NEAR EAST UVIVERSITY

Faculty of Engineering

Department of Electrical and Electronics Engineering

BLUETOOTH CELL PLANNING

Graduation Project
EE- 400

Student: Marwan Habib Shraideh (20032938)

Supervisor: Mr.Jamal Abu-Hasna

Nicosia-2008

ACKNOWLEDGEMENT

First of all, I would like to thanks Allah {God} for guiding me through my study.

I feel proud to pay my special regards to my project advisor "Dr. Jamal abu-Husna ". He gave me too much information and did his best of efforts to make me able to complete my project.

More over I want to pay special regards to my family. They encouraged me in crises. I shall never forget their sacrifices for my education so i can start my successful life and enjoy it as they are expecting. I am nothing without their prayers.

I want to honor all those persons who have supported and helped me in my project and send to them the best of regards and acknowledge. Also my special thanks to all my friends who gave me their precious time to complete my project. Also my especial thanks go to my friends, Wael Bamedhaf, Ahmed Bamedhaf, Mahmoud Mazin, Omer Touqan, Rami Zeedat, Abedalazeez Al-Natsheh, Mohammad Sabri, all the other friends.

At the end I am thankful to all persons who helped and encouraged me to complete my project, and complete the first step of my future life.

TABLE OF CONTENTS

ABSTRACT

Our aim in this project is to describe the construction of Bluetooth, which is the most elementary form, is defined as a global specification for wireless connectivity.
Because it is intended to replace cables, cost must be low and operation must be intuitive and robust. These requirements for Bluetootlı create many challenges. Bluetooth meets these challenges by several means.

The radio unit employs frequency hopping spread spectrum (FHSS), and the design emphasis is on very low power, extremely low cost, and robust operation in the uncoordinated, interference-dominated RF environment of the industrial, scientific, and medical (ISM) radio band.

A wide variety of Bluetooth radio block diagrams are in use. For transmission, these range from direct voltage controlled oscillator (VCO) modulation to IQ mixing at the final radio frequency (RF.) in the receiver, a conventional frequency discriminator or IQ down-conversion combined with analog-to-digital conversion is noted.

While many options can satisfy the Bluetooth radio specifications, each will have its own characteristics if not operating correctly. The Bluetooth system consists of a radio unit, a baseband link control unit, and link management software. lt also includes higher-level software utilities that focus on interoperability features and functionality.

INTRODUCTION

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™s will be modeled after the Bluetooth specification from the Bluetooth SIG. Microsoft® has announced support for Bluetooth in the next release of Windows® XP.

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.

1. INTRODUCING BLUETOOTH

1.1 Introduction

Bluetooth is a technology that promises to eliminate most of the cables that connect your various personal computing devices-and to create new types of smart_ wireless communications.

This project is your guide to Bluetooth, throughout the rest of this project you'll learn all sorts of details about Bluetooth-what it is, what it does, how it does it, and how you'll use it. Before we get to those details, however, this chapter provides you with a general overview of the Bluetooth technology. So even if you've never heard of Bluetooth before, you'll find out what all the fuss is about-and discover how and why you'll soon be using Bluetooth technology in your daily life.

1.2 Visions of a Wireless World

The computing, communications, and consumer electronics industries have introduced many benefits to today's consumers. Of course, they've also introduced many headaches, not the least of which is the necessity of connecting all these devices to each other, usually with a phalanx of cables and wires that are both annoyingly messy and mind-numbingly confusing.

Wouldn't it be great if you could connect your printer to your PC-or your PC to your PDA or your PDA to your phone line-without fumbling with the necessary cabling and worrying about whether you're using the right type of connector?
If you'd like to nix all that messy cabling, Bluetooth is for you. Bluetooth technology enables wireless connections between any number of computing, communications, and consumer electronics devices-and promises much more than that, including "smart" device recognition and synchronization.

At its most basic, Bluetooth technology will usher in a world of wireless connections. Using short-range radio wave transmissions, Bluetooth technology will enable all your different electronic devices to connect to each other-without wires.

1.3 Cable less Computing

Consider the common chore of hooking up a printer to your personal computer. Today you have to buy a big, thick, ungainly cable with multi-pin connectors on either end, plug the cable into the proper ports on the back of both your PC and your printer, and go through a complex setup procedure to make sure your PC recognizes the printer. Even when everything goes right-and it often doesn't!-the process is a pain in the rear, especially if you want to put your printer in a place that is either awkward to get to or far enough away from your PC that the standard cables won't quite reach.

Now imagine that same task in a Bluetooth-enabled world. In this world, your printer sends and receives data to and from your PC via a wireless connection, so you don't have to mess with that bulky computer cable. That means that you can place your printer anywhere you want-even clear across the room!-because you're not limited by the constraints imposed by cable connections. Plus, since Bluetooth is a technology that automatically recognizes all active devices in the vicinity, the process of configuring your computer for your specific printer will become much easier-in many cases, totally automatic.

If the thought of hooking up your printer without a cable sounds appealing, think of all the other devices you currently have plugged into your PC. If you're like many computer users, you have at least a half-dozen different items wired to your system unit, including your keyboard, mouse, joystick, speakers (two or more, most likely), microphone, personal digital assistant, scanner, digital still camera, PC/Web camera, video camera, and, of course, your printer. In addition, you can't forget the connection between your PC's modem and the nearest phone jack, or the network connection that is required of any PC connected to a local area network. Today, every one of these connections is made with a cable; with Bluetooth technology, almost all of these connections can be wireless.
Think of how cluttered the back of your computer (and the back of your desk!) looks today, and then try to envision the same setup, but without cables. That is how things will look when Bluetooth technology invades your desktop.

1.4 Automatic Synchronization

Bluetooth is more than just a cable-replacement technology, however. It's also a technology that enables any electronic device to communicate with any other electronic device, automatically. This means that, over short distances (30 feet or so), your cell phone or personal digital assistant (PDA) can connect to synchronize with, and even control the other electronic devices in your home or office-such as your personal computer, printer, television set, home alarm system, or home/office telephone system. All of this communication can take place in an ad hoc fashion, without your being aware, totally automatically.

Consider this scenario. You have a PDA that contains your contact list and daily schedule.

You need to synchronize the data on your PDA with similar data on your desktop computer.

Today, you do this by connecting your PDA to your computer, typically via a serial cable. (Another cable)

Once the proper connections are made, you have to manually synchronize the data between the two devices. And you have to go through this rigmarole every time you make a new appointment or add a new contact.

Now imagine the same scenario, but using Bluetooth technology. As soon as you walk into your office, your Bluetooth-enabled personal computer senses the presence of your Bluetooth enabled PDA, and sends out a signal asking, in effect, what new data has been added to the PDA. Without your pressing a button-or even being aware that any exchange is going on- your two devices synch up with each other, ensuring that your database of information is current on both machines. No fuss, no muss-and, once again, no cables. Just automatic "smart" communication enabled by Bluetooth technology.

1.5 An All-In-One Phone

Another application of Bluetooth technology is in the world of telecommunications. If you're like most high-tech consumers, you're currently juggling several different phones, and several different phone numbers. You probably have a cordless phone at home and a more complex phone system in the office. You also have a mobile phone to use on the go, and you might even have a fourth phone in your car. Plus, depending on your situation, you could have a fifth telecommunications device in your possession-an alphanumeric pager. All of these phones are separate devices, and all have their own individual phone numbers.

How much more confusing can you get?

In a Bluetooth world, things will be much simpler. For one thing, you'll only have one telephone handset, and you'll carry it with you at all times. When you're at home, it will connect (via Bluetooth technology) to your normal telephone line. When you're at work, it will connect to your office phone system. When you're on the go, it will function as a cellular phone. And when you're in the car, it will connect (wirelessly, of course) to your car's built-in hands-free phone system. It will even, if you choose, function as an alphanumeric pager-as well as an e-mail retrieval device and a miniature Web browser. You'll choose which phone numbers to use, and where; if you want, a single phone number will travel with you, no matter where you go.

One phone, one number-how much simpler can you get?

Knowing that Bluetooth enables smart, totally ad hoc wireless communications between different electronic devices, one doesn't have to think hard to imagine other uses of this technology. For example, imagine

• A PDA that controls a desktop computer used to display a PowerPoint-based presentation-and that you can also use to record meeting minutes and then "beam" those notes to other attendees at the end of the meeting.

• A single device that turns your home security system on and off, locks and unlocks your front door, operates your automatic garage door, and monitors and controls your home's heating and air conditioning systems.

• A portable device that can be used by factory supervisors to check the status of inventory or equipment-and then automatically send that data to a master computer.

• A PDA or mobile phone that also functions as a digital "wallet" for payment at stores and restaurants-and that downloads and stores movie tickets, car park tickets, and other important information.

• A portable device that stores your plane, hotel, and rental car reservations-and can be programmed on the fly to function as a digital key to your hotel room.

• An in-car device that communicates with other Bluetooth devices along your route to provide driving directions and sight-seeing information-in addition to functioning as a digital car key that contains your personal settings for your car radio, air conditioner, and seat adjustments.

• A mobile phone or PDA that stores all your personal contact information-and can send that data, automatically, to people with similar devices at trade shows, in meetings, or at your local bar.

• Bluetooth-compatible electronic components-CD players, DVD players, VCRs, audio/video receivers, speakers, and the like-that can combine to create a totally wireless home theater system.

• A Bluetooth-enabled controller in theaters and other public venues that can automatically tum off the ringers on all mobile phones in the audience when the movie or performance starts.

Would you be interested in any of these potential uses of the Bluetooth technology? Hundreds and hundreds of companies are betting so, and have invested billions of dollars in the technology that can enable these and other applications.

1.6 How Bluetooth Technology Works

Bluetooth is a global technology standard that attempts to bridge the computer and communications industries. It has been adopted by all the major players in the telecom and computer worlds, as well as an interesting cross-section of companies in other industries-including the home entertainment, automotive, health care, industrial automation, and toy industries. (Yes, that's right-Bluetooth technology can be used in children's toys!)

While there is lots of pie-in-the-sky ideas floating around that may or may not materialize, at the very minimum, the Bluetooth standard promises to do the following:

• Eliminate wires and cables between both stationary and mobile devices over short (30 foot) distances.

• Facilitate both data and voice communication.

• Enable ad hoc networks and provide automatic synchronization between multiple Bluetooth devices.

Put simply, Bluetooth technology enables short-range wireless communication-both data and voice-between all sorts of electronic devices. This communication takes place without the explicit manual intervention of the user; whenever one Bluetooth-enabled device detects another Bluetooth-enabled device, the two devices automatically synch up and a type of ad hoc wireless network is created.

1.7 Radios Waves and Piconets

Bluetooth does all this by embedding a small, low-powered radio-on-a-chip into a traditional electronic device. This radio-and the chip-based software associated with it-are capable of transmitting and receiving both data and voice communications from other such devices.

Bluetooth radios use a radio band (called the industrial, scientific, and medical band-or ISM, for short) between 2.4 and 2.48 gigahertz (GHz). Because the radios are incorporated into small computer chips, they have a very small form factor and can eventually, be produced at relatively low cost. The combination of small size and low cost should help to make Bluetooth technology ubiquitous in a variety of electronic devices-especially in those with portable applications.

Note The ISM band is unlicensed, and thus available for use at no charge. (It is also shared with other types of non-Bluetooth communications.)

When one Bluetooth device senses another Bluetooth device (within about a 30-foot range), they automatically set up a connection between themselves. This connection is called Piconet, and is a kind of mini-network-a personal area network (PAN), to be specific. In a Piconet, one Bluetooth device is assigned the role of master, whiles the other device-and any subsequent devices, up to eight in total-is assigned the role of slave. The master device controls the communications, including any necessary transfer of data between the devices.

Since Bluetooth signals are sent via radio waves, walls and other physical barriers do not present the same problem that they do for infrared signals, which must operate within a narrow line-of-sight window. Bluetooth's radio frequency (RF) signals can travel through most solid objects, so Bluetooth devices can be used in a small office (walls and cubicles are invisible) or from inside a contained space (such as a briefcase or shirt pocket). As long as two Bluetooth-enabled devices are no more than 30 feet apart, they'll always be able to talk to each other.

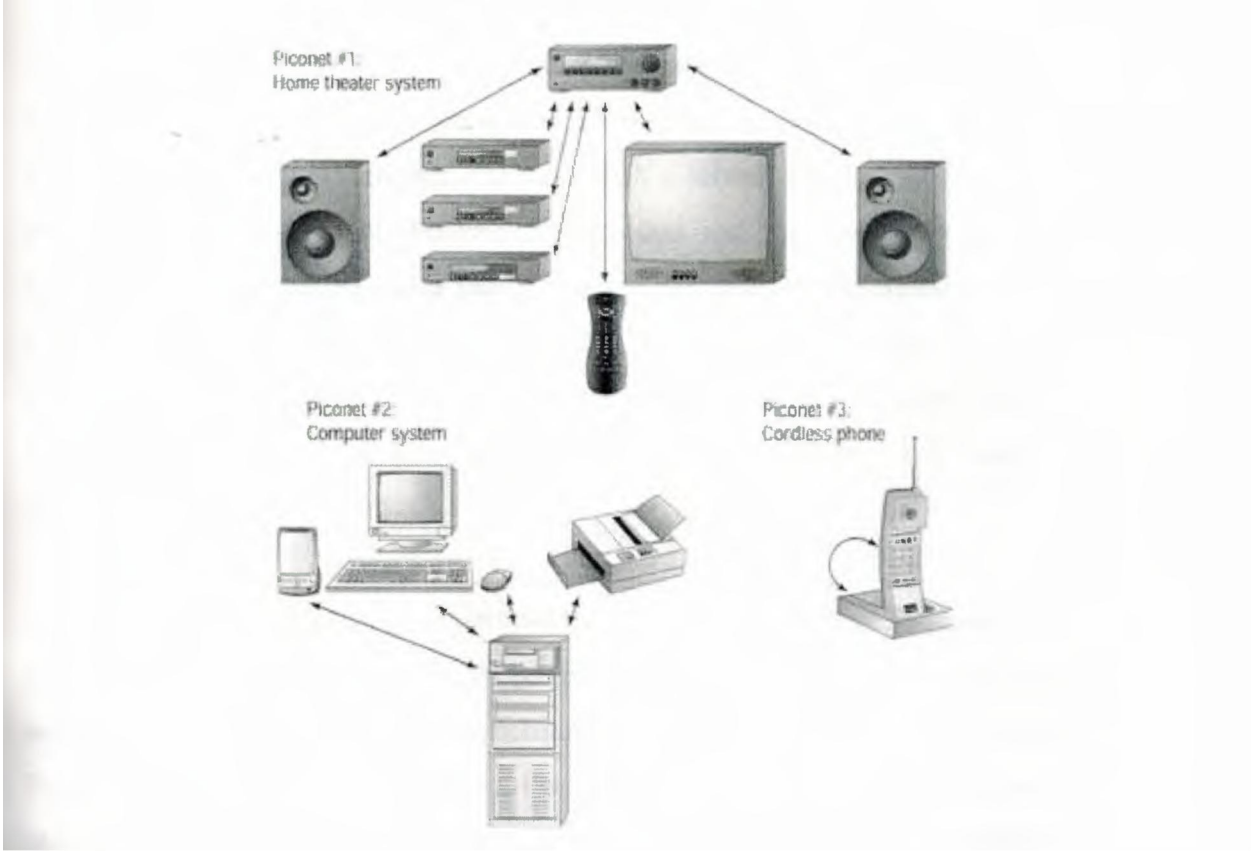

Figure 1.1: Bluetooth technology can connect all your household electronics.

Let's look at an example of how Bluetooth technology might be employed in a network of devices within your home. As you can see in Figure 1.1, in this home of the not-too-distant future, every electronic device is enabled with Bluetooth technology—a desktop PC, printer, scanner, PDA, cordless telephone, and all the components in the home theater system.

Figure 1.1: Bluetooth technology can connect all your household electronics.

Each of these devices is assigned a specific electronic address by its manufacturer. In addition, each device is programmed to automatically look for other devices within a predefined range, so that all similar devices automatically recognize each other—and automatically establish their own private Piconet. This is done when each device, as it powers up, sends out a signal asking for responses from other devices within the predefined range; any responding devices are automatically added to the first device's Piconet.

Note each type of Bluetooth device is assigned a particular range of addresses—so that all cordless phones, for example, have addresses that fall within a predefined range.

As each device in our home of the future is powered on, three separate Piconets are established. The home theater components establish one Piconet, the personal computer and accessories (printer, scanner, etc.) establish a second Piconet, and the cordless phone establishes a third Piconet (between the handset and the base station-both of which include Bluetooth radios). Data (and voice, in the case of the cordless phone) are then routinely exchanged between all the devices within each individual Piconet-the DVD player beams a movie to the A/V receiver, the computer sends formatted data to the printer, and so on. And all this happens without any data being inadvertently sent to the wrong device or network.

Of course, some devices can be instructed to work across different Piconets. In our wireless home example, let's say that we've programmed the PDA to function not only with the computer Piconet (automatically synchronizing key data) but also with the home theater Piconet. Programmed in this fashion, the PDA can function not only as a personal digital assistant, but also as a wireless remote control unit for the home theater system, essentially bridging the two individual networks.

Note in Bluetooth terminology, when you connect two or more Pico nets together, you create a scatter net.

One can also imagine the desktop PC operating across Piconets. There is no reason why your PC, which might contain thousands of songs encoded in the MP3 format, can't use Bluetooth to beam the MP3 playback directly to your audio/video receiver-and also connect your home theater system directly to the huge database of audio files available on the Internet.

The neat thing about this type of Bluetooth-enabled home is that all this interaction-and more that we can't even imagine today-will take place relatively invisibly, and without messy cables strung around and across the room.

Note Of course, Bluetooth isn't the only technology available for short-range wireless communications. Home RF and IEEE 802.11 are two competing standards for wireless networking that can be used either beside or in place of Bluetooth. While it's probably a good bet to assume that the combined industry might assembled behind Bluetooth bodes

well for its ultimate acceptance as the de facto industry standard, there are no guarantees that a better or cheaper solution won't come along and steal Bluetooth's thunder-and market potential.

1.8 What Bluetooth Will Do for You

You now know that Bluetooth is a technology for wireless connections and communications. So what? It sounds neat and sufficiently high-tech, of course, but just how will this technology impact your life?

The Bluetooth SIG-the organization pushing the development and adoption of the Bluetooth technology-has developed several different "usage models." These models attempt to define the specific situations where consumers might utilize the Bluetooth technology.
Here's a brief overview of how you might be using Bluetooth in the future.

The Cordless Desktop One of the most likely models, this scenario envisions cordless connections between your desktop PC and all manner of peripherals, from keyboards and printers to scanners and LANs.

The Internet Bridge In this scenario, Bluetooth technology is utilized to provide a wireless Internet connection, either to a mobile phone, portable PC, PDA, or some other portable device.

LAN Access This model is similar to the Internet Bridge model, except that the connection (Via Bluetooth wireless technology) is between a computer (either portable or desktop) and a local area network.

File Transfer This scenario envisions the capability to transfer any type of data file from one device to another-from a PDA to a desktop computer, for example.
This general model creates several other scenarios with more specific uses-including the Forbidden Message, Briefcase Trick, Interactive Conference, Automatic Synchronizer, and Instant Postcard models.

The Briefcase Trick This model describes how you can access e-mail while your portable PC is still in your briefcase-by transferring the messages, wirelessly, from your PC to your mobile phone.

The Forbidden Message Although this model has an ominous title (some companies prefer to call it the Flight Time With a Purpose model), it really has to do with composing e-mail messages while on the fly-literally inside an airplane, or anyplace where you don't have a live phone or network connection-and then having them sent automatically when you land (And walk by a Bluetooth transmitter/receiver in the airport).

The Interactive Conference This model contemplates using Bluetooth wireless technology to share electronic documents, business cards, contact and scheduling information, and meeting notes with other meeting participants via their portable computers-as well as using Bluetooth technology to facilitate control of a desktop PC or data projector via a Bluetooth enabled PDA.

The Automatic Synchronizer In this scenario (also dubbed the Hidden Computing model), data located on separate Bluetooth-enabled devices are automatically synchronized when the different devices come into radio range of each other. Thus you could synchronize the calendar or address book on your mobile phone or PDA with your desktop PC, simply by walking into your office.

The Instant Postcard Under this model, still pictures taken with a Bluetooth-enabled digital camera are automatically sent over the Internet (via a Bluetooth-enabled mobile phone) to a Bluetooth-enabled personal computer.

The Three-in-One Phone this model envisions telephone handsets that can connect to three different types of telephone services-as ~ cordless phone connected to the public switched telephone service (your normal phone service), as a mobile phone connected to a cellular service provider, and as a type of "walkie-talkie" connected directly to similarly equipped Bluetooth phones.

The Ultimate Headset In this scenario, Bluetooth technology is behind a separate wireless headset that enables you to engage in telephone conversations without actually holding a phone in your hand. This product could be used in the home (the headset acts in the place of a traditional phone headset) or with your mobile phone-even when your phone is stuck in your pocket or briefcase.

The PC Speaker Phone This model envisions using Bluetooth technology to create a wireless connection between your cordless headset and your personal computer, to use the PC's built-in speaker as a speaker phone.

The Hands-Free Car Kit Under this model, there is no need to hook up your mobile phone to a hands-free kit when you get into your car; the Bluetooth mobile phone in your pocket (or briefcase) will automatically connect wirelessly to the hands-free kit built into your car, and all dialing and answering is voice controlled.

1.9 Why High-Tech Companies Are Excited about Bluetooth?

The idea that eventually became Bluetooth was born in 1994, when engineers at Ericsson Mobile Communications investigated the feasibility of a low-power, low-cost radio interface between mobile phones and their accessories. This quickly developed into the concept of incorporating a small radio into both a cellular telephone and a portable PC, to connect the two devices without the traditional cable.

As work on the concept continued, however, the true potential of the technology eventually surfaced. If you could connect a cell phone to a PC, why not connect other devices as well? Why couldn't this radio-based technology become a universal bridge between devices- and to existing voice and data networks? And why limit the technology to "dumb" connections- why not provide the means for devices to automatically recognize each other, and perform key functions automatically upon connection?

As the concept of Bluetooth developed, Ericsson (in 1997) approached several manufacturers of portable electronic devices to discuss the development of this new short-range wireless technology, and in 1998 five key companies-Ericsson, IBM, Intel, Nokia, and Toshiba- formed the Bluetooth Special Interest Group (SIG), to coordinate the

development of and promote the Bluetooth technology. Bluetooth was formally announced in May of 1998, and the Bluetooth SIG released version 1.0 of the Bluetooth specification in July of 1999.

Since then, membership in the Bluetooth SIG has grown to include more than 2000 different companies. Four other large companies-3Com, Lucent Technologies, Microsoft, and Motorola-have joined the five founding companies as so-called promoter members; these nine companies provide direction and promotion for the entire 2000-company Bluetooth effort. (The Bluetooth technology itself is available to all member companies via a royalty free license-in other words, just about any company can use Bluetooth technology at no charge.)

Why are so many different companies interested in Bluetooth? Ask the companıes themselves, and you'll get the standard "enabling the consumer with new technology" line. That may be true (and probably is true), but their motives are not entirely altruistic. The reality is that all of these companies are in bed with Bluetooth because they think there's money to be made-and lots of it.

Everybody expects Bluetooth to be a big deal-but how big is big? All the major market analysis firms are weighing in their forecasts, and the numbers are almost mind-boggling. On the computer front, JDC predicts that 88.7% of all portable computers shipped in 2003 will incorporate integrated Bluetooth technology. On the mobile phone front, Cahners in-Stat Group predicts that 40% of all digital cellular phones shipped in 2003 will be Bluetooth enabled. Add it all up and you find that the folks who should know expect that the market will be flooded with hundreds of millions of Bluetooth-enabled devices, starting now and hitting a full stride no later than 2002. Merrill Lynch predicts that by 2005 there will be more than 2.1 billion Bluetooth-compatible devices on the market-creating a brand new $4 billion market.

With those kinds of numbers, you can imagine the dollar signs forming in the eyes of the world's major consumer electronics, telecommunications, and computer manufacturers. If the Internet was the last gold rush, Bluetooth could very well represent the next huge moneymaking opportunity, with literally billions and billions of dollars to be made

annually. The leaders in Bluetooth technology stand to reap a veritable bonanza when the market finally develops.

Of course, every company chasing the Bluetooth rainbow expects to be a leader. All the companies are betting that you'll become a huge user of the technology in general, and that you'll pick one of their devices as your primary Bluetooth controller-using it to handle your phone calls, control your electronic equipment, and store your electronic payment, ticketing, and personal information. The telecommunications companies (Ericsson, Nokia, Siemens, etc.) hope that some form of mobile phone becomes the dominant Bluetooth controller; the computer companies (Intel, Microsoft, 3Com, etc.) hope that some form of mobile computer (Such as an enhanced PDA) becomes the dominant controller. It probably won't be a winner take- all battle, but nobody wants to miss the revenues promised by this next big thing.

1.10 What to Expect in the Future

As with any new technology, it will take time for Bluetooth to become accepted and established. Despite all the hype over the past few years, the very first Bluetooth-enabled devices are just now hitting the market; it will take several years for Bluetooth-enabled products to become both common and affordable, and even more years for Bluetooth products to replace traditional wired products.

The first wave of Bluetooth-enabled products includes a variety of different high-tech devices, including:

• Adapters and PC cards to use with existing non-Bluetooth mobile phones and personal computers
• High-end (and high-priced!) mobile phones, cordless phones, portable PCs, and PDAs with built-in Bluetooth communication capability
• Wireless telephone headsets

That's just the first wave. As we move into 2002 and beyond, not only will you see lower prices on first-wave products, but you'll also see a new wave of totally different Bluetooth enabled products, including:

- Desktop PCs with Bluetooth technology built into the motherboard
- Wireless printers, scanners, fax machines, digital still cameras, and the like
- Bluetooth-enabled home audio/video equipment
- Wireless products developed for use in specific industries, such as the industrial automation and medical industries
- Bluetooth technology integrated into various in-car functions and products-such as hands-free cell phone capability for your traditional mobile phone

Beyond this, the sky's the limit. Can you imagine Bluetooth-enabled kitchen appliances? (Some companies can, and have a vision of your toaster talking to your refrigerator and your refrigerator printing out a shopping list-based on how many slices of bread you've toasted.) How about Bluetooth-enabled sunglasses? (They would incorporate a heads-up map display for when you're driving, and an Internet-driven MP3 player for when you're not.) Or a Bluetooth-enabled key chain (No physical keys, just encoded electronic impulses.) The possibilities, as they say, are endless.

The reality is that Bluetooth has the potential to be one of the defining technologies of the 21st century. By taking the wires out of the currently wired worlds of computing, communications, and consumer electronics, Bluetooth can make the real world a much more mobile, much more flexible, much more user-friendly place. If Bluetooth truly becomes the enabling technology for wireless connections and communications, expect many new and innovative applications to emerge-applications that could have the same impact on our future lives as the first computers and mobile phones had on our recent past.

1.11 Summary

The technology is an open specification for wireless communication of data and voice. It is based on a low-cost, short-range radio link built into a 9 x 9mm microchip, facilitating protected ad hoc connections for stationary and mobile communication environments.

Bluetooth technology allows for the replacement of the many proprietary cables that connect one device to another with one universal short-range radio link. For instance, Bluetooth radio technology built into both the cellular telephone and the laptop would replace the cumbersome cables used today to connect a laptop to a cellular telephone. Printers, PDAs, desktops, fax machines, keyboards, joysticks, and virtually any other digital device can be part of the Bluetooth system.

Bluetooth radio technology provides 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. Designed to operate in a noisy radio frequency environment such as a home, the Bluetooth radio uses a fast acknowledgement and frequency-hopping scheme to make the link robust.

Bluetooth radio modules avoid interference from other signals by hopping to a new frequency after transmitting or receiving a packet. Compared with other systems operating in the same frequency band, the Bluetooth radio typically hops faster and uses shorter packets. This makes the Bluetooth radio more robust than other systems. Similar to Home RF, Bluetooth radios also operate in the unlicensed ISM band at 2.4 GHz.
Bluetooth has a maximum data capacity of only 1 Mbps, which translates to a throughput of only 780 Kbps once the protocol overhead is taken into account.

From a security perspective, Bluetooth provides user protection and information privacy mechanisms at the lower layers of its protocol stack. Authentication is based on a challenge response algorithm. Authentication is a key component of any Bluetooth home networking system, allowing you to develop a domain of trust between personal Bluetooth devices, such as allowing only your personal notebook to communicate through your cellular telephone.

2. WIRELESS

2.1 Introduction

The term wireless is normally used to refer to any type of electrical or electronic operation which is accomplished without the use of a "hard wired" connection. Wireless communication is the transfer of information over a distance without the use of electrical conductors or "wires". The distances involved may be short (a few meters as in television remote control) or very long (thousands or even millions of kilometers for radio communications). When the context is clear the term is often simply shortened to "wireless". Wireless communications is generally considered to be a branch of telecommunications.

It encompasses various types of fixed, mobile, and portable two way radios, cellular telephones, personal digital assistants (PDAs), and wireless networking. Other examples of wireless technology include GPS units, garage door openers and or garage doors, wireless computer mice and keyboards, satellite television and cordless telephones.

Wireless operations permits services, such as long range communications, that are impossible or impractical to implement with the use of wires. The term is commonly used in the telecommunications industry to refer to telecommunications systems (e.g., radio transmitters and receivers, remote controls, computer networks, network terminals, etc.) which use some form of energy (e.g. radio frequency (RF), infrared light, laser light, visible light, acoustic energy, etc.) to transfer information without the use of wires. Information is *transferred in this manner over both short and long distances.*

Figure 2.1: Handheld wireless radios such as this Maritime VHF radio transceiver use electromagnetic waves to implement a form of wireless communications technology.

2.2 Wireless communication

The term "wireless" has become a generic and all-encompassing word used to describe communications in which electromagnetic waves or RF (rather than some form of wire) carries a signal over part or the entire communication path. Common examples of wireless equipment in use today include:

- Professional LMR (Land Mobile Radio) and SMR (Specialized Mobile Radio) typically used by business, industrial and Public Safety entities
- Consumer Two Way Radio including FRS (Family Radio Service), GMRS (General Mobile Radio Service) and Citizens band ("CB") radios
- The Amateur Radio Service (Ham radio)
- Consumer and professional Marine VHF radios
- Cellular telephones and pagers: provide connectivity for portable and mobile applications, both personal and business.
- Global Positioning System (GPS): allows drivers of cars and trucks, captains of boats and ships, and pilots of aircraft to ascertain their location anywhere on earth.
- Cordless computer peripherals: the cordless mouse is a common example; keyboards and printers can also be linked to a computer via wireless.
- Cordless telephone sets: these are limited-range devices, not to be confused with cell phones.
- Satellite television: allows viewers in almost any location to select from hundreds of channels.

Wireless networking (i.e. the various flavors of unlicensed 2.4 GHz Wi-Fi devices) is used to meet a variety of needs. Perhaps the most common use is to connect laptop users who travel from location to location. Another common use is for mobile networks that connect via satellite. A wireless transmission method is a logical choice to network a LAN segment that must frequently change locations. The following situations justify the use of wireless technology:

- To span a distance beyond the capabilities of typical cabling,
- To avoid obstacles such as physical structures, EMI, or RFI,
- To provide a backup communications link in case of normal network failure,
- To remotely connect mobile users or networks.

Wireless communication may be via:

- Radio frequency communication,
- Microwave communication, for example long-range line-of-sight via highly directional antennas, or short-range communication, or
- Infrared (IR) short-range communication, for example from remote controls or via IRDA.

The term "wireless" should not be confused with the term "cordless", which is generally used to refer to powered electrical or electronic devices that are able to operate from a portable power source (e.g., a battery pack) without any cable or cord to limit the mobility of the cordless device through a connection to the mains power supply. Some cordless devices, such as cordless telephones, are also wireless in the sense that information is transferred from the cordless telephone to the telephone's base unit via some type of wireless communications link. This has caused some disparity in the usage of the term "cordless", for example in Digital Enhanced Cordless Telecommunications.
In the last 50 years, wireless communications industry experienced drastic changes driven by many technology innovations.

2.3 **The Electromagnetic Spectrum**

Light, colors, AM and FM radio and electronic devices make use of the electromagnetic spectrum. In the US the frequencies that are available for use for communication are treated as a public resource and are regulated by the Federal Communications Commission. This determines which frequency ranges can be used for what purpose and by whom. In the absence of such control or alternative arrangements such as a privatized electromagnetic spectrum, chaos might result if, for example, airlines didn't have specific frequencies to work under and an amateur radio operator was interfering with the pilot's ability to land an airplane. Wireless communication spans the spectrum from 9 kHz to 300 GHz. (Also see Spectrum management)

2.4 Applications of Wireless Technology

2.4.1 Security systems

Wireless technology may supplement or replace hard wired implementations in security systems for homes or office buildings

2.4.2 Television remote control

Modern televisions use wireless (generally infrared) remote control units. Now we also use radio waves.

2.4.3 Cellular telephony (phones and modems)

Perhaps the best known example of wireless technology is the cellular telephone and modems. These instruments use radio waves to enable the operator to make phone calls from many locations world-wide. They can be used anywhere that there is a cellular telephone site to house the equipment that is required to transmit and receive the signal that is used to transfer both voice and data to and from these instruments.

2.5 LAN and WLAN

In 1970 University of Hawaii, under the leadership of Norman Abramson, developed the world's first computer communication network using low-cost ham-like radios, named ALOHA net. The bi-directional star topology of the system included seven computers deployed over four islands to communicate with the central computer on the Oahu Island without using phone lines.

"In 1979, F.R. Gfeller and U. Bapst published a paper in the IEEE Proceedings reporting an experimental wireless local area network using diffused infrared communications. Shortly thereafter, in 1980, P. Ferrert reported on an experimental application of a single code spread spectrum radio for wireless terminal communications in the IEEE Nati onal Telecommunications Conference. In 1984, a comparison between Infrared and CDMA spread spectrum communications for wireless office information networks was published by Kaveh Pahlavan in IEEE Computer Networking Symposium which appeared later in the IEEE Communication Society Magazine. In May 1985, the efforts of Marcus led the FCC

to announce experimental ISM bands for commercial application of spread spectrum technology. Later on, M. Kavehrad reported on an experimental wireless PBX system using code division multiple access. These efforts prompted significant industrial activities in the development of a new generation of wireless local area networks and it updated several old discussions in the portable and mobile radio industry.

The first generation of wireless data modems was developed in the early 1980's by amateur radio operators. They added a voice band data communication modem, with data rates below 9600 bit/s, to an existing short distance radio system, typically in the two meter amateur band. The second generation of wireless modems was developed immediately after the FCC announcement in the experimental bands for non-military use of the spread spectrum technology. These modems provided data rates on the order of hundreds of k bit/s. The third generation of wireless modem [then] aimed at compatibility with the existing LANs with data rates on the order of M bit/s. Several companies [developed] the third generation products with data rates above 1 M bit/s and a couple of products [had] already been announced [by the time of the first IEEE Workshop on Wireless LANs]."

"The first of the IEEE Workshops on Wireless LAN was held in 1991. At that time early wireless LAN products had just appeared in the market and the IEEE 802.11 committee had just started its activities to develop a standard for wireless LANs. The focus of that first workshop was evaluation of the alternative technologies. [By 1996], the technology [was] relatively mature, a variety of applications [had] been identified and addressed and technologies that enable these applications [were] well understood. Chip sets aimed at wireless LAN implementations and applications, a key enabling technology for rapid market growth, [were] emerging in the market. Wireless LANs [were being] used in hospitals, stock exchanges, and other in building and campus settings for nomadic access, point-to-point LAN bridges, ad-hoc networking, and even larger applications through internetworking. The IEEE 802.11 standard and variants and alternatives, such as the wireless LAN interoperability forum and the European HIPERLAN specification [had] made rapid progress, and the unlicensed PCS [Unlicensed Personal Communications Services and the proposed SUPER Net, later on renamed as U-NII, bands also presented new opportunities."

On July 21, 1999, AirPort debuted at the Macworld Expo in New York City with Steve Jobs picking up an iBook supposedly to give the cameraman a better shot as he surfed the Web. Applause quickly built as people realized there were no wires. This was the first time Wireless LAN became publicly available at consumer pricing and easily available for home use. Before the release of the Airport, Wireless LAN was too expensive for consumer use and used exclusively in large corporate settings.

Originally WLAN hardware was so expensive that it was only used as an alternative to cabled LAN in places where cabling was difficult or impossible. Early development included industry-specific solutions and proprietary protocols, but at the end of the 1990s these were replaced by standards, primarily the various versions of IEEE 802.11 (Wi-Fi). An alternative ATM-like 5 GHz standardized technology, HIPERLAN, has so far not succeeded in the market, and with the release of the faster 54 M bit/s 802.11a (5 GHz) and 802.11g (2.4 GHz) standards, almost certainly never will.

In November 2006, the Australian Commonwealth Scientific and Industrial Research Organization (CSIRO) won a legal battle in the US federal court of Texas against Buffalo Technology which found the US manufacturer had failed to pay royalties on a US WLAN patent CSIRO had filed in 1996. CSIRO are currently engaged in legal cases with computer companies including Microsoft, Intel, Dell, Hewlett-Packard and Net gear which argue that the patent is invalid and should negate any royalties paid to CSIRO for WLAN-based products.

-Benefits

The popularity of wireless LANs is a testament primarily to their convenience, cost efficiency, and ease of integration with other networks and network components. The majority of computers sold to consumers today come pre-equipped with all necessary wireless LAN technology.

The benefits of wireless LANs include:

- Convenience: The wireless nature of such networks allows users to access network resources from nearly any convenient location within their primary networking

environment (home or office). With the increasing saturation of laptop-style computers, this is particularly relevant.

• Mobility: With the emergence of public wireless networks, users can access the internet even outside their normal work environment. Most chain coffee shops, for example, offer their customers a wireless connection to the internet at little or no cost.

• Productivity: Users connected to a wireless network can maintain a nearly constant affiliation with their desired network as they move from place to place. For a business, this implies that an employee can potentially be more productive as his or her work can be accomplished from any convenient location.

• Deployment: Initial setup of an infrastructure-based wireless network requires little more than a single access point. Wired networks, on the other hand, have the additional cost and complexity of actual physical cables being run to numerous locations (which can even be impossible for hard-to-reach locations within a building).

• Expandability: Wireless networks can serve a suddenly-increased number of clients with the existing equipment. In a wired network, additional clients would require additional wmng.

• Cost: Wireless networking hardware is at worst a modest increase from wired counterparts. This potentially increased cost is almost always more than outweighed by the savings in cost and labor associated to running physical cables.

- Disadvantages

Wireless LAN technology, while replete with the conveniences and advantages described above has its share of downfalls. For a given networking situation, wireless LANs may not be desirable for a number of reasons. Most of these have to do with the inherent limitations of the technology.

• Security: Wireless LAN transceivers are designed to serve computers throughout a structure with uninterrupted service using radio frequencies. Because of space and cost, the antennas typically present on wireless networking cards in the end computers are generally relatively poor. In order to properly receive signals using such limited antennas throughout even a modest area, the wireless LAN transceiver utilizes a fairly considerable amount of power. What this means is that not only can the wireless packets be intercepted by a nearby

adversary's poorly-equipped computer, but more importantly, a user willing to spend a small amount of money on a good quality antenna can pick up packets at a remarkable distance; perhaps hundreds of times the radius as the typical user. In fact, there are even computer users dedicated to locating and sometimes even cracking into wireless networks, known as war drivers. On a wired network, any adversary would first have to overcome the physical limitation of tapping into the actual wires, but this is not an issue with wireless packets. To combat this consideration, wireless networks users usually choose to utilize various encryption technologies available such as Wi-Fi Protected Access (WPA). Some of the older encryption methods, such as WEP are known to have weaknesses that a dedicated adversary can compromise. (See main article: Wireless security.)

• Range: The typical range of a common 802.1 lg network with standard equipment is on the order of tens of meters. While sufficient for a typical home, it will be insufficient in a larger structure. To obtain additional range, repeaters or additional access points will have to be purchased. Costs for these items can add up quickly. Other technologies are in the development phase, however, which feature increased range, hoping to render this disadvantage irrelevant.

• Reliability: Like any radio frequency transmission, wireless networking signals are subject to a wide variety of interference, as well as complex propagation effects (such as multipath, or especially in this case Rician fading) that are beyond the control of the network administrator. In the case of typical networks, modulation is achieved by complicated forms of phase-shift keying (PSK) or quadrature amplitude modulation (QAM), making interference and propagation effects all the more disturbing. As a result, important network resources such as servers are rarely connected wirelessly.

• Speed: The speed on most wireless networks (typically 1-108 M bit/s) is reasonably slow compared to the slowest common wired networks (100 M bit/sup to several G bit/s). There are also performance issues caused by TCP and its built-in congestion avoidance. For most users, however, this observation is irrelevant since the speed bottleneck is not in the wireless routing but rather in the outside network connectivity itself. For example, the maximum ADSL throughput (usually 8 M bit/s or less) offered by telecommunications companies to general-purpose customers is already far slower than the slowest wireless

network to which it is typically connected. That is to say, in most environments, a wireless network running at its slowest speed is still faster than the internet connection serving it in the first place. However, in specialized environments, higher throughput through a wired network might be necessary. Newer standards such as 802.11n are addressing this limitation and will support peak throughputs in the range of 100-200 M bit/s.

Wireless LANs present a host of issues for network managers. Unauthorized access points, broadcasted SSIDs, unknown stations, and spoofed MAC addresses are just a few of the problems addressed in WLAN troubleshooting. Most network analysis vendors, such as Network Instruments, Network General, and Fluke, offer WLAN troubleshooting tools or functionalities as part of their product line.

2.6 Architecture

All components that can connect into a wireless medium in a network are referred to as stations.

All stations are equipped with wireless network interface cards (WNICs).
Wireless stations fall into one of two categories: access points, and clients.

Access points (APs) are base stations for the wireless network. They transmit and receive radio frequencies for wireless enabled devices to communicate with.

Wireless clients can be mobile devices such as laptops, personal digital assistants, IP phones, or fixed devices such as desktops and workstations that are equipped with a wireless network interface.

2.6.1 Basic service set

The basic service set (BSS) is a set of all stations that can communicate with each other.
There are two types of BSS: Independent BSS (also referred to as IBSS), and infrastructure BSS.

Every BSS has an identification (ID) called the BSSID, which is the MAC address of the access point servicing the BSS.
An independent BSS (IBSS) is an ad-hoc network that contains no access points, which means they can not connect to any other basic service set.
An infrastructure BSS can communicate with other stations not in the same basic service set by communicating through access points.

2.6.2 Extended service set

An extended service set (ESS) is a set of connected BSSes. Access points in an ESS are connected by a distribution system. Each ESS has an ID called the SSID which is a 32-byte (maximum) character string. For example, "Linksys" is the default SSID for Linksys routers.

2.6.3 Distribution system

A distribution system connects access points in an extended service setup. The concept of a DS can be to increase network coverage thru roaming between cell's.

2.7 Types of wireless LANs

An ad-hoc network is a network where stations communicate only peer to peer (P2P). There is no base and no one gives permission to talk. This is accomplished using the Independent Basic Service Set (IBSS).

A peer-to-peer (P2P) allows wireless devices to directly communicate with each other. Wireless devices within range of each other can discover and communicate directly without involving central access points. This method is typically used by two computers so that they can connect to each other to form a network..
If a signal strength meter is used in this situation, it may not read the strength accurately and can be misleading, because it registers the strength of (he strongest signal, which may be the closest computer.

802.11 specs define the physical layer (PHY) and MAC (Media Access Control) layers. However, unlike most other IEEE specs, 802.11 includes three alternative PHY standards: diffuse infrared operating at 1 M bit/s in; frequency-hopping spread spectrum operating at

1 M bit/s or 2 M bit/s; and direct-sequence spread spectrum operating at 1 M bit/s or 2 M bit/s. A single 802.11 MAC standard is based on CSMNCA.

The 802.11 specification includes provisions designed to minimize collisions. Because two mobile units may both are in range of a common access point, but not in range of each other. The 802.11 has two basic modes of operation: Ad hoc mode enables peer-to-peer transmission between mobile units. Infrastructure mode in which mobile units communicate through an access point that serves as a bridge to a wired network infrastructure is the more common wireless LAN application the one being covered. Since wireless communication uses a more open medium for communication in comparison to wired LANs, the 802.11 designers also included a shared-key encryption mechanism, called wired equivalent privacy (WEP), or Wi-Fi Protected Access, (WPA, WPA2) to secure wireless computer networks.

2.8 Metropolitan area network (MAN)

Metropolitan area networks, or MANs, are large computer networks usually spanning a city. They typically use wireless infrastructure or Optical fiber connections to link their sites.

2.8.1 IEEE definition

The IEEE 802-2001 standard describes a MAN as being:

A MAN is optimized for a larger geographical area than a LAN, ranging from several blocks of buildings to entire cities. MANs can also depend on communications channels of moderate-to-high data rates. A MAN might be owned and operated by a single organization, but it usually will be used by many individuals and organizations. MANs might also be owned and operated as public utilities. They will often provide means for intemetworking of local networks. Metropolitan area networks can span up to 50km, devices used are modem and wire/cable

2.8.2 Implementation

Some technologies used for this purpose are ATM, FDDI, and SMDS. These older technologies are in the process of being displaced by Ethernet-based MANs (e.g. Metro

Ethernet) in most areas. MAN links between LANs have been built without cables using either microwave, radio, or infra-red laser links. Most companies rent or lease circuits from common carriers due to the fact that laying long stretches of cable can be expensive.
DQDB, Distributed Queue Dual Bus, is the Metropolitan Area Network standard for data communication. It is specified in the IEEE 802.6 standard. Using DQDB, networks can be up to 30 miles (50km) long and operate at speeds of 34 to 155 M bit/s.
Several notable networks started as MANs, such as the Internet peering points MAE-West, MAE-East, and the Sohonet media network.

2.9 Personal Area Network (PAN)

A personal area network (PAN) is a computer network used for communication among computer devices (including telephones and personal digital assistants) close to one person. The devices may or may not belong to the person in question. The reach of a PAN is typically a few meters. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink).

Personal area networks may be wired with computer buses such as USB and FireWire. A wireless personal area network (WPAN) can also be made possible with network technologies such as IrDA, Bluetooth, UWB, and ZigBee.

- Technology

A Bluetooth PAN is also called a piconet, and is composed of up to 8 active devices in a master-slave relationship (a very large number of devices can be connected in "parked" mode). The first Bluetooth device in the piconet is the master, and all other devices are slaves that communicate with the master. A piconet typically has a range of 10 meters, although ranges of up to 100 meters can be reached under ideal circumstances.

Recent innovations in Bluetooth antennas have allowed these devices to greatly exceed the range for which they were originally designed. At DEF CON 12, a group of hackers known as "Flexilis" successfully connected two Bluetooth devices more than half a mile (800 m) away. They used an antenna with a scope and Yagi antenna, all attached to a rifle stock. A

cable attached the antenna to a Bluetooth card in a computer. They later named the antenna "The Blue Sniper."

Skinplex, another PAN technology, transmits via the capacitive near field of human skin. Skinplex can detect and communicate up to one meter from a human body. It is already used for access control for door locks and jamming protection in convertible car roofs.

2.10 Wide Area Network (WAN)

Wide Area Network (WAN) is a computer network that covers a broad area (i.e., any network whose communications links cross metropolitan, regional, or national boundaries). Or, less formally, a network that uses routers and public communications links [1]. Contrast with personal area networks (PANs), local area networks (LANs), campus area networks (CANs), or metropolitan area networks (MANs) which are usually limited to a room, building, campus or specific metropolitan area (e.g., a city) respectively. The largest and most well-known example of a WAN is the Internet.

WANs are used to connect LANs and other types of networks together, so that users and computers in one location can communicate with users and computers in other locations. Many WANs are built for one particular organization and are private. Others, built by Internet service providers, provide connections from an organization's LAN to the Internet. WANs are often built using leased lines. At each end of the leased line, a router connects to the LAN on one side and a hub within the WAN on the other.

Leased lines can be very expensive. Instead of using leased lines, WANs can also be built using less costly circuit switching or packet switching methods. Network protocols including TCP/IP deliver transport and addressing functions. Protocols including Packet over SONET/SDH, MPLS, ATM and Frame relay are often used by service providers to deliver the links that are used in WANs. X.25 was an important early WAN protocol, and is often considered to be the "grandfather" of Frame Relay as many of the underlying protocols and functions of X.25 are still in use today (with upgrades) by Frame Relay.
Academic research into wide area networks can be broken down into three areas: Mathematical models, network emulation and network simulation.

2.11 ZigBee

ZigBee is the name of a specification for a suite of high level communication protocols using small, low-power digital radios based on the IEEE 802.15.4 standard for wireless personal area networks (WPANs), such as wireless headphones connecting with cell phones via short-range radio. The technology is intended to be simpler and cheaper than other WPANs, such as Bluetooth. ZigBee is targeted at radio-frequency (RF) applications that require a low data rate, long battery life, and secure networking.

2.11.1 Overview

ZigBee is a low-cost, low-power, wireless mesh networking standard. The low cost allows the technology to be widely deployed in wireless control and monitoring applications, the low power-usage allows longer life with smaller batteries, and the mesh networking provides high reliability and larger range.

The ZigBee Alliance, the standards body which defines ZigBee, also publishes application profiles that allow multiple OEM vendors to create interoperable products. The current list of application profiles either published or in the works are: Home Automation, ZigBee Smart Energy, Telecommunication Applications, and Personal Home and Hospital Care.

The relationship between IEEE 802.15.4-2003 and ZigBee is similar to that between IEEE 802.11 and the Wi-Fi Alliance. The ZigBee 1.0 specification was ratified on December 14, 2004 and is available to members of the ZigBee Alliance. Most recently, the ZigBee 2007 specification was posted on October 30, 2007. The first ZigBee Application Profile, Home Automation, was announced November 2, 2007.

For non-commercial purposes, the ZigBee specification is available free to the general public. An entry level membership in the ZigBee Alliance, called Adopter, costs US$ 3500 annually and provides access to the as-yet unpublished specifications and permission to create products for market using the specifications.

ZigBee operates in the industrial, scientific and medical (ISM) radio bands; 868 MHz in Europe, 915 MHz in countries such as USA and Australia, and 2.4 GHz in most jurisdictions worldwide. The technology is intended to be simpler and cheaper than other

WPANs such as Bluetooth. ZigBee chip vendors typically sell integrated radios and microcontrollers with between 60K and 128K flash memory, such as the Free scale MC13213, the Ember EM250 and the Texas Instruments CC2430. Radios are also available stand-alone to be used with any processor or microcontroller. Generally, the chip vendors also offer the ZigBee software stack, although independent ones are also available.

2.11.2 Uses

ZigBee protocols are intended for use in embedded applications requiring low data rates and low power consumption. ZigBee's current focus is to define a general-purpose, inexpensive, self-organizing mesh network that can be used for industrial control, embedded sensing, medical data collection, smoke and intruder warning, building automation, home automation, etc. The resulting network will use very small amounts of power so individual devices might run for a year or two using the originally installed battery.

Typical application areas include:

- **Home Entertainment and Control:** Smart Lighting, Advanced Temperature Control, Safety & Security and Movies & Music
- **Home Awareness:** Water Sensors, Power Sensors, Smart Appliances and Access sensors
- **Mobile Services:** m-paymerıt, m-monitoring and control, m-security and access control, m- healthcare and Tele-assist
- **Commercial Building:** Energy Monitoring, HVAC, Lighting, Access Control
- **Industrial Plant:** Process Control, Asset Management, Environmental management, Energy Management, industrial device control

2.11.3 Device types

There are three different types of ZigBee devices:

- ZigBee coordinator (ZC): The most capable device, the coordinator forms the root of the network tree and might bridge to other networks. There is exactly one ZigBee coordinator in each network since it is the device that started the network originally. It is able to store information about the network, including acting as the Trust Centre & repository for security keys.

- ZigBee Router (ZR): As well as running an application function a router can act as an intermediate router, passing data from other devices.
- ZigBee End Device (ZED): Contains just enough functionality to talk to the parent node (either the coordinator or a router); it cannot relay data from other devices. This relationship allows the node to be asleep a significant amount of the time thereby giving long battery life. A ZED requires the least amount of memory, and therefore can be less expensive to manufacture than a ZR or ZC.

2.11.4 Software and hardware

The software is designed to be easy to develop on small, cheap microprocessors. The radio design used by ZigBee has been carefully optimized for low cost in large scale production. It has few analog stages and uses digital circuits wherever possible.

Even though the radios themselves are cheap, the ZigBee Qualification Process involves a full validation of the requirements of the physical layer. This amount of concern about the Physical Layer has multiple benefits, since all radios derived from that semiconductor mask set would enjoy the same RF characteristics. On the other hand, an uncertified physical layer that malfunctions could cripple the battery lifespan of other devices on a ZigBee network. Where other protocols can mask poor sensitivity or other esoteric problems in a fade compensation response, ZigBee radios have very tight engineering constraints: they are both power and bandwidth constrained. Thus, radios are tested to the ISO 17025 standard with guidance given by Clause 6 of the 802.15.4-2003 Standard. Most vendors plan to integrate the radio and microcontroller onto a single chip.

2.12 Wireless USB

Wireless USB is a short-range, high-bandwidth wireless radio communication protocol created by the Wireless USB Promoter Group. Wireless USB is sometimes abbreviated as "WUSB", although the USB Implementers Forum discourages this practice and instead prefers to call the technology "Certified Wireless USB" to differentiate it from competitors (see below, "Competitors"). Wireless USB is based on the WiMedia Alliance's Ultra-Wide Band (UWB) common radio platform, which is capable of sending 480 M bit/s at distances up to. 3 meters and 110 M bit/s at up to 10 meters. It was designed to operate in the 3.1 to

10.6 GHz frequency range, although local regulatory policies may restrict the legal operating range for any given country.

2.12.1 Uses

Wireless USB is used in game controllers, printers, scanners, digital cameras, MP3 players, hard disks and flash drives. It is also suitable for transferring parallel video streams.

2.12.2 Host wire adapters, device wire adapters, and dual-role devices

The WUSB architecture allows up to 127 devices to connect directly to a host. Because there are no wires or ports, there is no longer a need for hubs.

However, to facilitate the migration from wired to wireless, WUSB introduced a new Device Wire Adapter (DWA) class. Sometimes referred to as a "WUSB hub", a DWA allows existing USB 2.0 devices to be used wirelessly with a WUSB host.

WUSB host capability can be added to existing PCs through the use of a Host Wire Adapter (HWA). The HWA is a USB 2.0 device that attaches externally to a desktop or laptop's USB port or internally to a laptop's Mini Card interface.

WUSB also supports dual-role devices (DRDs), which in addition to being a WUSB device, can function as a host with limited capabilities. For example, a digital camera could act as a device when connected to a computer and as a host when transferring pictures directly to a printer.

2.12.3 Relation to ultra-wideband (UWB)

A common source of confusion is about the relationship between WUSB, WiMedia, and UWB. The UWB and WUSB technologies are not the same, and the terms WUSB and UWB are not synonymous.

UWB is a general term for a new type of radio communication using pulses of energy which spread emitted Radio Frequency energy over 500 MHz+ of spectrum or exceeding 20% fractional bandwidth within the frequency range of 3.1 GHz to 10.6 GHz as defined by the FCC ruling issued for UWB in Feb. 2001. UWB is NOT specific to WiMedia or any other company or group and there are in fact a number of groups and companies

developing UWB technology totally unrelated to WiMedia. Some companies use UWB for Ground Penetration RADAR, through wall RADAR and yet another company Pulse-LINK uses it as part of a whole home entertainment network using UWB for transmission over both wired and wireless media. WUSB is a protocol promulgated by the USB-IF that uses WiMedia's UWB radio platform. Other protocols that have announced their intention to use WiMedia's UWB radio platform include Bluetooth and the WiMedia Logical Link Control Protocol.

2.12.4 **WUSB** vs. **Bluetooth**

Wireless USB and Bluetooth are two different protocols trying to accomplish two entirely different goals. Wireless USB is a high bandwidth wireless protocol with a smaller range than Wi-Fi (and larger bandwidth, and a much reduced power profile), but with higher transfer rates than Bluetooth (though both share a similar range and may be able to use the same PHY/Transceiver hardware much like combo Bluetooth + Wi-Fi devices). Theoretically, a single 2.4 GHz radio device could be constructed that works with all three protocols seamlessly, with any necessary decoding/encoding performed within software.

Bluetooth specification 3.0 is currently ongoing and has the goal to also use UWB. In parallel also Wi-Fi shall be seamlessly integrated. From throughput point of view there will be no differences when the specification 3.0 is finished. From connection establishment Bluetooth has advantages compared to Wireless USB. Wireless USB does not have service level security and service discovery. Bluetooth has long experience with connection establishment so a connection can be established from any device. In Wireless USB connection establishment can only be done from the device side.

table2.1: Comparis~n with other digital RF communication systems.

Wireless USB vs. 802.11a/b/g & Bluetooth				
Specificatio	**Wireless U Specification R 1.0**	**Bluetooth 3.0(proposed)**	**IEEE802.11a/b/g**	**Bluetooth 2.0 EDR**
Frequency band	3.1 GHz–10.6 GH	UWB (not decided)	2.4 GHz/5 GHz	2.4 GHz
Transfer sp((distance)	480 M bit/s (3 1 110 M bit/s (10 m	53 - 480 M b (unknown distance)	Max. 54 M b (100 m)	Max. 3 M b (1 m–100 depending output)
Modulation	MB-OFDM	MB-OFDM	DSSS, DBPS DQPSK, CCK, OFDM	GFSK

CCK: Complementary code keying
DBPSK: Differential binary phase-shift keying
DQPSK: Differential quadrature phase-shmultiplexing
keying
DSSS: Direct sequence spread spectrum
EDR: Enhanced Data Rate
GFSK: Gaussian frequency-shift keying
OFDM: Orthogonal frequency division
MB-OFDM: Multi band-OFDM

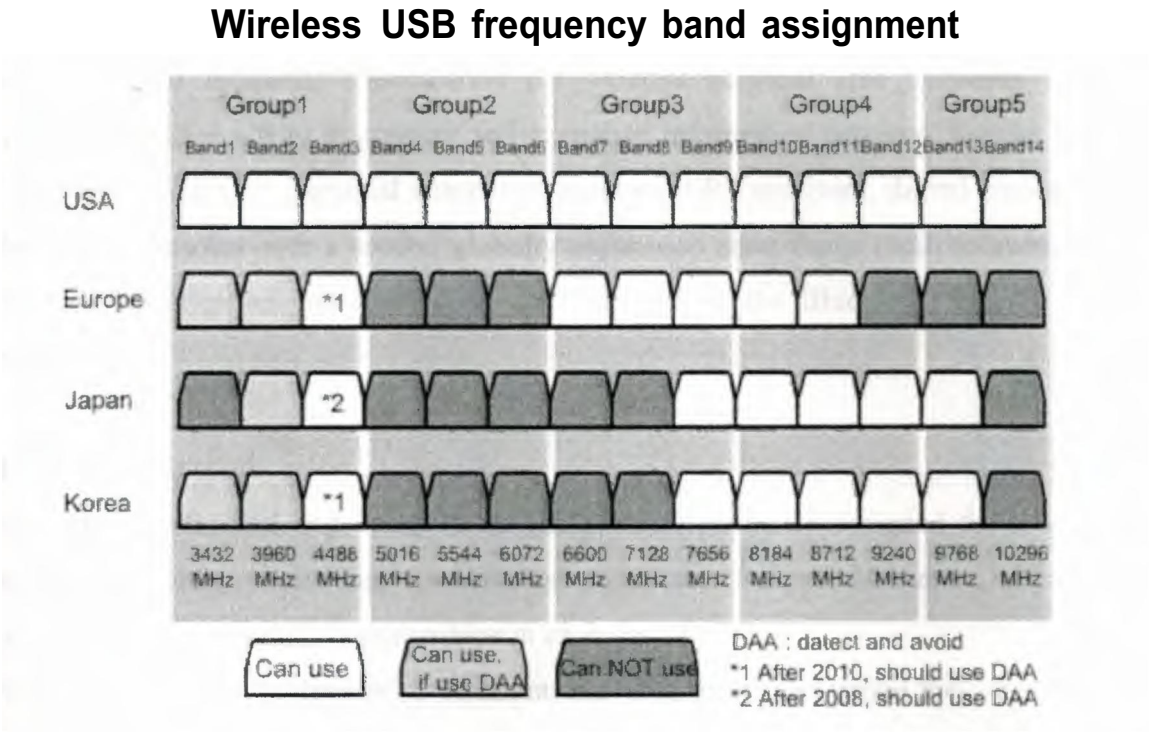

Figure 2.2: Comparison of 4 regions RF bands.

2.12.5 Competitors: Certified Wireless USB vs. Wireless USB™

"Wireless USB" by Cypress Semiconductor is not related to "Certified Wireless USB". Cypress's "Wireless USB" is a protocol that uses the 2.4 GHz band with a range from 10 meters (at max 1 M bit/s) to 50 meters (at max 62.5 k bit/s) and is designed for Human Interface Devices (HIDs), with current offerings from companies such as Belkin, Logitech, and Virtual Ink.

2.12.6 UWB

Other forms of USB over wireless exist, such as those based on the competing direct sequence UWB technology by Free scale (Cable-Free USB). The same is also true for other radio frequency based wire replacement systems which can carry USB. The result is that the name 'Certified Wireless USB' was adopted to allow consumers to identify which products would be adherent to the standard and would support the correct protocol and data rates.

2.13 Bluetooth and Wireless

Bluetooth is an industrial specification for wireless personal area networks (PANs). Bluetooth provides a way to connect and exchange information between devices such as mobile phones, laptops, personal computers, printers, OPS receivers, digital cameras, and video game consoles over a secure, globally unlicensed short-range radio frequency. The Bluetooth specifications are developed and licensed by the Bluetooth Special Interest Group.

2.13.1 Uses

Bluetooth is a standard and communications protocol primarily designed for low power consumption, with a short range (power-class-dependent: 1 meter, 10 meters, 100 meters) based on low-cost transceiver microchips in each device.

Bluetooth enables these devices to communicate with each other when they are in range. The devices use a radio communications system, so they do not have to be in line of sight of each other, and can even be in other rooms, as long as the received transmission is powerful enough.

In most cases the effective range of class 2 devices is extended if they connect to a class 1 transceiver, compared to pure class 2 network. This is accomplished by the higher sensitivity and transmission power of Class 1 devices.

2.13.2 Bluetooth vs. Wi-Fi in networking

Bluetooth and Wi-Fi have slightly different applications in today's offices, homes, and on the move: setting up networks, printing, or transferring presentations and files from PDAs to computers. Both are versions of unlicensed spread spectrum technology.

Bluetooth differs from Wi-Fi in that the latter provides higher throughput and covers greater distances, but requires more expensive hardware and higher power consumption. They use the same frequency range, but employ different modulation techniques. While Bluetooth is a replacement for a variety of applications, Wi-Fi is a replacement only for local area network access. Bluetooth can be thought of as wireless USB whereas Wi-Fi is wireless Ethernet, both operating at much lower bandwidth than cable networking systems.

However, this analogy is not entirely accurate since any Bluetooth device can, in theory, host any other Bluetooth device-something that is not universal to USB devices, therefore it would resemble more a wireless FireWire.

2.13.3 Bluetooth Devices

Bluetooth exists in many products, such as telephones, printers, modems and headsets. The technology is useful when transferring information between two or more devices that are near each other in low-bandwidth situations. Bluetooth is commonly used to transfer sound data with telephones (i.e. with a Bluetooth headset) or byte data with hand-held computers (transferring files).

Bluetooth simplifies the discovery and setup of services between devices. Bluetooth devices advertise all of the services they provide. This makes using services easier because there is no longer a need to set up network addresses or permissions as in many other networks.

2.13.4 Wi-Fi

Wi-Fi is more like a traditional Ethernet network, and requires configuration to set up shared resources, transmit files, and to set up audio links (for example, headsets and hands-free devices). It uses the same radio frequencies as Bluetooth, but with higher power resulting in a stronger connection. Wi-Fi is sometimes called "wireless Ethernet." This description is accurate as it also provides an indication of its relative strengths and weaknesses. Wi-Fi requires more setup, but is better suited for operating full-scale networks because it enables a faster connection, better range from the base station, and better security than Bluetooth.

2.13.5 Computer requirements

A personal, computer must have a Bluetooth adapter in order to be able to communicate with other Bluetooth devices (such as mobile phones, mice and keyboards). While some desktop computers and most recent laptops come with a built-in Bluetooth adapter, others will require an external one in the form of a dongle.

Unlike its predecessor, IrDA, which requires a separate adapter for each device, Bluetooth allows multiple devices to communicate with a computer over a single adapter.

2.13.6 Operating system support

Apple has suppprted Bluetooth since Mac OS X vl 0.2 released in 2002.

For Microsoft platforms, Windows XP Service Pack 2 and later releases have native support for Bluetooth. Previous versions required users to install their Bluetooth adapter's own drivers, which were not directly supported by Microsoft. Microsoft's own Bluetooth dongles (packaged with their Bluetooth computer devices) have no external drivers and thus require at least Windows XP Service Pack 2.

Linux provides two Bluetooth stacks, with the Blue Z stack included with most Linux kernels. It was originally developed by Qualcomm and Affix. Blue Z supports all core Bluetooth protocols and layers. FreeBSD features Bluetooth support since its 5.0 release. Net BSD features Bluetooth support since its 4.0 release. Its Bluetooth stack has been ported to Open BSD as well.

2.13.7 Specifications and features

The Bluetooth specification was developed in 1994 by Jaap Haartsen and Sven Mattisson, who were working for Ericsson Mobile Platforms in Lund, Sweden.The specification is based on frequency-hopping spread spectrum technology.

The specifications were formalized by the Bluetooth Special Interest Group (SIG), organised by Mohd Syarifuddin. The SIG was formally announced on May 20, 1998. Today it has a membership of over 7000 companies worldwide. It was established by Ericsson, Sony Ericsson, IBM, Intel, Toshiba, and Nokia, and later joined by many other companies.

2.13.8 Bluetooth 1.0 and 1.0B

Versions I.O and I.OB had many problems, and manufacturers had difficulty making their products interoperable. Versions 1.0 and 1.0B also included mandatory Bluetooth hardware device address (BD_ADDR) transmission in the Connecting process (rendering anonymity impossible at the protocol level), which was a major setback for certain services planned for use in Bluetooth environments.

2.13.9 Bluetooth 1.1

- Ratified as IEEE Standard 802.15.1-2002.
- Many errors found in the 1.0B specifications were fixed.
- Added support for non-encrypted channels.
- Received Signal Strength Indicator (RSSI).

2.13.10 Bluetooth 1.2

This version is backward-compatible with 1.1 and the major enhancements include the following:

- Faster Connection and Discovery
- Adaptive frequency-hopping spread spectrum (AFH), which improves resistance to radio frequency interference by avoiding the use of crowded frequencies in the hopping sequence.
- Higher transmission speeds in practice, up to 721 k bit/s, as in 1.1.
- Extended Synchronous Connections (e SCO), which improve voice quality of audio links by allowing retransmissions of corrupted packets, and may optionally increase audio latency to provide better support for concurrent data transfer.
- Host Controller Interface (HCI) support for three-wire UART.
- Ratified as IEEE Standard 802.15.1-2005.

2.13.11 Bluetooth 2.0

This version, specified on November 10, 2004, is backward-compatible with 1.1. The main enhancement is the introduction of an Enhanced Data Rate (EDR) of 3.0 M bit/s for both data (ACL) and voice (e SCO) packets. This has the following effects:

- Three times faster transmission speed-up to 10 times in certain cases (up to 2.1 M bit/s).
- Lower power consumption through a reduced duty cycle.
- Simplification of multi-link scenarios due to more available bandwidth.

The practical data transfer rate is 2.1 megabits per second and the basic signaling rate is about 3 megabits per second. The "Bluetooth 2.0 + EDR" specification given at the Bluetooth Special Interest Group (SIG) includes EDR and there is no specification "Bluetooth 2.0" as used by many vendors. The HTC TYTN pocket PC phone, shows "Bluetooth 2.0 without EDR" on its data sheet. In many cases it is not clear whether a product claiming to support "Bluetooth 2.0" actually supports the EDR higher transfer rate.

2.13.12 Bluetooth 2.1

Bluetooth Core Specification Version 2.1 is fully backward-compatible with 1.1, and was adopted by the Bluetooth SIG on July 26, 2007. This specification includes the following features:

- **Extended inquiry response:** provides more information during the inquiry procedure to allow better filtering of devices before connection. This information includes the name of the device, a list of services the device supports, as well as other information like the time of day, and pairing information.
- **Sniff sub rating:** reduces the power consumption when devices are in the sniff low-power mode, especially on links with asymmetric data flows. Human interface devices (HID) are expected to benefit the most, with mouse and keyboard devices increasing the battery life by a factor of 3 to 10. It lets devices decide how long they will wait before sending keep alive messages to one another. Previous Bluetooth implementations featured keep alive message frequencies of up to several times per second. In contrast, the 2.1 specification allows pairs of devices to negotiate this value between them to as infrequently as once every 5 or 10 seconds.
- **Encryption Pause Resume:** enables an encryption key to be refreshed, enabling much stronger encryption for connections that stay up for longer than 23.3 hours (one Bluetooth day).
- **Secure Simple Pairing:** radically improves the paınng experience for Bluetooth devices, while increasing the use and strength of security. It is expected that this feature will significantly increase the use of Bluetooth.
- **NFC cooperation:** automatic creation of secure Bluetooth connections when NFC radio interface is also available. For example, a headset should be paired with a Bluetooth 2.1 phone including NFC just by bringing the two devices close to each other (a few

centimeters). Another example is automatic uploading of photos from a mobile phone or camera to a digital picture frame just by bringing the phone or camera close to the frame.

2.13.13 Future of Bluetooth

- **Broadcast Channel:** enables Bluetooth information points. This will drive the adoption of Bluetooth into mobile phones, and enable advertising models based around users pulling information from the information points, and not based around the object push model that is used in a limited way today.
- **Topology Management:** enables the automatic configuration of the piconet topologies especially in scattemet situations that are becoming more common today. This should all be invisible to the users of the technology, while also making the technology just work.
- **Alternate MAC PHY:** enables the use of alternative MAC and PHY's for transporting Bluetooth profile data. The Bluetooth Radio will still be used for device discovery, initial connection and profile configuration, however when lots of data needs to be sent, the high speed alternate MAC PHY's will be used to transport the data. This means that the proven low power connection models of Bluetooth are used when the system is idle, and the low power per bit radios are used when lots of data needs to be sent.
- **QoS improvements:** enable audio and video data to be transmitted at a higher quality, especially when best effort traffic is being transmitted in the same piconet.

2.13.14 High-speed Bluetooth

On 28 March 2006, the Bluetooth Special Interest Group announced its selection of the WiMedia Alliance Multi-Band Orthogonal Frequency Division Multiplexing (MB-OFDM) version of UWB for integration with current Bluetooth wireless technology.

UWB integration will create a version of Bluetooth wireless technology with a high-speed/high-data-rate option. This new version of Bluetooth technology will meet the high-speed demands of synchronizing and transferring large amounts of data, as well as enabling high-quality video and audio applications for portable devices, multi-media projectors and television sets, and wireless VOIP.

At the same time, Bluetooth technology will continue catering to the needs of very low power applications such as mice, keyboards, and mono headsets, enabling devices to select

the most appropriate physical radio for the application requirements, thereby offering the best of both worlds.

2.13.15 Bluetooth 3.0

The next version of Bluetooth after v2.1, code-named Seattle (the version number of which is TBD) has many of the same features, but is most notable for plans to adopt ultra-wideband (UWB) radio technology. This will allow Bluetooth use over UWB radio, enabling very fast data transfers of up to 480 M bit/s, while building on the very low-power idle modes of Bluetooth.

2.13.16 Ultra Low Power Bluetooth

On June 12, 2007, Nokia and Bluetooth SIG announced that Wibree will be a part of the Bluetooth specification as an ultra low power Bluetooth technology. Expected use cases include watches displaying Caller ID information, sports sensors monitoring your heart rate during exercise, as well as medical devices. The Medical Devices Working Group is also creating a medical devices profile and associated protocols to enable this market.

2.13.17 Technical information

A master Bluetooth device can communicate with up to seven devices. This network group of up to eight devices is called a piconet.

A piconet is an ad-hoc computer network, using Bluetooth technology protocols to allow one master device to interconnect with up to seven active devices. Up to 255 further devices can be inactive, or parked, which the master device can bring into active status at any time.

At any given time, data can be transferred between the master and one other device, however, the devices can switch roles and the slave can become the master at any time. The master switches rapidly from one device to another in a round-robin fashion. (Simultaneous transmission from the master to multiple other devices is possible, but not used much.)

Bluetooth specification allows connecting two or more piconets together to form a scattemet, with some devices acting as a bridge by simultaneously playing the master role and the slave role in one piconet.

Many USB Bluetooth adapters are available, some of which also include an IrDA adapter. Older (pre-2003) Bluetooth adapters, however, have limited services, offering only the Bluetooth Enumerator and a less-powerful Bluetooth Radio incarnation. Such devices can link computers with Bluetooth, but they do not offer much in the way of services that modem adapters do.

2.13.18 Setting up connections

Any Bluetooth device will transmit the following information on demand:

- Device name.
- Device class.
- List of services.
- Technical information, for example, device features, manufacturer, Bluetooth specification used, clock offset.

Any device may perform an inquiry to find other devices to connect to, and any device can be configured to respond to such inquiries. However, if the device trying to connect knows the address of the device, it always responds to direct connection requests and transmits the information shown in the list above if requested. Use of device services may require pairing or acceptance by its owner, but the connection itself can be initiated by any device and held until it goes out of range. Some devices can be connected to only one device at a time, and connecting to them prevents them from connecting to other devices and appearing in inquiries until they disconnect from the other device.

Every device has a unique 48-bit address. However these addresses are generally not shown in inquiries. Instead, friendly Bluetooth names are used, which can be set by the user. This name appears when another user scans for devices and in lists of paired devices.

Most phones have the Bluetooth name set to the manufacturer and model of the phone by default. Most phones and laptops show only the Bluetooth names and special programs that are required to get additional information about remote devices. This can be confusing as, for example, there could be several phones in range named T610 (see Blue jacking).

2.13.19 Pairing

Pairs of devices may establish a trusted relationship by learning (by user input) a shared secret known as a passkey. A device that wants to communicate only with a trusted device can cryptographically authenticate the identity of the other device. Trusted devices may also encrypt the data that they exchange over the airwaves so that no one can listen in. The encryption can, however, be turned off, and passkeys are stored on the device file system, not on the Bluetooth chip itself. Since the Bluetooth address is permanent, a pairing is preserved, even if the Bluetooth name is changed. Pairs can be deleted at any time by either device. Devices generally require pairing or prompt the owner before they allow a remote device to use any or most of their services. Some devices, such as mobile phones, usually accept OBEX business cards and notes without any pairing or prompts.

2.13.20 Air interface

The protocol operates in the license-free ISM band at 2.4-2.4835 GHz. To avoid interfering with other protocols that use the 2.45 GHz band, the Bluetooth protocol divides the band into 79 channels (each I MHz wide) and changes channels up to 1600 times per second. Implementations with versions I.I and 1.2 reach speeds of 723.1 k bit/s. Version 2.0 implementations feature Bluetooth Enhanced Data Rate (EDR) and reach 2.1 M bit/s. Technically, version 2.0 devices have a higher power consumption, but the three times faster rate reduces the transmission times, effectively reducing power consumption to half that of l.x devices (assuming equal traffic load)

2.13.21 Security

Bluetooth implements confidentiality, authentication and key derivation with custom algorithms based on the SAFER+ block cipher. In Bluetooth, key generation is generally based on a Bluetooth PIN, which must be entered into both devices. This procedure might be modified if one of the devices has a fixed PIN, e.g. for headsets or similar devices with a restricted user interface. During pairing, an initialization key or master key is generated, using the E22 algorithm. The E0 stream cipher is used for encrypting packets, granting confidentiality and is based on a shared cryptographic secret, namely a previously generated link key or master key. Those keys, used for subsequent encryption of data sent via the air interface, rely on the Bluetooth PIN, which has been entered into one or both devices.

2.13.22 Blue jacking

Blue jacking allows phone users to send business cards anonymously using Bluetooth wirelesstechnology. Blue jacking does NOT involve the removal or alteration of any data from the device. These business cards often have a clever or flirtatious message rather than the typical name and phone number. Blue jackers often look for the receiving phone to ping or the user to react. They then send another, more personal message to that device. Once again, in order to carry out a blue jacking, the sending and receiving devices must be within range of each other, which is typically 10 meters for most mobile devices. Devices that are set in non-discoverable mode are not susceptible to blue jacking. However, the Linux application Red fang claims to find non-discoverable Bluetooth devices.

2.13.23 Health concerns

Bluetooth uses the microwave radio frequency spectrum in the 2.4 GHz to 2.4835 GHz range. Maximum power output from a Bluetooth radio is 100 mW, 2.5 mW, and 1 mW for Class 1, Class 2, and Class 3 devices respectively, which puts Class 1 at roughly the same level as mobile phones, and the other two classes much lower. Accordingly, Class 2 and Class 3 Bluetooth devices are considered less of a potential hazard than mobile phones, and Class 1 may be comparable to that of mobile phones.

2.13.24 Origin of the name and the logo

Bluetooth was named after a late tenth century king, Harald Bluetooth, King of Denmark and Norway. He is known for his unification of previously warring tribes from Denmark (including now Swedish Scania, where the Bluetooth technology was invented), and Norway. Bluetooth likewise was intended to unify different technologies, such as personal computers and mobile phones.

The name may have been inspired less by the historical Harald than the loose interpretation of him in The Long Ships by Frans Gunnar Bengtsson, a Swedish Viking-inspired novel.
The Bluetooth logo merges the Germanic runes analogous to the modem Latin letter H and B: (for Harald Bluetooth) (Hagall) and (Berkanan) merged together, forming a bind rune.

2.14 Summary

A wireless home network is an intriguing alternative to phone line and power line wiring systems.

Wireless home networks provide all the functionality of wire line networks without the physical constraints of the wire itself. They generally revolve around either IR or radio transmissions within your home. Radio transmissions comprise of two distinct technologies-narrowband and spread-spectrum radio. Most wireless home networking products are based upon the spread spectrum technologies. To date, the high cost and impracticality of adding new wires have inhibited the wide spread adoption of home networking technologies. Wired technologies also do not allow users to roam about with portable devices. In addition, multiple, incompatible communication standards have limited acceptance of wireless networks in the home.

3. SURVIVABLE BLUETOOTH LOCATION NETWORKS

3.1 Introduction

3.1.1 Motivation

This chapter analyzes survivability issues of auxiliary Bluetooth Location Networks (BLN) for location-aware or context driven mobile networks.

M-commerce (mobile e-commerce) has a promising future. In a typical m-commerce *scenerio, customers in a large commercial area carry wireless PDAs. A PDA client allows* its user not *only* to purchase *items,* make reservations or request information, but *also to* receive (possibly context driven) store coupons, advertisements and advice. Another interesting application field is electronic guidance. Exhibition visitors receive specific information associated to their current location.

In any of those scenarios, there exist service servers that need to know user location in real-time, and send context oriented information to user handhelds when necessary.
The BLN transmits position information to the service servers, without user participation. It is not subject to line of- sight constraints and its base technology is supported by existing commercial handhelds. As a fully operational data network, the BLN admits alternative uses as a security network when the target area is closed to the public, or as a spare network for emergencies.

BLN users carry both a Bluetooth-enabled handheld or any mobile data terminal and a Bluetooth badge (thus, the BLN may provide location services to any mobile data terminal).

We must remark that we simply rely on Bluetooth responses to inquiry cycles and, as a consequence, we do not need specific client programming. The BLN is composed by wireless Bluetooth nodes, which establish a spontaneous network topology at system initialization. The BLN can coexist with other Bluetooth systems, such as printers.

3.1.2 Background

Many user-positioning solutions have been proposed in previous research, but they are based on specialized devices that are not supported by commercial data terminals. If we review positioning systems supported by commercial terminals, we find the following:

• Cell phone location services and GPS are quite effective for outdoor applications (especially GPS), and possibly the best choice. However, they are useless indoors.

• HP's Cool town is based on IR beacons, which push position-dependent URLs into handheld IR ports (included in most state-of-the-art PDAs and WAP phones).

Cool town is user-dependent, because the user must aim the infrared port to location beacons. It could be argued that this is not a drawback, since automatic detection of location information (without user participation) may have severe consequences in terms of nuisance value.

For example, when users are annoyed because the Web page they are viewing is suddenly supplanted by one advertising frozen peas from a grocery store nearby.

User-independence is only a disadvantage in aggressive systems, which are not a desirable scenario. Consider, for example, a museum, where updates could only take place when users enter new halls, showing the previous page with a tiny flashing icon at its bottom meaning "do you want to update context information?" Also, asking the user to locate IR beacons each time he enters a room full of visual distractions may be tiring, and signaling IR beacons with large red arrows unsightly.

We can conclude that, depending on the specific application, user-dependent line-of-sight IR systems may be more advantageous than user-independent RF ones or vice versa.
In fact, they are complementary. For example, in a museum, a Pocket PC could use Cool town to retrieve information on a single object (e.g. "Celtic fibula"), and Bluetooth-assisted context awareness to retrieve information on the surrounding hall (e.g. "Iron Age").

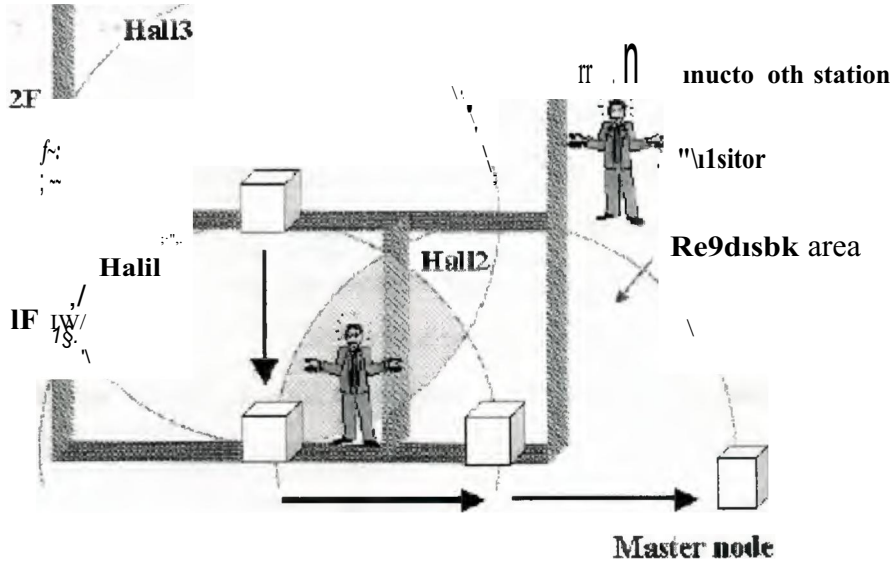

Figure 3.1: Cooperative Bluetooth Location.

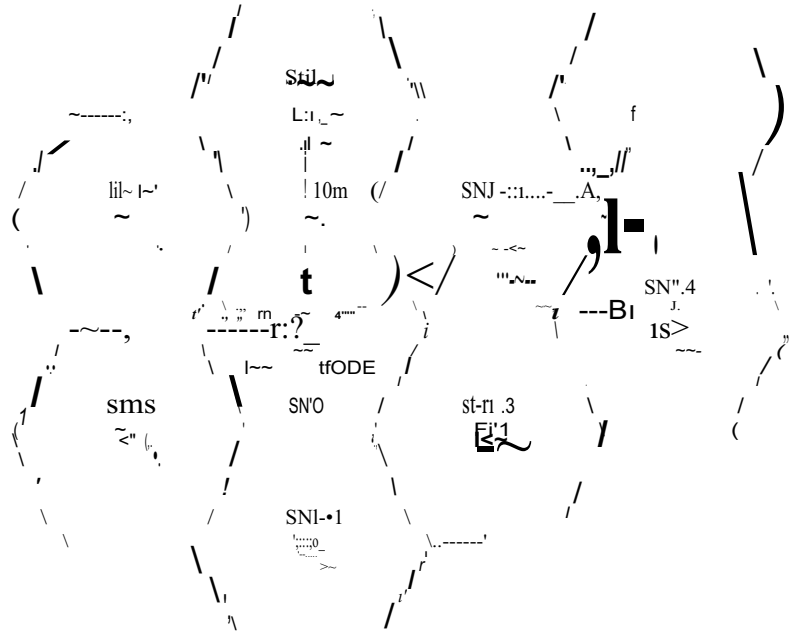

Figure 3.2: Bluetooth Location Network.

3.1.3 Bluetooth location networks

In this chapter, we evaluate survivability in Bluetooth Location Networks (BLN), which satisfy the requirements in section I-A. We assume that the users carry a Bluetooth enabled terminal, or any mobile data terminal and an independent Bluetooth location badge. The users must access the Web/WAP service servers from their handhelds, and enter their badge address. By doing so, the Bluetooth address of the badge becomes valid from the BLN's point of view (obviously, the location network must work even if invalid addresses are present, as we will see later). The service server associates the user IP address or WAP session to his badge number, for all subsequent transactions. The badge (or the Bluetooth modem in the user's terminal) interacts with the BLN, which provides service servers with real-time user position. The service servers may use this information to push URLs into user terminals via TCP/IP sockets, or to update WAP cards.
Thus, no user action is involved in context-driven updates.

Although the authors claimed some of the advantages we enumerate in section IA, they also stated that Bluetooth range does not provide enough location precision. Consider the example in Figure 3.1.

In principle, if the three Bluetooth stations detect the user modem, the user could be located in any hall if considering full range. The key point in our philosophy is establishing a cooperative location network. The network transmits user modem addresses and the addresses of the Bluetooth stations that detect those modems to a master node. In the example in figure 1, the master node would determine that the user is located inside the gray region. Note that most of that region is part of the hall were the user is actually located.

The cooperative BLN in this paper is intended to cover 2D target areas, although it can be generalized to cover 3D ones.

3.2 BLN Protocols

3.2.1 BLN configuration

The BLN is composed by mobile badges and static Bluetooth units (located at the ceiling, for example). We will refer to the latter as static nodes. Static nodes (SNs) are arranged in a network that covers the whole target area. Hexagonal tiling is a typical solution in 2D cellular network planning, which we have followed in this research (Figure 3.2). Other arrangements where any SN has at most seven closest neighbors within its range could be used as well (10 m for class 2 Bluetooth modems). For example, meshes for 2D areas or k-ray 3-cubes for 3D areas.

Each cell in the ideal case in Figure 3.2 has an area of 86.55 m2. SN units scan their surroundings periodically, by means of Bluetooth inquiry calls. All SNs are organized in a radial scatternet around a master node, SNO, connected to the service servers (not shown).

The remaining SNs are arranged in "circular" layers around SNO. The notation SNX-Y is used to support the explanation and stands for the Bluetooth address of SN Y in layer X. In any layer, SNX-1 is placed right above SNO, and the remaining Y values are increased clockwise. Our example shows the six cells in the first layer, SNl-1 to SNl-6, and two cells in the second layer, SN2-3 and SN2-4. Each SN is a slave of its six neighbors.

All SNs perform inquiry cycles periodically, to *publish* their existence. If SN a detects an inquiry from SN b, and b is not currently listed in a's routing table, a must send its minimum distance to the master node in number of hops to b (in a distance packet with an 8-bit control field and a 8-bit distance field, which fits in a DM-1 packet). All SN minimum distances are set to _ at power up, except the master node's, which is set to 0. Thus, the master node initiates the configuration by sending O-hop distance packets to its neighbors on demand. Later, if a SN performing an inquiry cycle does not receive an answer from one of its neighbors, it deletes the corresponding entry. If this changes its minimum distance to the master node, the SN transmits a new minimum distance packet to all its slaves.

Whenever a SN receives a distance packet, it searches its routing table to check if the corresponding distance is lower than its current lowest distance to the master node. If so, the SN builds a new distance packet and transmits it to its entire slave SNs, excepting those included in minimum-distance routes to the master node. This algorithm is similar to the split horizon algorithm.

Therefore, the configuration process also restarts in case of SN failures, and propagates changes from the failure neighborhood (possibly only affecting a BLN region).
If a SN receives a distance packet, it must update its routing table. The routing table stores pairs of neighbor SN addresses and their distances to the master node, and is sorted by distance. The best path to the master node is always the first table entry.
Figure 3.3 depict a BLN region. We describe two configuration steps to illustrate the general procedure.

Once the master node initiates the process, the distance from SNl-2 to the master node changes. Node SNl-2 transmits the new minimum distance (1) to all its slaves, on demand.

SN2-4 receives the distance packet from SNl-2. Since this distance plus 1 is lower than the current local minimum distance LJ, SN2-4 increments the received distance by 1, stores it in its routing table, and sorts the table again.

As we said previously, if a SN detects that the minimum distance to the master node has changed, it builds a new distance packet with this minimum distance, and transmits it to its slaves (neighbors) except to those who are in the minimum distance path. Those SNs receive an infinite distance packet, to prevent loops (see SN2-4 in Figure 3.3).

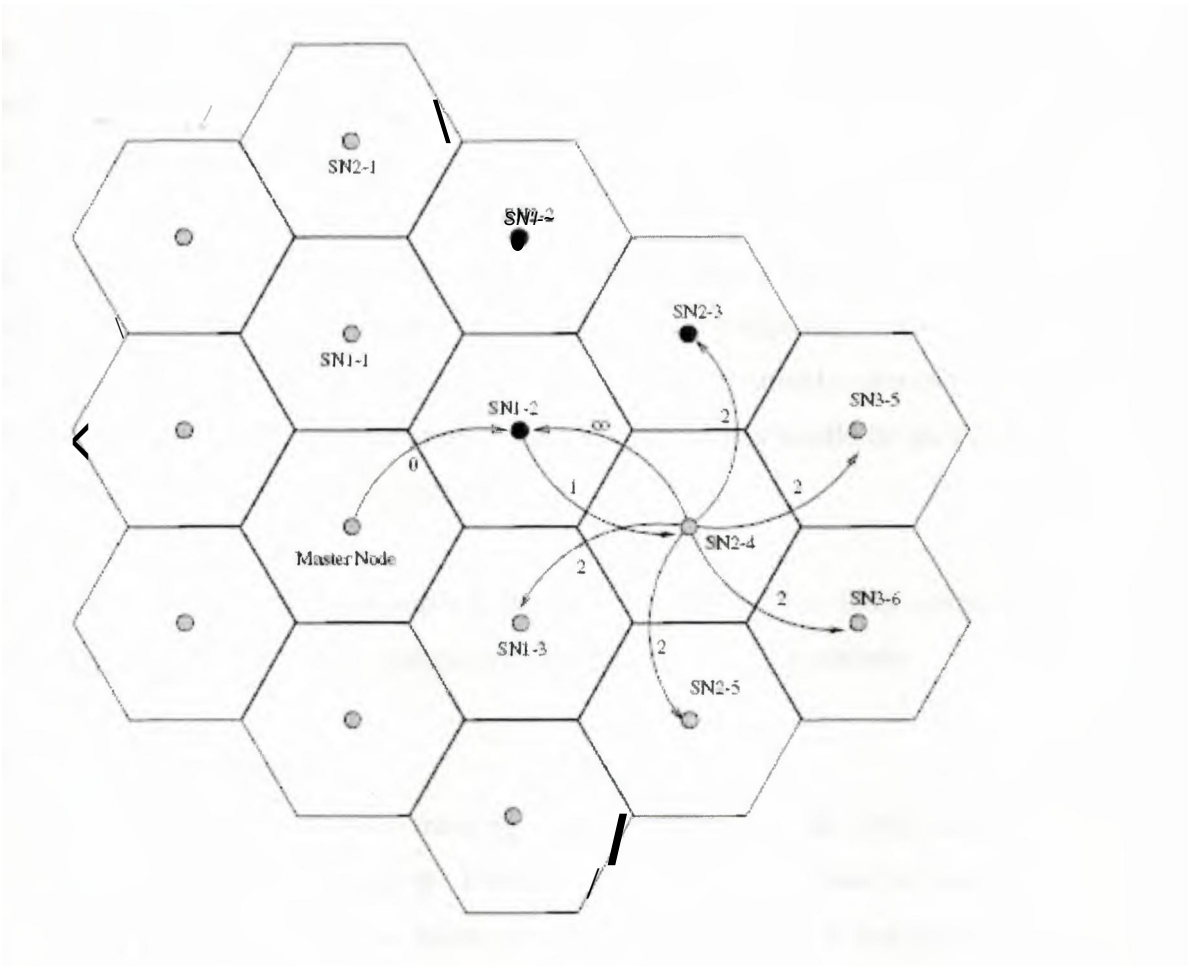

Figure 3.3: BLN configuration.

Table 3.1: SN CACHE EVOLUTION.

Bluetooth addr.	Before inq.		After inq.	
	Detected	New	Detected	New
BD-3	NO	NO	YES	NO
BD-i	NO	NO	NO	NO
BD-JI	NO	NO	NO	NO
BD-'13	NO	NO	YES	NO
B.D-J,	NO	NO	YES	NO
BD-'IU			YES	YES

Remark 1: If a SN has less than seven neighbors within its range, it is possible to ımplement pe91anent links with them (the seven-slave transmission constraint holdsllfhis is valid for hexagonal-tiling, mesh and k-ray 3-cube BLNs.

Remark 2: A simple authentication handshake avoids connection establishment with invalid Bluetooth modems, which are considered invalid badges for simplicity. Typically, invalid badges will answer inquiry cycles with FHS packets, which is relatively harmless.
However, in case they answered with another kind of packet, they would be easily detected by the authentication handshake and rejected.

Remark 3: Badges do not try to establish data connections with SNs. They simply answer inquiries with FHS packets, which does not violate the seven-slave constraint.

3.2.2 BLN location protocol

The main goal of the BLN is user tracking. To meet that goal, all SNs have to send inquiries and collect badge responses. Every SN has a cache where it stores badge addresses. When it detects a response from a badge whose address was not in the cache, it builds a location packet (which fits in a DM-1 packet) with its own address, the badge address (64+64 bits) and an 8-bit control field, and transmits it to the SN on top of its routing table.

For example, Table 3.1 (second and third columns) shows the current SN cache state (BD-X identifies the badge with address X) when the SN is performing an inquiry cycle.

Before the cycle starts, the detected and new columns are unmarked (set to NO).
When a badge detects an inquiry, it answers with a FHS packet. The SN extracts the badge address from the FHS packet and checks it in the cache. If the address is already listed, the corresponding detected column is marked (set to YES). Otherwise, a new row with the address is added and both the detected and new columns are marked with YES.

When the inquiry cycle ends, all marked (YES) new columns are switched to unmarked (NO) state, and location packets for the corresponding entries are transmitted to the master node to report that new badges have entered SN range. All entries with unmarked (NO)

detected column are deleted, and generate location packets to report that the corresponding badges have left SN range.

Location packets carry two Bluetooth addresses: SN address and badge address. The packets have a bit to report if the badge arrives to the cell or leaves it.

It should be understood that the SN that detects a badge is in charge of building location packets. All SNs placed along the transmission path to the master node simply forward them to the SN on top of their routing tables.

The fourth and fifth columns in table I represent a possible SN cache state after an inquiry cycle. A new badge, BD-19, has been detected. Thus, a location packet with BD-19 payload will be sent to the master node. The corresponding new column will be unmarked. Two badges, BD-7 and BD-11, have left the cell. Therefore, two location packets will be sent to the master node with the detected bit set to 0, and the corresponding entries will be removed. Badges BD-3, BD-13 and BD-17 are still around, but do not generate location packets.

Remark 4: SN responses to SN inquiry cycles are ignored by the location protocol, because answering SNs are listed in the routing table of the requesting SN.

Remark 5: Obviously, invalid badges will answer to SN inquiries, and will generate location packets. However, those packets will be filtered by the master node. suggest that, even if a large target area is crowded, the BLN can carry a large number of location packets, valid or invalid.

Moreover, note that, if invalid badges correspond to static devices (such as printers), they will generate only one location packet, because their new column in SN location caches will be unmarked afterwards.

3.2.3 Location zones

The master node (or a service server attached to it) estimates that badge x is placed in a location zone that depends on the SNs that send location packets containing address x.

Room-scale precision may be enough for many context-driven services in the scenarios in section I, while keeping SN complexity reasonably low. So far, we do not take signal strength nor signal delay into consideration. Location precision depends on the number of SNs that detect a given badge, and on the range of their modems. In a hexagonal tiling topology without SN failures, badge position is determined with worst precision if only four SNs detect it. In this case, the estimated location area has 18.12 m2. For example, when only SN2-2, SN2-3, SN3-2 and SN3-3 in Figure 3.4 detect a badge (zone II).

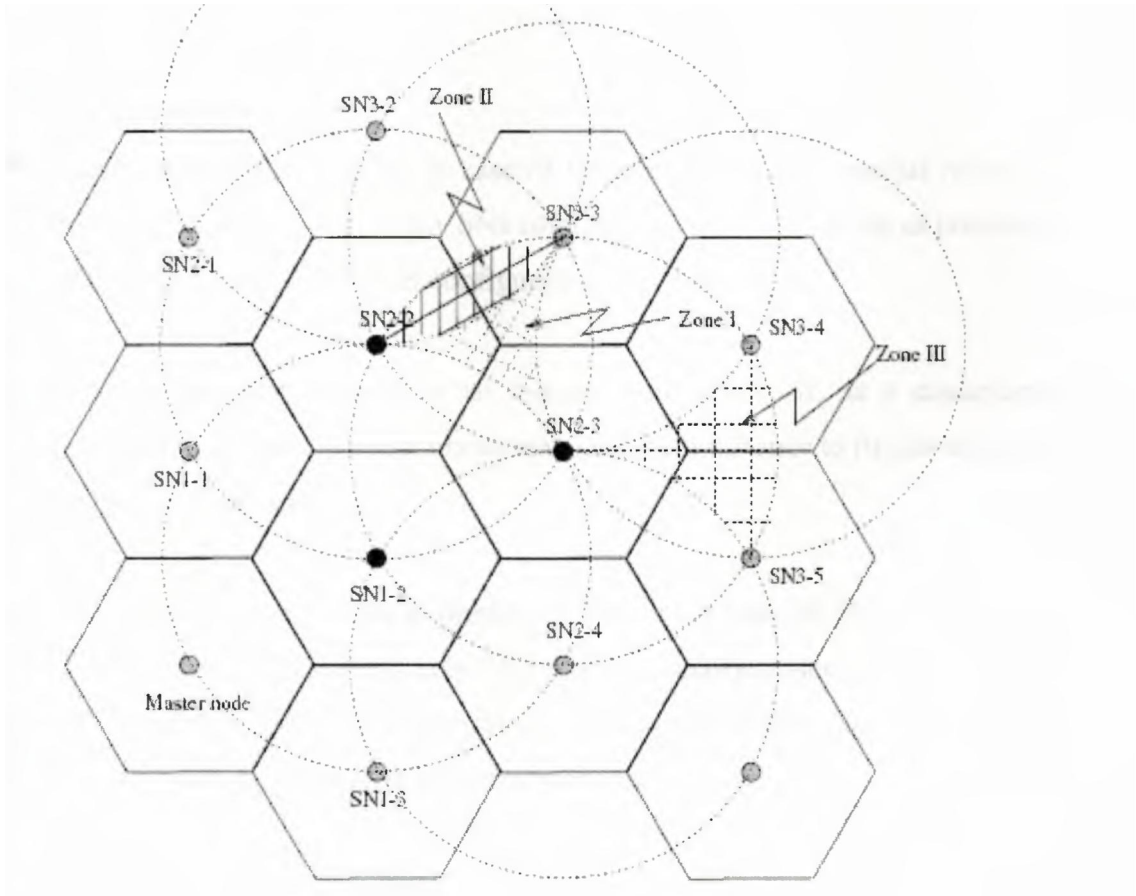

Figure 3.4: Location zones.

Table 3.2: ROUTING TABLE OF SN2-l.

SN2-1 routing table					
Beginning		SN1-2 down		SN1-1 down	
Route	Dist.	Route	Dist.	Route	Dist.
SN1-1	2	SN1-1	2	SN2-12	3
SN2-2	3	SN2-2	3	SN3-18	4
SN2-12	3	SN2-12	3	SN2-2	∞
SN3-18	∞	SN3-18	∞	SN1-1	∞
SN3-1	∞	SN3-1	∞	SN3-1	∞
SN3-2	∞	SN3-2	∞	SN3-2	∞
SN1-6 down		SN1-5 down		SN1-4 down	
Route	Dist.	Route	Dist.	Route	Dist.
SN2-2	5	SN2-2	5	SN2-2	5
SN3-2	6	SN3-2	6	SN3-2	6
SN3-18	6	SN3-18	∞	SN3-18	∞
SN3-1	∞	SN3-1	∞	SN3-1	∞
SN2-12	∞	SN2-12	∞	SN2-12	∞
SN1-1	∞	SN1-1	∞	SN1-1	∞

3.3 Survivability

3.3.1 BLN reconfiguration

BLN detection capabilities survive in case of failures, due to spontaneous reconfiguration when a SN dies, which keeps as many SNs connected to the master node as possible. Survivability is inherent to the BLN configuration protocol.

Suppose SN a does not respond to an inquiry from SN b. If, as a consequence, the minimum distance changes, b transmits its new minimum distance to its slaves, propagating the change to the outer layers.

As an example, table II shows the evolution of the routing table of SN2-1, when all SNs in the first layer but one fails successively. When SNl-3 finally crashes, all SNs in the second layer (and therefore all SNs in higher layers) are isolated. Only after all SNs in the first layer die, SN2-1 will be isolated from the master node.

3.3.2 Badge detection survivability

As SNs crash, it could happen that a badge crosses a region of the target area undetected. We performed different simulations of a three-layer BLN to evaluate survivability of BLN detection capabilities in multiple failure scenarios. Figure 3.5 shows the results, for a

single, two or four symmetrically distributed master nodes. The simulations have a quality of 90 % and a tolerance of 5 %, using the Batch Means Method.
In our simulation, master nodes are protected against failure.
This is certainly realistic, since the whole BLN relies on them.
It is important to mention that, in a real scenario, no more than 5%-10% of the SNs should be ignored if dead (in other words, they are maintained as frequently as light bulbs.

A percentage of over 10% dead SNs means that the target area is simply not properly maintained). Note that, for as many as 10% dead SNs, only 1% of the badges were undetected.

3.3.3 **Isolated** SNs **in** case **of failure**

As another survivability measure, we evaluated the percentage of SNs that must die to isolate a single operational SN (it is impossible to establish a path between that SN and the master node), for a single master node. Figure 6 shows the simulation results. Note that, in the three-layer BLN of the previous example, more than 20% of the SNs should die to isolate a single operational SN.

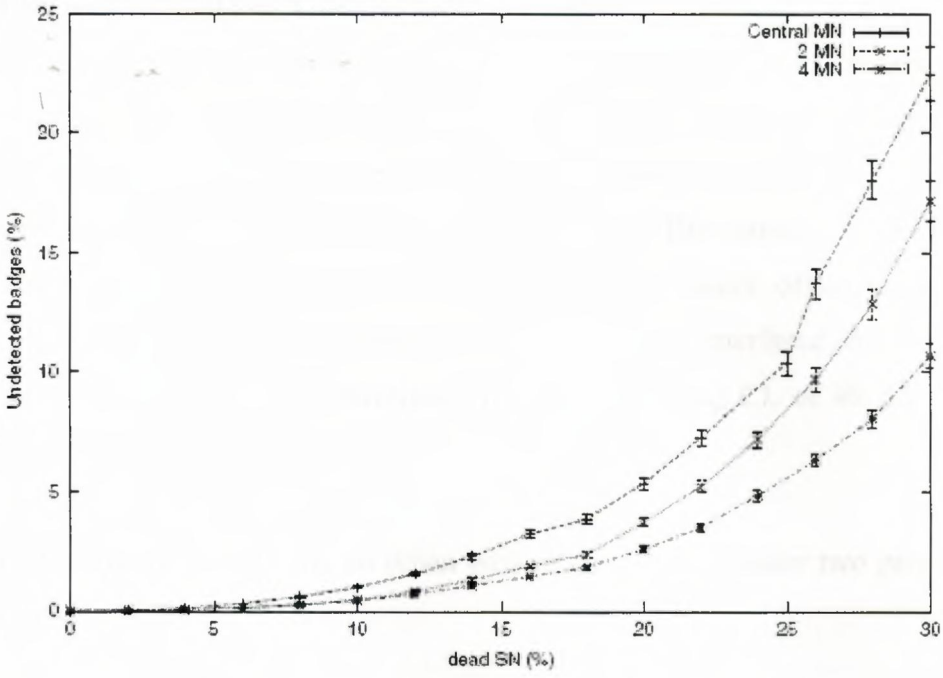

Figure 3.5: Undetected badges.

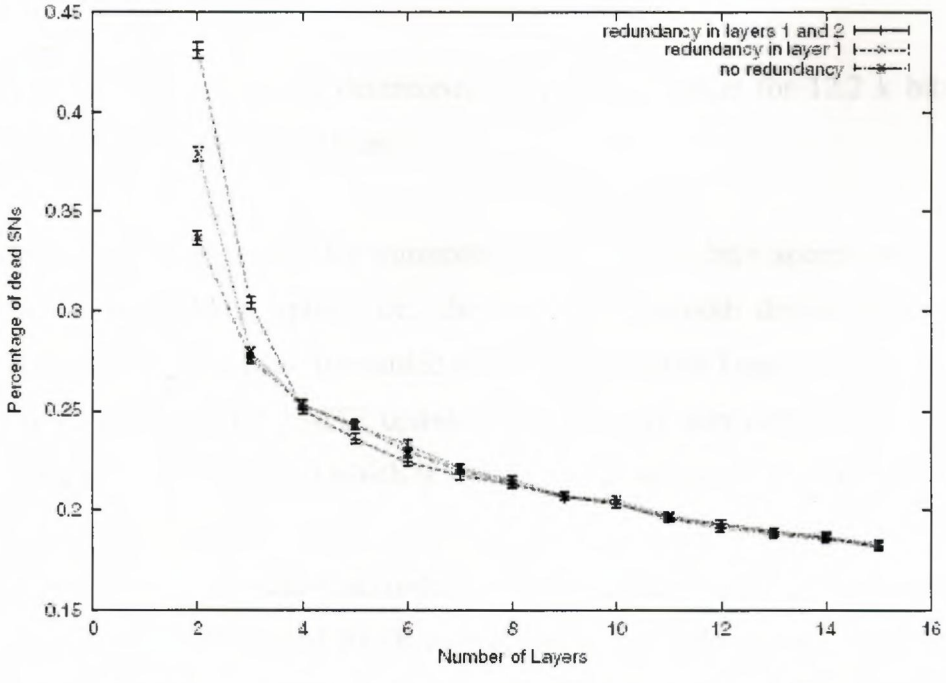

Figure 3.6: Dead SNs to isolate a single operational SN.

3.4 Simulation Setup for Coexistence Analysis

Depending on the position of the mobile station (MS) within the cell coexistence might be strongly affected due to high UMTS blocking power, since we consider interference from the UMTS uplink transmitter into the BT receiver integrated into the same terminal. For this scenario we can assume a coupling loss CL of 20 dB. The external BT device and the cellular UMTS device are assumed to be located in an indoor office environment as depicted in Figure 3.7. Another interesting scenario is an interfered BT receiver at a distance of 1 m from the UMTS terminal, where a decoupling CL of 40 dB due to free space propagation can be assumed.

For the UMTS uplink we assume an urban environment and consider two predefined cell size scenarios:

- Urban I: The basic specification of the cell parameters, where measurements being performed in Paris are discussed with an average UMTS base station (BS) distance of 700 meters and the UMTS planning for the metropolitan area of Paris with a cell radius of R = 0.23 km is described.

- Urban II: The cell size is determined by the link budget for 12.2 k bit/s speech resulting in a cell radius of R = 0.48 km.

Both scenarios will be evaluated for transmission of a 12.2 k bit/s speech or a 64 k bit/s data service for the UMTS uplink, i.e., the external Bluetooth device either transmits speech or data packets which are forwarded to the network after Trans coding in the UMTS mobile. It is assumed that the UMTS uplink is continuously transmitting. For the BT link free space propagation is assumed which is justified for short indoor distances dl.

The UMTS link has been modeled according to the extended Hata propagation model and we have considered a wall loss of 10 dB to account for the indoor scenario. Shadowing is assumed to be spatially correlated among all possible UMTS links with a correlation factor of 0.5. The UMTS uplink is modeled with power control of 1 dB step size and soft handover.

The radio network simulation iterates over a sufficiently high number of snapshots in order to produce statistically stable results for each set of considered parameters. Each snapshot comprises 1000 power control steps, where propagation path loss and randomly generated shadowing remain fixed, while the channel changes according to temporally correlated fading for a velocity of 3 km/h. The MS and BT device shall be 1.5 meters above ground, and the BS height is assumed to be 30 meters.

3.4.1 Cell structure

The cell structure has the common hexagonal form. Each base station has three assigned sectors each of which is covered by a beam of 65 degrees as illustrated in Figure 3.8.

The sectors are arranged such that the main beam of each sector is directed towards the coverage gap of another sector which is depicted in Figure 3.9.

The BT performance has been considered for azimuth angles a from -600 to 0o degrees to represent the whole cell, which is allowed due to the symmetry of the cell layout.

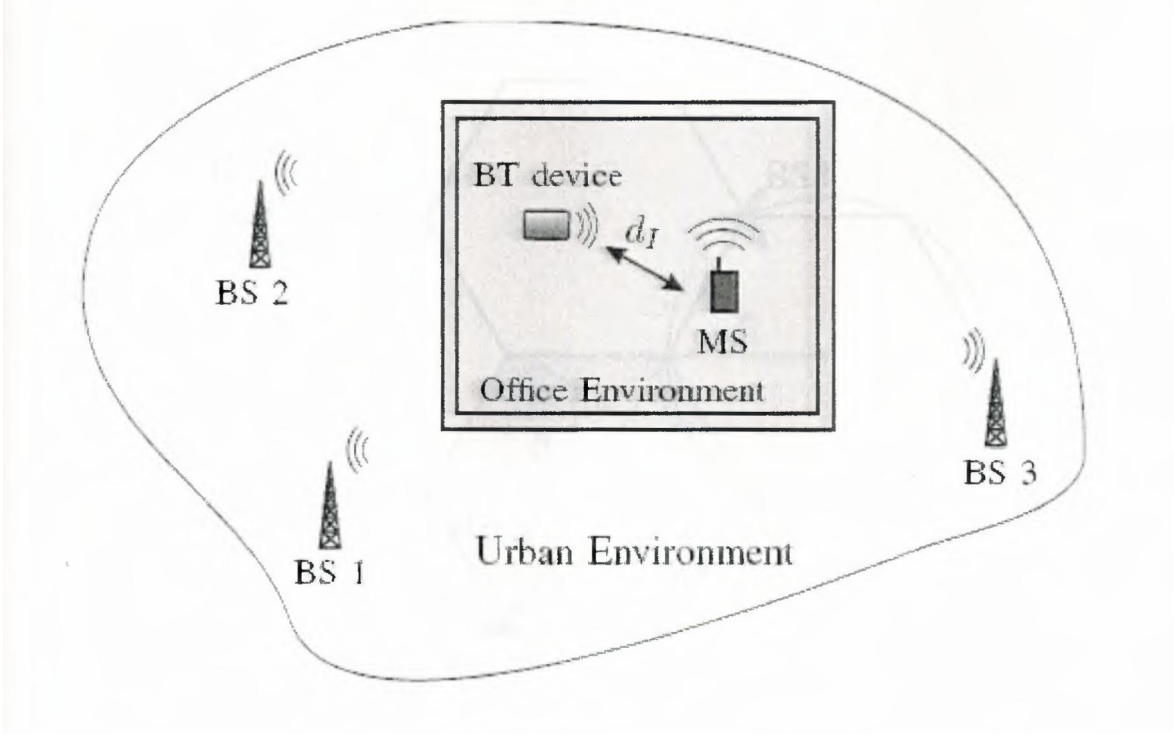

Figure 3.7: Bluetooth and UMTS indoor coexistence in an urban multi-cell scenario.

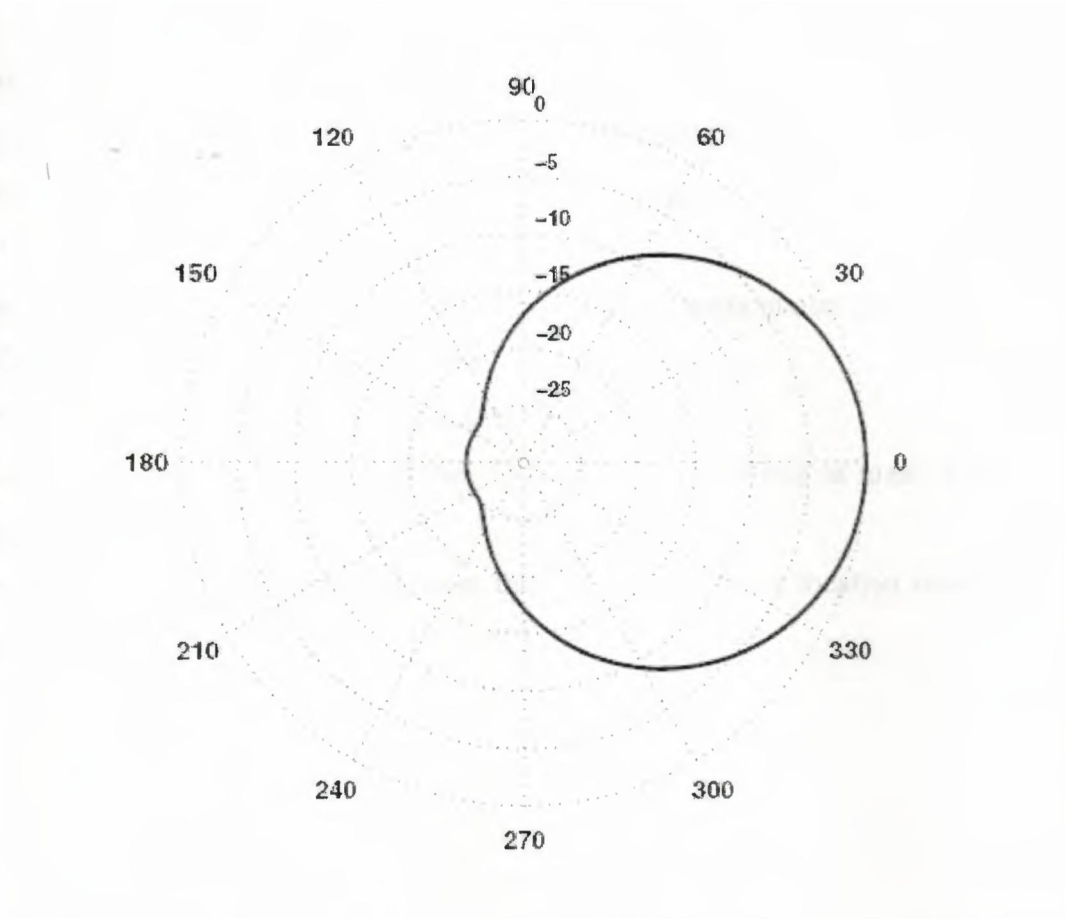

Figure 3.8: UMTS base station: Horizontal antenna pattern depicting the antenna gain in [dB l] normalized to the maximum gain.

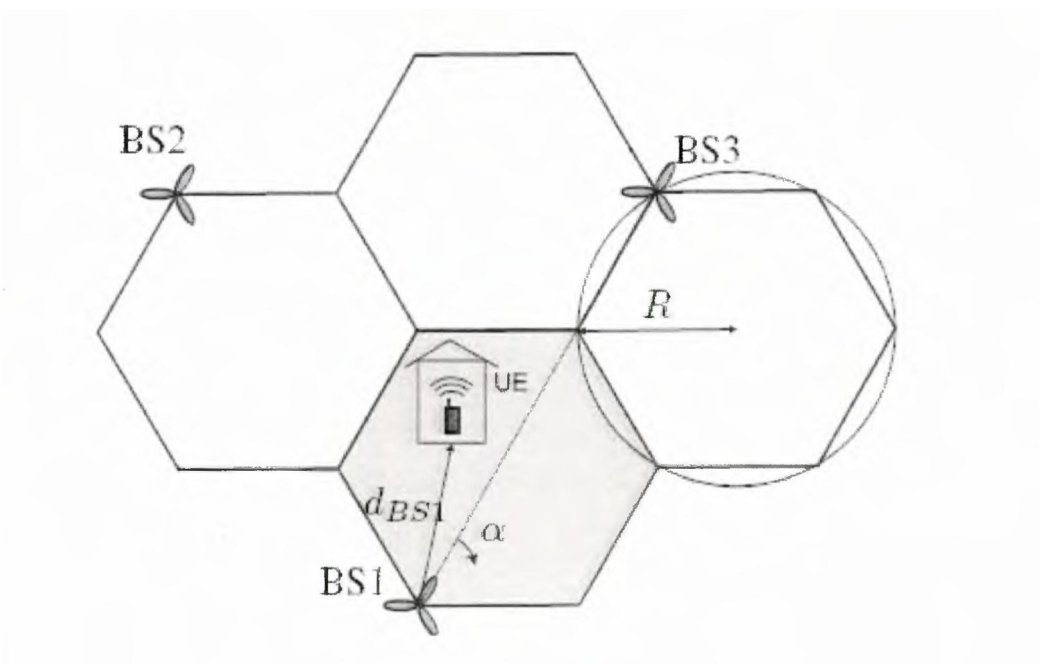

Figure 3.9: UMTS cells with tri-sector antennas.

3.5 **Summary**

We have evaluated survivability in Bluetooth Location Networks for context-driven ervices. These networks have the following characteristics:

- They transmit position information to the service servers without user participation.
- Their RF technology is available in commercial handhelds.
- They can be used as general-purpose data networks.
- The spontaneous topology configuration is scalable, by installing as many master nodes as necessary.
- They can coexist with Bluetooth devices that are not part of the location system, such as printers or headphones.

4. DISTRIBUTED TOPOLOGY CONSTRUCTION OF BLUETOOTH

4.1 Introduction

An ad hoc network is a wireless network formed by nodes that cooperate with each other to forward packets in the network. Almost all experimental ad hoc networks to date have been built on top of single channel, broadcast based 802.11 wireless LANs or IR LANs. In such networks, all nodes within direct communication range of each other share a common channel using a CSMA style MAC protocol. In addition, multi hop routing is used as a means for forwarding packets beyond the communication range of the source's transmitter. Since a single channel is used throughout the network, the topology of the ad hoc network is implicitly (and uniquely) determined by distance relationship among the participating nodes.

This chapter is aimed at addressing a new problem which arises when multiple channels are available for communication in an ad hoc network. The problem is that of determining which subgroup of nodes should share a common channel and which nodes should act as relays and forward traffic from one channel to another. The channel assignment should be done so that all constraints posed by the underlying physical layer are satisfied while ensuring that the resultant graph formed by all nodes is connected.

We address an instance of the above problem which occurs in Bluetooth based ad hoc networks, known as scattemets.

Bluetooth is a promising new technology which is aimed at supporting wireless connectivity among cell phones, headsets, PDAs, digital cameras, and laptop computers. Initially, the technology will be used as a replacement for cables, but in due course chime solutions for point-to-multipoint and multi-hop networking over Bluetooth will evolve.

Bluetooth is a frequency hopping system which defines multiple channels for communication (each channel defined by a different frequency hopping sequence). A group of devices sharing a common channel is called a piconet. Each piconet has a master unit which selects a frequency hopping sequence for the piconet and controls the access to the

channel. Other participants of the group known as slave units are synchronized to the hopping sequence of the piconet master.

Within a piconet, the channel is shared using a slotted time division duplex (TDD) protocol where a master uses a polling style protocol to allocate time-slots to slave nodes. The maximum number of slaves that can simultaneously be active in
a piconet is seven.

Multiple piconets can co-exist in a common area because each piconet uses a different hopping sequence. Piconets can also be interconnected via bridge nodes to form a bigger ad hoc network known as a scatternet. Bridge nodes are capable of timesharing between multiple piconets, receiving data from one piconet and forwarding it to another. There is no restriction on the role a bridge node can play in each piconet it participates in. A bridge can be a master in one piconet and slave in another (termed as M/S bridge) or a slave in all piconets (termed as S/S bridge).

It is possible to organize a given set of Bluetooth devices in many different configurations. Figures 4.lb and 4.lc show two example configurations in which nodes in a Bluetooth network can be arranged. All nodes are assumed to be in radio proximity of each other. Fig. lb shows an example in which all nodes are part of a single piconetl. Figure le illustrates another configuration in which node A is master of piconet 1, node E is master of piconet 3, node B is an M/S bridge (master of piconet 2 and a slave of piconet 1), node D is a slave of piconet 1 and node C is an S/S bridge (slave in piconets 2 and 3). In contrast to the above two configurations the node interconnection topology in a single channel system will be a complete graph
(Fig. 4.la) since all nodes will hear each other's transmission.

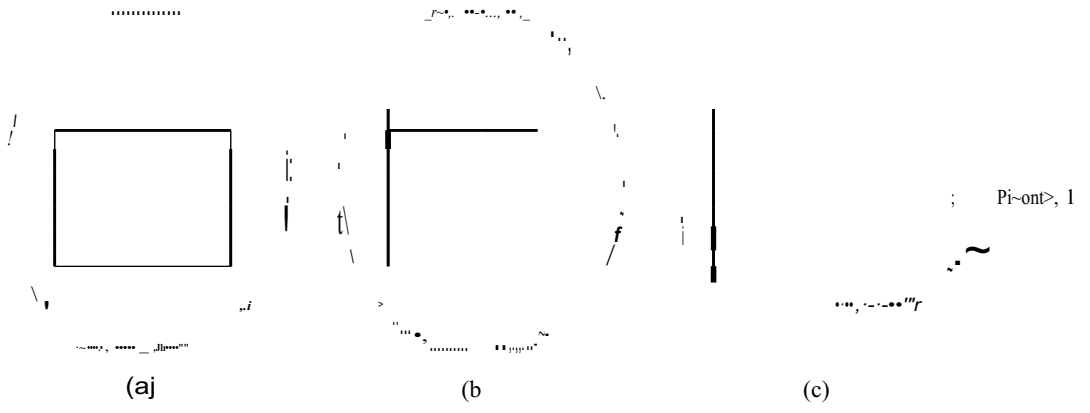

Figure 4.1: (a) Single channel model. (b), (c) Different configurations according to the Bluetooth multiple channel model.

Given a collection of Bluetooth devices, an explicit topology construction protocol is needed for forming piconets, assigning slaves to piconets, and interconnecting them via bridges such that the resulting scatternet is connected. Such a protocol should be asynchronous, totally distributed and nodes should start with no information about their surroundings.

But all the efforts so far were aimed at solving the problem by assuming a single broadcast channel and a CSMA style MAC protocol. The problem is significantly harder for frequency hopping based wireless systems as will be evident in the later discussion.

This chapter attempts to address the topology construction problem in the multiple FH channel setting imposed by the Bluetooth technology. In order to solve it, we design our protocol in a bottom-up fashion:

First, in section 2 we examine the wireless link provided by Bluetooth by presenting the asymmetric "sender-receiver" point to point link establishment protocol as defined in the Bluetooth specifications.

In section 3 we enhance this protocol by proposing a symmetric variant of the link establishment protocol where two devices alternate independently between the "sender" and "receiver" state until they discover and connect to each other. Such a protocol is

necessary for establishing a connection between a pair of identical devices or in situations when any external means for selecting initial device states are not available.

Section 4 introduces the Bluetooth Topology Construction Protocol (BTCP), which is an asynchronous distributed connection establishment protocol that extends the point to point symmetric protocol to the case of many nodes. This protocol is based on a leader election process where each node uses a timeout to independently decide about the leader election termination.

The timeout delay factor introduces a correctness-delay tradeoff of the network formation. By using the delay analysis of section 3 we show in section 5 how to best choose the protocol parameters in order to maximize the probability of forming a connected scatternet while minimizing delays.

4.2 Link Establishment in Bluetooth: Background

The Bluetooth Baseband Specification defines the Bluetooth point to point connection establishment as a two step procedure. First neighborhood information is collected through the Inquiry Procedure. The Paging procedure is subsequently used to establish the connections between neighboring devices. Both the Inquiry and Paging procedures are asymmetric processes; they involve two types of nodes (which we call senders and receivers) each performing different actions. During Inquiry, "senders" discover and collect neighborhood information provided by "receivers". During Paging, "senders" connect to "receivers" discovered during a previous inquiry procedure.

During the inquiry or paging procedure, although senders and receivers use the same (inquiry or paging) frequency hopping sequence2, it is likely that they will be out of phase since each unit starts at a different hop frequency derived from its local clock value. This (unavoidable) phase difference introduces a phase uncertainty among the devices participating in the procedure. To overcome this phase uncertainty, senders and receivers hop at different speeds. A receiver hops at a slow rate over the common frequency pattern listening on each hop for sender messages and the sender transmits at a much higher rate listening in between transmissions for an answer, in hope of discovering the frequency a

receiver is currently listening to. Given two units, one operating as a sender and the other as a receiver, the term Frequency Synchronization delay (or FS delay) refers to the time until the sender transmits at the frequency the receiver is currently listening on3.

Even if the two procedures have the same synchronization mechanism, a difference is that during the paging procedure the sender tries to bypass the FS delay by estimating the phase of the receiver. If paging is performed directly after the Inquiry procedure, the sender has acquired the clock value of the receiver unit and can use it to determine its phase and connect to it instantaneously.

The functional difference between the Inquiry and Paging Procedures lies in the use of a universal FH sequence in the first and a common point to point FH sequence in the second.

Using a universal inquiry hopping sequence, a sender node effectively "broadcasts" an Inquiry Access Code (IAC) packet that can be heard only by receiver nodes that listen for such a packet. During the paging procedure, by using the receiver's page hopping sequence a sender node initiates connection establishment by effectively "unicasting" a Device Access Code (DAC) packet that can be heard only by the corresponding receiver device. Thus the Inquiry Procedure involves many units, where a sender can discover more than one receiver while the paging procedure involves only two units, where a sender pages and connects to a specific receiver.

4.2.1 The Bluetooth Asymmetric protocol for link formation

According to the Bluetooth Baseband specification the protocol starts by the sender starting in the INQUIRY state and the receiver in the INQUIRY SCAN state. As was described in the previous section there is an initial FS delay until the sender hits the frequency the receiver is listening to. Upon receiving the IAC packet, the receiver backs off for an amount of time that is uniformly distributed between 0 and 639.375ms. This happens in order to prevent the contention problem that would arise if there were two receivers listening on the same hop frequency. If both of them responded immediately, the response message would get garbled and the sender would not receive it. We call the time while the receiver backs off the Random Backoff delay (or RB delay). When the receiver unit wakes up, it starts listening again at the hop it was listening to before backing off. After a second

FS delay (same as the first one), a second IAC packet is received from the sender. Then the receiver sends back to the sender an FHS packet that contains:

1. The receiver's address: This is used by the sender to derive the DAC of the receiver and the page hopping sequence it will use later in order to page the receiver.

2. The receiver's clock value: This is used to estimate the phase of the receiver and thus eliminate the FS delay during the paging procedure that follows.

The timing diagram in Figure 4.2 summarizes the point to point connection establishment procedure between the two units. The dashed arrows denote events on each unit's timeline and each event is numbered in the order it happens during the connection establishment procedure. The timing diagram shows that the receiver enters the PAGE SCAN state after sending the inquiry response FHS packet to the sender.

When the sender receives the FHS packet, it enters the PAGE state and uses the clock information in the FHS packet to send a DAC packet on the frequency the receiver is listening to in the PAGE SCAN state. Then the receiver responds immediately with a DAC packet and the sender sends an FHS packet to the receiver. The receiver uses the FHS information to determine the channel hopping sequence and the phase of the sender and becomes the slave of the point to point connection. It then acknowledges the FHS packet with another DAC packet. As soon as the sender receives the acknowledgment, it becomes the master of the connection and may start exchanging data with the synchronized receiver-slave.

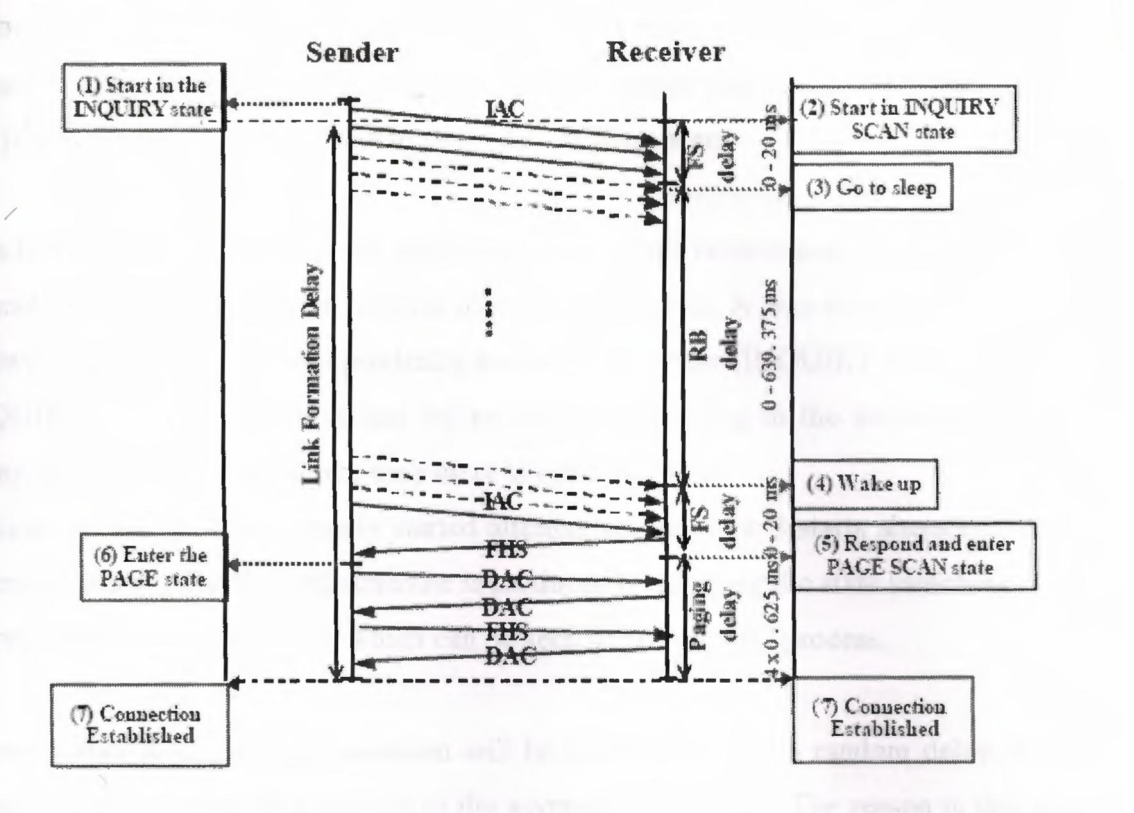

Figure 4.2: The Bluetooth asymmetric link formation protocol.

By observing Figure 4.2, we can easily identify the link formation delay components. The inquiry procedure delay consists of a first FS delay, the RB delay and a second FS delay that is taking place when the receiver waits for the second IAC packet after it wakes up. The paging procedure delay is negligible since it immediately follows the inquiry procedure. (As soon as the first DAC packet is received by the receiver the rest of the steps are happening in consecutive 625ms slots). Thus we can approximate the link formation delay R using the following equation:

$$R=2FS+RB \quad (4.1)$$

4.3 A Symmetric Protocol for Link Formation

The asymmetric protocol provided by the Bluetooth specification, yields a very short connection establishment delay provided that the sender and receiver roles are reassigned.

When two or more users are trying to establish links between their Bluetooth devices in an ad hoc fashion, they will not be able to explicitly assign sender and receiver roles. They will just press a button and expect to connect with their peers.

Thus there should be a symmetric mechanism that forms connections in an ad hoc fashion without any explicit sender or receiver role pre-assignment. A way to do this is by forcing the two nodes to alternate independently between the sender (INQUIRY state) and receiver (INQUIRY SCAN state) roles and try to connect according to the asymmetric protocol during an overlap interval where they meet in opposite states.
In Figure 4.3, Unit A has already started alternating, and Unit B starts alternating at some arbitrary time 0 t. The merged schedule is produced by merging the state switching times of the two units into a single one, which can be seen as an "on, off' process.

By using state alteration, a connection will be established after a random delay, which in principle will be larger than the one of the asymmetric protocol. The reason is that starting at each "on" interval of the merged process, the two units will connect after a random interval R = 2FS + RB, given that they both remain fixed at their (complementary) states for an amount of time greater than R. Otherwise, they have to wait for the next "on" interval. The time Tc from time 0 t up to the point where the two units come to a complementary state for a sufficient amount of time is essentially the link formation delay between the two units.

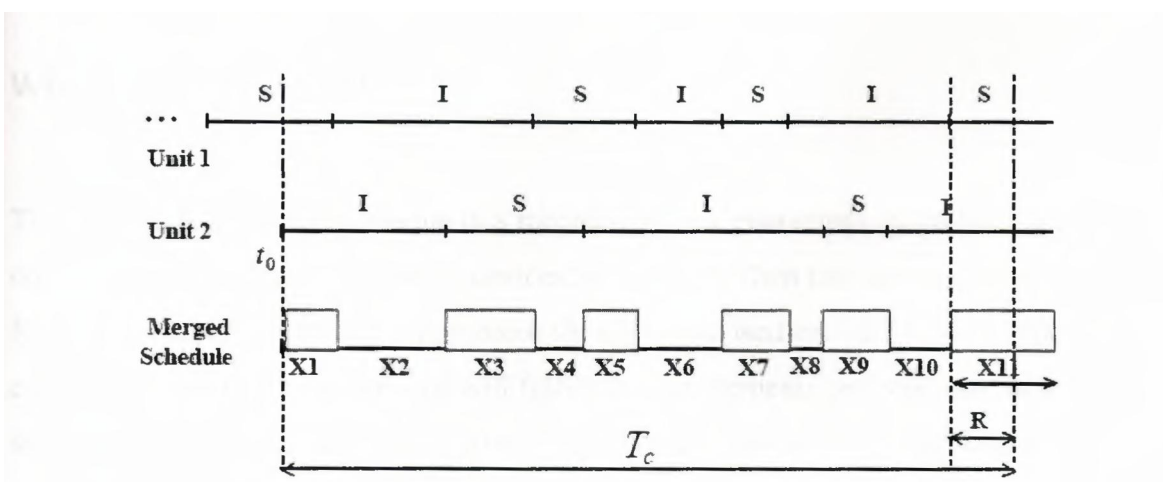

Figure 4.3: A symmetric link formation protocol: Nodes alternate between sender and receiver state until they connect.

There are some interesting questions arising from the proposed "alternating states" technique. First of all what should the alternating schedule be? Should the states alternate in a periodic or random fashion? It can be analytically proven that the mean connection time is infinite when each unit changes states deterministically. Intuitively, if the state residence intervals are fixed, the intervals of the merged process in Figure 4.3 will be fixed as well. Then the connection time will depend on the fixed phase difference of the two devices. If this phase is very small, then the "on" intervals in the merged process will be very small and the link formation delay very large since the units will use arbitrarily many "on" intervals until they finally connect.
Alternatively, a random schedule can be imposed on the state residence times.

The way to calculate the connection set up delay is to determine the cdf and pdf of the merged schedule process X given that the two nodes alternate independently according to an identical distribution Z. The mean and variance of the link formation delay of the symmetric protocol are given by:

$$E[T] = \frac{E[X]}{2} + \frac{(E\{XfR>X\} + E[X])(1-P)}{P} + E[R] \quad (4.2)$$

$$Var[T] = \frac{Var[X]}{2} + \frac{(Var[XIR>X] + Var[X])(1-P)}{p} + Var[R] \quad (4.3)$$

$$\text{Where } p = P[R < X] \quad (4.4)$$

The "alternating states" technique is a mechanism that guarantees an ad hoc point to point connection between two Bluetooth devices. When more than two devices exist and wish to form a scatternet "on the fly", a protocol should be devised on top of this mechanism, that ensures that the resulting network will fulfill the requirements and structure of a Bluetooth scatternet. This protocol should also be efficient in terms of network establishment delay.

4.4 BTCP: A Distributed Scatternet Formation Protocol

Our motivation for the scattemet formation problem arises from a "conference-scenario" of an ad hoc network establishment. Suppose that there are many users in a room that wish to form an ad hoc network using their Bluetooth enabled devices. Each user presses a "start" button and waits for the device to show on the screen a "network connection established" message after a short period of time. After this message appears, the user will be able to exchange information with any other user in the room. The description of this application actually contains the elements of a successful connection establishment protocol:

- Network connection establishment should be performed in a totally distributed fashion. This means that each device starts operating asynchronously on its own and it initially does not have any knowledge about the identities or number of nodes in the room.
- After completion, the protocol must guarantee a connected scattemet. "Connected" means that there should be at least one path between any two nodes in the network.

- The network set up delay should be minimized such that it is tolerable by the end user.

In general there are no restrictions regarding the final form of the scattemet. The only requirements are that:

- There should be piconets that have one master and less than seven slaves and that piconets are interconnected through S/S or M/S bridge nodes.

- Every node must be able to reach every other node in the resulting network i.e. the network must be connected.

In addition to satisfying connectivity, a desirable feature of the protocol would be to be able to shape the network topology according to scattemet formation criteria imposed by specific applications. For example the same node may need to have different roles in different applications. Also it may be possible for a node to have more restrictive degree constraints than seven due to its own nature as a device; for example a palm pilot would not

have the processing power to be a master of a seven slave piconet. Scatternet formation criteria could also be in the form of traffic demands that need to be satisfied by the nodes participating in the network construction process. These criteria should be taken into \Ccount during the topology construction process if they exist. The problem of defining scatternet forrmation criteria is itself an open research issue that is heavily dependent on the envisioned applications.
Although we do not address it in this paper, our approach takes it into account by collecting information about all nodes participating in the process at a single point before actual connection happens.

BTCP is based on a leader election process. Leader election is generally an important tool for breaking symmetry in a distributed system. Since the nodes start asynchronously and without any knowledge of the total number of participating nodes in the network construction process, an elected coordinator will be able to control the network formation and ensure that the resulting topology will satisfy the connectivity requirements of a Bluetooth scatternet.

In the absence of any scatternet formation criteria, and in order to design a simpler and faster protocol, we propose and justify the following default properties that the resulting network will satisfy:

1. A bridge node may connect only two piconets. (Bridge degree constraint): A bridge node forwards data from one piconet to another by switching between them in a time division manner. Given that each portable device may have limited processing capabilities, a maximum bridge degree of two relieves a node of being an overloaded crossroad of multiply originated data transfers.

2. Given the number of nodes N, the resulting scatternet should consist of the minimum number of piconets possible. The impact of this is similar to the motivation of solving the problem in [6] of finding the minimum number of routers in an ad hoc network. A minimum number of piconets yield an easier network to control.

3. The resulting scatternet should be fully connected. This means that every master will be connected to all other masters through bridge nodes. Scatternets are expected to change and be reformed over time. A fully connected scatternet in its initial state provides higher robustness against topology changes. Also no routing is needed in this original state since every master can reach every other master through a bridge node and every slave can reach everybody else through its own master.

4. Two piconets share only one bridge (Piconet overlap constraint). This condition is used in order to provide a means of terminating easily the connection establishment protocol and calculating the minimum number of piconets. If two masters later wish to share another bridge between them they can do so by means of a bridge negotiation protocol.
The protocol consists of three phases:

Phase I: Coordinator Election During this phase, there is an asynchronous, distributed election of a coordinator node that will eventually know the count, identities and clocks of all the nodes participating in the network construction process.

Each node x has a variable called VOTES which is set to 1 as soon as the node is powered up. After initialization, the node starts alternating between the INQUIRY and INQUIRY SCAN state.

Any two nodes x and y that discover each other will form a point to point connection, enter a "one-to-one confrontation" and compare their VOTES variables. The node with the larger variable is the winner of the confrontation. If the two nodes have equal VOTES variables the winner is the node with the larger Bluetooth address.

Without loss of generality, suppose that xis the winner and y is the loser. The loser y sends all the device FHS packets of the nodes it has won so far to the winner x, it tears down the connection and enters the PAGE SCAN state. In this way it will not be able to hear inquiry messages any more but only page messages from nodes that will page it in the future. This action has the effect of eliminating the loser from the coordinator election process and preparing it for the next phases of the protocol.

The winner x increases its VOTES variable by VOTES(y) and continues on the leader election process by resuming alternating between INQUIRY and INQUIRY SCAN.

If there are N nodes participating in the scatternet formation, there will be N-1 one-to-one confrontations. The winner of the N-lst confrontation will be the coordinator node and the rest of the nodes will be in the PAGE SCAN state waiting to be paged by a node that has information about them.

Phase II: Role Determination The coordinator that was elected during phase I, has the FHS packets (i.e. identities+ clocks) of all the nodes and hence knows the total number of nodes N that participate in the network connection establishment.

At the start of phase II, the coordinator checks if the number of nodes that it has discovered during Phase I is less than eight. If this is the case, it pages and connects to all of the nodes in PAGE SCAN and one piconet is formed with the coordinator as the master and all the other nodes as its slaves.

In this special case the protocol terminates at this point. If the number of nodes is greater than seven then more than one piconet must be formed and interconnected via bridge nodes. Given the global view of the network the coordinator can decide on the role that each node will perform in the final scatternet. If the participating nodes impose specific scatternet formation criteria, they can be communicated to the coordinator during the election process in addition to the FHS information, and can aid it in determining the roles of the nodes in the final scatternet. By using the default criteria cited at the start of this section the coordinator first calculates the number of piconets P.
The minimum number of masters P in order for the resulting scatternet to be fully connected can be calculated by the following relation:

$$p = \left\lceil \frac{17-\sqrt{289-8N}}{2} \right\rceil, \quad 1 \le N \le 36 \tag{4.5}$$

As we observe from the above relation, the default scheme works for a number of nodes less than or equal to 36 due to the desired properties 2-4 described at the beginning of this section. A larger number of nodes may lead to a default scheme that does not require a fully connected scattemet.

After calculating P, the coordinator selects itself and P-1 nodes to be the designated masters and iP'(~-lJ other nodes to be the scattemet bridges. Consequently, the coordinator equally distributes to the designated masters the remaining nodes to be their "pure" slaves.

After the role assignment, for each master x (including itself), the coordinator has a connectivity list set (SLAVESLIST(x), BRIDGELIST(x)) consisting of the master's assigned slaves and bridges. Each entry of these lists contains FHS packets (identities + clocks) so that the designated master can later page its connectivity list set instantaneously.

Then the coordinator connects to the designated masters it selected by paging them. (Recall that at the end of phase I all remaining nodes were in the PAGE SCAN state). Thus a temporary piconet is formed instantly with the coordinator as the "master" and the designated masters as the "slaves".

The coordinator transmits to each designated master its connectivity list set, instructs the designated master to start phase III, and consequently tears down the temporary piconet and starts phase III as a master node itself.

Phase III: The actual connection establishment, during this phase, each master x pages and connects to the slaves and bridges defined in its SLAVESLIST(x) and BRIDGELIST(x) respectively.

As soon as a node is notified by its master that it is a bridge, it waits to be paged by its second master. When this happens, the bridge node sends a CONNECTED notification to both masters.

When a master receives a CONNECTED notification from all its assigned bridges, a fully connected scattemet of P piconets is guaranteed to be formed and the protocol terminates.

It is evident that the most time consuming part of the protocol is the leader election phase. Phase II and Phase III involve only paging and connecting which is happening almost instantaneously due to the previous discovery phase.
The tricky part of the protocol is actually the phase I termination. Ideally it should stop as soon as the coordinator is found. But how does a node know that it is the final winner of the election process? All nodes have a "state alternation" timeout period ALT_TIMEOUT that is set once a node is powered up and reset each time it wins a "one to one confrontation".

When ALT_TIMEOUT expires, the node assumes it is the elected coordinator and that all other nodes are in the PAGE SCAN state waiting to be paged.

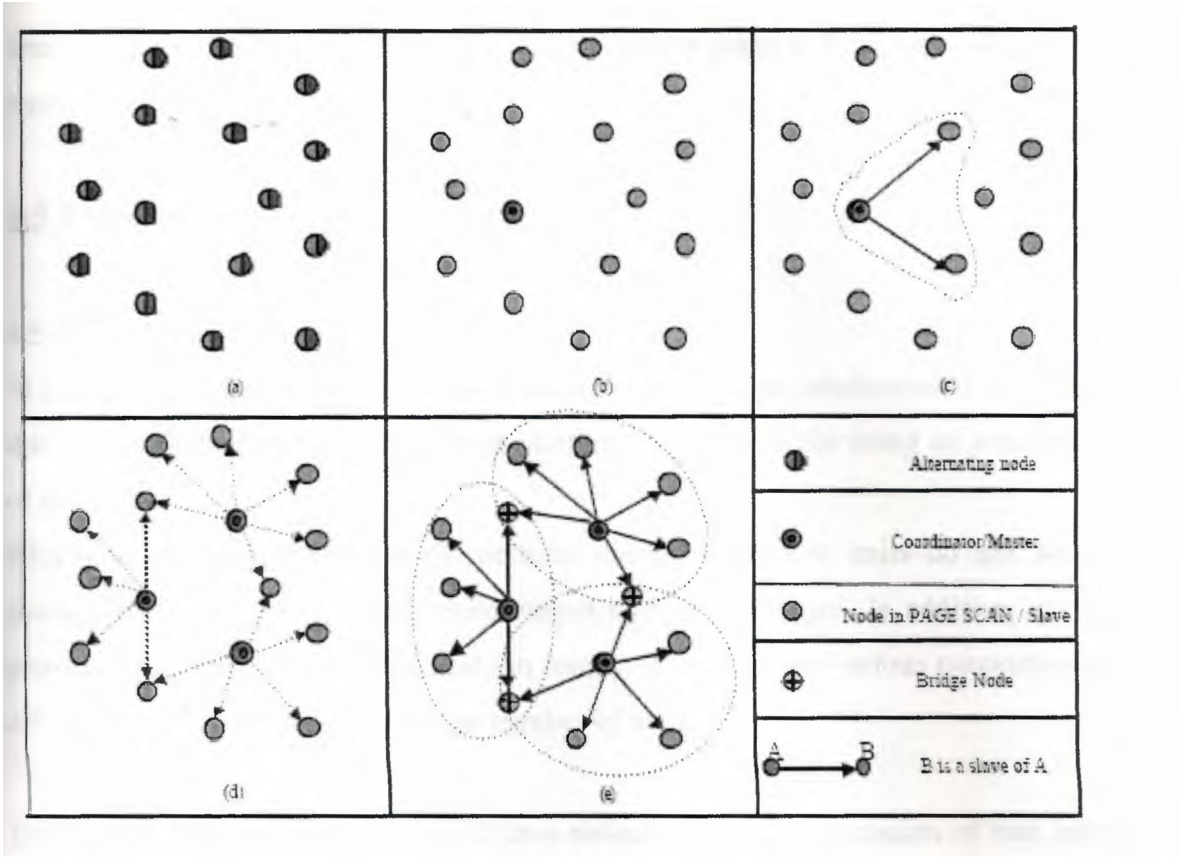

Figure 4.4: The connection establishment protocol for a set ofN=16 nodes. (a) Start of Phase I: All nodes start alternating trying to discover their neighborhood. (b) At the end of phase I the coordinator has been elected. Since N=16 the coordinator computes P=3 and selects the masters, bridges and slaves accordingly (c) Phase II: Coordinator forms a temporary piconet with the designated masters and sends them their connectivity lists. (d) Phase III: Each master pages the nodes specified within its connectivity list. (e) Final scatternet formation.

The question that is raised now is "what is a good value for ALT_TIMEOUT"? A very large value will result in a node having won the competition and continuing alternating without knowing it is the only one left. This will result in a very slow phase I (and hence a very slow connection establishment protocol). On the other hand a very small timeout value may result in a case where more than one nodes assume they are the coordinator and hence a protocol that will result in a disconnected scatternet.

We address the above problem by making the following observation. When there are N nodes alternating and trying to discover and connect to each other, the time for the first

connection to happen is generally less than the time it takes if there were only two of them trying to connect.

4.5 Experiments

4.5.1 Emulating Bluetooth

We have implemented BTCP on top of an existing prototype implementation that emulates the Bluetooth environment on a Linux platform. The reason for using an emulator instead of the
Bluetooth devices themselves are because current Bluetooth units do not support the piconet switching function and hence cannot operate as bridges. In addition, an emulator provides a higher degree of flexibility in testing the system for various parameters and can afford testing the protocol for a large number of nodes.

Each Bluetooth host is implemented as a process that mainly consists of two interacting modules. The Bluetooth Baseband (BB) module emulates in software the Inquiry, Paging and piconet switching procedures as defined in the Bluetooth Baseband specification. The BTCP module interacts with the BB module through the HCI control specification functions as.

The use of HCI functions allows us to later replace the Bluetooth software module with a hardware module, when the bridging capabilities become available in hardware.

The wireless medium is simulated by an Nf -hop channel process which is used for the exchange of IAC and FHS packets during the inquiry and paging procedures. The Nf-hop channel process also determines the frequency hopping collisions that are happening between the devices and emulates the FS delays. Note that this channel process is not similar to a CSMA channel since the senders or receivers cannot perform carrier sensing or any kind of intelligent back off.

We also assume that all the devices are within range of each other. This is a logical assumption for networking many short range wireless devices in a single room. This fact is

mapped in our architecture by having all Bluetooth host processes initially connected to the Nf -hop wireless channel process and executing the topology construction protocol.

4.5.2 Determining ALT_TIMEOUT

Using the Periodic Inquiry Mode HCI command, it is possible to program Bluetooth units to alternate between INQUIRY and INQUIRY SCAN states with uniformly distributed state residence times. In this case the cdf of the merged process X (see Figure 4.3) when each unit has state residence times uniformly distributed in [0, b] is:

$$F_x(X) = P[X \le x] = \frac{1}{b^3}x^3 - \frac{3}{b^2}x^2 + \frac{3}{b}x, \quad 0 \le x \le b \tag{4.6}$$

By using (4) and (1) in (2.1), (2.2), (2.3) we can calculate analytical expressions for the mean and variance of the link formation time Tc of the symmetric protocol.
Given (2.1) and (2.2), we choose ALT_TIMEOUT according to the empirical relation:

$$ALT\_TIMEOUT = E[Tc] + Var[Tc] + rm.a.x \tag{4.7}$$

Figure 4.5 shows the mean connection establishment time and the standard deviation in the connection establishment time in the point to point case when the state residence times are uniformly distributed. We observe that for every alternating mean state residence time the resulting standard deviation is almost equal to the mean connection time. This means that the link formation time distribution is not centered around the mean. This justifies the inclusion of the $Var(Tc)$ term in our empirical formula.

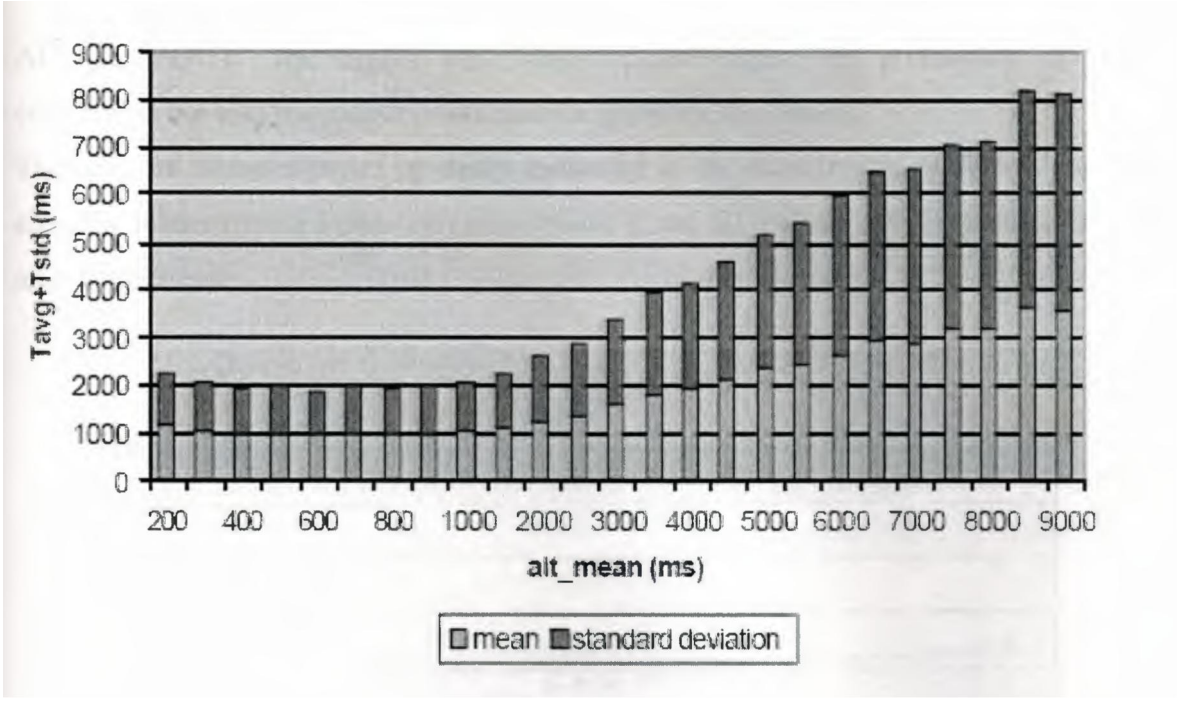

Figure 4.5: Means and standard deviation delays for the point to point connection establishment time where nodes alternate with state residence times according to a uniform distribution.

The term rmax was more subtle and was determined only after performing experiments and observing the protocol behavior on many runs. It seems like the following case was happening very frequently: After the N-2nd confrontation the winner A would start alternating by resetting ALT_TIMEOUT while there was one node Bin SLEEP mode (and all the rest in PAGE SCAN).

The two nodes A and B would start trying to form the N-lst connection only after node B woke up! The additional term rmax is the upper limit for the back off interval and thus eliminates the concern about this case.

In our experiments we choose a mean state residence time of 600ms which according to equation (5) and Figure 4.5 yields the smallest ALT_TIMEOUT value of2527.223ms.

4.5.3 Protocol Performance

The performance metrics associated with the protocol are the network connection set up delay and the probability of protocol correctness which depends on the value of

ALT_TIMEOUT. The higher this value is, the higher the probability of protocol correctness but also the longer it will take the network to connect.

The network connection set up delay measured in the experiments is always the time to elect the leader (phase I duration) since phase II and III include only instantaneous paging and connections.

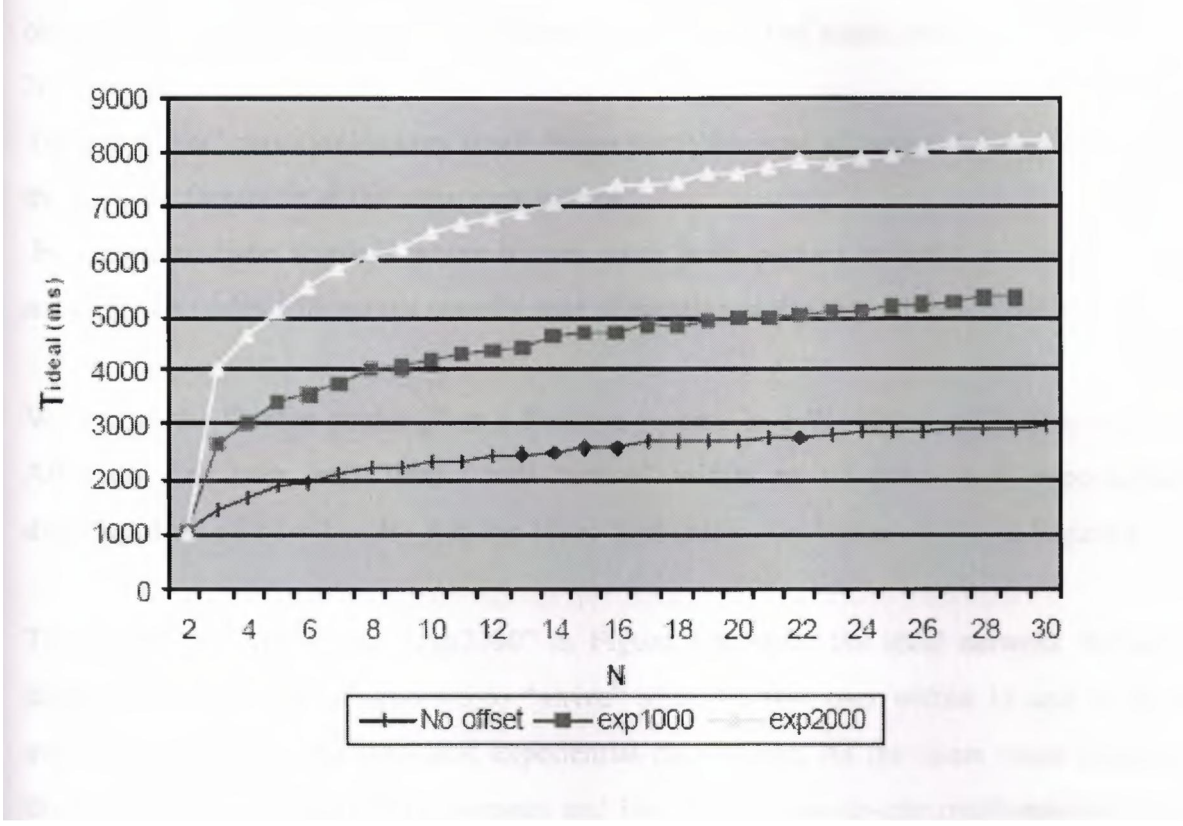

Figure 4.6: Average ideal connection establishment time for various application scenarios. Units alternate according to uniformly distributed state residence times with mean lOOOms.

The "no offset" curve in Figure 4.6, shows the mean network connection establishment delay Tideal when all nodes start alternating at the same time t0. By "ideal" we mean the time where the coordinator is actually elected. The node itself will assume it is the coordinator when its timer expires after time ALT_TIMEOUT. Thus the actual network connection time Tactual will be:

$$T_{actual} = T_{ideal} + ALT\_TIMEOUT \quad (4.8)$$

The curve shows a delay that is increasing slowly with the number of nodes that participate in the network formation. The reason is that there are many one-to-one confrontations occurring in parallel until the coordinator is elected. This is actually a desirable asset of a network establishment protocol.

We wouldn't for example like the delay increasing linearly with the number of nodes. We observe that the delay ranges from 1sec to 3sec for a set of nodes that span from N=2 to N=30.

The "no offset" curve yields very small delays partly because all nodes start participating in the network formation at the same time instant.

In a more realistic scenario where human users push buttons in order to connect to the network, the nodes will not necessarily start alternating at the same time.

We model the "button pushing" as a Poisson process in a W=l 0sec application window. After the first user, each user I will "arrive" within an iid (truncated) exponentially distributed time *Li, i* = l ... *N* - l in the 10sec application window as shown in Figure 4.7.

The graphs "exp 1000" and "exp2000" in Figure 4.6, show the ideal network formation delay when each user is expected to "arrive" after the first user within 1s and 2s in the average according to the truncated exponential distribution. As the mean value increases, the system becomes more asynchronous and less parallel one-to-one confrontations occur at each time instant. This has an effect of increasing the delay of connection establishment. Nevertheless, the protocol's immunity to the increase of N is preserved. This is illustrated by a constant delay offset between the curves for the same number ofN.

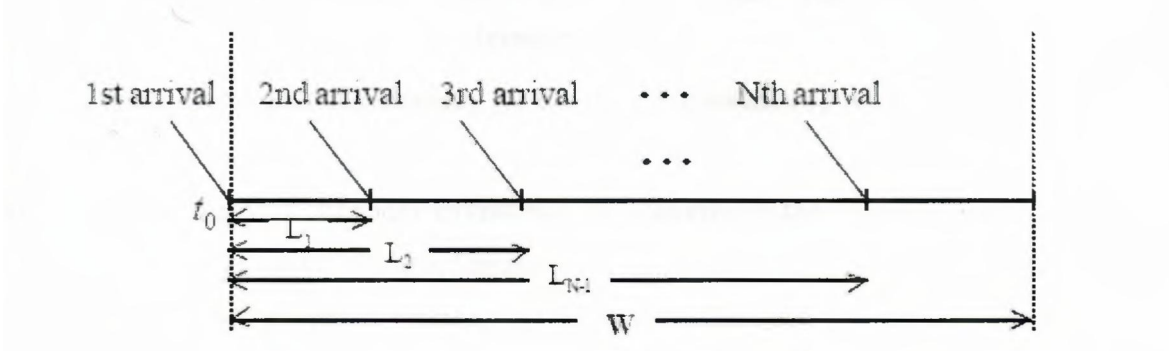

Figure 4.7: The "push button" arrival process.

The timeout may be viewed as a penalty that has to be paid in order to have a distributed algorithm. A large ALT_TIMEOUT value will satisfy the "correctness" condition with higher probability (higher "timeout efficiency") but will accumulate a larger extra overhead in.the actual network connection time Tactual.

Figure 4.8 illustrates this trade-off by demonstrating the timeout efficiency as a function of different candidate values of ALT_TIMEOUT. For all application scenarios, the timeout efficiency initially increases rapidly as a function of the timeout and then reaches a steady state. It is clear that the value of ALT_TIMEOUT where the curves start stabilizing is at 2500ms which is very close to the value 2527.223ms chosen by our empirical formula (5).

The combination of Figures 4.6 and 4.8 provide practical guidelines to the designer using the topology construction protocol.

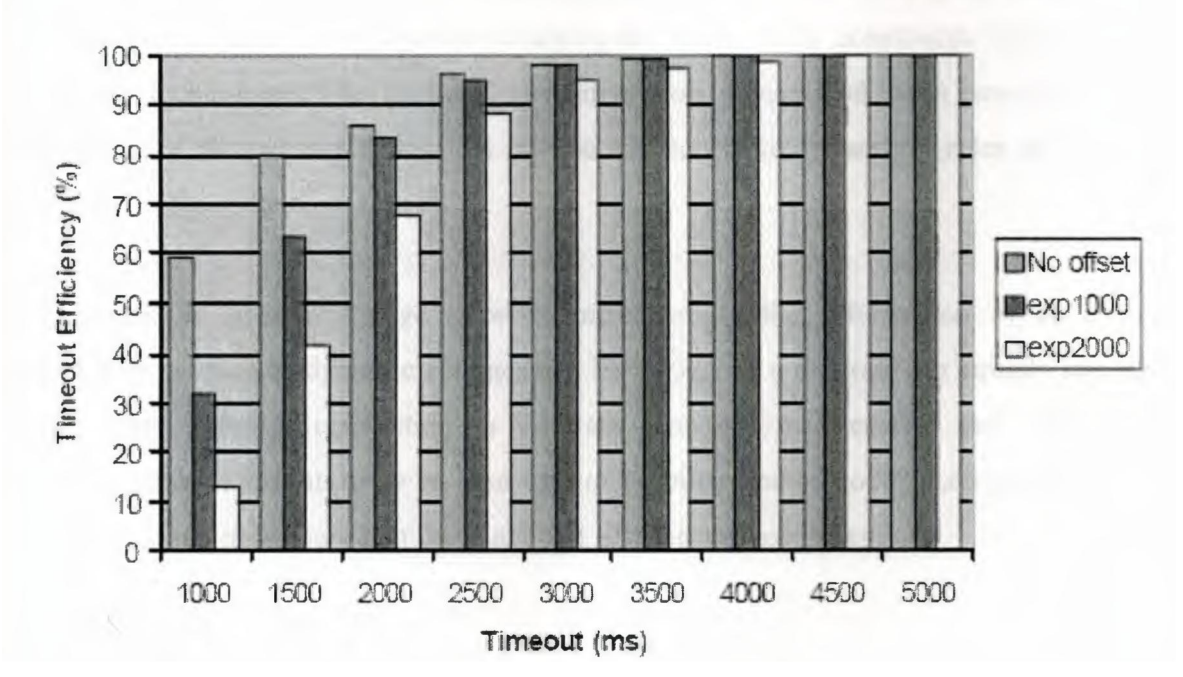

Figure 4.8: Timeout efficiency for the three conference application scenarios.

For example if there are 30 nodes envisioned participating in the protocol and we choose an ALT_TIMEOUT equal to 2500ms, Figure 4.6 shows that the average delay experienced by each user will be roughly 3000ms+2500ms=5.500sec and Figure 4.8 shows that a connected scattemet will be formed with a probability of 96.13% in the case of the "no offset" application scenario.

4.6 Summary

In ad hoc networks using frequency hopping technology, nodes can be grouped into multiple communication channels.

This physical layer setting provides a new way of viewing higher layer functions like topology construction algorithms.

Motivated by this environment and using the Bluetooth technology as our research vehicle, we first study the Bluetooth standard asymmetric "sender-receiver" point to point link establishment scheme and then propose a symmetric mechanism for establishing a connection without any role reassignment.

Based on the ad hoc link formation mechanism we present BTCP, a distributed topology construction protocol where nodes start asynchronously without any prior neighborhood information and result in a network satisfying the connectivity constraints imposed by the Bluetooth technology. The protocol is centered on a leader election process where a coordinator is elected in a distributed fashion and consequently assigns roles to the rest of the nodes in the system.

In addition to zero-knowledge network initialization, the reformation of an existing network in the face of dynamic changes can be viewed as a separate but equally important issue. After network connection, a separate topology maintenance and optimization protocol needs to run, in order to take care of mobility and/or nodes entering and leaving the network and make sure that the scattemet is reformed accordingly.

CONCLUSION

Bluetooth was designed to enable wireless communication between different types of devices, cell-phones, computers etc. The architecture and design is meant to enable secure and low power wireless transmissions over a short distance to a relative low cost.

The name Bluetooth comes from the late tenth century king Harold Bluetooth king of Denmark and Norway. He is known for uniting the warring tribes in Scandinavia, the same purpose as the standard intents to have uniting different technologies.

We have evaluated survivability in Bluetooth Location Networks for context-driven services. These networks have the following characteristics:

- They transmit position information to the service servers without user participation.
- Their RF technology is available in commercial handhelds.
- They can be used as general-purpose data networks.
- The spontaneous topology configuration is scalable, by installing as many master nodes as necessary.
- They can coexist with Bluetooth devices that are not part of the location system, such as printers or headphones.

In ad hoc networks using frequency hopping technology, nodes can be grouped into multiple communication channels.

This physical layer setting provides a new way of viewing higher layer functions like topology construction algorithms.

REFERENCES

1. http://www.anywhereyougo.com/bluetooth/
2. http:/-lwww.bluetooth.weblogs.com
3. http://www.howstuffworks.com/bluetooth.htm
4. http://www.mobileinfo.com/Bluetooth/index.htm
5. http://www.palowireless.comlbluetooth/
6. http://www.thebluelink.com
7. http://www.wuzap.org/bluetooth/
8. http://www.Bluetooth.com
9. http://www.Bluetooth.com
10. http://www.isr.umd.edu/TechReports
11. http://www.exploratorium.edu/guidebook
12. http://www.compaq.com/products/handhelds/ pocketpc/options/expansion packs.html
13. http://www.nokia.com/phones/6210/bluetooth.html
14. http://www.ti.com/tiris/default.htm
15. http://www.lOmeters.com/blue 802.htrnl
16. http://www-124.ibm.com/developerworks/ opensource/bluehoc/
17. http://www.ero.dk