i.e., having landed), would activate a mobile phone or any other device capable of connecting to a network. The laptop would then automatically initiate a network join by using the phone as a modem and automatically send the e-mails after the individual logs on.

- Internet connectivity: Bluetooth is supported by a variety of devices and applications. Some of these devices include mobile phones, PDAs, laptops, desktops, and fixed telephones. Intemet connectivity is possible when these devices and technologies join together to use each other's capabilities. For example, a laptop, using a Bluetooth connection, can request a mobile phone to establish a dial-up connection; the laptop can then access the Internet through that connection. Bluetooth is expected to be built into office appliances (e.g., PCs, faxes, printers, and laptops), communication appliances (e.g., cell phones, handsets, pagers, and headsets), and home appliances (e.g., DVD players, cameras, refrigerators, and microwave ovens). Applications for Bluetooth also include vending machines, banking, and other electronic payment systems; wireless office and conference rooms; smart homes; and in-vehicle communications and parking.

2.4 Bluetooth and Security

Bluetooth has been altemately touted as a taste of things to come and the answer to all our wireless connectivity prayers. It promises everything from the ability to program our microwaves fröın work, to pushing ads from pop machines to your pocket device. The Gartner Group seems to agree that it will catch on in a big way it predicts a market of $700 million for Blüetooth chips by 2006. Put simply, Bluetooth is a wireless standard that facilitates colİ1lllunicationsbetween devices. A Bluetooth capable device sends out a signal in a 30-foöffadiu.s, allowing any Bluetooth enabled device to speak to another. Therein lie the biggesfadvarıtages and people's worst fears of Bluetooth. The Gartner Group predicts that by 2004, 70 percent of new cell phones and 40 percent of Personal digital assistants (PDA) will use some sort of wireless technology to communicate with other devices, and a great deal of that technology will include Bluetooth. Millions of other devices will be shipped with Bluetooth capability as well, including computers, stereos, even refrigerators. In short, Bluetooth will be everywhere. But Bluetooth's promise of seamless, pervasive wireless connectivity begs an important question is it secure? Researchers from Lucent technologies recently discovered security holes in the Bluetooth specification, making this question even more important and pressing. If Microsoft's own servers can be hacked, why not your Hiuetooth capable laptop or the Bluetooth equipped security system in your home?

Because Bluetooth will be so widespread, security will be of paramount importance. IrDA, a wireless data transfer method based on infrared signals, provided a measure of security by requiring a line of sight to devices. Bluetooth provides no such requirement. It is not hard to envision a scenario where a shadowy figure could sit on the other side ofa wall :from an executive's Bluetooth-enabled PC and hack his way into it via the wireless connection, mining whatever data he can from the information stored on the PC, or even the network the computer is connected to. Even more frightening to many people, but a much less likely scenario, is that someone could sit in a coffee shop and search for Bluetooth devices within range, pulling personal information, even credit card numbers, off the devices. Weaknesses in the encryption scheme could allow a hacker to listen and determine the aııthentication/pairing key thus be able decipher even encrypted data being sent between authenticated bluetooth devices. Another possible issue is a type of "denial of service attack" that drains batteries by forcing constant intensive utilization ofa device's processor. The Bluetooth specification provides little to no protection against that sort of attack. These scenarios are highly unlikely, but plausible without serious attention given to the security of Bluetooth. The Bluetooth protocol already has several security measures built in at the hardware level, but they are only truly effective .if device manufacturers work to understand and take advantage of them. Security issues associated with scattemets within Bluetooth are still being ironed out as well. Bluetoöth security starts at the hardware level. The Bluetooth chips themselves have built-in security considerations. The Bluetooth hardware specifications include encryption, randofü>mumber generation, encryption key management, authentication (unidirectional and bi-directional), and authorization. These are based on a secret link key that is shared by a pair of devices. The key is generated by a technique referred to as "pairing/bonding". Authentication is the process of verifying 'who' is at the other end of the link. It is performed for devices and is not done on a per user or service level. Authorization is the process of deciding if device X is allowed to have access to service Y. This is where the concept of "trusted" comes in. Authorization always includes authentication. Bluetooth allows selective security in that it allows device X access to service Y and not service Z, while allowing device M to have unrestricted access to all services (once paired) and provide no access to device N. In addition, the :frequency-hopping and power-adaptation features within Bluetooth set a limited range on the signal, making the system difficult to eavesdrop on. However, these measures only go so far. Bluetooth currently provides adequate security for smaller applications, but for larger ad-hoc applications there still are quite a few unanswered questions because the Bluetooth Special Interest Group (SIG) initially left many aspects of Bluetooth security implementation specific. Device manufacturers have to take the next step and add their own security measures to make Bluetooth truly secure, especially given the recently discovered security holes. The first issue is for manufacturers to simply take advantage of the built-in security features Bluetooth offers. it all starts\with the link, where Bluetooth devices initially establish communications with .one another. Other built-in security features of Bluetooth also play heavily into creating a secure networking environment. Frequency hopping, where the device rapidly cycles through preset frequencies on the Bluetooth wavelength, occurs at 1600 hops per second. This may seem like a minor feature, but it makes it much more difficulffo intercept Bluetooth signals. Without having a device in sync with the frequency hop, bits of <lata can be intercepted, but the full stream cannot. Adaptive power. cııpabilities make it difficult to eavesdrop on Bluetooth transmissions. Bluetooth deviceshııye variable ranges, potentially reaching 30 feet away. However, that sort of range isfüt necessary in devices like PDAs and cell phones. The hardware allows device deve:lg;p~rs, and even consumers if the developers code the necessary interfaces and optioiıs in, tp rnodify the coverage area to reduce the chances of someone hacking their wayifit()a.:E.lluetooth-enableddevice from 30 feet away. Should someone manage to intercept a cl,ta/ stream, the Bluetooth specification includes hardware encryption, which makes itçiiffiçlllt to make any sense of the <lata, but unfortunately far from impossible.

2.4.1 Bluetooth Security Mo<les

The General Access profile in the Bluetooth Profiles specification specifies three security modes within a device:

- No security (mode 1): A device will not initiate any security procedure.
- Service level (mode 2): A device does not initiate security procedures before channel establishment at the L2CAP level; security is only enforced after channel establishment. This mode allows different and flexible access policies for applications, especially running applications with different security requirements in parallel.

- Link level (mode 3): A device initiates security procedures before the link set-up at the LMP level is completed.

2.4.2 Security Levels

There are two levels to Bluetooth security: the device level and the service level.

2.4.2.1 Device Trust Level

At the device level, Bluetooth devices fit in one oftwo categories when making a link:

- Trustedı The device has a fixed relationship with the other device and has unrestricted access to all services on the host device.. A tnısted device is allowed total access to the host and provides an authenticated encrypted key to the device it is paired with upon Iogin.
- Untrustede The device has no permanent relationship and is not paired with the host device so has restricted access to services. Without the encrypted key, access to services on the host device is restricted according to whatever security protocols are in place on the device.

2.4.2.2 Security Levels of Services

At the service level, security may be again set at 3 levels:

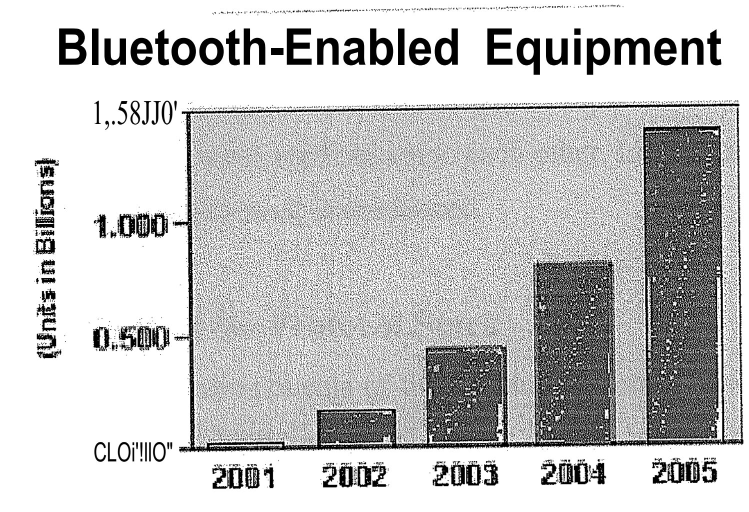
- Services open to all devices: Neither authentication nor authorization is needed.
- Services that require .authentication only: Authorization is not needed.
- Services that require authorization and authentication: Automatic access is only granted to trusted devices. Other devices need a "manual" authorization.

in addition, some services may require encryption once authorization and/or authentication are complete. Legacy applications are provided a default security level that would be used unless a different policy is defined in the security database.

2.5 Projected Market Growth

Cahners in-Stat group estimates that the Bluetooth market will grow from virtually zero in 1999 to over 1 billion Bluetooth-enabled devices that will ship in 2005. According to Ma[illegible] Reynolds, an analyst with Gartner Group's Dataquest, "The thing about

Bluetooth is that it really will ship in the billions of units once it gains momentum. It's really a multibillion-dollar market."



Source: Cahners In-Stat Group

Figure 2.5 Bluetooth Marketing aspects (Number of equipments)

The manufacturing market for Bluetooth will focus on the sale of embedded chips for various products, with analysts Frost & Sullivan predicting a $700 million market by 2006.

3. STUDY OF THE BLUETOOTH SPECIFICATION

3.1 The Protocol Stack of Bluetooth

The protocol stack constitutes the seeds of the Bluetooth specification. This stack allows; the settlement ofthe equipment, the communication between each other, data transfers and providing interacted applications to each other. in this stage the main parts and some layers ofthe protocol stack is mentioned.

3.2 The Components of the Protoeol Stack

in figure 3.1 the high layer components of the Bluetooth protocol stack is shown. The elements ofthe stack (protocols, layers, applications) are divided to three parts.

- transport protocol group
- middleware protocol group
- application group

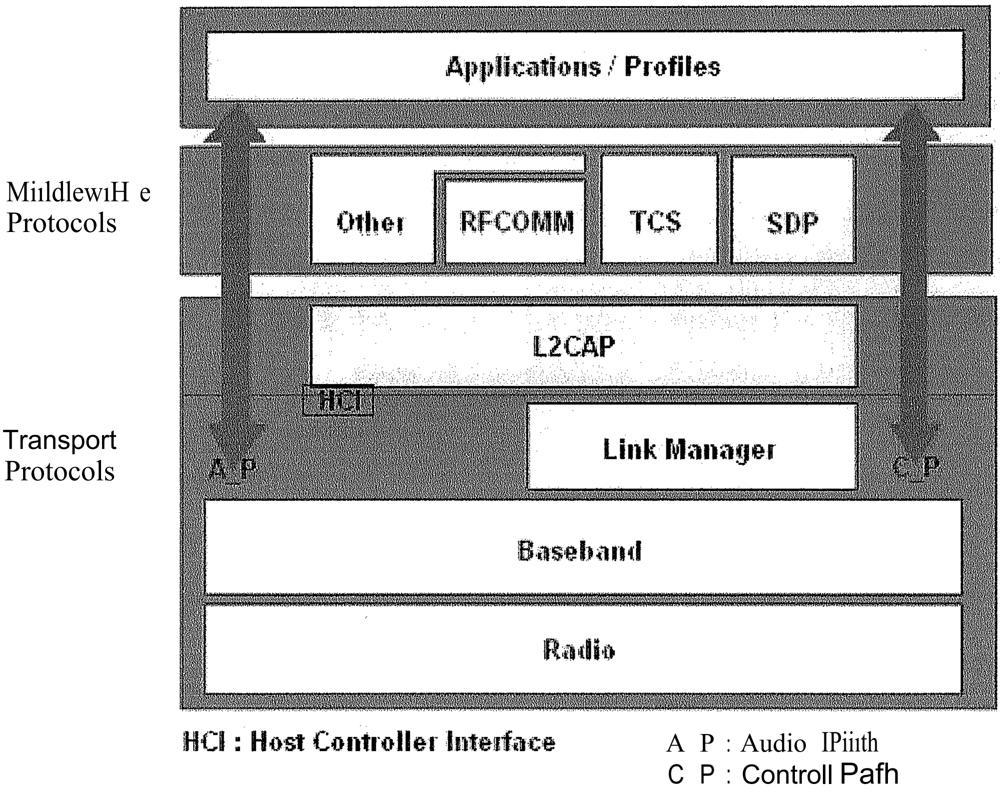


Figure 3.1 the high layer components ofthe Bluetooth protocol.

Transport Protocol Group: This the protocol group which is designed for allowing the Bluetooth equipments, the settling and constitution of each one, the high layer protocols and applications, allowing the <lata' s transportation in this transport protocols in a physical and logically construction and managing them. The protocols in this group: radio, base band link manager, logical link, adaptation and host control interval units and included.

Middleware Protocol Group: the middleware protocol group includes the protocols which are developed for both the third party and industrial standard protocols and by the SIG group for Bluetooth cordless communication. The first contents; İnternet related protocols (PPP, iP, TCP ETC), cordless application protocols and lrDA and other related applications adaptations object change protocols consists. The second contents, is constituted by the protocols which is designed for running more then one applications on Bluetooth links with the effect of Bluetooth communication. RFCOMM named as series port emulator is used for making them work without a problem on the Bluetooth communication normally the old applications which constructs interval units with series port. The packet provides the developed inspection of; telephone signalization protocol, group managing and cordless headphones and such telephone operations as base stations. Service investigation protocol allows finding the services that equipments use and how to gain information about these services.

Applteation Group: This group includes the real applications which mak:e the Bluetooth link's use. These applications are; such old applications, unaware of Bluetooth transports, like web browsing. Also which defines the Bluetooth cordless cômmunication system, for example the applications which use the telephone control pretocol for the control ofthe telephone devices.

3.3 Transport Protocol Group

In figure 3 .2 the order of protocols which are in transport group is seen. These transport protocols are the protocols which carry the <lata and the sound traffic which is developed by the SIG group. in this stage the presentation of these protocols are dialed from up to down or in another word dialed with the point of view of the messenger device. The traffic's from up transmittal layer to the down layer. in the receiver device

the traffic is in the opposite way. This projection is the end to end <lata course to transport group protocols.

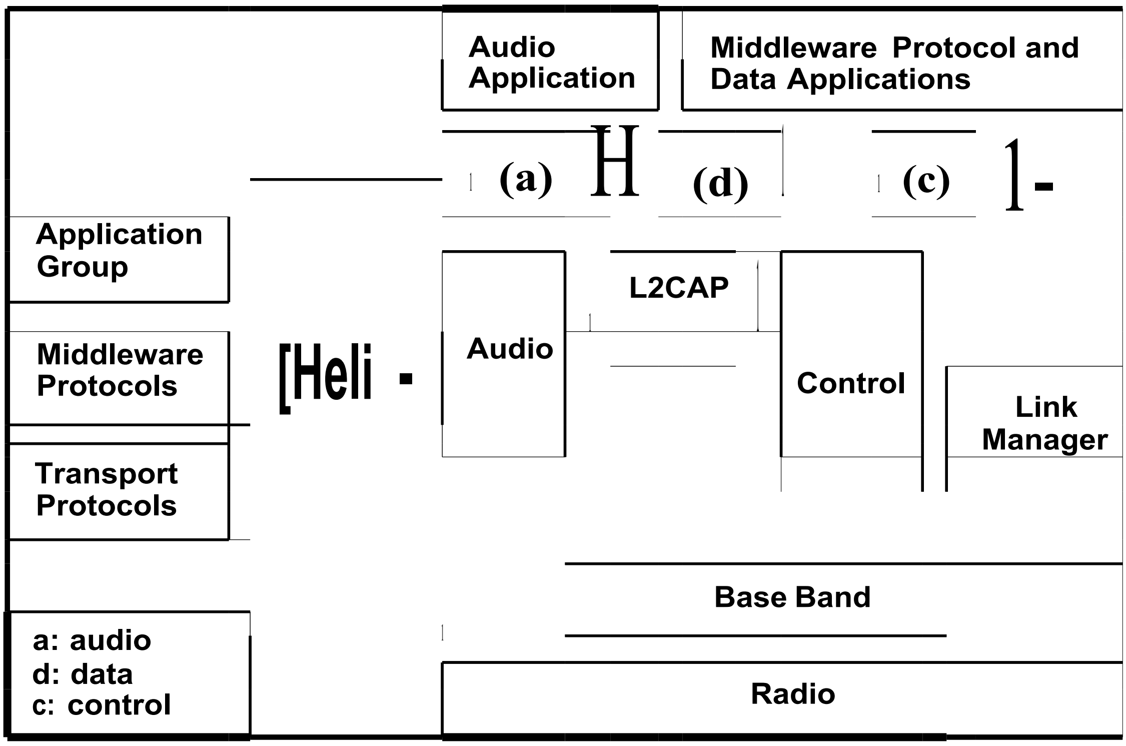


Figure 3.2 Transport protocol group stack 2

Transport protocol supports both asynchronous transports for <lata transports and telephony grade (64 kbps) for sound communication it supports the temporal or synchronous transrnittal. To produce high quality in audio applications the .audio traffic has great irnportance. The audio traffic passes all the rnid level protocols and reaches 'the base band layer directly :frorn audio application. And then the audio traffic directly transmitted with Bluetooth air units in little packets. The protocols in the transport protocol group, seven-layer OSI is not included in the transport layer in the protocol model. The set shape of the protocols in the transport protocol group looks like a visual pipe and this pipe shape is used to transport <lata :from equipment :from equipment with the help of Bluetooth air interval units. All the protocols in this group are necessary for the communication between the Bluetooth equipments.

3.3.1 L2CAP Layer

The traffic that comes from the <lata applications is diverting to L2CAP layer first. The L2CAP layer protects the high layer protocols and applications from low layer transmittal protocols and its parts. By this way the high layers are unaware of the frequency leaps in the radio or base band or unaware of such format packets used in the transport made with Bluetooth air interval units. L2CAP allows the multiple protocols and applications sharing the air interval units and supports the increase of protocols. Besides L2CAP activates the base band transmittal, for the collection packets by receiver equipments, use of high layers and the breaking into parts of large packets to small packets. The L2CAP in to similar leveled equipment it facilitates the care of the services wanted degrees by deciding the services acceptable layer. According to the services wanted degree the L2CAP application can manage the control of the new coming traffic and can coordinate the services wanted degree with low layers.

3.3.2 Link Management Layer

The link managers in both two equipments, can decide the properties of Bluetooth air interval units between them by using the LMP (link manager protocol).these properties, includes the periodic band wideness reservation to support the audio traffic and to supports the settlement of band wideness for wanted degree of the service in the <lata traffic. The link manager in the communication equipments uses the challenge response approach for identification check of. equipments. The linkrmatıağers <inspec:t the password system of pairing and the \air interval unit betweem equipments when necessary. If the ID check is un.suc:c:essful the link manager cancel the connection between two equipments and by this way bans the communication between equipments. also the link managers support the power control by comparing the low activity base band modes that execute information change operations with the parameters like low activity base band modes times. The link managers may want adjustments in transmittal power levels for more power save.

3.3.3 Base Band and Radio Layers

The base band layer determines the Bluetooth air interval unit. It defines which devices are sought for which one and how they should make the connection. Base band layer deterrnines the master slave roles for devices. In a connection the device that starts the connection is master and the other one is in the slave position. The base band layer also determines that how should the :frequency leap row be by using formed communication devices. This layer determines how the air interval units should be shared among devices in certain rules. These rules depend on, TDD (time division duplex) and packet based row plan (polling). Also determines how the synchronous and asynchronous traffics should share the air interval unit. For example in synchronous transportation the master device sends the (and/or) survey periodically. The base band determines the supported packet types for synchronous and asynchronous traffics such as error sort and correction, signal clipping, passwording, packet transportation and retransformation ete. The master and slave concepts can not be spread more then the link managers. it depends on the L2CAP layer and upon it communication between match model and at master and slave devices there can't be a preparations made for other devices.

3.3.4 HCI Layer

Maybe the radio, base band, link manager could be packed together in the Bluetooth module. And then the module gets connected to the host device and activates this device with Bluetooth cordless communication technology. In this configuration it includes the fit parts of the host L2CAP layer and the high layers of the mass. The module gets connected to the host with physical interval units called host transport; USB, RS 232 port or UART. To improve the Bluetooth modules together working with different supplies, independent :from the physical interval units that connect the specification, module to the host, a general interval unit is defined to reach the low layers of pile that is located in the module. HCI (host controller interface) allows the piles high layers for, reaching the rigging records and link manager includes applications, on to base band :from a standard interval unit. In the HCI orders there could be introduction of such operations modes like; ID check, device paging. In the HCI results there could be; the results of the device interrogate operation, inform of the masses high layers, reading the setting for audio coder and code solver which is located in the base band, reading the signal force of the received transmittals. The traffic goes through the HCI synchronous and asynchronous like received and transmitted by the host. When the HCI layer is located typically on the L2CAP layer is not necessary as a part of the specification. The HCI is developed for working along between the Bluetooth and host devices modules.

The product applications must be concord anted with the HCI specification to completely support the Bluetooth air interval units. For example; in the entire dense buried system the HCI maybe not exist completely or in a different place in the mass, could place on the L2CAP. For sending the control information the control paths are used between layers. For example; could notify the expectations of the service quality to the L2CAP link manager, or an application could notify the request of low power safe of its last user.

3.4 Middleware **Ptôtocol** Group

Middleware group gets the transmittal protocol which is in base in a useful form and presents the standatd füterval units used in the trans to the application layers. The middleware protocôt'ğroup includes these:

- RFCOMM;serial port abstractation
- SDJ? (service discovery protocol) defining proper services and locating the necessary services.
- IrDA wofkiiig along protocol team.
- TCS (telephöny control protocol) used for the control ofthe telephone calls.

3.4.1 RFCOMM Layer

Nowadays the serial pôrts are the most common way of interval units of communication and calculating systems; Most of the serial communication systems require cable for <lata transfer. Since the Blüetöoth cordless communication has wanted to cancel the cables support and concented applicaıions for serial communication has been an important feature for cordless môdels in start. File and object transfer between pairs, <lata synchronization and dial-up networks are the applications that use serial communication generally. For easing the use of serial communication on Bluetooth cordless links, protocol mass, the serial port abstractation has defined named as RFCOMM. The RFCOMM presents an imaginary serial port for applications. By this way the applications modeled for the RFCOMM corded serial communication, easiest the emigration to the cordless serial communication land. A whoever application uses the RFCOMM like a corded serial port to materialize some scripts well. These applications could be; synchronization, dial-up networks and derivatives also for these important changes on applications are not necessary. Thus the aim of the RFCOMM

protocol, use of the Bluetooth technology for old serial port based applications. The RFCOMM protocol is modeled on the 07.10 standards of ETSI (European Telecommunications Standards Institute).this standard defines the majority serial communication on a single serial link. The Bluetooth specification, has assumed the subset of ETSI 07.10 standard and also adaptations are defined for Bluetooth communication designed in such form. Serial communication is used commonly in digital devices. The serial port abilities that RFCOMM provides to applications; especially by the cause of activating old applications, RFCOMM becomes the most important part ofthe protocol stack.

3.4.2 SOP Layer (Service Diseovery Protocol)

The first cause ofbuilding the networks between devices, by network these devices can be in interaction and to make use of each others services. In traditional networks like Ethemet and LAN such services like, filename presentation, bridges and network passages are provided by some devices (server) and other devices (client) uses these. In many cases the client devices locates these network services from some static configurations. This configuration is built and carried by the system manager those configurative client devices. Against the dynamic Ad Hoc networks technical by the Bluetooth cordless communication, static networks are unwrought. Two or more devices can make connection immediately on the Bluetooth links. If these devices have the ability to use each others services, they would need dynamic atmosphere to determine the location of the services. When first the comtnunication channels are built then the logical step to do is to Iearn .the proper services for devices. In Bluetooth communication SDP makes this step. SDP is determining a standard method for Bluetooth devices for leaming and discovering the services of other devices. Service discovery is a key component to activate the last user' s user data in dynamic networks. The Bluetooth SDP protocol, is designed for in the environments that use the Bluetooth cordless communication technology been used in the best way.

3.4.3 IrDA along Workable Protocol

IrDA (infrared data association) in cordless atmosphere has defined a protocol for data transfer and synchronization. SIG group has assumed the IrDA protocol and data models because IrDA and the Bluetooth cordless communication system shares some important self grade using scripts and applications. in the data transfer between the devices the first necessary is to determine the format, determining the meaningful of data' s syntax, semantic. Infrared object exchange (lrOBEX) or OBEX protocol is developed by lrDA as a session protocol in communications between pairs. The application that is used in OBEX in applications is well defined object exchange application. Like all data objects exchange electronic business cards, e-mail or other messages, personal calendar inputs, is materialized by using OBEX protocols. The OBEX protocols, contracts the base of file transfer uses. To add infrared mobile communications, developed by IrDA is a protocol that provides the synchronization of same data' s.

3.4.4 Network Layers

The Bluetooth cordless communication system uses the topology of network between pairs more then .LAN type topology. Thus the technology allows big networks connection with dial-up or network arrival points. For dial-up network, for making the network connection at the command layer is used in the stack of middleware protocol. in lots of situation the arrival to İnternet, resorting to iP networks, is provided by the use of the internet protocols. iP network in connection of dial-up, the devices can use the İnternet protocols for starting the connection. Also a device can provide the connection to iP network with the network arrival points. in this case the Bluetooth-link connects the device to network arrival point, from there could pass totwidenetworks.·PPP (point to point protocol) is used for connection for network arrivalpoitıts on Bluetooth links. Like dial-up network connection,inbuilding ofPPP coıili.ectionthe İnternet protocols can be used. The WAP network can be work 'inthe similar way by passing to WAP web passages. To build the interaction with İnternet on standard WAP protocols, the PPP connection is materialized to iP network. in the specifications 1.0 version, on the Bluetooth links the protocol stack or profile is defined which support the use of TCP/IP protocols. in the specification on iP network arrival, on the use of PPP protocols are defined. With the support of Bluetooth cordless communication system the activity of IP protocol mass is available, like these operations the SIG group has not defined along working. With all these probabilities the revision of the specification; is defined as the use of the İnternet protocols directly by Bluetooth cordless communication system.

3.4.5 TCS Layer and Audio

like sad before one another important property of the Bluetooth technology, just like data traffic the aııdio traffic can be transmitted. The TCS layer of Bluetooth is designed for supporting telephone functions like; telephone call control and group management. TCS is used for construction of call parameters. When the call is connected the Bluetooth audio channel can transmit the audio features. TCS can also construct the data calls used in dial-up network profile. In this case call features can be transmitted as standard data packets on L2CAP. TCS protocols. ITU-T (Intemational Telecommunications Union-Telecommunication). Is concordant with Q.931 specification. Because these protocols are coded as binary and is known as TCS-BIN in the specification. In the process of developing the specification the SIG group, has continued works ona second TCS protocol called TCS-AT. The TCS-AT, defines the modem control protocol which flows to RFCOMM layer using at commands. Although the at commands are used on RFCOMM, the specification does not define a protocol for TCS-AT. TCS-BIN is proper for some telephone based profiles in specifications 1.0 version. the at commands on the RFCOMM serial interval unit that applications need is free for use but the specification has defined these at commands as another protocol. In the profiles on version 1.0, headphone, fax, dial-up network, more then TCS-BIN protocols on RFCOMM at commands are used. The TCS-BIN protocol includes, call control functions, group management functions and the change of the call signalization information developing methods. In Bluetooth cordless communication system takes hand the audio alone. Because the audio traffic is synchronous. Thus the audio has time elements. Audio traffic typically directly diverted to base band layer or from base band layer. Does not be diverted to high layers like·L2CAP. Special base band packets named as SCO (Synchronous Connection Oriented) are for use in typical base band traffic. Bluetooth communication technology allows 3 audio channels in one time. Bluetooth audio communication is 64kbps. This speed can be reached by using one of the modulations; 8 bit logarithmic PCM (Pulse Code Modulation) or CVSD (Continuous Variable Slope Delta). The zip techniques for PCM aııdio are in law a and µ. The portable audio traffic on Bluetooth base band is not only voice. Long audio series can be transmitted and received at 64kbps on Bluetooth links. Thus added to voice, Bluetooth audio channels can transmit high quilted music or short audio elips.

3.5 Bluetooth Profiles

The profiles describe how different parts of the specification can be used to accomplish a desired function for a Bluetooth device. Profiles represent the default solution for a usage model and form the hasis for Bluetooth interoperability and logo requirements. Each Bluetooth device must support at least one profile, but may support several profiles. The idea is that if two devices support the same profile, then they should be able to interoperate. A profile can be viewed as a vertical slice through the protocol stack. It defines options in each protocol that are mandatory for the profile. It also defines parameter ranges for each protocol. The profile concept is used to decrease the risk of interoperability problems between different manufacturers' products. The profiles are:

- Generic Access Profile (GAP)
- Service Discovery Application Profile (SDAP)
- Cordless Telephony Profile (CTP)
- Intercom Profile (IP)
- Serial Port Profile (SPP)
- Headset Profile (HP)
- Dial-up Networking Profile (DNP)
- Fax Profile (FP)
- LAN Access Profile (LAP)
- Generic Object Exchange Profile (GOEP)
- Object Push Profile (OPP)
- File Transfer Profile (FTP)
- Synchronization Profile (SP)

3.5.1 Generic Access Profile

The Generic Access Profile defines the generic procedures related to discovery of Bluetooth devices and link management aspects of connecting to Bluetooth devices. It is the core on which all other Profiles are based.

3.5.2 Service Discovery Application Profile

The Service Discovery Application Profile defines the features and procedures for an application in a Bluetooth device to discover services registered in other Bluetooth devices and retrieve any desired available information pertinent to these services.

3.5.3 Cordless Telephony Profile

The Cordless Telephony Profile defines the features and procedures that are required for interoperability between different units active in the 3-in-l phone use case. This profile also shows how the use case can be applied generally for wireless telephony in a residential or small office environment.

3.5.4 Intercom Profile

The Intercom Profile: defines the requirements for Bluetooth devices necessary for the support of the intercom functionality within the 3-in-1 phone use case. This is also referred to as the 'yvalkie:-talkie' usage of Bluetooth.

3.5.5 Serial Port Profile

The Serial Port Profile defines the requirements for Bluetooth devices necessary for setting up emulated serial cable connections using RFCOMM between two peer devices.

3.5.6 Headset Profile

The Headset Profile defines the requirements that shall be used by devices implementing the usage model called 'Ultimate Headset'.

3.5.7 Dial-up Networkmg Profile

The Dial-up Networking Profile definesthe requirements that shall be used by devices (modems, cellular phones) implementirtğthe'usage model called 'Internet Bridge'.

3.5.8 Fax Profile

The Fax Profile defines the requirements for Bluetooth devices necessary to support the fax use case. This allows a Bluetooth cellular phone (or modem) to be used by a computer as a wireless fax modem to send/receive a fax message.

3.5.9 LAN Access Profile

The LAN Access Profile defines how Bluetooth enabled devices can access the services ofa LAN using PPP. Also, this profile shows how the same PPP mechanisms are used to form a network consisting of two Bluetooth enabled devices.

3.5.10 GenericObject Exchange Profile

The Generic Object ..Exchange Profile lays the basis (defines the protocols and procedures) for Bluetoöth devices necessary for the support of the object exchange usage models. Theusage .model can be the Synchronization, File Transfer, or Object Pushmodel.

3.5.11 ObjectPush Profile

The Object Push Profile defines the requirements for applications providing the object push usage model.[jypical scenarios covered by this profile involve the pushing/pulling of <lata objects bet.w~~11 Bluetooth devices.

3.5.12 File Transfer Profile

The File Transferı>rôfile defines the requirements for applications providing the file transfer usage 111.ğq.~l. Typical scenarios involve a Bluetooth device t>rowsing, transferring and manipulatiiıg objects on/with another Bluetootlsdevice.

3.5.13 Synchronization Profile

The Synchronization Profile defines the requirements for applications providing the synchronization usage model. Typical scenarios covered by this profile involve manual or automatic synchronization of PiM (Personal lnformation Management)) <lata when two Bluetooth devices come within range. Namely, the scenarios covered by this profile are:

- Usage ofa mobile phone or PDA by a computer to exchange PiM (Personal Information Management) <lata, including necessary log infomıation to ensure that the <lata contained within their respective Object Stores is made identical. Types of the PIM <lata are, for example, phonebook and calendar items.
- Use ofa computer by a mobile phone or PDA to initiate the previous scenario (Sync Command Feature).

- Use of a mobile phone or PDA by a computer to automatically start synchronization when a mobile phone or PDA enters the RF proximity ofthe Computer

3.5.14 Profile Structure

The Bluetooth profile structure and dependencies are depicted in Figure 3.8.1. A profile is dependent upon another profile if it re-uses parts of that profile, by implicitly or explicitly referencing it. Dependency is illustrated in the figure: a profile has dependencies on the profile(s) in which it is contained ~ directly and indirectly. For example, the Object Push profile is dependent on Generic Object Exchange, Serial Port, and Generic Access profiles.

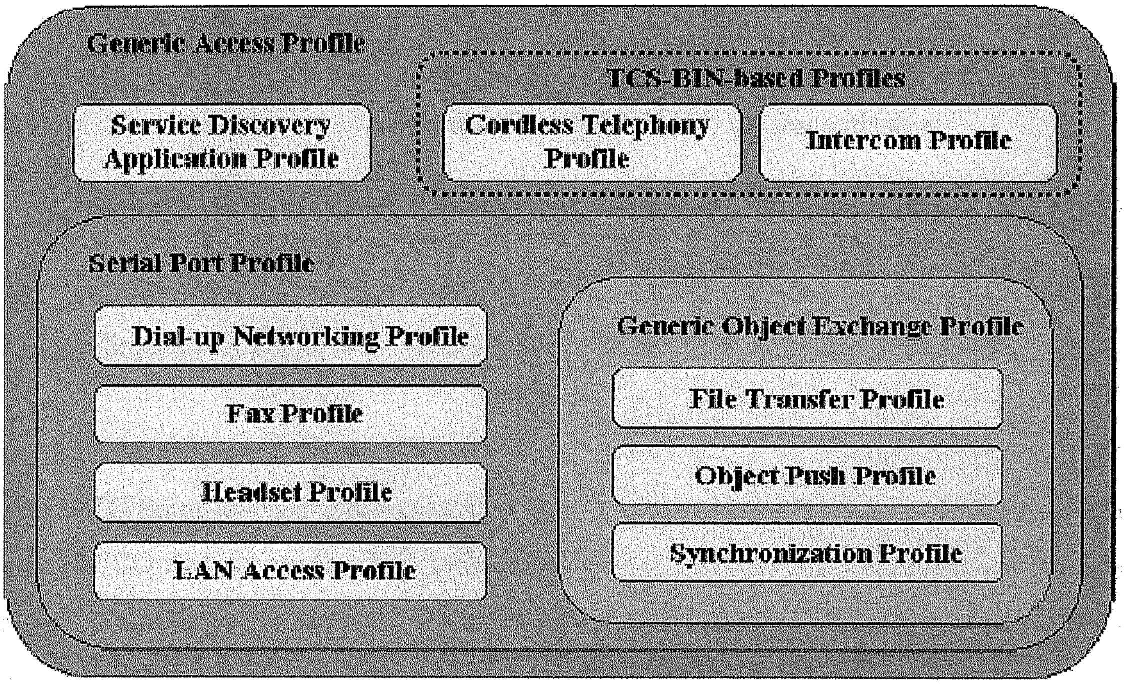


Figure 3.8.1. Bluetooth Profile Stnıcture

The key challenge and primary reason for the delay in Bluetooth adoption has been getting Bluetooth-enabled products to work in interoperability tests with other products.

3.5.15 Telephony control protocol

Telephony Control - Binary

The Telephony Control protocol - Binary, TCS Binary or TCS BIN, is a bit oriented protocol, which defines the call control signaling for the establishment of speech and <lata calls between Bluetooth units. The protocol defines the signaling for establishment and release of calls between Bluetooth units. As well as signaling to ease the handling of groups of Bluetooth units. Furthermore, TCS Binary provides functionality to exchange signaling information unrelated to ongoing calls. Establishment of a voice or <lata call in a point-to-point configuration as well as in a point-to-multipoint conflguration is covered in this protocol (note, after establishment, the transmission is from point to point). The TCS Binary is based on the ITU-T Recommendation Q.931.

Telephony Control -AT Commands

A number of AT-commands are supported for transmitting control signals for telephony control. These use the serial port emulation, RFCOMM, for transmission.

3.5.16 Adopted protocols

This section describes a number of protocols that are defined to be adopted to the Bluetooth protocol stack. Note some ofthese adaptations are at the moment incomplete.

ppp

The IETF Point-to-Point Protocol (PPP) in the Bluetooth technology is designed torun over RFCOMM to accomplish point-to-point connections. PPP is a packet oriented protocol and must therefore use its serial mechanisms to convert the packet <lata stream into a serial <lata stream.

TCP/UDP/IP

The TCP/UDP/IP standards are defined to operate in Bluetooth units allowing them to communicate with other units connected, for instance, to the Internet. Hence, the Bluetooth unit can act as a bridge to the Internet. The TCP/IP/PPP protocol configuration is used for all Internet Bridge usage scenarios in Bluetooth 1.0 and for

OBEX in future versions. The UDP/IP/PPP configuration is available as transport for WAP.

OBEX Protocol

IrOBEX, shortly OBEX, is an optional application layer protocol designed to enable units supporting infrared communication to exchange a wide variety of <lata and commands in a resource-sensitive standardized fashion. OBEX uses a client-server model and is independent of the transport mechanism and transport API. The OBEX protocol also defines a folder-listing object, which is used to browse the contents of folders on remote device. RFCOMM is used as the main transport layer for OBEX

Content formats

The formats for transmitting vCard and vCalendar information are also defined in the Bluetooth specification. The formats do not define transport mechanisms but the format in which electronic business cards and personal calendar entries and scheduling information are transported. vCard and vCalendar is transferred by OBEX.

Wireless Applieation Protocol, WAP

The Wireless Application Protocol (WAP) is a wireless protocol specification that works across a variety of wide-area wireless network technologies bringing the Intemet to mobile devices. Bluetooth can be used like other wireless networks with regard to WAP; it can be used to provide a bearer for transporting <lata between the WAP Client and its adjacent WAP Server. Furthermore, Bluetooth's ad hoc networking capability gives a WAP client unique possibilities regarding mobility compared with other WAP bearers. The traditional form of WAP communications involves a client device that communicates with a Server/Proxy device using the WAP protocols. Bluetooth is expected to provide a bearer service as specified by the WAP architecture. The WAP technology supports server push. If this is used over Bluetooth, it opens new possibilities for distributing information to handheld devices on location hasis. For example, shops can push special price offers to a WAP client when it comes within Bluetooth range.

4. BLUETOOTH USAGE MODELS AND PRODUCTS

4.1 Bluetooth Usage Models

in this section a number of Bluetooth usage models are described. For each usage model there is one or more corresponding profiles defining protocol layers and functions to be used. The profiles are not described in detail in this document, for more information refer to the Bluetooth standardization documents.

4.1.1 File Transfer

The File Transfer usage model offers the capability to transfer <lata objects from one Bluetooth device to another. Files, entire folders, directories and streaming media formats are supported in this usage model. The model also offers the possibility of browsing the contents of the folders on a remote device. Furthermore, push and exchange operations are covered in this usage model, e.g. business card exchange using the vCard (Electronic Business Card) format. The File Transfer model is based on GOEP.

4.1.2 Internet Bridge

The Intemet Bridge usage model describes how a mobile phone or cordless modem provides a PC with dial-up networking capabilities without the need for physical connection to the PC. This networking scenario requires a two-piece protocol stack, one for AT-commands to control the mobile phone and another stack to transfer payload data.

4.1.3 LAN Access

The LAN Access usage model is similar to the Intemet Bridge user model. The difference is that the LAN Access usage model does not use the protocols for AT commands. The usage model describes how <lata terminals use a LAN access point as a wireless connection to a Local Area Network. When connected, tlıe <lata terminals operate as if it they were connected to the LAN via dial-up networking.

4.1.4 Synchronization

The synchronizations usage model provides the means for automatic synchronization between for instance a desktop PC, a portable PC, a mobile phone and a notebook. The synchronization requires business card, calendar and task information to be transferred and processed by computers, cellular phones and PDAs utilizing a common protocol and format.

4.1.5 Three-in-One Phone

The Three-in-One Phone usage model describes how a telephone handset may connect to three different service providers. The telephone may act as a cordless telephone connecting to the public switched telephone network at home, charged at a fixed line charge. This scenario includes making calls via a voice base station, and making direct calls between two terminals via the base station. The telephone can also connect directly to other telephones acting as a "walkie-talkie" or handset extension i.e. no charging needed. Finally, the telephone may act asa cellular telephone connecting to the cellular infrastructure. The cordless and intercom scenarios use the same protocol stack.

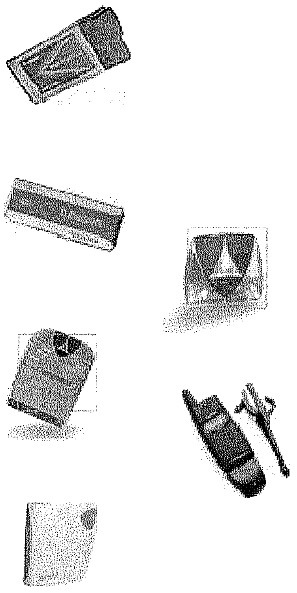
4.1.6 Ultimate Headset

The Ultimate Headset usage model defines how a Bluetooth equipped wireless headset can be connected, to act as a remote unit' s audio input and output interface. The unit is probably a mobile phone or a PC for audio input and output. As for the Intemet Bridge user model, this model requires a two-piece protocol stack; one for AT-commands to control the mobile phone and another stack to transfer payload <lata, i.e. speech. The AT-commands control the telephone regarding for instance answering and terminating calls.

4.2 Early Products and Prototypes

4.2.1 Plug-in modules

Initial products consist of plug-in modules to allow users to Bluetooth enable existing devices. These are basic cable replacement devices that interface through existing ports, and include the following:



Pigure 4.1 Plug-in modules

- PCMCIA card
- USB dongle
- Memory stick
- Serial portdôri.gle
- Parallel pört' dôngle
- Springboard'for'Handspring Visor
- LAN access points
- Cellular phone dongle

As chip prices drop and ufacturers begin integrate Bluetooth chips into motherboards and other devices, integrated solutions will become more widely available.

4.2.2 Dlgttal image messaging

Pictured are a Bluetooth-enabled Nokia 9110 and a Fuji Film digital camera that can communicate with one another using Multimedia Messaging Services (MMS). In this example, Bluetooth is enabling digital image messaging, A user takes a digital picture, transfers the image via Bluetooth to the Nokia 9110, adds a few lines of text, and then mails it to another 9110, a PC, or to FugiFilm.net for prints and saving to CD-R.

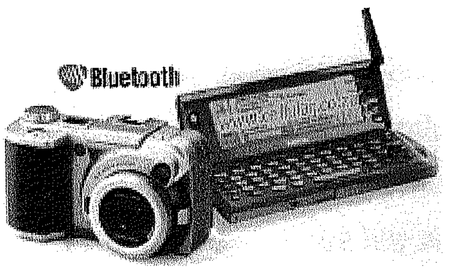


Figure 4.2 Digital image messagers

4.2.3 Bluetooth Infowear

In what the Bluetooth community calls "unconscious" or "hidden" computing, Bluetooth-enabled products will automatically seek each other out and configure themselves into networks - most often, with just two nodes. Though small, such networks can be quite useful. In this example, a prototype wristwatch that acts as an organizer and synchronizes information wirelessly with a PC is shown. At the Bluetooth Developers Conference in December 2000, IBM demonstrated a working prototype of a Linux-based wristwatch, complete with VGA touch-screen, speaker, microphone, and Bluetooth radio. During a keynote presentation, the presenter used this watch to control his PowerPoint presentation, while 3000 people looked on in amazemeiit.

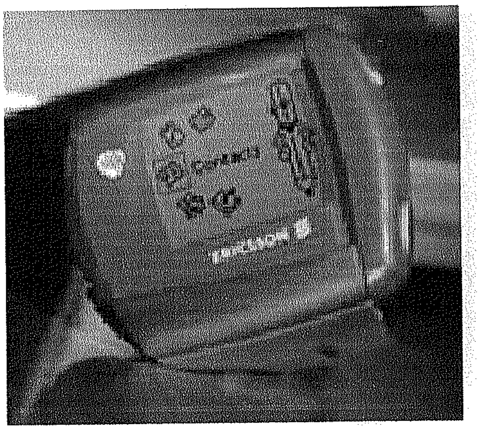
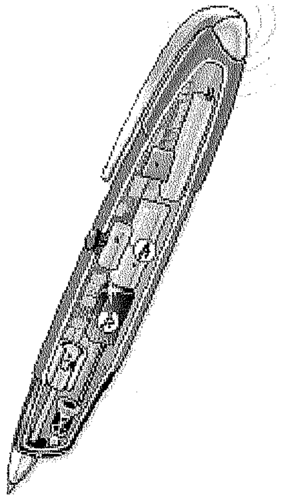


Figure 4.3 Bluetooth Info wear

4.2.4 Bluetooth Pen

With the Anoto Bluetooth pen, e-mails, faxes and e-commerce orders can be sent electronically by simply putting pen to paper. The technology was developed by Ericsson, Anoto and Time Manager, and is scheduled forintroduction in the second half of 2001. The device looks, feels, handles and writes like an ordinary ink pen, albeit a bulky one with a little LED indicator on the side. in additionto the usual ink cartridge, the Anoto pen contains image processing and Bluetooth radio .iCİfcuitry designed to automatically transmit what is written to a Bluetooth enabled celfülar phone, handheld computer or network base station. A pressure sensor at the backserıd öf the ink cartridge senses when the pen is actually writing, and a small imagin.giseıisor under the ink cartridge tracks the motion of the pen on the paper. The system'fequires special paper with a pattem printed on it, too small to be seen with the naked eye,toia.llow the pen's image processor to track the movements of the pen.



Fjgure 4.4 Bluetooth Pen

4.2.5 Xyloc

Ensure Technologies patented Xyloc technology allows a user to wear a key in the form of an ID badge-sized KeyCard ora small, pager-sized KeyFob. A Lock attaches to the user's PC through the keyboard, USB or serial port. The Lock and Key use an encrypted two-way Bluetooth radio link to identify the user to the Xyloc software on the computer. When a user approaches a Xyloc secured computer, the Key transmits a unique encrypted code to the Lock, which relays the information to a security database for validation. If the user is authorized; the system unlocks the keyboard and screen; if unauthorized the system remains secure. When the user steps away from the computer Xyloc immediately and automatically secures the computer. At eeBIT 2001, Seiko Instruments ine. and Ensure Technologies demonstrated Xyloc technology incorporated into an interactive Bluetooth wristwatch [4 7]. This technology is one to follow, as it could have wide application for ese and its clients, both commercial and government.

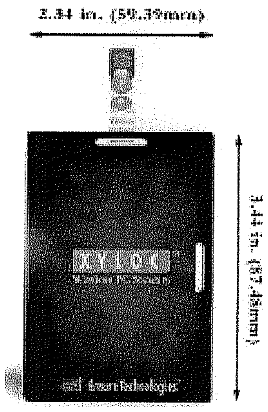


Figure 4.5 Keyeard

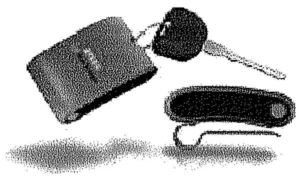
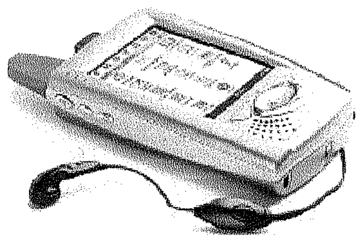


Figure 4.6 Key Fob

4.2.6 Convergence Products

The Ericsson Communicator Platform is an example of some ofthe capabilities that the next generation of products will offer, combining features of the hottest technologies into one device. This prototype device combines mobile Internet browsing, messaging, imaging, location based applications and services, mobile telephony and personal information management. This kind of product convergence will truly make life more pleasant by eliminating the need to carry multiple devices. And, of course, Bluetooth will mean that proprietary cables will no longer be needed in order to connect to other devices.



Flgure 4.7 Bluetooth based prototype device

5. BLUETOOTH & IEEE 802.11b & IrDA & COMPARASION

5.1 Competing Techniques

There are a number of competitors to the Bluetooth technology. However, there is no obvious single competitor in all the market segments in which the Bluetooth technology can operate.

5.2 IrDA

The main competitor in the cable replacement market segment is IrDA. IrDA is an infrared interface standard providing wireless solutions between, for instance, mobile phones and PDAs. The technique is well known in the market but has had problems because some IrDA manufacturers have made ımplementatiöns incompatible with standard implementations. The maximum payload in the IrDA technology exceeds the maximum Bluetooth payload. The two main disadvantages with IrDA are that it is limited to point-to-point connections (only two parties in a connectiorl) and its need for line of sight (since it is based on infrared light).

5.3 General IrDA Charaeteristics

Characteristics include:

- Proven worldwide universal cordless connection.
- Installed base of over 50 million units.
- Wide range of supported hardware and software platforms.
- Designed for point-to-point cable replacement.
- High <lata rates; 4 Mbps currently, 16 Mbps under development

IrDA and Bluetooth technologies provide complementary 'implemeııtations for <lata exchange and voice applications. For some devices, having both Bluetooth and IrDA will provide the best short-range wireless sohıtion. For other devices, the choice of adding Bluetooth or IrDA will be based ôn'the applications and intended usage models.

The story on short-range wireless communication technology is still being written and IrDA and Bluetooth will be the major forces driving this area.

5.4 Implementations Based On IEEE 802.11

The main competitors in the market segment for wireless LAN are the implementations based on the IEEE 802.11 standard. Some of these implementation.s also use the frequency hopping technology. The main differences between Bluetööthaand these implementations are:

- Implementations based on IEEE 802.11 have higher transmission capacity
- The number of simultaneous users is higher for IEEE 802.11-based systems
- The Bluetooth hardware size is considerably smaller
- The five Euro unit is 10 to 20 times cheaper than an IEEE 802.11 unit
- The number of frequency hops is considerably higher for Bluetooth than.:fôr an IEEE 802.11 implementation

Bluetooth is designed primarily for the personal-area network between an individual's personal devices, such as a phone, handheld device, laptop, printer and fax. By contrast, analysts see 802.11b networks as designed for workgroups or other settings(where wireless connections can be 100 meters or so apart.

5.5 Ultra-Wideband Radio, UWB

Ultra-Wideband Radio, UWB, is a new radio technology. The concept is similar 'to radar. Short pulses are transmitted in a broad frequency range. The infottı:iatibn is modulated by the pulses' time and frequency. The technique is not fully develbpedbut might be a threat to the Bluetooth concept since its superiority in capacity and power consumption. UWB prototypes indicate payloads up to 1.25 Mbit/s with 70 meters range at just 0.5 mW power consumption.

5.6 HomeRF

Home RF is a technique developed by a consortium with, among others, Microsoft, Intel, HP, Motorola and Compaq. The technique is developed from the DECT concept and operates in the 2.4 GHz frequency band (the same as Bluetooth). The intention has been to develop a technique for the home market. There are many simil~~~1~';~th Bluetooth, price per unit, range, transmitting power ete. The major differences it,~;tlfatif.\ Home RF can handle up to 127 units per net and it uses'just SQ frequency hops per second. The figures for Bluetooth are 8 and 1600 respectively.

5.7 Bluetooth Strengths

The Bluetooth concept offers several benefits compared with other techniques. main advantages ofBluetooth are:

- The minimal hardware dimensions
- The low price on Bluetooth components
- The low power consumption for Bluetooth connections

The advantages make it possible to introduce support for Bluetooth in many types of devices at a low price. The diversity in product offerings (mobile phones, PDAs, computers, computer hardware, notebooks ete) from companies in the Bluetooth SIG and their broad support for the technique creates a unique market position. Both hardware and device manufacturers will work for the introduction of Bluetooth in many different devices. The capabilities provided by Bluetooth, approximately 720 kbit/s, can be used for cable replacement and several other applications such as speech, LAN and so on, (These will be examined in the part, Bluetooth Usage Models). Defining of specific user models and corresponding profiles combined with the four general profiles will most likely lead to a market situation where applications covered by the user models will use the defined user models and their profiles. Furthermore, it is likely that new applications will use the standard profiles and thereby avoid interoperability problems between different manufacturers.

Table 5.1 Bluetooth Competing Technologies.

Technology	Data Rate	Range	Frequeney	Speçificatioıı	Status
	Mb/s	Meter	GHz		
802.11	2	100	2.4	1999	Now
802.llb	11	100	2.4	1999	Now
802.1 la	~40	TBD	5	N/A	2+ Years
802. 1 5(Bluetooth)	1	10	2.4	1999	Now
802.1 S(High Rate)	+20	TBD	2.4/5	TBD	N/A
HOmeRF	1.6	50	2.4	1999	Now
HOme RF(Next Gen)	10	50	2.4	N/A	FCC Approve
IrDA	4	1	Infrared		Now

6. BLUETOOTH EFFECTS ON HUMAN HEALT

It is a matter of concern for some people that the carrier waves used by Bluetooths transmitters use the same frequency range as microwave owens (Bluetooth uses 2.402 GHz to 2.480 GHz). Someone may wonder about how it feels like to get in the patlı of such waves.

Actually, the transmitting pôwefis far too weak to be noticeable for humans. Moreover, the radiation is not cô11c6ıitfated iıı a beam, but dispersed more or less in all directions. When using a wireless phôıieôf.a<Bfüetooth device, the body absorbs some of the emitted RF energy. The penetratföıide:pthis about 1.5 cm at 2450 MHz (about 2.5 cm at 900 MHz), which means that the abs~~Ji~:f~t:ry. superficial. The main absorption mechanism is field-induced rotation of pQlW .molecules (for example *HıO),* which generates heat through molecular "frictiôri.'1.

Heating by means of radio frequencies is p~ssi~l~~~~~₤;~~~~~ ~e;:ency range. This is taken advantage ofin microwave ovens at 2450;~0t0~~J~:~,=~l)~~:r.levels (up to 1,000,000 times the power used by Bluetoothdevices).I-I()weyer,2450 MHz is nota resonance frequency ofwater. But whether the Bhıetôôth:R.Fex:pôsuresto emission heat the human body? No, it does not. The output power ofa Bhıetööth...enabled device is far too low to cause any detectable temperature füctease. A.ga.iı'i; \in cônıparisön, the maximum increase from handheld cellular phônesiSlesstlian OJ "C.

There is, however, another side to this; some peopleiare demori.strablyover-sensitive to electromagnetic radiations. Long exposure to strong fields makes some individuals so sensitive, after a few years that they can no Ionger be near such fields without considerable discomfort. Bluetooth fits into a general development pattem where antennas for GSM-transmission and other sources of electromagnetic radiations become more and more prevalent in our cities. The future will show whether this is a healthy development.

CONCLUSION

Bluetooth is an enabling technology. As such, it is created to change our world in ways we can not imagine. New usage pattems will emerge asa result ofthis new technology.

lf Bluetooth is successful, it will be so in a big way, but even if Bluetooth fails in one area, there is probably enough industry support to ensure success elsewhere. The providers of Bluctooth'such as Nokia, Ericsson and Intel do not let it to go had anyway. That's why, there are'söıfiething to be done before hopping more.

In addition, Bluetooth fitsbestin low-power mobile devices for use in PANs. It should not try to compete with wireless LAN technologies, but it needs to co-exist with them . This is already one of nınning strategies of the Bluetooth. Moreover, there are already numerous applicatiön>areasfor Bluetooth, and many that have yet to be imagined. Some of the corporatio:nsiiarei>developing software for wireless e-commerce, providing hardware for wireless\security, or designing and implementing smart workspaces, and by the time allthis applicatiôns will be runable on Bluetooth chip.

Bluetooth is comi:ıiğ,a:ıidwe need to understand where it fits, and where it does not. I personaly wait for whafrri.ôrea.boutthe Bluetooth, from now on.

REFERENCES

1. Muller, Nathan J. *Bluetooth Demystified,* McGraw-Hill, Inc 2001

2. Miller, Brent A. Bisdikian, Chatschik. *Bluetooth Revealed,* Printice Hall, ine. 2001

3. Hodgson, David. Rab in, JeffPlı}fJ.Dundee Security Corporation, *The Oncoming Bluetooth Juğğernaut,* Növeınber 9, 2000

4. Bisikian, Chatschic. IEEE Communica.tiôrıs[Sılağazine, An overview ofthe Bluetooth Wireless Technology, December 2001

5. Bluetooth Special Interest Group. *Specification of the Bluetooth S,fm... v1.1,* volume I, available from http://www.bluetoott ı.com, Lecenıber 2000.

6. Palo wireless Bluetooth Resource Center, tutorials, available from, http://www.palowireless.com/infotooth/tutorial.asp, 2002

7. Biuetooth Special Interest Group. ŜpecitiĈatiöns of the Bluetooth Systems Profiles volume 2, available from, http://wwwfülıeföOth.côm, 22 February 2001

8. AU-System. Bluetooth White Paper 1.1, available from http://www.ausystem com, January 2000.

APPENDIXA

Common Wireless Frequencies and Applications

EM Band Designation	Frequency Range	Wireless Device/Application
VLF: Very Low Frequency	9 kHz–30 kHz	
lf: Low Fn:qLiencii'	3,{Ji kHz-3{MJ, k.Hz	
MF: MecliUm Frequency	300 k.Hz-3 MHz	AM raclio statioiis (535 kHi:-1 MHz}
I-IF: High Freqiaency	3 MH.z - .::,0 MHz	
VHF: Ver:,i High Frequency	31:ir MHz-300 MHz	FM mclio sta!iomi
		VHF television statioiis 7-'r3, NTSC Stam!ard 074 MHz-220 MHz)
		Garnge eoor openers ("-40 MHz)
		Standiird corciiessleiieplhcmes{40 MHz-SO MHzJ,
		Alarm s,rstems (~40MHz)
		Paging Systems (50 MHlz-30iJ MHz)
UHF: rntra High Frequency ı	300 MHz-3 GHlz	.Pagiiig systems (300 MHz-500 MHz)
		'1G mobile f.eleplıones (824 MHz-629 MHz)
		2G mol,i!e !eReplione (ôCıQ MHz-90'1) MHlz)
		Global sii~stem *tor* Mobile Oommunication(GSM}
		Eiihaiicecl Data Rates for Global Eimlution{EDGE) (80Qi'gioo.rian,onaooMHz bancls)
		3G Mobile terephoiies(internationai stl!mdard)('1,,755 MHz-2200 MHlz}
		Blcietooih de',~ces (2.4-2.4835 GHz)
		I-tlome RF (2.4 GHz ISM Bancl)
		WIAN (2.4, 5 GHz)
SHF: Sur,:ier Higli Frequency	3 GHz-30GHz	A:pplica.tiornsnn ilie short rang,e, poini-to-poinc comniunicatiornsim:ludin•g remoie coiitroi systems, PO.A.s, ete.
		'iJ'il'ILAN (5J!, GHz}.
		loca! Multir,:i,oint Distribution Services (LMIDS)., a nxecl wireless teclimologythat opemtes .im the 28 •GHz bancl am:l ofiifers rnne-orr-sigliicoverage ever clistarices tip to 3 !o 5, kilometern.
EHF: Extremely High t=requericy	3[], GHz-300 GHZ	Satemte oommunic:atiOris
!R: Infrar,ecl	300 GH.z	:Remofie coniirofis tor home audio-visuaK compoiients
		[R !'ihks For periplieral de\oices
		PDA am:l celliularteleplione IR Hinks