NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Computer Engineering

THE EFFECT OF BLUETOOTH EAR ON THE HUMAN

Graduation Project
COM- 400

Student: Khaled Smadi (20010687)

Supervisor: Mr. Jamal Fathi

Nicosia - 2006

Dedicated to my parents, brothers and sisters
And friends

ACKNOWLEDGMENTS

First of all I am happy to complete the task which I had given with blessing of God and also I am grateful to all the people in my life who have, supported me, advised me, taught me and who have always encouraged me to follow my dreams and ambitions. My dearest parents, my brothers and sisters, my friends and my tutors. They have taught me that no dream is unachievable. As in the words of Walt Disney "If you can dream it, you can do it."

I wish to thank my advisor, Mr.jamal fathi, for intellectual support, encouragement, and enthusiasm, which made this project possible, and his patience for correcting both my stylistic and scientific errors.

Finally, I wish by this project to be useful for all students, especially Computer engineering to support our improvement.

And above, I thank God for giving me stamina and courage to achieve my objectives.

To all of them, my love and respect

ABSTRACT

Bluetooth has been the subject of much hype and media attention over the last couple of years. As various manufacturers prepare to launch products using Bluetooth technology, an unsuspecting public is about to be catapulted into the next stage of the information technology revolution. Bluetooth is a low cost, low power short-range radio technology originally developed as a cable replacement to connect devices such as mobile phone handsets, headsets, and portable computers. This in itself sounds relatively innocuous; however, by enabling standardized wireless communications between any electrical devices, Bluetooth has created the notion of a Personal Area Network (PAN), a kind of close range wireless network that looks set to revolutionize the way people interact with the information technology landscape around them.

No longer do people need to connect, plug into, install, enable or configure anything to anything else. Through a ubiquitous standardized communications subsystem, devices will communicate seamlessly. One does not need to know where one's cellular phone is, or even if it is switched on. As soon as the Web browser appears on the mobile computer screen, a link is established with the phone, the Internet Service Provider is connected to, and the user is surfing the Web.

The Bluetooth specification is an open, global specification defining the complete system from the radio right up to the application level. The protocol stack is usually implemented partly in hardware and partly as software running on a microprocessor, with different implementations partitioning the functionality between hardware and software in different ways.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Overview

Bluetooth has been the subject of much hype and media attention over the last couple of years. As various manufacturers prepare to launch products using Bluetooth technology, an unsuspecting public is about to be catapulted into the next stage of the information technology revolution.

Bluetooth is a low cost, low power short-range radio technology originally developed as a cable replacement to connect devices such as mobile phone handsets, headsets, and portable computers. This in itself sounds relatively innocuous; however, by enabling standardized wireless communications between any electrical devices, Bluetooth has created the notion of a Personal Area Network (PAN), a kind of close range wireless network that looks set to revolutionizes the way people interact with the information technology landscape around them. No longer do people need to connect, plug into, install, enable or configure anything to anything else. Through a ubiquitous standardized communications subsystem, devices will communicate seamlessly. One does not need to know where one's cellular phone is, or even if it is switched on. As soon as the Web browser appears on the mobile computer screen, a link is established with the phone, the Internet Service Provider is connected to, and the user is surfing the Web.

The Bluetooth specification is an open, global specification defining the complete system from the radio right up to the application level. The protocol stack is usually implemented partly in hardware and partly as software running on a microprocessor, with

1.2 What Is Bluetooth

Bluetooth is a wireless communication protocol mainly used for short distance and in devices with low power consumption. Because Bluetooth is capable of communicating in an omni-directional manner of up to 30 feet at 1 Mb/s it is far superior to infrared. Where infrared requires a distance of a few feet or less and requires a direct line of site for transmissions. Okay what about WiFi, which typical can transmit up to 300 feet at 11 Mb/s. Well the fact is these are really two different beasts; Bluetooth was developed for small data transfers and/or voice communications. Which makes it an excellent candidate for peripherals devices such as wireless microphones, headsets, mice, keyboards and of course mobile handsets. WiFi in general was developed to transmit large amounts of data and to serve as an extension of an existing network such as LAN. Not only does Bluetooth does away with wired cabled connections such as serial, parallel, USB and Fire; but also, it presents to us an unified standard that truly makes connecting to devices to each other ubiquitous. There are hundreds if not thousands ways Bluetooth and be used to enhance our daily lives. Aside from entertainment value of playing games head to head in multiplayer mode there are many business solutions for us to explore. Here are a couple of ideas:

1. Efficient and easy way to update your PIM from home to office, where ever you go .
2. Easy to exchange information with others like mobile business cards.
3. Concurrent exchange of data, this comes in handy when a group of people are in meetings or at conferences.
4. Accessing devices such as printers and fax machines, this would definitely come in handy when visiting other offices of your company or client site
5. Monitoring systems, for example if you were a maintenance man doing routine system checks in a factory, it allows you to easily interface at each check point.
6. Going beyond the peer-to-peer use of Bluetooth there is what is called BlipNet used in enterprise scenarios.
7. Profile Holder - This may be best explained with an example, say you are using your buddies gaming console that is Bluetooth enabled you can upload your saved games and download your current game. Another example, you visit your local drug store and beam your prescription and once it is filled out you get notified on your phone this allows you to continue shopping without the hassle of waiting inline or trying to decipher what is being said over the PA system.
8. Provide entertainment during waiting periods, for example waiting in line to buy a ticker form ovieyou could play Bluetooth movie trivia games.

Who invented Bluetooth? Bluetooth was originally researched and developed by the Ericsson organization and were the ones who named the technology after King Harald Blatand (Bluetooth) of Denmark. Ericsson formed the Bluetooth Special Interest Group. Definitely checkout all the products that are Bluetooth enabled, this definitely will if not already provide plenty of opportunity for us developers to make some innovative applications Bluetooth is an always-on, short-range radio hookup that resides on a microchip. It was initially developed by Swedish mobile phone maker Ericsson in 1994 as a way to let laptop computers make calls over a mobile phone. Since then, several thousand companies have signed on to make Bluetooth the low-power short-range wireless standard for a wide range of devices. Industry observers expect Bluetooth to be installed in billions of devices. The Bluetooth standards are published by an industry consortium known as the Bluetooth SIG (special interest group).

The concept behind Bluetooth is to provide a universal short-range wireless capability. Using the 2.4 GHz band, available globally for unlicensed low-power uses, two Bluetooth devices within 10 m of each other can share up to 720 Kbps of capacity. Bluetooth is intended to support an open-ended list of applications, including data (such as schedules and telephone numbers), audio, graphics, and even video. For example, audio devices can include headsets, cordless and standard phones, home stereos, and digital MP3 players. Following are some examples of the capabilities that Bluetooth can provide consumers:

1. Make calls from a wireless headset connected remotely to a cell phone.
2. Eliminate cables linking computers to printers, keyboards, and the mouse.
3. Hook up MP3 players wirelessly to other machines to download music.
4. Set up home networks so that a couch potato can remotely monitor air conditioning, the oven, and children's Internet surfing.
5. Call home from a remote location to turn appliances on and off, set the alarm, and monitor activity.

1.3 What is Bluetooth Technology?

Bluetooth technology is an industry wireless specification standard for use in various devices for short-range communications. As a radio-based technology it allows devices to share information over a maximum range of 10 meters. Bluetooth enables mobile computers, mobile phones, portable handhelds, and the Internet to "talk the talk" without cables. With Bluetooth, devices don't need to be 'looking' at each unlike other wireless technologies (i.e. infrared). As long as two Bluetooth devices are close enough to each other, it's possible to make a connection. With Bluetooth technology getting connected takes on a whole new meaning.

Bluetooth technology allows a variety of devices, from cell phones to PDAs to desktop computers, to communicate with each other without connecting them via cables. Bluetooth has more applications in the mobile and embedded devices area where, according to industry observers, 80% of mobile phones will support Java by 2006. The reason for this is two-fold: the number of Java developers (and their technology demands) are increasingly on the rise and the standard Application Programming Interface (API) for Bluetooth technology was just defined for the Java programming language in February 2002. This book explains how to program to this API, gives details on why it was created, how it will help exploit the power of Java and Bluetooth, and show how to create an implementation of a device. With Bluetooth™ technology, all connections are instant and automatic. The tiny Bluetooth™ microchip, incorporating a radio transceiver, is built into the devices and ensures fast and secure transmissions of both voice and data. The radio operates in a globally available frequency band, ensuring compatibility worldwide.

The Bluetooth technology is designed to be fully functional even in a very noisy radio environment, and its voice transmissions are audible under severe conditions.The technology also provides a very high transmission rate, and all data are protected by advanced error-correction methods, as well as encryption and authentication routines for the user's privacy.

1.4 Bluetooth Tutorial - Profiles

The profiles have been developed in order to describe how implementations of user models are to be accomplished. The user models describe a number of user scenarios where Bluetooth performs the radio transmission. A profile can be described 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.

Bluetooth specifies a telephony control protocol. TCS BIN (telephony control specification-binary) is a bit-oriented protocol that defines the call control signaling for the establishment of speech and data calls between Bluetooth devices. In addition, it defines mobility-management procedures for handling groups of Bluetooth TCS devices. The adopted protocols are defined in specifications issued by other standards-making organizations and incorporated into the overall Bluetooth architecture. The Bluetooth strategy is to invent only necessary protocols and use existing standards whenever possible.

1.5 There are the adopted protocols

1.5.1 The point-to-point protocol (PPP)

is an Internet standard protocol for transporting IP data-grams over a point-to-point link.

1.5.2 TCP/UDP/IP

These are the foundation protocols of the TCP/IP protocol suite.

1.5.3 OBEX

The object exchange protocol is a session-level protocol developed by the Infrared Data Association (IrDA) for the exchange of objects. OBEX provides functionality similar to that of HTTP, but in a simpler fashion. It also provides a model for representing objects and operations. Examples of content formats transferred by OBEX are vCard and vCalendar, which provide the format of an electronic business card and personal calendar entries and scheduling information, respectively.

1.5.4 WAE/WAP

Bluetooth incorporates the wireless application environment and the wireless application protocol into its architecture.

1.6 Bluetooth Profiles

Bluetooth Profiles - defined functionality for Bluetooth such as Fax Profile that enables a Bluetooth device to send a fax via Bluetooth fax machine. These profiles may seem similar to the J2ME profiles but they aren't. It isn't an add-on to J2ME but rather an add-on to Bluetooth. Bluetooth profiles can be implemented in other languages like C/C++.

The network between Bluetooth enabled devices is called a PAN, which stands for Personal Area Networks. A PAN can be a Pico net or scatter net, where a Pico net is when there is one master and several slaves. A scatter net consists of 2 or more masters and several slaves, in other words one of the Bluetooth devices is both a master and a slav.

1.7 Current aspects

Bluetooth technology enables a lot of functions to make life easier. It allows you to send files from one mobile computer to another as easily as over a LAN, or to surf the Internet regardless of your location.

By installing a Bluetooth network at your office, you will no longer be bound to certain locations for connection and you don't need to draw new cables for new installations.

1.8 Future aspects

Because Bluetooth wireless technology can be used for a variety of purposes, it will also potentially replace multiple cable connections via a single radio link. This creates the possibility of using mobile data in a different way for different applications, such as "surfing on the sofa", "three in one phone", and many others.

1.9 Summary

Bluetooth wireless technology is finally here. Originally conceived as a low-power short range radio technology designed to replace cables for interconnecting devices such as printers, keyboards, and mice, its perceived potential has evolved into far more sophisticated usage models. The requirement to do this in a totally automated, seamless, and user-friendly fashion, without adding appreciable cost, weight, or power drain to the associated host is an enormous engineering challenge. Bluetooth devices can form piconets of up to seven slaves and one master, enabling discovery of services and subsequent implementation of many varied usage models including wireless headsets, Internet bridges, and wireless operations such as file exchange, data synchronization, and printing. Despite talk of Bluetooth competing with wireless LANs, Bluetooth products work over shorter distances and are designed to solve different problems. The Bluetooth SIG publishes the Bluetooth specification. The IEEE has formed the working group to define standards for wireless PANs.

2. WIRELESS

2.1 Wireless Overview

WLAN technology and the WLAN industry date back to the mid-1980s when the Federal Communications Commission (FCC) first made the RF spectrum available to industry. During the 1980s and early 1990s, growth was relatively slow. Today, however, WLAN technology is experiencing tremendous growth. The key reason for this growth is the increased bandwidth made possible by the IEEE 802.11 standard. As an introduction to the 802.11 and WLAN technology.

2.2 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 data, 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, and security issues is presented in this section.

2.3 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 "tetherless" 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. for a list of common wireless frequencies.) This document focuses on WLAN and WPAN technologies.

2.4 Brief History

Motorola developed one of the 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 project 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 international interoperability standard. Then, in 1999, the IEEE ratified the 802.11a 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 802.11a standard uses orthogonal frequency division multiplexing (OFDM) to reduce interference. This technology uses the 5 GHz frequency spectrum and can process data at up to 54 Mbps. Although this section of the document focuses on the IEEE 802.11 WLAN standard, it is important to note that several other WLAN technologies and standards are available from which consumers may choose, including HiperLAN and HomeRF. For information on the European Telecommunications Standards Institute (ETSI) developed

HiperLAN, For more information on HomeRF, This document does not address those technologies.

2.5 Frequency and Data Rates

IEEE developed the 802.11 standards to provide wireless networking technology like the wired Ethernet that has been available for many years. The IEEE 802.11a standard is the most widely adopted member of the 802.11 WLAN family. It operates in the licensed 5 GHz band using OFDM technology. The popular 802.11b standard operates in the unlicensed 2.4 GHz–2.5 GHz Industrial, 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 standard (that sends data at up to 2 Mbps) and slightly faster than standard Ethernet.

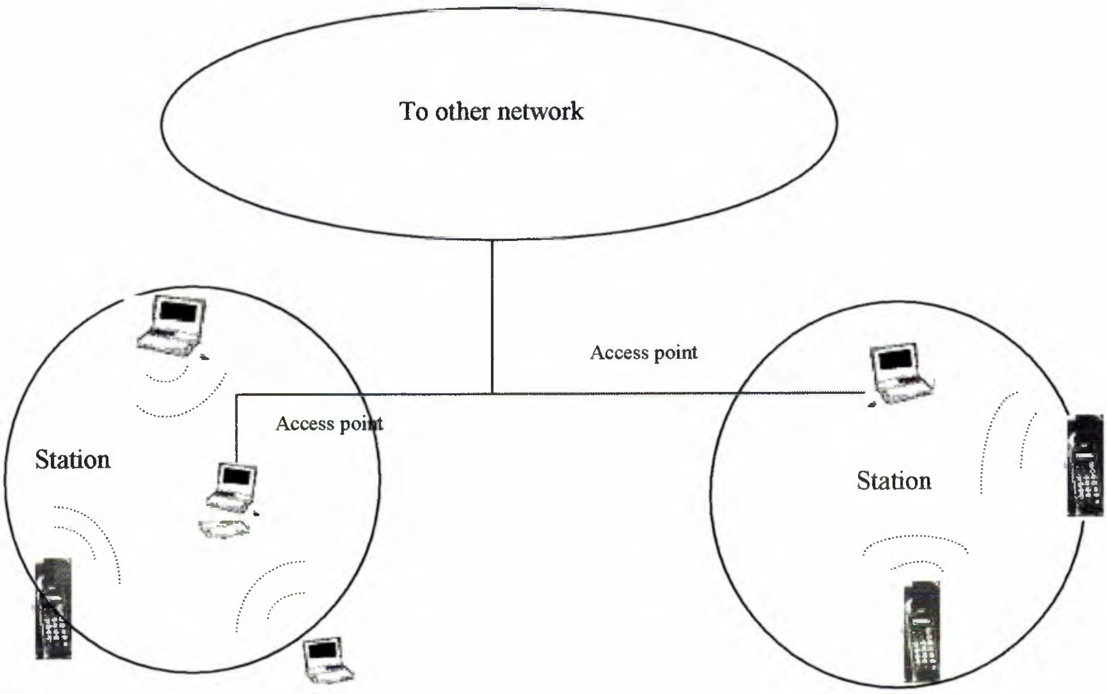

Figure 2.1 Fundamental 802.11 Wireless LAN Topology

Although most WLANs operate in the “infrastructure” mode and architecture described above, another topology is also possible. This second topology, the ad hoc network, 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 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 2.2 below.

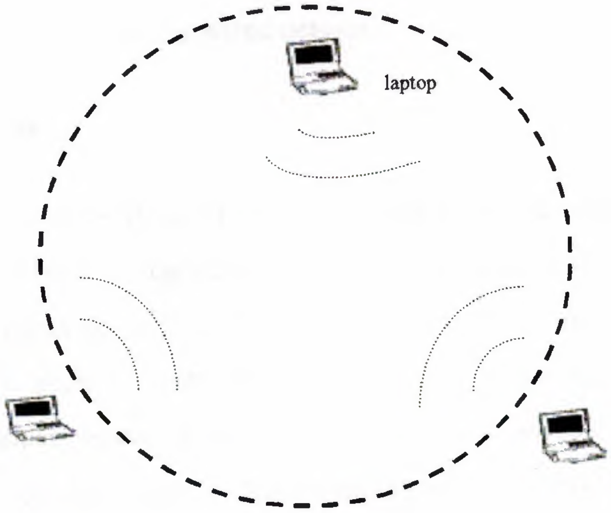

Figure 2.2 802.11 Wireless LAN Ad Hoc Topology

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.

2.6 Wireless LAN 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 or equipment within a kiosk on a manufacturing floor or other publicly accessed area. Wireless laptops and notebooks "wireless enabled" are identical to laptops 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 International 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 as a base station for the wireless network, aggregating multiple wireless stations onto the wired network.

2.6.1 Wireless LANs

WLANs allow greater flexibility and portability than do traditional wired local area networks (LAN). Unlike a traditional LAN, which requires a wire to connect a user's computer to the network, a WLAN connects computers and other components to the network using an access point device. An access point communicates with devices equipped with wireless network adaptors; it connects to a wired Ethernet LAN via an RJ-45 port. Access point devices typically have coverage areas of up to 300 feet (approximately 100 meters). This coverage area is called a cell or range. Users move freely within the cell with their laptop or other network device. Access point cells can be linked together to allow users to even "roam" within a building or between buildings.

2.6.2 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 configurations, 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 networks. It also controls the flow of data 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 2.3 illustrates an example of a Bluetooth-enabled mobile phone connecting to a mobile phone Network.

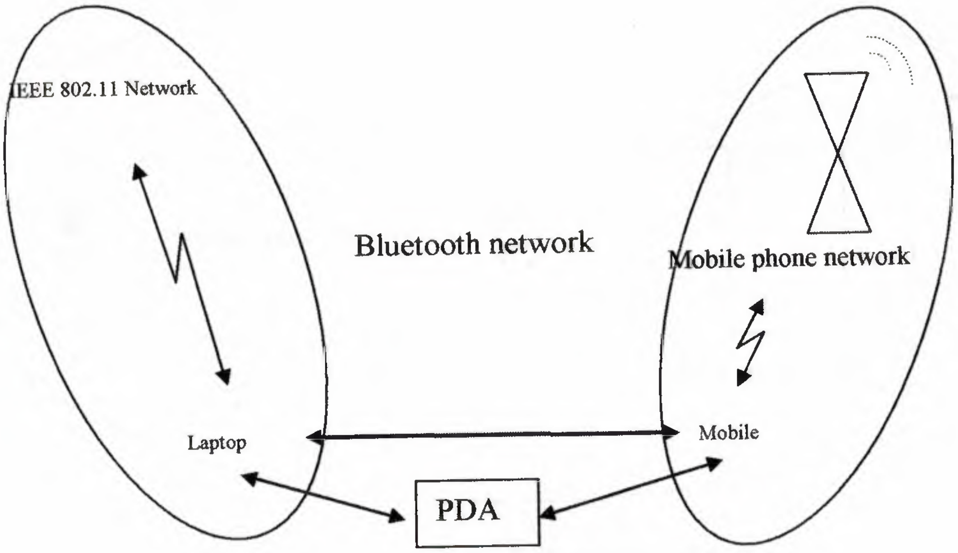

Figure 2.3 National Ad Hoc Network

2.7 Range

The reliable coverage range for 802.11 WLANs 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 indoors. A range of 400 meters, nearly ¼ 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.

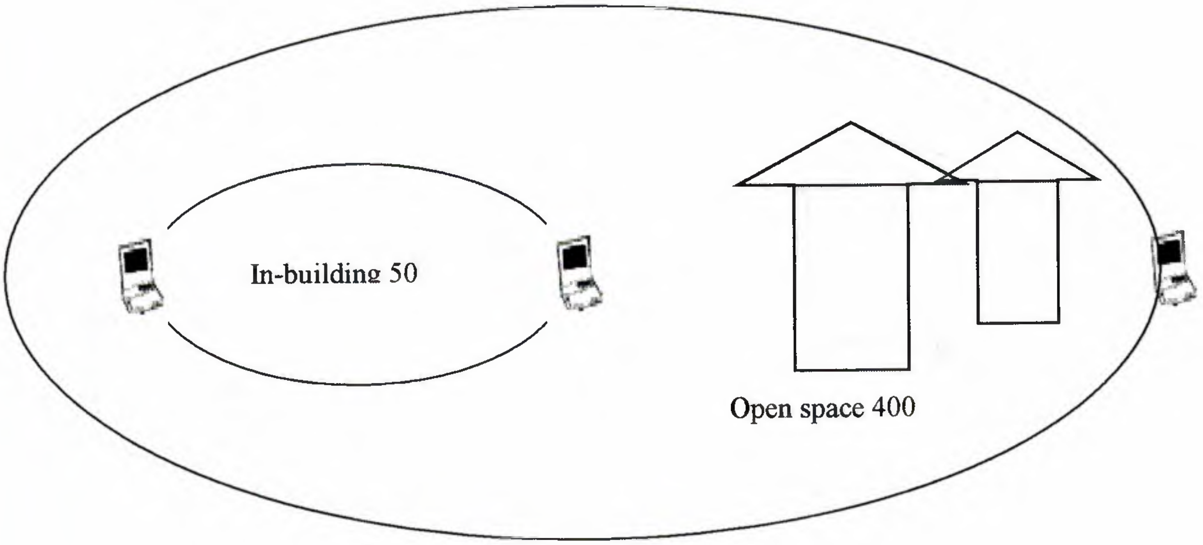

Figure 3.4 Typical Range of 802.11

APs may also provide a "bridging" function. Bridging connects two or more networks 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. LANs' respective APs. In multipoint bridging, one subnet on a LAN is connected to several other subnets on another LAN via each subnet AP. For example, if a 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 APs. 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 2.5 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 to AP bridge located on the building's roof. That AP bridge then transmits the data to the bridge on nearby building B. The building AP bridge then sends the data over its wired LAN to Laptop B.

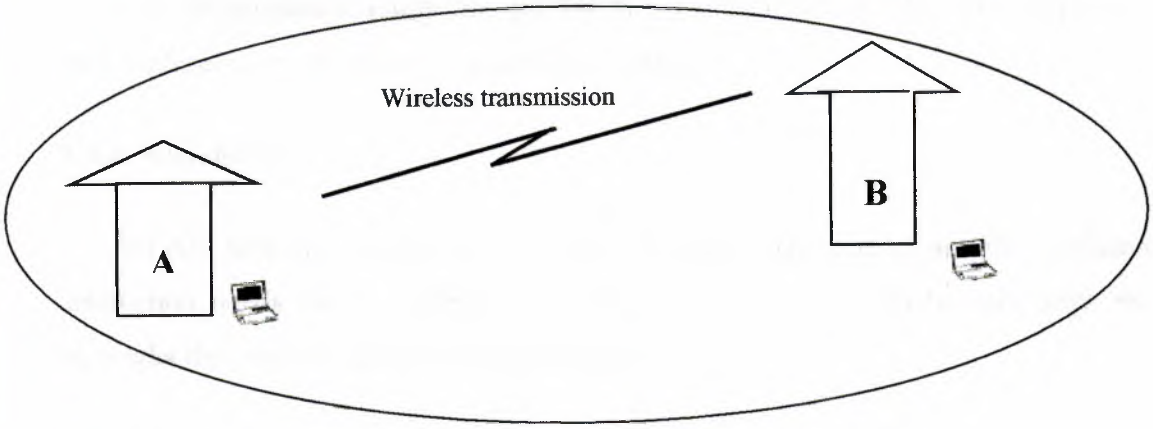

Figure 2.5 Access Point Briding

2.8 Benefits

WLANs offer four primary benefits:

2.8.1 User Mobility

Users can access files, network resources, and the Internet 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.

2.8.2 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 LAN installations possible in buildings that are subject to historic preservation rules.

2.8.3 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 temporary needs such as a conference, trade show, or standards meeting.

2.8.4 Scalability

WLAN network topologies can easily be configured 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.

2.9 Wireless Devices

A wide range of devices use wireless technologies, with handheld devices being the most prevalent form today. This document discusses the most commonly used wireless handheld devices such as textmessaging devices, PDAs, and smart phones.

2.9.1 Personal Digital Assistants

PDAs are data organizers that are small enough to fit into a shirt pocket or a purse. PDAs offer applications such as office productivity, database applications, address books, schedulers, and to-do lists, and they allow users 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 Internet. 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 Internet and wireless network.

2.9.2 Smart Phones

Mobile wireless telephones, or cell phones, are telephones that have shortwave 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 Internet access. Mobile phones with information-processing and data networking capabilities are called “smart phones.” This document addresses the risks introduced by the information-processing and networking capabilities of smart phones.

2.10 Wireless Standards

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 to allow products from multiple vendors to interoperate. For this document, the discussion 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 techniques or are based on the Bluetooth standard, which was developed by a consortium of commercial companies making up the Bluetooth Special Interest Group (SIG). These standards are described below.

2.10.1 IEEE 802.11

WLANs are based on the IEEE 802.11 standard, which the IEEE first developed in 1997. The IEEE designed 802.11 to support medium-range, higher data rate applications, such as Ethernet networks, and to address mobile and portable stations. 802.11 is the original WLAN standard, designed for 1 Mbps to 2 Mbps wireless transmissions. It was followed in 1999 by 802.11a, 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 802.11b standard has been so widely adopted, the security weaknesses in the standard have been exposed. These weaknesses will be discussed in Section 3.3.2. Another standard, 802.11g, still in draft, operates in the 2.4 GHz waveband, where current WLAN products based on the 802.11b standard operate. Two other important and related standards for WLANs are 802.1X and 802.11i. The 802.1X, a port-level access control protocol, provides a security framework for IEEE networks, including Ethernet and wireless networks. The 802.11i standard, also still in draft, was created for wireless-specific security functions that operate with IEEE 802.1X.

2.11 Wireless Security Threats and Risk Mitigation

The NIST handbook An Introduction to Computer Security generically classifies security threats in nine categories ranging from errors and omissions to threats to personal privacy. *6* All of these represent potential threats in wireless networks as well. However, the more immediate concerns for wireless communications are device theft, denial of service, malicious hackers, malicious code, theft of service, and industrial and foreign espionage. Theft is likely to occur with wireless devices because of their portability. Authorized and unauthorized users of the system may commit fraud and theft; however, authorized users are more likely to carry out such acts. Since users of a system may know what resources a system has and the system's security flaws, it is easier for them to commit fraud and theft. Malicious hackers, sometimes called crackers, are individuals who break into a system without authorization, usually for personal gain or to do harm. Malicious hackers are generally individuals from outside of an agency or organization (although users within an agency or organization can be a threat as well). Such hackers may gain access to the wireless network access point by eavesdropping on wireless device communications. Malicious code involves viruses, worms, Trojan horses, logic bombs, or other unwanted software that is designed to damage files or bring down a system. Theft of service occurs when an unauthorized user gains access to the network and consumes network resources. Industrial and foreign espionage involves gathering proprietary data from corporations or intelligence information from governments through eavesdropping. In wireless networks, the espionage threat stems from the relative ease with which eavesdropping can occur on radio transmissions. Attacks resulting from these threats, if successful, place an agency's systems and, more importantly, its data at risk. Ensuring confidentiality, integrity, authenticity, and availability are the prime objectives of all government security policies and practices. Security Self-Assessment Guide for Information Technology Systems, states that information must be protected from unauthorized, unanticipated, or unintentional modification. Security requirements include the following:

2.11.1 Authenticity

A third party must be able to verify that the content of a message has not been changed in transit.

2.11.2 Nonrepudiation

The origin or the receipt of a specific message must be verifiable by a third party.

2.11.3 Accountability

The actions of an entity must be traceable uniquely to that entity.

2.12 Privacy

The 802.11 standard supports privacy (confidentiality) through the use of cryptographic techniques for the wireless interface. The WEP cryptographic technique for confidentiality also uses the RC4 symmetric key, stream cipher algorithm to generate a pseudo-random data sequence. This "key stream" is simply added modulo 2 (exclusive-OR-ed) to the data to be transmitted. Through the WEP technique, data can be protected from disclosure during transmission over the wireless link. WEP is applied to all data above the 802.11 WLAN layers to protect traffic such as Transmission Control Protocol/Internet Protocol (TCP/IP), Internet Packet Exchange (IPX), and Hyper Text Transfer Protocol (HTTP). As defined in the 802.11 standard, WEP supports only a 40-bit cryptographic keys size for the shared key. However, numerous vendors offer nonstandard extensions of WEP that support key lengths from 40 bits to 104 bits. At least one vendor supports a keysize of 128 bits. The 104-bit WEP key, for instance, with a 24-bit Initialization Vector (IV) becomes a 128-bit RC4 key. In general, all other things being equal, increasing the key size increases the security of a cryptographic technique. However, it is always possible for flawed implementations or flawed designs to prevent long keys from increasing security. Research has shown that key sizes of greater than 80-bits, for robust designs and implementations, make brute-force cryptanalysis (code breaking) an impossible task. For 80-bit keys, the number of possible keys a keyspace of more than 1026 exceeds contemporary computing power. In practice, most WLAN deployments rely on 40-bit keys. Moreover, recent attacks have shown that the WEP approach for privacy is, unfortunately, vulnerable to certain attacks regardless of keysize. However, the cryptographic, standards, and vendor WLAN communities have developed enhanced WEP, which is available as a prestandard vendor-specific implementations. The attacks mentioned above are described later in the following sections. The WEP privacy is illustrated conceptually in Figure 2.6.

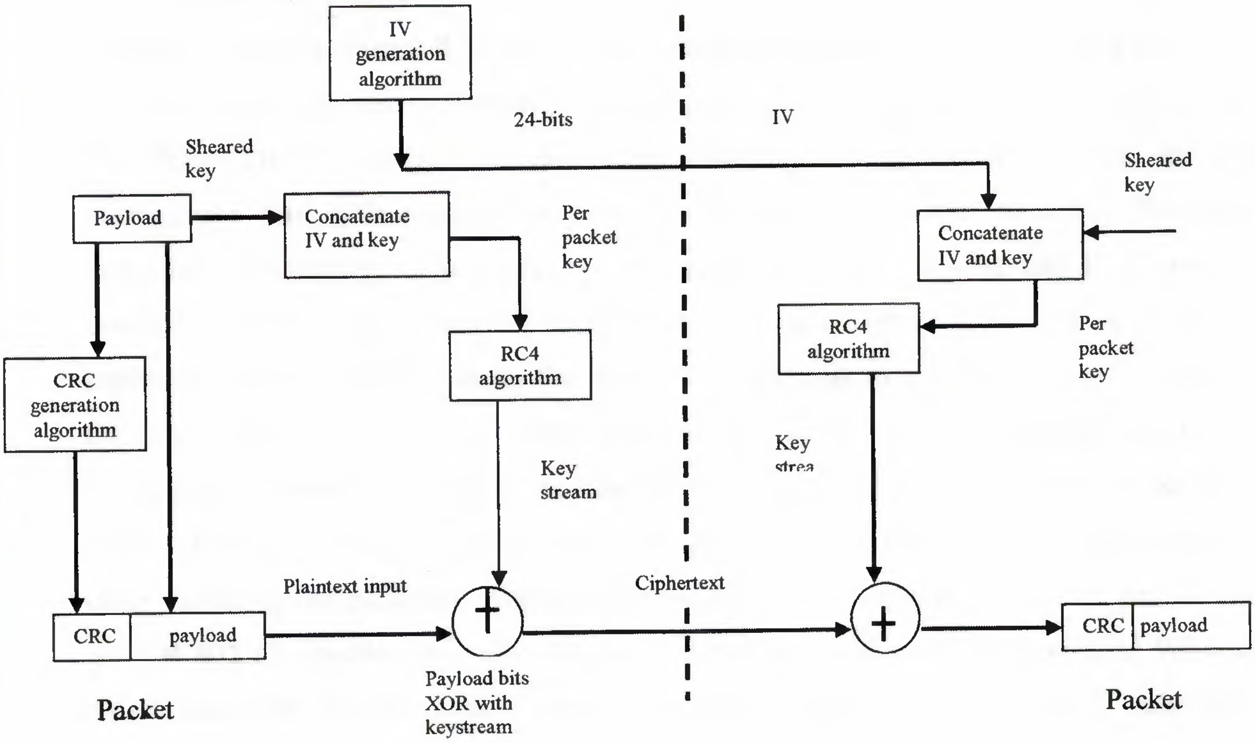

Figure 2.6 WEP Privacy Using RC4 Algorithm

2.13 Integrity

The IEEE 802.11 specification also outlines a means to provide data integrity for messages transmitted between wireless clients and access points. This security service was designed to reject any messages that had been changed by an active adversary "in the middle." This technique uses a simple encrypted Cyclic Redundancy Check (CRC) approach. As depicted in the diagram above, a CRC-32, or frame check sequence, is computed on each payload prior to transmission. The integrity-sealed packet is then encrypted using the RC4 key stream to provide the cipher-text message. On the receiving end, decryption is performed and the CRC is recomputed on the message that is received. The CRC computed at the receiving end is compared with the one computed with the original message. If the CRCs do not equal, that is, "received in error," this would indicate an integrity violation and the packet would be discarded. As with the privacy service, unfortunately, the 802.11 integrity is vulnerable to certain attacks regardless of key size. In summary, the fundamental flaw in the WEP integrity scheme is that the simple CRC is not a "cryptographically secure" mechanism such as a hash or message authentication code. The IEEE 802.11 specification does not, unfortunately, identify any means for key management (life cycle handling of cryptographic keys and related material). Therefore, generating, distributing, storing, loading, escrowing, archiving, auditing, and destroying the material is left to those deploying WLANs. Key management (probably the most critical aspect of a cryptographic system) for 802.11 is left largely as an exercise for the users of the 802.11 network. As a result, many vulnerabilities could be introduced into the WLAN environment. These vulnerabilities include WEP keys that are non-unique, never changing, factory-defaults, or weak keys (all zeros, all ones, based on easily guessed passwords, or other similar trivial patterns). Additionally, because key management was not part of the original 802.11 specification, with the key distribution unresolved, WEP-secured WLANs do not scale well. If a enterprise recognizes the need to change keys often and to make them random, the task is formidable in a large WLAN environment. For example, a large campus may have as many as 15,000 APs. Generating, distributing, loading, and managing keys for an environment of this size is a significant challenge. It is has been suggested that the only practical way to distribute keys in a large dynamic environment is to publish it. However, a fundamental tenet of cryptography is that cryptographic keys remain secret. Hence we have a major dichotomy. This dichotomy exists for any technology that neglects to elegantly address the key distribution problem.

3.14 Security Requirements and Threats

As discussed above, the 802.11 WLAN or WiFi industry is burgeoning and currently has significant momentum. All indications suggest that in the coming years numerous organizations will deploy 802.11 WLAN technology. Many organizations including retail stores, hospitals, airports, and business enterprises plan to capitalize on the benefits of "going wireless." However, although there has been tremendous growth and success, everything relative to 802.11 WLANs has not been positive. There have been numerous published reports and papers describing attacks on 802.11 wireless networks that expose organizations to security risks. This subsection will briefly cover the risks to security-i.e.,

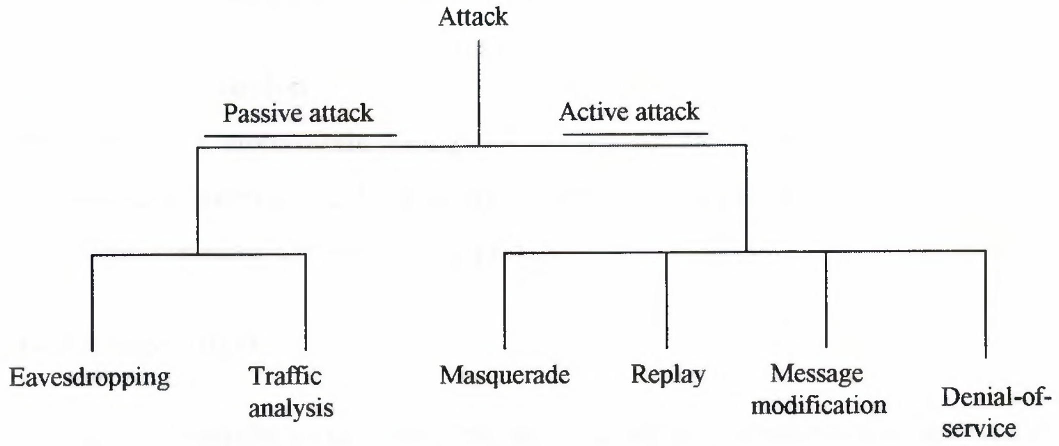

Figure 2.7 Taxonomy of Security Attacks

attacks on confidentiality, integrity, and network availability. Figure 2.7 provides a general taxonomy of security attacks to help organizations and users understand some of the attacks against WLANs.

Network security attacks are typically divided into passive and active attacks. These two broad classes are then subdivided into other types of attacks. All are defined below.

2.14.1 Passive Attack

An attack in which an unauthorized party gains access to an asset and does not modify its content (i.e., eavesdropping). Passive attacks can be either eavesdropping or traffic analysis (sometimes called traffic flow analysis). These two passive attacks are described below.

2.14.1.1 Eavesdropping

The attacker monitors transmissions for message content. An example of this attack is a person listening into the transmissions on a LAN between two workstations or tuning into transmissions between a wireless handset and a base station.

2.14.1.2 Traffic analysis

The attacker, in a more subtle way, gains intelligence by monitoring the transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages between communicating parties.

2.14.2 Active Attack

An attack whereby an unauthorized party makes modifications to a message, data stream, or file. It is possible to detect this type of attack but it may not be preventable. Active attacks may take the form of one of four types (or combination thereof): masquerading, replay, message modification, and denial-of-service (DoS). These attacks are defined below.

2.14.2.1 Masquerading

The attacker impersonates an authorized user and thereby gains certain unauthorized privileges.

2.14.2.2 Replay

The attacker monitors transmissions (passive attack) and retransmits messages as the legitimate user.

2.14.2.3 Message modification

The attacker alters a legitimate message by deleting, adding to, changing, or reordering it.

2.14.2.4 Denial-of-service

The attacker prevents or prohibits the normal use or management of communications facilities.

2.15 Risk Mitigation

Government agencies can mitigate risks to their WLANs by applying countermeasures to address specific threats and vulnerabilities. Management countermeasures combined with operational and technical countermeasures can be effective in reducing the risks associated with WLANs. The following guidelines will not prevent all adversary penetrations, nor will these countermeasures necessarily guarantee a secure wireless networking environment. This section describes risk-mitigating steps for an agency, recognizing that it is impossible to remove all risks. Additionally, it should be clear that there is no "one size fits all solution" when it comes to security. Some agencies may be able or willing to tolerate more risk than others. Also, security comes at a cost: either in money spent on security equipment, in inconvenience and maintenance, or in operating expenses. Some agencies may be willing to accept risk because applying various countermeasures may exceed financial or other constraints.

2.16 Summary

Wireless communications offer organizations and users many benefits such as portability and flexibility, increased productivity, and lower installation costs. Wireless technologies cover a broad range of differing capabilities oriented toward different uses and needs. Wireless local area network (WLAN) devices, for instance, allow users to move their laptops from place to place within their offices without the need for wires and without losing network connectivity. Less wiring means greater flexibility, increased efficiency, and reduced wiring costs. Ad hoc networks, such as those enabled by Bluetooth, allow data synchronization with network systems and application sharing between devices. Bluetooth functionality also eliminates cables for printer and other peripheral device connections. Handheld devices such as personal digital assistants (PDA) and cell phones allow remote users to synchronize personal databases and provide access to network services such as wireless e-mail, Web browsing, and Internet access. Moreover, these technologies can offer dramatic cost savings and new capabilities to diverse applications ranging from retail settings to manufacturing shop floors to first responders.

However, risks are inherent in any wireless technology. Some of these risks are similar to those of wired networks; some are exacerbated by wireless connectivity; some are new. Perhaps the most significant source of risks in wireless networks is that the technology's underlying communications medium, the airwave, is open to intruders, making it the logical equivalent of an Ethernet port in the parking lot. The loss of confidentiality and integrity and the threat of denial of service (DoS) attacks are risks typically associated with wireless communications. Unauthorized users may gain access to agency systems and information, corrupt the agency's data, consume network bandwidth, degrade network performance, launch attacks that prevent authorized users from accessing the network, or use agency resources to launch attacks on other networks.

3. BLUETOOTH

3.1 Bluetooth 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 provide a mechanism for creating small wireless networks on an ad hoc basis. Bluetooth is considered a wireless PAN technology that offers fast and reliable transmission for both voice and data. Undeterred Bluetooth devices will eliminate the need for cables and provide a bridge to existing networks.

3.2 Bluetooth

Bluetooth is a wireless communications and networking technology designed to eliminate cables between computers and cell phones, printers, scanners, digital cameras and other such peripherals. Bluetooth technology supports both voice and data. In the words of the official Bluetooth web site, this technology enables "users to connect a wide range of computing and telecommunications devices easily and simply, without the need to buy, carry, or connect cables". Because Bluetooth wireless technology can be used for a variety of purposes, it should eventually replace multiple cable connections with a single radio link. In summary, as noted at the Ericsson Bluetooth site "Bluetooth wireless technology is a low-cost, low-power, short-range radio link for mobile devices and for WAN/LAN access points". It offers "fast and reliable digital transmissions of both voice and data over the globally available 2.4 GHz ISM (Industrial, Scientific and Medical) band." From the idea of simply replacing cables, Bluetooth technology soon evolved to become more diversified, to become "a universal bridge to existing data networks, a peripheral interface, and a mechanism to form small private ad hoc groupings of connected devices away from fixed network infrastructures.

3.3 Bluetooth works

3.3.1 Network Topology

Any Bluetooth device can be a master or a slave, depending on the application scenario. Bluetooth employs frequency hopping spread spectrum (FHSS) to communicate. So in order for multiple Bluetooth devices to communicate, they must all synchronize to the same hopping sequence. The master sets the hopping sequence, and the slaves synchronize to the Master.

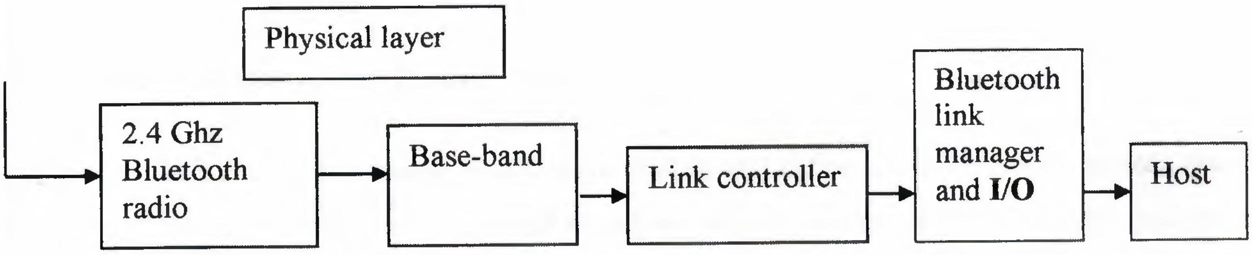

Figure 3.1 Functional Block of Bluetooth System

A scatter net can be formed by linking two or more piconets. When a device is present in more than one piconet, it must time-share and synchronize to the master of the piconet with which it is currently communicating. While the topology and hierarchical structure of WLAN networks are relatively simple, Bluetooth networks are far more diverse and dynamic. They are constantly being formed, modified, and dissolved, as Bluetooth devices move in and out of range of one another. And because different Bluetooth devices can represent many different usage profiles, there are many different ways in which Bluetooth devices can interact.

3.3.2 Service Discovery

The concept of service discovery is utilized to determine what kind of Bluetooth devices are present and what services they desire or offer. When a Bluetooth device requires a service, it begins a discovery process by sending out a query for other Bluetooth devices and the information needed to establish a connection with them. Once other Bluetooth devices are found and communication is established, the Service Discovery Protocol (SDP) is utilized to determine what services are supported and what kinds of connections should be made. In order for the above to happen, devices willing to connect must be located. Some devices may be set up so that they are invisible. In this case, they can scan for other Bluetooth devices, but will not respond if they are likewise queried. Applications determine whether a device is connectable or discoverable, and thus applications determine the topologies of networks and their internal hierarchies.

3.4 Bluetooth profiles

3.4.1 General Access Profile (GAP)

This profile is required by all usage models and defines how Bluetooth devices discover and connect to one another, as well as defines security protocols. All Bluetooth devices must conform to at least the GAP to ensure basic interoperability between devices.

3.4.2 Service Discovery Application Profile (SDAP)

The SDAP uses parts of the GAP to define the discovery of services for Bluetooth devices.

3.4.3 Serial Port Profile

This profile defines how to set up and connect virtual serial ports between two devices. This serial cable emulation can then be used for tasks such as data transfer and printing.

3.4.4 Generic Object Exchange Profile (GOEP)

GOEP is dependent on the Serial Port Profile and is used by applications to handle object exchanges. This capability is then used, in turn, by other profiles to perform such functions as Object Push, File Transfer, and Synchronization .

3.4.5 Object Push

This profile is used for the exchange of small objects, such as electronic calling cards.

3.4.6 File Transfer

This profile is used to transfer files between two Bluetooth devices.

3.4.7 Synchronization

This profile is used to synchronize calendars and address information between devices.

3.4.8 Power Levels and Range

Most Bluetooth devices, dependent on batteries for power, are designated as class 3 devices and are designed to operate at a power level of 0 dBm (1 mW), which provides a range of up to 10 m. Class 2 devices can utilize as much as 4 dBm (2.5 mW) output power, and class 1 devices can utilize up to 20 dBm (100 mW) of output power. Class 1 devices can have a range up to 100 m. Bluetooth class 2 and 3 devices can optionally implement adaptive power control. Required for class 1 devices, this mechanism allows a Bluetooth radio to reduce power to the minimum level required to maintain its link, thus saving power and reducing the potential for interfering with other nearby networks.

3.5 Protocol Architecture

Bluetooth is defined as a layered protocol architecture consisting of core protocols, cable replacement and telephony control protocols, and adopted protocols. The core protocols are as following:

3.5.1 Radio

Specifies details of the air interface, including frequency, the use of frequency hopping, modulation scheme, and transmit power.

3.5.2 Base-band

Concerned with connection establishment within a Pico net, addressing, packet format, timing, and power control.

3.5.3 Link manager protocol (LMP)

Responsible for link setup between Bluetooth devices and ongoing link management. This includes security aspects such as authentication and encryption, plus the control and negotiation of base-band packet sizes.

3.5.4 Logical link control and adaptation protocol (L2CAP)

Adapts upper-layer protocols to the base-band layer. L2CAP provides both connectionless and connection-oriented services.

3.5.5 Service discovery protocol (SDP)

Device information, services, and the characteristics of the services can be queried to enable the establishment of a connection between two or more Bluetooth devices. RFCOMM is the cable replacement protocol included in the Bluetooth specification. RFCOMM presents a virtual serial port that is designed to make replacement of cable technologies as transparent as possible. Serial ports are one of the most common types of communications interfaces used with computing and communications devices. Hence, RFCOMM enables the replacement of serial port cables with the minimum of modification of existing devices. RFCOMM provides for binary data transport and emulates EIA-232 control signals over the Bluetooth base-band layer. EIA-232 (formerly known as RS-232) is a widely used serial port interface standard.

3.6 The Evolving Bluetooth Standard

3.6.1 The Bluetooth SIG

Since the original Bluetooth specification was published in 1999, more than 2000 additional companies have signed on as associate members, able to participate in development of future standards and extensions by contributing efforts to various working groups.

3.6.2 The Current Specification

The current specification, Ver. 1.12, defines a radio which operates in the unregulated Industrial, Scientific, and Medical (ISM) band as 2.4 GHz, FHSS w/1600 hops/s over 79 channels: 1 Mbps

The fundamental elements of a Bluetooth product are defined in the two lowest protocol layers, the *radio layer* and the base-band layer. Included in these layers are hardware tasks such as frequency hopping control and clock synchronization, as well as packet assembly with associated FEC (Forward Error Correction) and ARQ (Automatic Repeat Request). The *link manager layer* is responsible for searching for other Bluetooth devices, creating and tearing down piconets, as well as authentication and encryption. Higher layer definitions include the Bluetooth profiles.

3.7 Bluetooth Communication

3.7.1 Connectivity

Bluetooth allows users to connect to a wide range of devices at one time without cables, and potentially without actively initiating the connection. For example, your PDA could automatically update a copy of your schedule stored on a desktop PC the minute you walked into your office. This connectivity is enabled by a tiny microchip incorporating a radio transceiver that is built into Bluetooth devices. This radio transceiver provides the advantage of being effective through obstacles. Thus, you could ostensibly use a Bluetooth connection to send data from a computer in one room to a printer in the next--right through the wall.

One concern when using such a system is privacy. As Bluetooth operates in the globally available 2.4 GHz frequency, it is conceivable that an unintended recipient could intercept a signal. To combat this, all Bluetooth devices are keyed for their own networks. The transmissions use a sophisticated encoding specification that not only guards against interference, it also ensures that only devices specifically programmed to receive a broadcast will be able to decode it.

Bluetooth uses a flexible, multiple piconet structure for communication. It supports both point-to-point and multipoint connections for full-duplex networks. Currently up to seven slave devices can be configured to use a master radio in one device. Several of the piconets can be established and linked in scatternets to allow flexibility among configurations. Devices in the same piconet have priority synchronizations, but other devices can enter the network at any time. In a full-duplex network, a multiple piconet structure with 10 fully loaded, independent piconets, can maintain aggregate data transfer speeds of up to 6 Mbps.

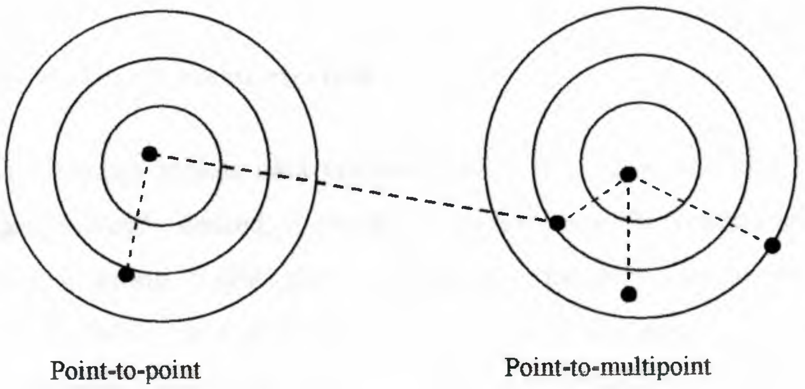

Figure 3.2 Bluetooth piconet communication structure

3.7.2 Class 1 and Class 2 Bluetooth

The major difference between the 2 classes of Bluetooth h adapter is communication range and power requirements. As a rule, you will typically trade power consumption for distance (though all Bluetooth devices typically have low power requirements relative to other types of computer add-in devices.) Class 2 Bluetooth devices have a communication range of 10 meters (30 feet), and Class 1 adapters provide a communication range of 100 meters (300 feet).

3.7.3 High and Low Power

The Bluetooth specification implements two power levels: a low power level designed for short distance communication such as within an office (Class 2), and a high power level that can accommodate a medium range, such as an entire building (Class 1). Additionally, Bluetooth limits power output to exactly what the device requires at any given time. For instance, when two devices connect and determine that they are close together, the transmitter immediately modifies its signal to the strength needed to accommodate that range. When traffic volume across a connection slows down, or stops completely, a receiving device will shift to a low power sleep mode that is intermittently interrupted for very short periods in order to maintain the network connection. With these power saving features, Bluetooth devices consume very small amounts of power, making them ideal for portable applications.

3.7.4 Bluetooth for Data Communication

Bluetooth technology makes data communication fast, easy, and convenient. As speeds and distances are currently limited, it should be viewed as a short-range solution for low to medium speed applications. It does provide remarkable flexibility, by communicating through walls and other obstacles, that makes it an ideal choice for home or office networks--for example sharing a printer among multiple PCs located in different rooms on the same floor. It also expands the functionality of a mobile phone, allowing it to serve as a modem for Internet connections, or allowing it to communicate with other devices--such as the prospect of using mobile phones to purchase drinks from vending machines.

3.8 Bluetooth Transmission Technologies

The dream for true, seamless, mobile data and voice communications that enables constant connectivity anywhere is quickly becoming a reality. Wireless and computer industries are clearly leading the way with revolutionary components that will shape our lives in the next century. In 1994, Ericsson Mobile Communications initiated a study to investigate the feasibility of a low power, low cost radio interface between mobile phones and their accessories. The aim of this study was to eliminate cables between mobile phones and PC Cards used to connect the phones to a computer for dial up networks (DUN). In 1998 Intel, IBM, Toshiba, Ericsson and Nokia began developing a technology that would allow users to easily connect to mobile devices without cables. This technological vision became a reality through the synergy of market leaders in laptop computing, telecommunications, and core digital signal processing. May 20th, 1998 marked the formation of the Bluetooth Special Interest Group (SIG) with the goal to design a royalty free, open specification, de facto, short range, low power wireless communication standard, as well as a specification for small-form factor, low-cost, short range radio links between mobile PCs, mobile phones and other portable devices codenamed Bluetooth. The result was an open specification for a technology to enable short-range wireless voice and data communications anywhere in the world. A simple 8 way to connect and communicate without wires or cables between electronic devices including computers, PDA's, cell-phones, network access and peripherals. Bluetooth is named after Herald Blatant, “Bluetooth”, a Viking 10th century king. Herald had a penchant for surrounding himself with the right group of people, which enabled him to strategically secure new lands for Viking settlements. Herald conquered all of Denmark and Norway and made the Danes Christian. Thus Herald's conquest inspired the name of a global wireless specification achieved through the cooperation of many leading companies within the computer and telecommunications industries. The technology operates in a globally available frequency band ensuring communication compatibility worldwide. One of the primary advantages of the Bluetooth system is ease of computer

vendor product integration. Other key benefits of this technology are low power, long battery life, low cost, low complexity, and wireless connectivity for personal space, peer-to-peer, cable replacement, and seamless and ubiquitous connectivity. To achieve the Bluetooth goal, tiny, inexpensive, short-range transceivers are integrated into devices either directly or through an adapter device such as a PC Card. Add on devices such as a USB or Parallel port connections are also available for legacy systems. By establishing links in a more convenient manner this technology will add tremendous benefits to the ease of sharing data between devices.

3.9 Bluetooth application

Bluetooth is designed to operate in an environment of many users. Up to eight devices can communicate in a small network called a piconet. Ten of these piconets can coexist in the same coverage range of the Bluetooth radio. To provide security, each link is encoded and protected against eavesdropping and interference. Bluetooth provides support for three general application areas using short-range wireless connectivity:

3.9.1 Data and voice access point

Bluetooth facilitates real-time voice and data transmissions by providing effortless wireless connection of portable and stationary communications devices.

3.9.2 Cable replacement

Bluetooth eliminates the need for numerous, often proprietary cable attachments for connection of practically any kind of communications device. Connections are instant and are maintained even when devices are not within line of sight. The range of each radio is approximately 10 m, but can be extended to 100 m with an optional amplifier.

3.9.3 Ad hoc networking

A device equipped with a Bluetooth radio can establish instant connection to another Bluetooth radio as soon as it comes into range.

3.10 Bluetooth Security

Bluetooth security, when compared with WLAN security, is both more complex and simpler. It is more complex in the sense that there are many different options for security based on different application scenarios. It is simpler in the sense that, for the most part, they are transparent to the user. With WLANs it is up to the network administrator to add security at higher levels. With Bluetooth, since the Bluetooth spec includes all levels, higher-level security features are already built into the devices when appropriate. Bluetooth security includes both authentication and confidentiality, and is based around the SAFER+ encryption algorithm. SAFER+ is a block cipher, but in this application is implemented as a stream cipher. SAFER+ was thoroughly analyzed and tested during the NIST's search for a national encryption standard. Although some versions were found to have very minor weaknesses, the 128-bit version as used in Bluetooth is considered very strong.

3.10.1 Link layer security – keys and more keys

The Bluetooth Base-band (link layer) specification defines methods for both authentications and encryption that are subsequently utilized by higher layers. These methods utilize a number of keys generated by a process that begins with three basic device entities: a public 48-bit device address, a random number generator, and a secret PIN which is either built into the unit by the manufacturer or programmed by the user. A typical PIN may consist of just four decimal digits. However, for applications requiring more security a PIN code up to 128-bits long can be entered.

The first of many keys is created the first time the Bluetooth device is installed on the host and is typically never changed. This is referred to as the unit key.

3.10.2 Authentication

When a Bluetooth session (defined as the time interval for which the device is part of a piconet) is initiated, a series of additional keys is generated. One of these keys, referred to as the link key or authentication key, is a one-time 128-bit secret key that is used only

during that session. The process of authentication employs the encryption of a random number by each device to verify that each is sharing the same secret link key.

3.10.3 Encryption

If encryption is required by the application, an encryption key is further derived from the link key, a ciphering offset number, and a random number. While the authentication key is always 128-bits, the encryption key may be shorter to accommodate government restrictions on encryption, which vary from country to country. A new encryption key is generated each time the device enters encryption mode. The authentication key, however, is used during the entire session.

3.10.4 Application layer security

The Bluetooth General Access Profile defines three security modes: Mode 1 is non-secure. Authentication is optional. Mode 2 gives service-level enforced security. The service provided by the application decides whether or not authentication or encryption is required. The Bluetooth SIG has published the Bluetooth Security Architecture white papers that defines a suitable architecture for implementing service-level enforced security on Bluetooth devices.

The white paper splits devices into different categories and trust levels, as well as suggesting three security levels for services. The utilization of a database is suggested for enabling the user to authorize devices to utilize only particular services. Because the implementation of security at this level does not affect interoperability, this white paper is advisory only, and is not part of the Bluetooth specification. Mode 3 is link-level enforced security. Both devices must implement security procedures in order for a connection to be established. In addition to the above modes, a device can be configured to not respond to paging, so that other devices cannot connect to it. Or it can be configured so that only devices that already know its address can connect to it. Such numerous and complex levels of security are necessary to accommodate the large variety of different usage scenarios. It falls on the designers of Bluetooth products to ensure that the complexity of Bluetooth is hidden from the user, while still providing the user with necessary security options.

3.12 Summary

Bluetooth wireless technology is conceived as a low-power short range radio technology designed to replace cables for interconnecting devices such as printers, keyboards, and mice, its perceived potential has evolved into far more sophisticated usage models. The requirement to do this in a totally automated, seamless, and user-friendly fashion, without adding appreciable cost, weight, or power drain to the associated host is an enormous engineering challenge. Bluetooth devices can form piconets of up to seven slaves and one master, enabling discovery of services and subsequent implementation of many varied usage models including wireless headsets, Internet bridges, and wireless operations such as file exchange, data synchronization, and printing. Despite talk of Bluetooth competing with wireless LANs, Bluetooth products work over shorter distances and are designed to solve different problems.

4. WIRELESS EAR

4.1 Overview

We know that from third chapter that Bluetooth is a short distance wireless technology for connecting devices, so handset Bluetooth is made to allow the users to obtain their calls. Those who wear hearing instruments have had difficulties with various kinds of electronic devices, especially the telephone. As the list of electronics grows, so does our desire to enable connections to those devices, especially since many of them are critical for providing both entertainment and information to the hearing impaired. Now, Bluetooth technology extends new possibilities for solving the problems of the past and expanding options for the future. And this chapter explains how that calls obtained

4.2 The promise of Bluetooth

Bluetooth technology represents a revolutionary development in wireless communication across devices in the digital world. Bluetooth is a short-range, wireless, digital communication standard. Bluetooth-compatible devices can carry either audio signals or data from one device to another in a secure, point-to-point, digital link that is highly resistant to most sources of interference. It is found in a growing list of electronics, including digital mobile phones, computers, personal digital assistants (PDAs), printers, fax machines, audio equipment and more. The elimination of wires, cables, connectors and plugs usually needed to connect electronics is Bluetooth's most visible advantage. The world's most accepted wireless communication protocol, Bluetooth sends a clear, clean, digital signal. For the audio concerns of the hearing industry, this means that the signal is not subject to the same sources of degradation that sometimes compromise the quality of analog (FM, AM or inductive) transmissions. In an analog signal path, electrical noise from a variety of sources is amplified along with the signal. However, the Bluetooth signal is extracted from the noise; it is therefore the only sound to be transmitted and ampli- fied. The low-power design of Bluetooth transmission systems has two advantages. First, it minimizes battery consumption for portable devices. Second, it places an intentional limit on the range of transmission (10 meters), which helps avoid interference among nearby devices. In addition, walls and other obstacles have little effect on Bluetooth transmission. Bluetooth-compatible devices are typically categorized as either a "master" or a "slave." As the names imply, the master is responsible for setting up and controlling the communication between the two devices. The slave simply does what it is told, receiving incoming signals and sending responses back to the master. is turned off or moves outside its usable range.

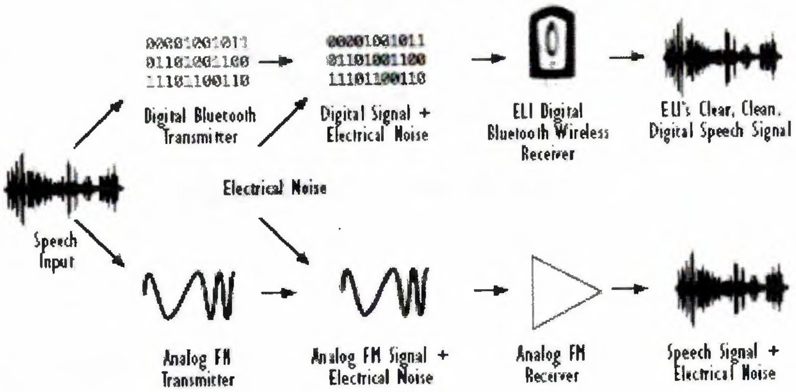
00001001011
01101001100
11101100110
Digital Bluetooth Transmitter
00001001011
01101001100
11101100110
Digital Signal + Electrical Noise
ELI Digital Bluetooth Wireless Receiver
ELI's Clear, Clean, Digital Speech Signal
Speech Input
Electrical Noise
Analog FM Transmitter
Analog FM Signal + Electrical Noise
Analog FM Receiver
Speech Signal + Electrical Noise

Figure 4.1 transmission media of Bluetooth

4.3 The operation

When the device is powered up, the program stored in the DSPEVM flash memory is loaded and executed, generating the desired signal. The signal passes through the amplifying circuit, amplified and shifted to the proper voltage values.

Then is sent to the host interface of the EBSK. The EBSK executes the set of commands contained in the signal, which sets the Bluetooth chip to a 'slave' mode, waiting for a connection request of a 'master' device.

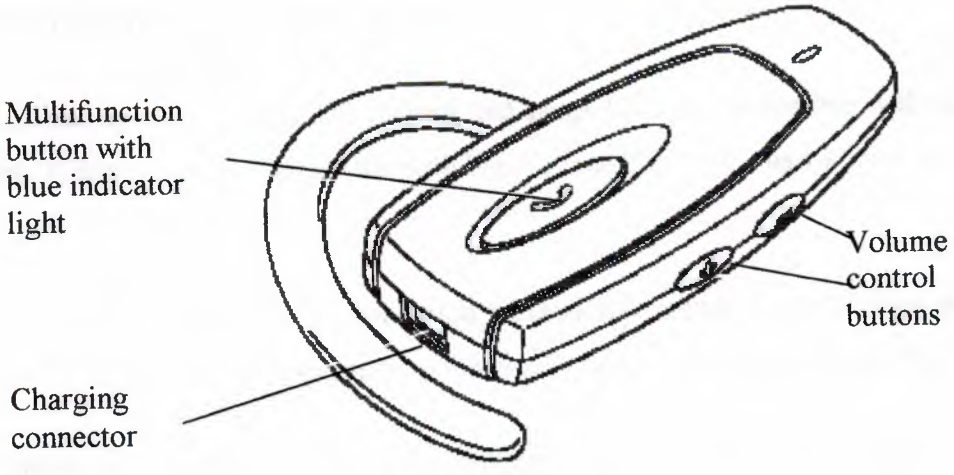

Figure 4.2 Bluetooth ear device

4.4 Headset Profile

4.4.1 Defines 2 Roles

1. Audio Gateway (AG) -Device that is the gateway for the audio channel.

2. Headset (HS) -Device acting as remote mechanism.

4.4.2 Constraints

1. The profile mandates the usage of CVSD for transmission of audio.
2. Between headset and audio gateway, only one audio connection at a time is supported.
3. The audio gateway controls the SCO link establishment and release.
4. The profile offers only basic interoperability for example, handling of multiple calls at the audio gateway is not included.
5. The only assumption on the headset's user interface is the possibility to detect a user initiated action .

4.5 Pairing with Bluetooth phone

Headset comes with an AC charger and plugs that are compatible with international outlets. Using the same charger for both headset and Trio 650 smart phone, so no need to carry two chargers.

Pairing creates a unique and encrypted wireless link between two devices enabled with Bluetooth wireless technology, such as Bluetooth phone and Bluetooth headset.

Headset is compatible with most Bluetooth phones that are compliant with the Bluetooth version 1.1 or 1.2 specification.

4.6 Choosing wearing performance

When turning the headset on or else it may begin the pairing process, and the blue indicator light will turn solid. If that happens, turn off the headset, wait 3 to 5 seconds, and then repeat the process for turning the headset on. the Bluetooth functionality on phone turned on in order to use phone with headset.

The headset ear grip is placed over the front of the ear. The headset must be ready to wear on the right ear, but adjust the ear grip to hang from the left ear. Follow the same procedure to switch the wearing preference from the left ear to right ear.

For optimal performance, wear headset and Bluetooth phone on the same side of body as shown in figure 4.2. In general, the user will get better performance when there are no obstructions (including parts of body) between the headset and the phone.

Figure 4.3 optimal performance

4.7 Summary

The work in the problem of helping hearing-impaired people to use telephones. There are two aspects, a wireless assistive phone adapter was designed based on the Bluetooth technology; a bandwidth-extension algorithm was developed to recover the high-frequency information of telephone speech.

The proposed phone adapter routes the telephone audio signal to the hearing aid or the CI processor through the Bluetooth wireless connection. Hence environmental noise and interference are disabled and the user can enjoy high quality speech. The adapter also provides users more mobility, as they are not confined by any cables.

5. EFFECT OF BLUETOOTH

5.1 Overview

The strongest signals emit from devices that contain radio transmitters or high-voltage, such as wireless telephones, microwave ovens and TV/PC screens. Lamps and fluorescent tubes also emit more radiation than what is commonly assumed.

Radiation from mobile phones is of the same frequency as microwave ovens and wireless phones. The radiation from a mobile phone in use will be just as modest as the radiation emitting from these devices. Also bluetooth affect the human becouse its relation with the mobile phone and this chapter will show how this effects during use of bluetooth.

5.2 The radiowaves effects

As with many new technologies, concerns have arisen about the effects on health from using a mobile telephone. Part of the radio waves emitted by a mobile telephone are absorbed by the human head; the radio waves emitted by a GSM-900 handset can have a power of up to 2 watts. The rate at which radiation is absorbed by the human body is measured by the Specific Absorption Rate (SAR), and its maximum levels for modern handsets have been set by governmental regulating bodies in many countries. Since the microwave spectrum is non-ionizing electromagnetic fields (EMF), according to the scientific consensus, the only effect on the human body is that the temperature of the head may increase by a harmless fraction of a degree during prolonged calling, actually several orders of magnitude less than that obtained during the exposure of head to direct sunlight for a time. The thick skull bones are a respectable heat shield developed by evolution, and the brain's blood circulation easily disposes of excess heat by instantaneously increasing local blood flow. However, some controversial studies claim that there exist other undesired effects on health as a direct result of the radiation. It has been claimed, for example, that some parts of the human head are more sensitive to damage due to increases in temperature, particularly in anatomical structures with poor vasculature, such as nerve fibers. More recent results from a Swedish scientific team have revealed that continous use of a mobile phone for a decade or longer can lead to a small increase in the probability of getting a certain type of brain tumor (acoustic neurinoma).

Another area of worry about effects on the population's health have been the radiation emitted by radio-base stations, because, in contrast to mobile handsets, it is emitted continuosly. Many measurements and experiments have shown, however, that radiation levels are low (particularly in modern antennas, in the range of 20 to 100 watts) and decay sharply with distance from the tower (with the square of distance). Thus, if international norms of safety are respected (in relation to minimal distance to human habitations and direction and intensity of field), there is no cause for additional precautions. Governmental authorities usually pass legislation which regulates the application of these norms.

the effects of electromagnetical fields on human health which periodically examines the scientific evidence on these aspects. So far (the next report is scheduled for 2006-2007) it has concluded that there are no demonstrable effects of EMF used in mobile phones and wireless telecommunication systems on human health, and the single great health risk is using mobile phones while driving .

5.3 Effect of Bluetooth on the Health

Bluetooth uses frequency spectrum in the range of 2400MHz to 2483.5MHz. This range encompasses the natural frequency of H2O molecular oscillation at 2450MHz, which is also used by microwave ovens specifically to excite water molecules inside food in order to cook it. Sharing the same frequency range as microwave ovens has led to some concerns that Bluetooth devices might *cook* their users. Some microwave radiation will be absorbed in flesh. It will be absorbed by field-induced rotation of polarized water molecules, which is converted to heat through molecular friction, basically, the microwaves shake the water in flesh, and it heats up as it shakes. But, as the radiated output power of Bluetooth devices is incredibly low and spread in spectrum in time, experts concur that Bluetooth radiation does not pose a risk to health. A 1mW Bluetooth radio emits 1/1000,000, the amount of power in a 1KW microwave oven. Also, in a microwave oven, all the power is directed inward at the food, whereas in a Bluetooth device, the power is radiated outward, so the user only ever intercepts the smallest fraction of the radio waves which are heading in their direction.

It is interesting to compare Bluetooth devices with other popular communications devices. Bluetooth operates at 2.4GHz and uses 1mW (0dBm) for most applications, with a maximum of 100mW (20dBm) for extended range. This means that Bluetooth signals have a penetration depth of only 1.5cm into flesh. In comparison, cellular handsets have a power of 10mW to

2W peak, using 450MHz to 2200MHz, and exhibit a penetration depth of 2.5cm in the middle of their range at 900MHz. So, mobile cellular handsets give rise to a measurable heating effect of 0.1°C, compared with no measurable increase for Bluetooth devices. Although studies have shown this small heating effect, it is too low to be noticed by the user. Most of the temperature increases that mobile phone users feel when holding a handset next to their ears is caused by an insulating effect. Since the head radiates a lot of heat, if a handset blocks that radiation, then the head heats up. Getting a hot ear from a mobile phone is not necessarily a sign that you are absorbing radiation!

There has already been some controversy regarding cellular handsets and whether they have a negative impact on health. Although scientific opinion is pretty conclusive that there are no risks, to be safe, various organizations have undertaken studies and research and have laid down guidelines for exposure to radio frequencies.

The WHO, ICNIRP, and IEEE have developed Radio Frequency (RF) exposure recommendations and these guidelines have been adopted by many national authorities. In the usual way of health and safety guidelines, they incorporate large safety margins. The guidelines specify near-field1 restrictions (referred to as SAR) between 10MHz, to 10GHz, which devices with an output power of less than 1.6mW are incapable of exceeding. So, all low-power Bluetooth devices will fall within these restrictions. Higher power Bluetooth devices may need to be tested for SAR limits, and this will be done as part of radio regulatory testing. The guidelines also specify a standard for total RF exposure. This is given as a power density of 10W/m2. This level of spectral density would require an unrealistic number of Bluetooth devices to operate continuously in a very small space, which would actually not be possible due to the limited spectrum in the ISM band.

Several expert panels formed from organizations such as WHO, ICNIRP, EC, and the Royal Society of Canada have debated the topic of health in the context of existing higher power cellular technology in recent years. They have all concluded that there is no credible or convincing evidence that RF exposure from wireless devices operating within accepted exposure limits causes adverse human health effects. They did, however, recommend additional research to clarify some areas and fill gaps in existing knowledge.

experts agree that Bluetooth devices are too low in power to have any negative health consequences, being as they are even for the higher power devices an order of magnitude lower in power than existing cellular devices which based on existing research and official guidelines have already been proven to be safe.

5.4 Bluetooth Dangerous Waves

Radiation from a headset is real, but far lower than even that from a cell phone, which is pretty low to begin with, Both wireless phones and Bluetooth devices emit nonionizing radiation, typically at frequencies from 1 to 2.5 gigahertz. The data on health hazards from wireless phone radiation are equivocal, with some studies showing a measure of risk and some showing no problems.

But because it's a good idea to err on the side of caution in such matters, regulatory bodies have set exposure standards. These are expressed in terms of the "specific absorption rate" (SAR), which attempts to measure the radiation actually reaching body tissue. The U.S. and Canadian governments have set a maximum SAR of 1.6 watts per kilogram, while the European Union permits a slightly higher level Bluetooth radios operate at much lower power levels than phones so, not surprisingly, the radiation added by a Bluetooth headset is insignificant by comparison. A study by William G. Scanlon of Queen's University in Belfast found that a typical Ericsson (ERICY) Bluetooth radio module generates an SAR of just 0.001 watts per kilogram. So, if you're worried about the health impact of radio waves, remember that the phone itself is a much greater source of concern than a Bluetooth headset. That's especially true because, when you're using Bluetooth, the BlackBerry is likely positioned much farther from your body -- and especially your brain -- than when holding the phone up to your ear

5.5 Precautionary Principle

Although scientific evidence for health hazards of low level cellphone radiation is weak, the World Health Organization has recommended that the precautionary principle could be voluntarily adopted in this case .It follows the recommendations. for environmental risks. According to the WHO, the Precautionary Principle is a risk management policy applied in circumstances with a high degree of scientific uncertainty, reflecting the need to take action for a potentially serious risk without awaiting the results of scientific research." Other less stringent recommended approaches are Prudent Avoidance Principle and ALARA (As Low as Reasonably Achievable). Although all of these are problematic in application, due to the widespread use and economical importance of wireless telecommunication systems in modern civilization, there is an increased popularity of such measures in the general public. They involve recommendations such as the minimization of cellphone usage, the limitation of use by at-risk population (such as children), the adoption of cellphones and microcells with ALARA levels of radiation, the wider use of hands-off and earphone technologies such as Bluetooth headsets, the adoption of maximal standards of exposure, RF field intensity and distance of base stations antennas from human habitations, and so forth.

5.6 SUMMARY

That there are no risks, to be safe, various organizations have undertaken studies and research and have laid down guidelines for exposure to radio frequencies.

The WHO, ICNIRP, and IEEE have developed Radio Frequency (RF) exposure recommendations and these guidelines have been adopted by many national authorities. In the usual way of health and safety guidelines, they incorporate large safety margins. The guidelines specify near-field1 restrictions (referred to as SAR) between 10MHz, to 10GHz, which devices with an output power of less than 1.6mW are incapable of exceeding. So, all low-power Bluetooth devices will fall within these restrictions. Higher power

Bluetooth devices may need to be tested for SAR limits, and this will be done as part of radio regulatory testing. The guidelines also specify a standard for total RF exposure. This is given as a power density of 10W/m2. This level of spectral density would require an unrealistic number of Bluetooth devices to operate continuously in a very small space, which would actually not be possible due to the limited spectrum in the ISM band.

Several expert panels formed from organizations such as WHO, ICNIRP, EC, and the Royal Society of Canada have debated the topic of health in the context of existing higher power cellular technology in recent years. They have all concluded that there is no credible or convincing evidence that RF exposure from wireless devices operating within accepted exposure limits causes adverse human health effects. They did, however, recommend additional research to clarify some areas and fill gaps in existing knowledge.

Experts agree that Bluetooth devices are too low in power to have any negative health consequences, being as they are even for the higher power devices an order of magnitude lower in power than existing cellular devices which based on existing research and official guidelines have already been proven to be safe.

6. CONCLUSION

The Bluetooth core promoters group has produced a specification for short-range, low cost wireless communications. This is the Bluetooth core specification. The complete Bluetooth specification also includes profiles which detail how applications should use the Bluetooth protocol stack, and a brand book which covers how the Bluetooth brand should be presented. The Bluetooth specification not only covers how to set up short-range wireless links, but also describes the Bluetooth qualification process. By putting their products through this process, companies that join the Bluetooth SIG can get a free license to use the Bluetooth wireless technology and Bluetooth brand.

Bluetooth wireless technology allows up to eight devices to connect together in a communicating group called a piconet. The maximum speed of a link in a piconet is 723.2 kb/s at the base-band layer (the data rate seen at the Application Layer will be lower due to the intervening layers of the protocol stack using some of the bandwidth). Different piconets can be linked into scatternets, but the data rate between scatternets will frequencies (LSF).

Mobile telecommunication has developed considerably in recent years: to date over half the population of the Netherlands posses a mobile telephone. Nevertheless, concerns also grow, particularly as to whether exposure to electromagnetic fields from antennas and mobile telephones can adversely affect health. In this advisory report, the Electromagnetic Fields Committee of the Health Council of the Netherlands provides, on the basis of the scientific literature, an overview of various aspects that may play a role. The Committee comes to the conclusion that there is at present no reason for concern. However, since mobile telephony leads to widespread electromagnetic field exposure and relatively little knowledge exists on, especially, long-term effects, it indicates areas for further research. In particular, the Committee indicates in what areas research can be conducted in the Netherlands.

Bluetooth wireless technology is finally here. Originally conceived as a low-power short-range radio technology designed to replace cables for interconnecting devices such as printers, keyboards, and mice, its perceived potential has evolved into far more sophisticated usage models. The requirement to do this in a totally automated, seamless, and user-friendly fashion, without adding appreciable cost, weight, or power drain to the associated host is an enormous engineering challenge.

Bluetooth devices can form piconets of up to seven slaves and one master, enabling discovery of services and subsequent implementation of many varied usage models including wireless headsets, Internet bridges, and wireless operations such as file exchange, data synchronization, and printing.

Despite talk of Bluetooth competing with wireless LANs, Bluetooth products work over shorter distances and are designed to solve different problems.

The Bluetooth SIG publishes the Bluetooth specification. The IEEE has formed the 802.15 working group to define standards for wireless PANs. The 802.15.1 standard for WPAN will be modeled after the Bluetooth specification from the Bluetooth SIG. The waters of Bluetooth security have yet to be tested. However, the Bluetooth specification has a robust key management scheme built in, as well as upper layers of security. Bluetooth uses the national standard AES algorithm for encryption and the general consensus is that the options for Bluetooth security are strong and robust.

With myriad applications for Bluetooth technology, its ultimate usefulness lies in its ability to allow these electronic devices to interconnect. For example, it will allow the control of any device using a mobile telephone. On arrival for a conference at a hotel, one could be guided via a mobile phone to the correct conference room. The hotel's guest system would recognize the attendee's mobile phone number and guide the attendee accordingly.

Bluetooth technology provides tremendous flexibility because it has the potential to allow all electronic devices to be interconnected. Indeed, mobile telephones that incorporate Bluetooth technology provide a fruitful source of potential applications. Today when visitors walk into an office building, their presence is announced by a receptionist. Using Bluetooth, a mobile telephone could do this automatically with a message on a monitor announcing the visitor no need for human intervention. Of course this could also work the other way around. If someone didn't want to see the visitor, he or she could become unavailable.

Another possibility introduced by Bluetooth technology is the ability to subdivide components of electronic equipment. For example, a manufacturer could build a mobile telephone with a remote earpiece. The earpiece could communicate to the telephone network via the telephone base using a Bluetooth radio link.

One of the best-publicized effects of Bluetooth will be the aesthetic effects: namely the removal of cables in offices and homes. Bluetooth technology replaces the need for such cabling. Bluetooth can also be combined with other technologies. It can be used in conjunction with triangulation technology, which determines the precise location of a mobile phone. In a building, such technology could be used to track the whereabouts of visitors. Alternatively, a Bluetooth device could be built into children's clothing so that if a child wandered away, the Bluetooth transmitter would signal a warning.

REFERNCE

1. Y. M. Cheng, D. O'Shaughnessy and P. Mermelstein, “Statistical recovery of wideband speech from narrowband speech,” *IEEE Transactions on Speech and Audio Processing*, vol. 2, issue 4, pp. 544-548, Oct. 1994.

2. S. Chennoukh, A. Gerrits, G. Miet and R. Sluijter, “Speech enhancement via frequency bandwidth extension using line spectral frequencies,” *Proc. of IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, vol.1, pp. 665-668, 2001.

3.Dervis Z. Deniz, “ISDN *and Its Applications to LAN Interconnection*”, Mc-Graw Hill, 1994, ISBN: 0-07-707883-7.