AN ANALYSIS OF THE BLUETOOTH TECHNOLOGY

- Features, Challenges, Future and Security

Malik Zaka Ullah
This thesis is submitted to the Department of Interaction and System Design, School of Engineering at Blekinge Institute of Technology in partial fulfillment of the requirements for the degree of Master of Science in Computer Science. The thesis is equivalent to 20 weeks of full time studies.

Contact Information:
Author(s):
Malik Zaka Ullah
Address:
Snapphanevagen 3A, 37140,
Karlskrona, Sweden
E-mail: malikzakas@hotmail.com

University advisor(s):
Yang Lie
School of Computing

School of Computing
Blekinge Institute of Technology
Soft Center
SE-37225 RONNEBY
SWEDEN

Internet : www.bth.se/tek
Phone : +46 457 38 50 00
Fax : + 46 457 102 45
ABSTRACT

In this thesis I present my analysis on various aspects of Bluetooth wireless technology. The Bluetooth technology is relatively new as compared to other technologies and there is huge potential of its growth and practical application. Therefore during in this thesis I try to analysis the current status of this technology and issue which are related to this technology. The first section introduces Bluetooth technology, in which I discussed the architecture of Bluetooth and different terminologies of Bluetooth. In the same section I presented the comparison of Bluetooth with other communication technologies. The main questions I hope to answer in this thesis and also discuss the methodology I employed. The subsequent sections discuss the core technical features and issues of security and interoperability of Bluetooth. In these sections I identify the key aspects of Bluetooth that make it standout from other wireless technologies and point out certain shortcomings of this technology. During this I went through different aspect of Bluetooth technology. Subsequently I present my analysis of the market player’s and user’s perspectives and identify the main drivers and barriers of Bluetooth from a business point of view.

Towards the end of this thesis I discuss how this technology can be used to provide some attractive solutions. I demonstrate my ideas by discussing how certain services can be used in future in different scenarios. In my proposed solution I discussed the possibilities and advantages of using Bluetooth technology in university campus to perform different routine tasks and this will beneficial for the university both student and teachers.

Keywords: Personal Area Networks, Asynchronous connection Link, Ultra Wide Band, Special Interest group, Bluetooth Technology
PREFACE

I would like to express my gratitude to people who have supported, encouraged and helped me in various ways through in this thesis. I would like to thank my thesis supervisor Yang Lie and Mr. Guohua Bai for his constant supervision, and advice which have been very valuable for me to write this thesis.

Bluetooth is an industry standard, later adopted by the IEEE 802.15 work group as the Wireless Personal Area Network Standard (WPAN). To clearly understand this, I need to understand what a PAN is. A Personal Area Network can be defined as a network of devices in close range to a person, which can communicate with each other. A typical PAN could consist of a Laptop, a Mobile Phone and a Printer.

I am thankful to Miss Asma (S. Engineer), FourB Telecommunication and Mr. Kamran, Multimedia Broadcast Technologies UK for answering my queries on the Bluetooth technology. This Telephonic Interview with them has given me insights into the product vendor’s perspective on Bluetooth technology.

I would like to thank my wife who supported me to finalize my studies by writing this thesis. I would like to thank Mr. Asad Riaz (S.E) and Mr. Yasir for proof reading of this thesis. I would also like to thank my family and friends.
Table of Contents

TABLE OF TABLES ........................................................................................................................................ 4

CHAPTER 1 ...................................................................................................................................................... 5

1.1 HISTORY OF BLUETOOTH .......................................................................................................................... 6
1.2 BACKGROUND .................................................................................................................................................. 6
1.3 PROBLEM STATEMENT ................................................................................................................................. 7
1.4 THESIS STRUCTURE ....................................................................................................................................... 8

CHAPTER 2 ...................................................................................................................................................... 9

2 RESEARCH METHODOLOGY .......................................................................................................................... 10

2.1 OVERVIEW .................................................................................................................................................... 10
2.2 LITERATURE REVIEW ................................................................................................................................... 11
2.3 INTERVIEWS ................................................................................................................................................... 11
2.4 QUESTIONNAIRE .......................................................................................................................................... 11

CHAPTER 3 ................................................................................................................................................... 12

3 BLUETOOTH TECHNOLOGY AND INTERFERENCE ISSUE ............................................................................. 13

3.1 OVERVIEW ................................................................................................................................................... 13
3.2 BLUETOOTH TECHNOLOGY .......................................................................................................................... 13
  3.2.1 Bluetooth profile specification .................................................................................................................. 13
3.3 PROTOCOL STACK OF BLUETOOTH .............................................................................................................. 14
  3.3.1 Radio Layer .............................................................................................................................................. 14
  3.3.2 Baseband Layer ........................................................................................................................................ 15
  3.3.3 Link Protocols .......................................................................................................................................... 16
  3.3.4 Service Discovery Protocol ...................................................................................................................... 16
  3.3.5 RFCOMM .................................................................................................................................................. 16
3.4 BLUETOOTH NETWORKING .......................................................................................................................... 17
  3.4.1 Piconet ................................................................................................................................................. 18
  3.4.2 Scatternet .............................................................................................................................................. 18
3.5 BLUETOOTH AND OTHER WIRELESS TECHNOLOGIES .......................................................................... 18
  3.5.1 Infrared Data Association (IrDA) ............................................................................................................ 19
  3.5.2 Wireless LAN ......................................................................................................................................... 19
  3.5.3 HOME RF Working Group (HRFWG) ...................................................................................................... 20
  3.5.4 Ultra Wide Band ................................................................................................................................... 20
3.6 BLUETOOTH AND IEEE 802.11 INTERFERENCE ISSUES .......................................................................... 20
  3.6.1 An example of interference ...................................................................................................................... 21
  3.6.2 The Technical challenge ........................................................................................................................... 21
    3.6.2.1 Collaborative mechanism ................................................................................................ ................ 21
    3.6.2.2 Non collaborative Mechanism .......................................................................................................... 22
3.7 BLUETOOTH COVERAGE .............................................................................................................................. 22
  3.7.1 Bluetooth Antennas ................................................................................................................................. 22

CHAPTER 4 ................................................................................................................................................... 24

4 SECURITY & INTEROPERABILITY .................................................................................................................... 25

4.1 BLUETOOTH SECURITY ISSUES .................................................................................................................. 25
  4.1.1 Channel(Medium) Security ....................................................................................................................... 25
  4.1.2 Connection Level Security ........................................................................................................................ 25
  4.1.3 Applications Level Security ..................................................................................................................... 26
  4.1.4 Data (Information) Level Security ........................................................................................................ 26
4.2 SECURITY MODEL ....................................................................................................................................... 27
  4.2.1 Generic Requirements ............................................................................................................................. 27
  4.2.2 Proposed Security Model ........................................................................................................................ 27
4.3 BLUETOOTH INTEROPERABILITY ................................................................................................................ 29
Chapter 1

Introduction
1.1 History of Bluetooth

The name “Bluetooth” and its logo are trademarked by the privately held trade association named the Bluetooth Special Interest Group (SIG). The name Bluetooth was a code name used by developers of this wireless technology. But as the time past name Bluetooth Stuck.

10th Century’s Danish king Harald Bluetooth had been influential in uniting Scandinavian tribes in single kingdom after the war when the region was turn into parts. Now these days Bluetooth implication of Bluetooth does the same reunite different industries such as Computers with cell phones with single low power globally available short range radio frequencies named as Bluetooth.

The concept behind Bluetooth had its origins in 1994 when Ericsson began researching the idea of replacing cables connecting accessories to mobile phones and computers with wireless links. Ericsson quickly realized that the potential market for Bluetooth products was huge but co-operation throughout the world would be needed for the products to succeed. Therefore the Bluetooth SIG founded in 1997 by Ericsson, IBM, Nokia, Intel and Toshiba. First Bluetooth technical specification 1.0A released in 1999 by 3Com, Lucent, Microsoft & Motorola joins SIG Promoter Group.

Second Bluetooth technical specification 1.0B released in 2000, 2.0 was introduced late in 2005. 2.1 with enhanced data rate in 2007 and latest version of Bluetooth is 3.0 released in April 2009.

AMP (Alternate MAC/PHY) is the main new feature of the Bluetooth version 3.0, the addition of high rate data transport with 802.11.

1.2 Background

In the present ‘Hi-Tech’ world, the technical standards seem to change and evolve faster than the headlines in daily news-papers. Although for the scientific community this is a reason of great joy and pride, these rapid developments tend to confuse the less informed end users. In the domain of wireless communication I have seen the emergence of a whole array of new standards and technologies in the past few years, from Wireless Local Area Network (WLAN) to Bluetooth and WiMAX. It is in such a case that a particular new technology has to differentiate itself from the rest and clearly define what it hopes to do for the users. For instance, WLAN and Bluetooth both operate in the license free 2.4 GHz frequency ranges. They are both wireless networking standards and hence without precise information, may cause the users to wonder why they need the new Bluetooth when they already have a WLAN capability on their devices?

Bluetooth is an industry standard, later adopted by the IEEE 802.15 work group as the Wireless Personal Area Network Standard (WPAN). To clearly understand this, I need to understand what a PAN is. A Personal Area Network can be defined as a network of devices in close range to a person, which can communicate with each other. A typical PAN could consist of a Laptop, a Mobile Phone and a Printer. The user can transmit images from the mobile phone equipped with a camera to his
computer which can then send it to the printer. And all this can be done without the need for wires as illustrated in Figure 1. The basic idea of PAN is to make the users experience richer in terms of reliability and flexibility and help him use all his devices in seamless interconnection. So, in this context one could argue that WLAN is an existing networking standard and hence could have been used to achieve the same. But, the reason for emergence of Bluetooth as a standard and its wide acceptance is because of the fact that Bluetooth is specifically aimed at close range ad hoc networking without the need for a pre determined infrastructure. Since the operating range in terms of distance and speed of WLAN is much higher, WLAN modules consume significantly more energy as opposed to Bluetooth devices. Bluetooth devices typically operate over a very short range of 1 to 10 meters and hence consume very little power. Bluetooth can hence be used to connect peripheral devices wirelessly thus eliminating the need for various types of communication cables.

![Figure 1 Bluetooth usage scenarios](image)

In this thesis I further examine the Bluetooth technology closely and present analysis on some issues that are discussed in our problem statement. I also present a case study to illustrate my analysis and insights I develop through the various sections of the Thesis. The Thesis is organized into different parts. At the end of these main sections I derive some conclusions in general about Bluetooth technology.

### 1.3 Problem Statement

In this thesis, I will answer the following questions:

1. What is the application of Bluetooth technology? What are the advantages of using Bluetooth? And how does it compare with other available technologies.
2. What is driving the deployment of Bluetooth? Both from the perspective of a user and that of the industry.
3. What are the general security issues in wireless technology and in specific what are the security issues in Bluetooth?
4. Demonstrate with a use case / case study, how Bluetooth can be used in a practical scenario?
1.4 Thesis Structure

Through the course of the thesis I have used various sources of literature as indicated in the reference along with the material presented. I have conducted two interviews [1], [2] to gain a market perspective on Bluetooth technologies. I have also conducted a survey amongst the students and staff at BTH to understand the user’s point of view. Through analysis, brainstorming and discussions I gained from above methods I have been able to address the questions I set out to answer and eventually propose a simple use case for Bluetooth technology.
Chapter 2

Research Methodology
2 RESEARCH METHODOLOGY

This section illustrates the research Methodology carried out in this thesis. Overview of the research methodology, literature review, interviews and informal discussion are described below.

2.1 Overview

Research methodology is the method to organize and conduct research. It helps us how to analyze the results. I have adopted the qualitative and quantitative approach research methodology. I have done research in different phases. In first phase I have studied literature review to understand about the Bluetooth Technology. Literature review helped me to implement the valuable method of questionnaire conducting and analyze the questionnaire. In second phase I have conducted interviews with different peoples. And finally I have designed the questionnaire on the basis of interviews.

Figure 2 Overview of Research Methodology
2.2 Literature Review

The research contains literature, review, survey and interviews. The qualitative part of research consists of analysis of Bluetooth technology and its advantages and disadvantages. Then comparison of Bluetooth technology presented.

The literature review is used to identify the major factors which are involved in Bluetooth technology.
The interviews are used to validate the literature review results.

After the survey I props’ the project, which was the practical implementation of Bluetooth technology’. At the end of this case study I analyze the result.

2.3 Interviews

After reading and analyzing the literature and discussion, I have conducted couple of interviews at different locations about the Bluetooth Technology.
First interview was done with Miss Asma who is working on Bluetooth Technology in 4B Telecommunication and 2nd interview was done with Mr.Kamran Multimedia Broadcast Technology, UK, who is working on Bluetooth Technology. During interview with him they clarifies that there are worms which use Bluetooth technology and infect some cell phones which use symbian operating systems.
During these interviews, I had asked questions mentioned below about the Bluetooth technology, use of Bluetooth technology in industry, daily life etc. In these interviews I have observed the key features and practical use of Bluetooth technology.

2.4 Questionnaire

I have designed the questionnaire on basis of interviews with two persons for the use of Bluetooth Technology in BTH campus. These questions were given to students and staff of BTH how much they are interested in using Bluetooth technology.
Questionaire was formulated with open ended and close ended questions that provide the opportunity to the students and staff to express their ideas about the use of Bluetooth technology in BTH campus.
Chapter 3

Bluetooth Technology and Interference Issues
3 Bluetooth Technology and Interference Issue

3.1 Overview

In this section I introduce the technology of Bluetooth. Like most wireless technologies, Bluetooth is fairly sophisticated and hence the complete technical specification is very vast. I identify some key technical features of this technology which actually makes it so interesting. Most of the actual technical details presented in this section as borrowed from [3]. I recommend the reader to refer the same for more elaborate technical details. The table 1 provides a summary of some key features of Bluetooth. [Entries in table are extracted from various sections of 2.1].

<table>
<thead>
<tr>
<th>Connection</th>
<th>Spread Spectrum(Frequency hopping)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency band</td>
<td>2.4 GHZ ISM</td>
</tr>
<tr>
<td>Modulation Technique</td>
<td>Gaussian Frequency Shift Keying(GFSK)</td>
</tr>
<tr>
<td>MAC Scheduling scheme</td>
<td>FH-CDMA</td>
</tr>
<tr>
<td>Transmission Power</td>
<td>&gt;20 dBm</td>
</tr>
<tr>
<td>Aggregate Data Rate</td>
<td>0.721-1 Mbps</td>
</tr>
<tr>
<td>Range</td>
<td>10m-100m</td>
</tr>
<tr>
<td>Supported Stations</td>
<td>8 devices( per Piconet)</td>
</tr>
<tr>
<td>Voice Channels</td>
<td>3</td>
</tr>
<tr>
<td>Data Security-Authentication key</td>
<td>128 bit key</td>
</tr>
<tr>
<td>Data Security-Encryption key</td>
<td>8-128 bits(configurable)</td>
</tr>
</tbody>
</table>

Table 1 Technical summary

3.2 Bluetooth Technology

3.2.1 Bluetooth profile specification

Bluetooth Profiles describe how to use a specification to fulfill the desired function in the usage models. (The usage models are identified by the SIG’s marketing group). The Bluetooth Special Interest Group (SIG) has specified the profiles for those usage models. The profile tells us how to implement a solution for a particular use case. Each profile defines the particular messages and procedures from the Bluetooth specification and each device must support at least one profile. Those devices can communicate with each other which have the same profiles for example a cellular phone and headset can communicate on the condition if they both have the headset profile.

The profile is used to decrease the interoperability problems amongst devices of different vendors. The Bluetooth certification authority uses the profiles to test and certify compliance, and grants permission for usage of the Bluetooth logo only to those products that qualify the methods and procedures defined in the profiles. The table 2 lists the important profiles and their usage model.
3.3 Protocol Stack of Bluetooth

A Protocol stack is Software/ Hardware implementation of the actual protocols specified within a standard which enables the devices based on that standard communicate with each other. The Bluetooth protocol stack is as shown in Figure 3 [3], [4] and [5].

3.3.1 Radio Layer

Bluetooth works similar to other wireless technologies. It transmits data in the form of bits (ones and zeros) over a radio frequency. This function is defined by radio layer. Bluetooth transceivers use Gaussian Frequency Shift Keying (GFSK). In GFSK, the binary zero is represented by negative frequency deviation and binary one is represented by positive frequency deviation. The Bluetooth transceivers are available in three Power classes. The range is without obstacles.

<table>
<thead>
<tr>
<th>Profile</th>
<th>Usage Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Discovery profile</td>
<td>To discover available services and devices in range</td>
</tr>
<tr>
<td>Cordless Telephony Profile</td>
<td>To enable use of Bluetooth enable devices as cordless telephones</td>
</tr>
<tr>
<td>Dial Up Networking profile</td>
<td>To enable Dial up internet connection</td>
</tr>
<tr>
<td>Headset Profile</td>
<td>To enable communication of audio between devices</td>
</tr>
<tr>
<td>LAN Access Profile</td>
<td>To enable local area networking</td>
</tr>
<tr>
<td>File Transfer Profile</td>
<td>To enable transfer of data as whole files</td>
</tr>
<tr>
<td>Object push Profile</td>
<td>To enable transfer of data onto Bluetooth devices</td>
</tr>
</tbody>
</table>

Table 2 Important Bluetooth profiles

Figure 3 Bluetooth Protocol stack [4]
The radio frequency assigned to Bluetooth is 2.4 GHz ISM (Industrial Scientific Medicine) band. The frequency band 2400 - 2483.5 MHz is used in most of the countries around the world. But some countries have national limitations in the frequency range. The range is divided into 79 MHZ channels (For Spain, France, it is divided into 23 MHZ channels.). Each one of these channel is divided into 625 microseconds and 1600 different slots per second (1600 hops) are being made. Spain, France and Japan have frequency limitations so there are special frequency hopping algorithms specified. The products with the reduced band frequency (e.g. Spain) will not work with products with the full band (America). These products must therefore be considered as local versions for a single market. In order to be compatible and eliminate the limitations, the SIG (Special Interest Group) is taking several initiatives. [6]

<table>
<thead>
<tr>
<th>Geography</th>
<th>Regulatory Range</th>
<th>RF Channels</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA, Europe and most other countries</td>
<td>2.400-2.4835 GHZ</td>
<td>F=2.402+K(GHZ)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>K=0,1,2........78 =79</td>
</tr>
<tr>
<td>Spain</td>
<td>2.445-2.475 GHZ</td>
<td>F=2.445+K(GHZ)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>K=0,1,2........22 =23</td>
</tr>
<tr>
<td>France</td>
<td>2.4465-2.4835 GHZ</td>
<td>F=2.4465+K(GHZ)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>K=0,1,2........22 =23</td>
</tr>
</tbody>
</table>

Table 4 Frequency spectrum [5]

3.3.2 Baseband Layer

This layer is performing the functions of frequency hopping for interference mitigation, medium access control and data packetization. The packets are alternated by TDD (Time division duplex) between the transmission and reception. In addition it controls links, channels, error correction and flow control.

The base band layer establishes two kinds of links depending on the kind of application and operating environment. A Synchronous Connection Oriented (SCO) link is established to emulate circuit switched connections for voice and data connection. While an Asynchronous Connection Link (ACL) is defined for bursts of data. This link can be symmetrical with same data rates in uplink and downlink or asymmetrical. This supports broadcasting and data rate control by the master device. Hence I believe this can be employed for applications which need some sort of Quality of Service (QoS).
Bluetooth packet consists of three entities. 72 bits for the access, 54 bits for the header and 0-2744 bits for the payload. The access code is used for time synchronization, paging and Piconet identification. There are three different kinds of access codes: Channel Access Code, Device Access Code and inquiry Code. The channel access code identifies a unique Piconet while the device access code is used for paging and its responses. The header contains information for packet acknowledgement, packet numbering, flow control, slave address and errors check for header. The packet payload contains data, voice fields or both. There are nine categories of standard packet format. DM1, DH1, DM3, DH3, DM5, DH5, HV1, HV2 and HV3. Each of the nine packet types have its own special purpose. Some of them are specially made for voice communication while others are made for high speed data transfer. Each of the packets has different data rates. An effective Forward Error Correction scheme is employed to reduce transmission errors for connections where Automatic Repeat request (ARQ) cannot be used, and vice versa.

3.3.3 Link Protocols

Link Manager Protocol (LMP) and Logical Link Control and Adaptation Protocol (L2CAP) are two protocols which enable establishment of links and their control correspondingly. These protocols are essential to govern pairing of devices, synchronization, QoS and encryption amongst other functions. I think one of the most important properties of L2CAP is that it multiplexes several higher layer protocols like SDP, RFCOMM and TCS Binary which enables the seamless operation of several applications using these various protocols.

3.3.4 Service Discovery Protocol

The service discovery protocol (SDP) defines which services are available in the RF proximity and to determine the characteristic of those available services. In order to establish a connection with each other, devices must have to support the same services. SDP only provides means for discovering of services, not for accessing. I identify this as one of the most important features of Bluetooth. It is this property which enables the ad-hoc networking and thus enabling several exciting applications. I also note that it is this property which is also one of the security issues in Bluetooth.

3.3.5 RFCOMM

RFCOMM is a transport protocol used to emulate the RS 232 serial ports. It is this protocol which enables applications like connecting to printers and scanners via Bluetooth. RFCOMM relies on the Bluetooth baseband to provide reliable in-sequence delivery of byte streams. RFCOMM data rates will be limited in devices where there is physical serial port involved. Implementations may optionally pace data on virtual serial ports. RFCOMM is a simple, reliable transport protocol with framing, multiplexing and the following additional provisions:

- Modem status- RTS/CTS, DSR/DTR, DCD, ring.
- Remote line status-Break, overrun, parity
Remote port settings-Baud rate, parity, number of data bits, etc.
Parameter negotiation (frame size)
Optional credit based flow control

There are two types of devices which are supported by RFCOMM
Type 1: Internal emulated serial port
Type 2: Intermediate device with physical serial port

3.4 Bluetooth Networking

Bluetooth communication is made possible by establishing a master device and one or more slave devices. Any device can be a master or a slave. It is this property which makes Bluetooth useful for creating ad-hoc networks. One of the most important features of Bluetooth is that unlike WLAN any Bluetooth device can communicate with other device in range by simply establish one of them as the master and rest as slaves. The master device determines the frequency hopping pattern based on its address. There are two different topologies through which Bluetooth communication occurs.

1. Piconet
2. Scatternet
3.4.1 Piconet

Piconet is ad-hock network in which all the devices have the same frequency hopping synchronization. Each Piconet has one master and one or more than one slave devices. A master is the only one that may initiate communication. When link is established, the slave may request to the master to become a master. The master is responsible for dividing the whole bandwidth amongst the slaves by deciding when and how to communicate with each other. Each Piconet can have 8 active devices addressed by 3 bits and 248 parked devices addressed with 8 bits and several more in standby. This intelligent use of device states in what makes networking in Bluetooth interesting. The active devices as the name suggests actively participate in the network while the parked devices can be initiated under 3 milli-seconds [page 272 [3]]. Hence in a network where several devices need to communicate with each other, devices can be pushed to parked and active state intelligently by the master to enable effective networking. One Piconet can be split into two piconets by one slave becoming a master and thus may increase the aggregate throughput. It is this splitting which is seen as the overlapping area in the Figure 5 [3].

3.4.2 Scatternet

Scatternet is the overlapping areas among multiple piconets. A master can leave its Piconet and can join another Piconet as a slave. Scatternet is used to optimize the use of the available spectrum. The entire units share the same frequency range within one scatternet but each Piconet uses different hope sequence to avoid interference with each other. A clever way to optimize the transmission data capability is to keep the piconets small [8]. All piconets share the 79 MHz band where each Piconet uses 1 MHz hop channels occur. [3]

Figure 5 A Scatternet comprising two Piconets [4]

3.5 Bluetooth and other wireless technologies

There are several wireless technologies which have various applications. Some of these technologies offer the similar features and use cases as Bluetooth. The table 5 compares various wireless technologies based on different characteristics.
By comparing information from the Table 5, I can see that although there are several wireless technologies with applications overlapping with Bluetooth. They all have certain limitations and do not cover all areas as Bluetooth. Below are some inferences I draw from this.

### Infrared Data Association (IrDA)

IrDA is a nice and simple cable replacement technology, but since uses optical transmission it is limited to very short range line of sight communication. It is also point to point communication technology and hence lacks the advantages of networking features of Bluetooth. At the same time I also note that due to line of sight communication, chances of eves dropping are almost remote, thus making IrDA inherently secure. But also at the same time the security features in Bluetooth almost always make up for it.

IrDA standards were published in 1993 and include the link specification Serial Infrared (SIR). In 1995, the extensions were released for 4 Mb/s operations.

### Wireless LAN

WLAN (IEEE 802.11) seems to outperform Bluetooth in almost all areas, however since it is based on Ethernet standard and is highly power consuming. WLAN’s application is primarily for local area networking and doesn’t justify its use in application areas of cable replacement or WPAN.

With IEEE802.11 technology there question as to whether the bandwidth can be maintained at the high end, the maximum data rates is up to 5 Mb/s.
The cost of these products start from 100$ and up to 200$ for HR version. This is as compared to Bluetooth devices very high.

3.5.3 HOME RF Working Group (HRFWG)

Home RF and Wireless USB are probably closest in application to Bluetooth. But I note that Home RF is not as widely supported in the industry since it only enables home networking owing to its higher power consumption and lack of profiles. Hence it wouldn’t be used on personal mobile devices unlike Bluetooth. Similarly Wireless USB is a technology which emulates a USB cable over wireless and hence lacks the strength of supporting various profiles like Bluetooth does. [9]

3.5.4 Ultra Wide Band

Ultra Wide band Radio, UWB is a new radio technology with similar concept as radar. This wireless technology is used in wireless personal area network (WPAN). It has a throughput around 400Mbs within a range of 30 feet with little power which is in superiority than Bluetooth in capacity and power consumption. It has enough bandwidth capacity to transmit several audio and video streams. The UWB does not create interference with other radio frequencies, which means can work without disturbing other equipments like; broadband television sets, cell phones or cordless phones. This certainly seems like a threat to Bluetooth.

3.6 Bluetooth and IEEE 802.11 Interference Issues

As pointed out earlier interference issue of Bluetooth and WLAN (IEEE 802.11) is one of the important issues since both these technologies make their way into our everyday lives almost always in the same places. This section presents the technical aspects of this problem. Most of the information here is from [3], [35] and [10]. The interference between IEEE 802.11 and Bluetooth devices is not entirely blocking each other’s transmissions, but they reduce the effective ranges and data throughput which shows the degradation of technology both with users and market perspective. IEEE 802.11 uses direct spread spectrum techniques while Bluetooth uses Frequency hopping techniques.

The important thing to be noted is that due to the differing use of frequency hopping techniques, Bluetooth is likely more interfere with IEEE 802.11 than an IEEE 802.11 is to interfere with Bluetooth. The main reason for this is the fact that Bluetooth hops 1600 times per second, while IEEE 802.11 only hops around 50 times. The studies show that the relatively long packets and slow rate frequency hoping (50 hops in IEEE 802.11 case) used by
IEEE 802.11 causes interference with high error rates in IEEE 802.11 than Bluetooth. Bluetooth and Wi-Fi (IEEE 802.11) technologies use the same frequency band (2.4 GHz). If Bluetooth and Wi-Fi operate at the same time in the same place, their channel will be overlapping and may cause interference (collide) with each other. Specifically, when these systems transmit signals, they create noise for each other [12].

3.6.1 An example of interference

The Company X runs its operation in two story building [10]. The company has internet access with local internet service provider (ISP) using ASDL connection. On each floor of the building, there are WLAN access points (hot spots) for the network access. The WLAN access points are connected via ISP to access internet. There are a number of offices within each floor of the building. Each office is equipped with WLAN laptops and PCs. Each office has shared facilities for printed output and scanning documents. These devices are connected to via an office Bluetooth network. Users daily synchronize their personal Digital Assistants (PDA) with their laptops to diaries and calendar updated. These connections are implemented using Bluetooth. They may cause the number of problems due to the interference issues. For example when the interference occurs between them, the data packets are lost and retransmissions take place which affects on the throughput. As a result some transactions are taking place at an acceptable rate but others such as printing where is a lot of data for printing taking very long time and in some times when the interference is too high, the association between devices being destroyed, which is the main reason for the users diversion.

3.6.2 The Technical challenge

The special interest group (SIG) formed its own task group to handle the interference issues. Both Bluetooth and IEEE 802.11 groups looking for some techniques that can eliminate the interference issues [11].

3.6.2.1 Collaborative mechanism

The groups agreed on the proposal that protocols to be implemented in the same device for independent solution and that solution will rely on the interference detection and estimation. This kind of solution is named as collaboration mechanism or Bluetooth interference aware scheduling (BIAS) which is based on MAC scheduling i.e. both protocols be implemented in the same device, for transmitting voice packets, the priority is given to Bluetooth while for transmitting data; IEEE 802.11 is given the priority.
The advantage of this techniques using scheduling policy is that it does not require any changes in the FFC rules; in addition, scheduling in the Bluetooth specification is vendor implementation specific. Therefore one can easily implement the scheduling policy with the currently available Bluetooth chipset. Another technique is known as overlap avoidance (OLA) which uses different encapsulations to avoid frequency collision between IEEE 80211 and Bluetooth.[8]

3.6.2.2 Non collaborative Mechanism

The Bluetooth and IEEE 802.11 interference testing is still in progress. For most of application the performance level is reasonable (less than 25% degradation throughput) but for Bluetooth audio or any real time streaming application, the performance is not satisfactory. The blocked channel caused by the interference results in the degradation of the performance of channel due to the retransmission of data again and again. And thus very difficult for audio or real time streaming to maintain it. The poor voice rate and reduced data rate compels Bluetooth specification of move to another technique called adaptive frequency hopping or non collaborative mechanism. Adaptation of frequency hopping was introduced by the Bluetooth special interest group (SIG) in the Bluetooth 1.2 version. Adaptive frequency hopping technique restores the bad performance of reduced data rate by identifying the high error rates or bad channels and after that these channels are excluded. In this way, the retransmissions are controlled. The channels which are used by WLAN are excluded and the Bluetooth packets are restricted to those channels where there is a less chance of interference. The adaptive frequency hopping technique increases the Bluetooth throughput and maximizing the spectrum usage [8].

3.7 Bluetooth Coverage

Bluetooth’s short range could be a problem for some applications, e.g., to cover a large area, more number of Bluetooth receivers would be required every 10-100 meters, but this is not the economical way to implement such thesis[13]. Here are few experiments by which the Bluetooth range could be extended when the internal built in antenna is replaced with the external one. The Bluetooth USB dongle has a small antenna which can communicate with Bluetooth device within a range of 10 meters. This small built-in antenna could be replaced with a more efficient one[14].

3.7.1 Bluetooth Antennas

The Bluetooth antennas are used to extend the range of Bluetooth. The main purpose is to transmit signals and receive. Blue antenna has many characteristics e.g. gain and
direction. It’s operation. Antenna performance is very important factor as the same antenna is used for sending the signals and receiving the signals. The main issues which are involved with Bluetooth antenna are power coupling losses between antenna and the transmitter. Then there are antenna placement issues.

![Bluetooh antenna sends and receive diagram](image)

Figure 8 Bluetooth antenna sends and receive diagram

The Figure 8 explains the process and functional of Bluetooth antenna, the antenna sends the signal \( P_i \) to receiver and \( P_t \) is the transmitted signal. \( P_r \) is reflected back antenna. The ratio at the transmitter is \( P_i/P_t \).

The maximum power which is radiated from antenna must be matched the connected device. Which in most RF circuit cases is 5-ohm impedance and it is consider best for the antenna feed points. [9]
Chapter 4

Security and Interoperability
4 SECURITY & INTEROPERABILITY

In a world where information is increasingly becoming the power, the need to protect it and prevent it from going into wrong hands is very important. By the very nature, wireless communications are unsafe. Anyone can receive the information when it is transmitted into air. Hence various encryption and authentication techniques are employed. The security is a concern in Bluetooth devices since they are increasingly being used to communicate personal information. At the same time since Bluetooth has to coexist with other wireless technologies, is it also a main concern.

This section presents my analysis of the interoperability and security issues in Bluetooth. I have worked out generic technical and non-technical requirements of security and interoperability to see how an ensure that the end use of this technology has a richer experience.

4.1 Bluetooth Security Issues

Bluetooth wireless technology included with many cell phones, laptops, digital cameras, palm tops was initially accepted as a cable replacement to enable information sharing/exchanging among devices. Its recent broader view is providing a set of delicious dishes such as web connectivity, online gaming and many more. However, any time a user is transmitting or receiving information, he can be exposed to spammers, hackers and attackers. Service discovery property of Bluetooth technology makes anonymous attackers very aggressive resulting in annoying conditions for consumers. Security issue has to be discussed at 4 levels as below [15], [16].

4.1.1 Channel(Medium) Security

Today’s Bluetooth networks can be illegitimately accessed although not very easily. Bluetooth is mainly based on ad-hoc networks. In ad-hoc networks, devices can connect to each other rather than going through central access point. So they don’t have any centralized security control mechanism [17] thus exposing important information on devices to others on Bluetooth networks. In one way increased range in Bluetooth devices is another security issue, now newer versions of Bluetooth devices have more than 100 meters range thus enabling more invisible users to hack your device.

4.1.2 Connection Level Security

When a device is configured to be in visible mode, other devices in range send signals indicating that it is available in its vicinity and ready for pairing. This is because of the Service discovery [18] property. This property is used by miscreants to discover devices left unattended in car parks, restaurants and other places and to eventually steal them. They also use high gain long range antennas for this kind of theft. Pairing [16] mechanism Figure 9 also makes free transmission and reception of data thus enabling criminals to infiltrate information. Sometimes attackers connect to the targeted device without alerting the target device and hence have great access to secured information and data.
4.1.3 Applications Level Security

When Bluetooth devices are connected in a trusted mode[16] then one device attempts to access services on another device since a trusted device has unrestricted access to all services on the other device. Although uncommon, a breach of this trust results in loss of valuable information owing to this privileged access. Off lately Bluetooth enabled devices like PDAs, cell phones are becoming the next target for viruses. However in the interview with us, Mr. Kamran[1] clarifies that this problem can be addressed by the terminal manufacturers by designing the software of the device intelligently. Now there are worms which use Bluetooth technology and infect some cell phones which use symbian operating systems[17]. Spamming[17] is always a big problem in cable networks now its also becoming a headache in the wireless networks applications like email web browsing etc.

Hackers approach to sensitive applications related to encryption algorithms leads to another problem for the machine security. Sometime user improperly uninstall applications and forget to remove completely the previous records settings like stored PINs, passwords etc and in result giving access to the hackers. Another severe problem is using the clients services in which attacker simply creates a serial profile connection to the device and gets complete access to the device and causing problems to the users and creating annoying situations for the users[19].

4.1.4 Data (Information) Level Security

Data security is of great importance and a user demands that his information be sent and received safely. But it does not happen every time. Sometimes in pairing, attackers are able to go into a hidden mode after attacking the device and hence become invisible to the users. In this issue unless the user gives precise consideration to his device he can’t capture the bug. Hence very often the targeted user doesn’t even notice that something is going wrong. With this attack the hacker is able to access information from the targeted device being undetected[19].

Another issue is also creating severe problems for data security in which the miscreant is primarily concerned about the victims most important data which includes phone books, calendars, messages, images, business cards, bank account details, property details and some credit cards secrets. Sometimes due to low level of data encryption algorithms the security is not very strong.
4.2 Security Model

A comprehensive security model is mainly dependent on determining the invasion mechanism, detection of attacks, protections against data corruption and retaliation to threats with enhanced measures. Also design should deal with the future needs and type of networks involved in the whole scenario.

4.2.1 Generic Requirements

Based on my analysis and investigation of the various security issues I divide the task of proposing an idea into the different technical categories according to their specific needs like integrity, availability, authenticity etc.

Authentication [20] is a definite requirement for Bluetooth enabled devices. Key exchanging should be identical for the devices. This key exchanging will further lead to authorization of devices in the network [9].

Users are concerned about data security. So this requirement helps in making possible that trusted information is sent and received between the devices and it is not scrambled, corrupted and duplicated during transmission. This also helps in ensuring packet integrity. By integrity a mobile user is also requires assurance that the hacker is blocked to reuse previous information in replay attack. So data integrity for Bluetooth enabled devices is of definite importance. Data encryption by public key is decrypted by private key and also in the reverse scenario cypher E0, AES and DES encryption [21] techniques are going very well in this context. A moderate privacy and one of the strongest tool for security is Public key authentication. Use of such strong encryption will enhance security in Bluetooth.

My survey and interviews shows that Blue tooth devices should be user’s friendly and more purpose oriented. Users always lose interests in impedes learning and counter intuitive. Applications vendors should think in a manner that they are going to make something which is intuitive to users. Abundant features and redundant functionalities are no substitutes. Compact, concise and specific devices with congruent actions increase ones attentions [1].

Users expectations for ease of use are always high. So one should be careful in defining security profiles. They should be easy to use. If a user has to set number of parameters for configuring the security settings then there is great chance he will get enjoyed and frustrated. This is the reason that some products are not famous among the users due to high profile setting parameters. Products should be for all categories of ages like kids, youth, professionals and old fellows. Another important requirement is proper time to feedback mechanism to make more robust applications profiles and bluetooth devices.

4.2.2 Proposed Security Model

After identifying the requirements and investigating the present security features I make suggestions for some improvements. However one must note that it is beyond the scope of this thesis to investigate the precise usefulness of such a model. But based on my understanding of the system and understanding the requirements of applications and insights gained during the interviews I make this suggestion.
Network integration is itself a big security issue. Due to non centralised security issue in ad-hoc networks the security is becoming a main concern. Security logs should be taken much more carefully. Some time people forget to switch off device when they are offline or even forget to make device invisible which is a most normal resulting in theft of PDAs and laptops as mentioned earlier. So at the grass root level, to enhance security in Bluetooth devices users should be educated and informed about the security threats and usage guidelines should be issued. So better usage practices will definitely help address this problem. However vendors could also ensure that the application software using Bluetooth connection warns the users when the devices are in idle mode, hence the user can decide for himself if it is safe or not.

Most of the problems like bluejacking, blusnarfing, bluebug, backdoors attacks [19] can be resolved with high end encryption techniques and algorithms for the safety of data to avoid abusing of pairing mechanism. Apply powerful or effective encryption algorithms like DES and AES might help improve security beyond the streaming cypher currently used. At the moment since computing power is expensive they are not used, but in the future when these devices pack much more computing power use of such algorithms would be more reasonable.

Secure variable length coding encryptions is an idea for future implementations in video streaming to avoid hacking attacks. Digital certificates and signatures in case of downloading informations are becoming popular day by day. As I don’t know how the downloading software is from trusted customer or and bad one, such techniques ensure that your personal information is not shared to anybody and all that you get is certified.

Based on my assumptions and considerations I have envisioned a security model which may fulfill some of the basics requirements of reliable security against the vulnerabilities. The Figure 10 is presenting the prototype concept by dividing the connection, application and data level securities to the Networks, authentications and the encryption/digital signatures respectively [22].

So introduce a system which increase your security. Make access to the networks more secure. If possible try to introduce systems like information does not flow from one system to other network like locked system development for special security. Introduce key management like public and private key mechanisms for login. For instance I don’t want to let someone without their valid ID to access data bars. At the same time one needs to ensure that people get access they are authorized to in order to be able to do their jobs. Hence additional improvement would be to define different rules for trusted users and different for nontrusted users. Hence use of
asymmetrical security can be used to find a balance between rigid security and ease of use for user.

4.3 Bluetooth Interoperability

I define interoperability in 2 parts. A: Interoperability of Bluetooth devices from different vendors and B: Interoperability of Bluetooth with other wireless technologies. Investigations show that interoperability issues are not severe but they still need to be addressed. They definitely demand the attention of vendors of devices and applications. With the ease of Bluetooth, the networks are getting wider and hence adding problems from interoperability point of view.

4.3.1 Bluetooth Enabled Devices Interoperability

Before launching a Bluetooth enabled device depending on the features as discussed before it is necessary to check its performance with other Bluetooth enabled devices. But due to massive productions of vendors applications and devices it is not feasible to test all devices with every other device in the market. I can check the interoperability by having some of them from the market but not all of them which obviously not possible. Also Bluetooth enabled devices are required to be compatible in applications profiles other wise they will fail in discovery and hence no pairing occurs. Also sometimes discovery is failed due to high level security policy in the application protocols, which may prevent clients from discovering services. So creating interoperability problems

Some of the known issues in the applications are switching problems, synchronization, packet losses. A more basic interoperability issue is related to different devices frequency hopping. Sometimes master and slave fail to synchronize then they cannot communicate. Hence devices which are built to work at different hops are incompatible with those built to work at other hops. Some interesting investigations show that some non radio frequency networks like industrial equipment, commercial microwave home appliance e.g. ovens also cause of interference like issues on Bluetooth devices resulting in reducing their efficiency.

4.3.2 Software Applications Interoperability

Software reliability is mainly dependent on the hardware configurations and settings which are provided along with some simple and main profiles. Problems in hardware parameters and network settings mostly the reason for corruption in applications thus leading to low reliability in Bluetooth usage.

Failure in connectivity cause a device to become invisible and causes inefficiency of the software platform running applications and hence eventually disconnects the device from the remote device. Due to incompatible applications profiles for instance like non compliance of a file transfer application on one device with another file transfer application on another device is one of the known interoperability issue.
Also some non standard softwares from some far east vendors[2] are creating interoperability problems for different devices and hence to consumer market. Authentication between devices is also another issue of interoperability. Some devices communicate with different encryption techniques for security purposes. When two Bluetooth devices try to establish a link and when the key exchange fails then device also fails to communicate each other. Sometimes delays in encryption of data cause synchronization issues [27] and hence results in interoperability.

4.3.3 Some more considerations

Systems with different build and vendor must be tested thoroughly for compatibility. A reliable wireless connection make critical applications more mission oriented and also helps in approaching the high demands on deterministic behavior along with real time performance measurements. Radio frequencies interference sources affect the Bluetooth band resulting in low throughput. Hence such interferences should be removed or atleast minimized for Bluetooth and other wireless medias, Wi-Fi microwaves cordless phones. To keep the link online for different connecting nodes the range of operation should also be carefully considered otherwise any out of range scenario disconnects the devices and results in information loss [28].

A basic interoperability need is to synchronize piconet nodes like master and slave by using frequency hoping spread spectrum. The nodes must be able to synchronize their adaptive movements for 2.4GHz frequency. An other requirements for real time devices connectivity though their application ends should have friendly and less time consuming acknowledgement periods so that they can execute applications in time to avoid any interoperability.

4.4 Generic Requirements for Better Interoperability

For a user, it is always interesting if a wireless device he is using is more adaptive in ranges and connection orientations. A demanding requirement of user is fast information processing devices. So the design of Bluetooth devices should take care of the interoperability of device’s hardware and software involved in order to get much better compatibility along with improved results. Also users are always interested in devices which are easier to plug and play, devices with simple configurations setting etc. So, in making a Bluetooth wireless connections users encourage a system which is easily and fastly configurable for different devices interoperabilities like printer, mouse, key board, cell phones, PDAs etc and doesn’t add additional difficulties in setting up a connections.

If Bluetooth is to become a more stable technology, an effective and intuitive solution for any of the usage models i.e. profiles has to be used. There must be an improvement on interoperability aspects. This not only means that a versatile interoperability architecture design is required for plug and play operation with full compatibility among products from different manufacturers, but also support for hybrid networks. For instance Universal Mobile Telecommunication Systems (UMTS) provides a hybrid architecture [22] for effective use of Bluetooth in devices used in UMTS networks.
Software interpreters or plug-ins must be introduced to facilitate the user to enjoy his Bluetooth devices along with his older versions or incompatible versions of devices. This however has been well addressed by the SIG. The Newer versions of Bluetooth, i.e. Bluetooth version 1.2, 2.0 and version 3.0 are interoperable even with the version 1.0. Different vendors devices should be compatible to get better performance in interoperability. Vendors should follow the special specifications of SIG while building applications services. For example protocols should also be fully compatible, applications profiles should be in compliance so that various manufactures devices can communicate with each others. By this method they can reduce the interoperability issues.

During connections of different devices the running services uses different services like synchronization and file transfer. To make sure the connections remain connected and improve their performance then there is a need of proper feedback mechanism. In this context asynchronous connection less link ACL helps Bluetooth to use fast acknowledgement and retransmission scheme to guarantee reliable transfer of information. [29]

Scatternets has also broaden the Bluetooth for more reliable and flexible use cases. Through Scatternet I can control the scheduling of traffic and can be of good use in network establishment which results in more reliable connections within Bluetooth network [30].

4.5 APIs Solutions for Security and Interoperability Issues

Through my investigations I have seen that security and interoperability issues are still inadequate in providing a more reliable and compatible environment for communications in a personal area networks. From applications vendors point of view I can say that now I am adding some bonus points for security and interoperability.

In this context JAVA APIs [31], are providing much helps for building more reliable applications by reducing the complexity of hardware programming. So now vendors can build applications for the same software specific platforms. This in turns helps the vendors to build more interoperable applications and makes compatible security parameters. Vendors like SUN [31], and BLIP [32] are working on JAVA APIs and providing software solutions for most of the mentioned issues.

Some Java APIs are helping vendors to build their applications for receiving and transmission of information with better capabilities. Java is providing help in writing applications based on it versatile APIs to support the device discovery mechanism with more elaborate inquiry mechanisms algorithm some fast processing of acknowledgments. Now through Java APIs one get manage and record information about the desired services. Also makes possible to establish interoperability between connections like RFCOMM for different devices. Bluetooth services, the Java APIs for Bluetooth provide interoperable solutions which provide help to allow connections to any service that uses RFCOMM, L2CAP, or OBEX Figure 3 (Section 2.3.1. Radio Layer) as its protocol [31].
Chapter 5

Future of Bluetooth Technology
5 FUTURE OF BLUETOOTH TECHNOLOGY

5.1 Drivers and Barriers

It is not always very easy to determine if a technology will be successfully accepted in the market or not. Companies and organizations do in depth research into the technology, its use cases, present and future markets, support and backing from regulatory authorities and standardization bodies before investing in a particular technology. In this regard one of the strong drivers for the Bluetooth standard and its wide acceptance in the industry is the Bluetooth Special Interest Group (SIG). From its initial founder members Ericsson, Nokia, Intel, IBM and Toshiba the SIG has added more than 2000 members. Since the SIG is an industrial consortium the process of standardization and release of subsequent upgrades is much faster than in the case of standards issued by central authorities like the International telecommunication Union (ITU). Moreover SIG ensures that any product labeled as Bluetooth enabled, conforms to their specification and is seamlessly interpretable with Bluetooth enabled devices of other manufacturers. It is these aspects of the SIG, which is one of the big drivers for this technology.

In this thesis, in order to gain an insight into the market player’s perspective I have conducted two interviews [1], [2]. I interviewed with Mr. Kamran and Miss Asma. From these interviews I can see that apart from the push from SIG, the biggest drivers for Bluetooth are the fact that it was adopted by the manufactures of Mobile phones. Initially Bluetooth was used in mobile phones to enable people exchange business cards wirelessly. The choice was Bluetooth obviously because of its lower power consumption and longer range as opposed to IrDA. This availability of Bluetooth on mobile phones together with the availability of several profiles in the specification paved the path for deeper penetration of Bluetooth in the market. Since a lot of mobile phones were already equipped with Bluetooth, wireless headsets and other phone accessories employing this technology became popular. Eventually this propelled the use of Bluetooth in portable computers and Personal Digital Assistants which enabled synchronization of address books, calendar and email applications with mobile phones. In the same way, because of its increased use in computers, Bluetooth enabled peripheral devices like printers, keyboards etc also became popular. This scenario where devices from different vendors interoperable and mutually promote sales of each other’s devices creates economies of scale, which are the best to sustain growth and ensure a market free of monopolies.

Any commodity can only be sold in the market when users accept it and create a demand for it. In order to aid us in evaluating this aspect and also to help us gain an understanding of the user’s point of view about my proposal, I conducted a survey amongst the students and staff at BTH. From my analysis of the survey results, I can see that the mobile industry has shifted from a primarily voice centric to data centric. People wish to use their mobile phones for more than just ‘voice calls’ and ‘SMS’. New applications like internet browsing using WAP, Multimedia and Location based services, gaming, and m-commerce applications are being developed. In short, mobile phones are becoming Personal Information Management Devices (PIMD).

This is fuelled by the integration of cameras, audio/video players, messenger clients, email clients, calendars and other applications into the mobile phones. Because of
this increasing functionality of mobile phones, there has been an increase in the need for exchange of such information between devices. Since Bluetooth offers the possibility of doing all this very easily and without the need for cables, it is becoming increasingly popular with the users. Although competing technology IrDA is present in mobile phones, it is limited to line of sight communication and hence reduces usability greatly. This increasing acceptance and demand from the users further pushes the manufacturers to introduce more innovative products and applications into the market which in turn could create a richer user experience and hence further increase demand for Bluetooth. Last, but not the least of the factors which is driving Bluetooth is the decreasing cost of the Bluetooth chipsets. This is not only a driver for the manufacturers but also for the customers. With lowered costs of Bluetooth chipsets, devices integrated with Bluetooth become cheaper and hence more people purchase Bluetooth enabled devices thereby increasing the need for other devices simultaneous.

Although the SIG is constantly revising the specifications and enhancing the Bluetooth functionality, as Mr.Kamran pointed out in his interview with me, it has perhaps made a mistake in not adding a USB profile to the list of Bluetooth profiles. This would have aided Bluetooth in addressing the threat of Wireless USB, an emerging wireless technology which emulates a USB over wireless media. Wireless USB offers a solution to replace USB cables in a far simpler manner as opposed to traditional Bluetooth. This could be thought of as one of the barriers for this technology. At the same time, vendors like NOKIA believe that Wireless USB is a complementary technology and hence is not a real threat or barrier to Bluetooth. However as I see it, perhaps the biggest barrier to Bluetooth has been Slow Vendor Adaptation (SVA). By SVA, I mean two things:

1. Although the Bluetooth SIG requires that products of different vendors be interoperable, it hasn’t completely been the case. This is because of several reasons. One of the main reasons is the fact that some of the Far East vendors are supplying Bluetooth devices without passing through the qualification process. Another reason is the fact that test specification does not test everything and some gaps still are not covered. But SIG is aware of these problems and is working around the problem by providing systems to conduct well defined testing on each product.

2. The second thing is that, vendors are slow in adapting the revised specification and hence most products available in the market are based on earlier specifications. Until not so long ago most products were based on Bluetooth 1.0 and hence had the interference problems with Wi-Fi (as discussed in chapter 2).This resulted in lower performance and hence users were dissatisfied. However after vendors eventually adopted the Version 2.0 and now a few of them have even adopted the latest version 3.0, these problems have been resolved.

5.2 Future Developments

As discussed in the previous section, one of the primary reasons for the success of Bluetooth is the fact that it is a standard developed and constantly upgraded by the Bluetooth Special interest Group (SIG). Bluetooth has constantly evolved from Bluetooth version 2.0 to the latest version 3.0 with enhanced data rate (EDR), which
increases data rate from 24Mbps to 3 Mbps and the overall transmission rate to 3 Mbps. The new specification also aims to reduce power consumption further by 50%. However one of the most important future developments in Bluetooth would be the incorporation of Ultra Wide Band (UWB) radio technology in Bluetooth. The Bluetooth SIG and the UWB work groups have decided to collaborate and work together to make this happen.

UWB is an emerging wireless technology for short range communication. UWB is also a low power technology like Bluetooth, but offers much higher data rates. As opposed to Bluetooth, UWB can offer up to 100 Mbps. Initially this could have been perceived as a threat to Bluetooth since this had the potential to replace Bluetooth as the standard of choice for Wireless Personal Area Networking (WPAN). SIG announced that it would collaborate and work together with the UWB work group to adopt the UWB technology to Bluetooth. The SIG’s decision to work with UWB workgroup is a very smart move to leverage the branding, trust and marketability of Bluetooth and the technical advantages of the emerging UWB technology to meet the customers growing needs. It can also be noted from [7] that the SIG is making sure that the present Bluetooth devices in use will be interoperable even with the future products. Applications not requiring the high data rates will still use the present technology, while multimedia applications can benefit from the UWB’s higher data rates. This not only benefits Bluetooth, but it also prevents standardization agencies from creating yet another technology with similar functionalities which would simply confuse the product manufacturers and end users.

Presently Bluetooth is the chosen wireless standard to interconnect various devices and hence is used in mobile phones, PDA’s, laptops, printers, etc. Although version 3.0 has been specified, most commonly used is Bluetooth versions 1.2, 2.0. This specification supports various profiles as listed in the table in chapter 1. However not all commercially available devices support all of them. In the future when these devices support more profiles and possibly when data rates are further increased by use of UWB, there will be plenty of other more sophisticated applications.

The future applications in Bluetooth could be categorized based on what would drive them. Some of them could be as follows:

- The cost of Bluetooth chipsets is fast reducing and further decrease together will decrease in power consumption will enable its use in disposable sensors, Personal tags etc. A pilot Project in this regard has been demonstrated at the Zoological Park in Denmark. Children visitors at the Zoo are given Bluetooth enabled tags which will help parents determine their location in Zoo, thus ensuring children’s safety [32]. Similarly Bluetooth enabled sensors and communication devices are used in the city of Oslo to monitor critical water levels at pumping stations.

- As noted in the previous section, mobile phones are increasingly becoming Personal Information Management Devices and most of today’s phones are equipped with Bluetooth. In the future when even low end mobile phones come equipped with Bluetooth as noted by Mr. Kamran in the interview, they can be used as devices which carry an electronic identity of people. This
electronic identity can be used for electronic authentication and authorization on company and university campuses. It can be used for enabling purchase of goods at supermarkets and can enable ticket-less travel [33]. It can be used to enhance security on office premises by automatic locking of computer terminals, managing of telephone calls etc at offices as demonstrated by the X Company Blue position [34] in their products.

- There are several wireless technologies available, which can be used to determine the location of a person. Global Positioning System (GPS) is perhaps the best of all, which provides exact coordinates of a person's location. However to deliver simple location based services with a limited geographical area like offices, shopping malls and university campuses such high accuracy is not needed. Especially since that accuracy comes at a very high price. GPS is a complex system and often requires a standalone GPS handheld device. Alternatively Wi-Fi has been demonstrated to be usable for location determination, but Wi-Fi is extremely power hungry and hence not feasible for this purpose. Hence in this context Bluetooth emerges as a simple and yet sufficiently reliable technology for location determination. Since Bluetooth is power efficient and is present on most mobile devices (mobile phones) it is clearly a good choice. Hence when Bluetooth is used to determine location of a user in a shopping mall or fun-fair, suitable information can be pushed to his mobile phone. This can be used to push advertisements, personalized services, information etc.

- Bluetooth can be used to interconnect various home appliances like refrigerator, oven, home security system, lights etc which can all be controlled by a Bluetooth enabled PDA or Mobile phone. Furthermore when Bluetooth data rates become higher it can be used to interconnect speakers, display monitors, to a multimedia player without the use of cables. This will enable easy exchange of digital multimedia connect across devices at home and make a truly wireless home.
Chapter 6

BT Campus Project
6 BT CAMPUS PROJECT

6.1 The premise

Through the various sections in this Thesis I have discussed and presented my analysis of what Bluetooth is and what it can be used for. In this section I present a use case for the technology to provide some value added services and create simple solutions for the problem at hand on my very own BTH Ronneby campus. As I have clearly learnt through this research, by no means is Bluetooth the only wireless solution for this case. However because of the fact that it operates in an unlicensed band and comes built into most of the mobile devices used on campus, I have decided that Bluetooth is a reasonably good choice. Some of the services discussed in this section could easily be delivered by using WLAN alone, but as I mentioned it is only found on portable computers and not as yet in mobile phones and it is power hungry as compared to Bluetooth. My solution is called the ‘BT CAMPUS Project ‘because the main technology of my concern is Bluetooth. However my proposal also involves the use of other wireless technologies where I find Bluetooth to be unsuitable.

![Figure 11 Example of BT](image-url)
6.2 Objectives

The primary objectives of this proposal are as follows:

1. Replace the presently used identity cards (ID cards) on BTH with a solution which will enable the students/staff to authenticate at the data bars, labs and other places requiring authentication, i.e., create a Mobile ID.

2. Provide a solution for enabling payment at canteen, cellar bar, the book shop and other places on campus using a mobile device.

At the outset, the ID cards at BTH work fine. So what is driving us to replace it with a Mobile ID? On closer analysis the problem with the ID cards is that they are static information, i.e., the information on the card cannot be easily updated. If it needs to be updated, the person has to physically take the card to an IT administrator at BTH and do the necessary changes. Moreover the ID is not always synchronized with the Campus net account of the user. This is definitely an inconvenience. That is, when a student registers for a course in a different department he does not always get the access to the department data bars which he would need to smoothly complete his course work. So he has to in person meet the IT administrator and get his access rights updated which could be difficult if he doesn’t always know where to find the administrator or doesn’t have the time to meet owing to other lectures. On the other hand there could be students who register for a course at the start of the semester but eventually drop it. If they have had the access to data bars which they do not require now, they could use up the resources at the departmental data bars which could be very important for students presently registered for the course. An electronic (Mobile) ID which is synchronized with the Campusnet account of the user could eliminate this problem.

From the survey I conducted amongst the students and staff on BTH, I can see that people are quite excited by the possibility of using their mobile phones to pay for various things on campus. People might often forget their wallet at home before coming to school and this should by no means stop them from eating lunch in the afternoon or relaxing with colleagues and friends with a cup of coffee or the cellar bar. Since a mobile phone is seldom forgotten by people, a mobile payment solution is one of my other important objectives.

Some more services can also be provided to enhance productivity of students on campus. Hence my additional objectives are as follows:

- Deliver notifications to mobile phones (lectures, meetings, seminars, parties, events)
- Deliver simple location based services
The figure below illustrates my model.

The Proposed Solution

I choose to name my solution the ‘BT CAMPUS PROJECT’ since it predominantly relies on Bluetooth technology which is my transport mechanism while at the same time relies on the Campusnet to manage the information. In the sense that it is a combination of ‘Bluetooth’ + ‘CAMPUSNET’ = BT CAMPUS PROJECT.

- **Information and Content Management:**

  The Campusnet is an extensively used service on campus. Every person on Campusnet has a user account on Campusnet to manage emails, calendar, course details, message exchanging etc. I propose to incorporate a Mobile Profile for each user on the Campusnet which will contain the users GSM/3G telephone number, authentications details which could be reconfigured by the user. This Mobile Profile will also contain information about user’s preferences regarding services, favorite news categories and tastes. This database will contain the registration details of users in the future when they wish to third party content delivered to them via Campusnet. Hence Campusnet will be the server which will serve users accessing it via Bluetooth enabled mobile devices via Bluetooth hotspots.

- **Network Setup:**

  The hotspots will be Bluetooth transceivers connected to a computer terminal which will access the server via a WLAN or Ethernet, all connected on a Local Area Network. If Bluetooth version 1.2 or higher is used, interference with WLAN will not be a problem as discussed in section 1 of this Thesis. This LAN need not be dedicated, but simply could use the existing BTH intranet. Thus the entire campus can be connected.
• **Access Setup:**

The users with a Bluetooth enabled device (mobile phone) will pair with a hotspot which can be a done by application software running on these terminal devices. Subsequently this pairing will be maintained by the device and the hotspot. When user goes out of range of the hotspot, he can go on standby mode thus enabling the hotspot to communicate with other users in the vicinity. This can be done dynamically even when user is in range and not requesting information to enable other users to access. This application (which could be called a Campusnet client) running on the phone can also carry out an authentication for Campusnet. After authentication the server will accept requests / push information based on user preferences.

A general concern in using Bluetooth for my solution is that only 8 devices can network at a time. But as discussed, the application software can control how the master in the Piconet actively reconfigures users in active, parked and standby modes to manage the number of users at an instance. Below I list the services I wish to provide based on this model and illustrate how this can be done.

1. **Mobile ID based authentication:** The present card readers at the entrance of the data bars and labs can be replaced with a Bluetooth hotspot. As described in the above setup, the user can use his mobile phone enabled with Bluetooth to authenticate himself. The Client running on his phone will do the necessary exchange of authentication information either automatically or by requesting a password from the user.

2. **Automatic Mobile Phone profile management:** All lecture halls, data bars, etc will have a Bluetooth hotspot inside in the room. When a user enters the room, the client on his phone will communicate with the hotspot and immediately trigger the phone to switch to a silent profile thus ensuring that nobody phones accidentally rings during the lecture and disturbs the others. This is an application which is already provided by a company Blue position [36] to its customers.

3. **Mobile Payment:** The above mentioned mobile ID could be used to record transactions and subsequently bill the user weekly/fortnightly/monthly. This can either be done in collaboration with the bank on campus or even by some treasury department of BTH. Alternatively as pointed out by Mr. Kamran the SIM access profile of Bluetooth can be used to pay on campus. Since the SIM is quite secure and is definitely individual, it can be used as an identification of user. And subsequently the user could pay via his ‘currency’ on his phones SIM card. This authentication could also be employed to create the Mobile ID as discussed above. In the event that a user wishes to change his SIM card, the new SIM can be registered on the Campusnet in the Mobile Profile.

4. **Calendar and Email updates:** Bluetooth hotspots could also be installed at various spots across the campus i.e. entrances of buildings with data bars and lecture halls, faculty corridors, canteen, Main lobby of building and other important spots. The user can connect to these using his Bluetooth enabled mobile phone. The client on the phone can then be used to access the Campusnet calendar and email inbox and synchronize with the phone. This
can already be done with personal computers; hence by adding this functionality to the client, this can be extended to synchronize with the server. The LAN access profile of Bluetooth can be employed to do this.

5. **BTH News, Lecture updates, Weather Updates:** Since the users mobile device can be detected to be located in a particular building or even particular lecture hall or data bar with the BTH campus. This will of course be in accordance with the user preferences which he would configure on the Campusnet Mobile Profile. Similarly general news about BTH, the local weather forecast for the day or change in lecture location can also be pushed onto the users Bluetooth enabled device.

6.3.1 Limitations

Although our proposed solution replacing the campus access cards but have same issues with Bluetooth enabled devices one has must submit the lost report to concerning department. For reactivation of Bluetooth enabled device the same process will repeat as first time issuing the Bluetooth enabled devices.

But the chances of damage after losing the Bluetooth device are less than the lost of access cards because the usage of Bluetooth active device for campus is not known by everyone against the access card.

Another limitation of Bluetooth enabled devices is they have some range limits outside the certain range they might not work properly. Unfortunately we have no mechanism to identify that the Bluetooth enable device holder is the actual owner of device until he press the wrong key for paring.
Chapter 7

Conclusions
My investigation of the Bluetooth technology was based on the classical triangular approach as shown in Figure 6.1 below. This approach has helped us to answer the main questions I set out to address in a holistic manner.

Based on my findings and analysis throughout this thesis, I draw the following conclusions.

- Bluetooth is a wireless technology which can do much more than just replace data cables between devices. With the release of the Bluetooth version 3.0 specification supporting higher data rates, Bluetooth is clearly a good choice for Wireless Personal Area Networks.

- The use of Bluetooth by mobile phone manufactures has been a great driver for this technology along with the push from the Bluetooth Special interest Group.

- In order to further increase market penetration, Bluetooth SIG should quickly address some of the security and interoperability issues I discussed.

- The device vendors must strictly adhere to the SIG’s Bluetooth specification and address interoperability issues on their own initiate as well. This will further increase users trust in this technology and also create a healthier market place.

- The SIG’s move to work together with UWB work group is a an excellent move and I believe that there should be more initiatives like that to increase the marketability of this technology and also to better serve the end users.
REFERENCES
REFERENCES


[2] Interview (via phone) with Miss Asma. Four Telecom Pakistan, Date May 2, 2009.


[8] This is extract from Bluetooth Dynamic Scheduling and Interference Mitigation by N. Golmie (National Institute of Standards and Technology Gaithersburg, Maryland Available from the internet: http://w3.antd.nist.gov/pubs/golmie_monet03.pdf [Cited 15 April 2009]


[10] This is extract from Forward by Dr. Sadie Creese Available from internet: http://www.nextwave.org.uk/downloads/forward_icwc.pdf [Cited 22 March 2009]


[12] This is extract from Bluetooth software works on UWB hardware (News from Open Interface North America) Available from internet:


[21] Analysis of the E0 Encryption System, By S. Fluhrer and S. Lucks Available from the internet: http://th.informatik.unimannheim.de/People/Lucks/papers/e0.ps.gz [Cited 8 March 2009]

[22] A hybrid architecture of UMTS and Bluetooth By Kwon, R. Kapoor, Y. Lee, M. Gerla Available from the internet:
[23] Figure Security  
Available from the internet: 
http://www.qualys.com/images/webservices/data_security_XL.gif  
[Cited 20 Feb 2009]

[24] Section 2.1 [Bluetooth Technology and Interference issues]

[25] Section 2.6 [Bluetooth Technology and Interference issues]

[26] Guest lecture by S. Ring, Spectrum allocation, regulation and standardization, 
3GPP vs. IEEE, UWB  
[Cited On 5 March 2009]

[27] Bluetooth synchronization  
Available from the internet: 
[Cited 1 March 2009]

[28] Bluetooth and WAP Push Based Location-Aware Mobile Advertising System  
By Lauri Nicklas  
Available from the internet: 
[Cited 1 March 2009]

[29] An Efficient and Fair Polling Scheme for Bluetooth  
By Yeng-Zhong Lee Rohit Kapoor Mario Gerla,  
Available from the internet: 
[Cited 26 Feb 2009]

[30] Bluetooth: An enabler for personal area networking  
Per Johansson, Ericsson Research, Manthos Kazantzidis, Rohit Kapoor, and Mario Gerla  
Available from the internet: 
http://www.ece.gatech.edu/research/labs/bwn/ee6610/supplements/blue.pdf  
[Cited 23 Feb 2009]

[31] SUN Java APIs  
Available from the internet: 
http://developers.sun.com/techtips/mobility/midp/articles/bluetooth2/  
[Cited 17 Feb 2009]

[32] A news article published on the official Bluetooth business portal  
Available from the internet: 
http://www.bluetooth.com/business/  
[Cited 13 Feb 2009]
[33] An article written by Brent Miller, referenced on the Prentice Hall technical reference portal
   Available from the internet:
   http://www.phptr.com/articles/article.asp?p=24243&rl=1
   [Cited 10 Feb 2009]

[34] Company portal and its product portfolio
   Available from the internet:
   www.Blueposition.com
   [Cited 8 Feb 2009]

   Available from the internet: Prentice Hall technical reference
   http://www.phptr.com/articles/article.asp?p=24265&seqNum=4&rl=1
   [Cited 29 April 2009]

[36] Company portal and its product portfolio
   Available from the internet:
   www.Blueposition.com
   [Cited 8 Feb 2009]

[37] An article written by Brent Miller, referenced on the Prentice Hall technical reference portal
   Available from the internet:
   http://www.phptr.com/articles/article.asp?p=24243&rl=1
   [Cited 10 Feb 2009]
APPENDIX
Appendix: Questionnaire

• Would you like to pay bills through BT ID Card enabling payment at canteen?
• Would you like to enter into the main library or class room without passing card into the machine readable?
• Would you like to enable your cell phone (BT enabled) as a student ID?
• Would you like to connect with university intranet through BT enabled device cell while you are on the move?
• Would you like to view the hotspot of other BT enabled devices within your BT device (cell phone) in order to communicate them would you like to make payments with BT enabled devices at canteen?
• Would you like to get calendar and emails updates?
• Would you like to get your lecture updates from your lecturers?
ABBREVIATIONS
List of Abbreviations

WLAN: Wireless Local Area Network
WPAN: Wireless Personal Area Network Standard
PAN: Personal Area Network
SIG: Special Interest Group
GFSK: Gaussian Frequency Shift Keying
ISM: Industrial Scientific Medicine
TDD: Time division duplex
SCO: Synchronous Connection Oriented
ACL: Asynchronous Connection Link
QoS: Quality of Service
ARQ: Automatic Repeat request
LMP: Link Manager Protocol
L2CAP: Logical Link Control and Adaptation Protocol
GPS: Global Positioning System
SDP: Service Discovery Protocol
IrDA: Infrared Data Association
HRFWG: HOME RF Working Group
UWB: Ultra Wide band Radio
PDA: Personal Digital Assistant
ISP: Internet Service Provider
DES: Data Encryption Standard
AES: Advanced Encryption Standard
UMTS: Universal Mobile Telecommunication Systems
ITU: International telecommunication Union
PIMD: Information Management Devices
SVA: Slow Vendor Adaptation