3-2004

Packet Analysis of Unmodified Bluetooth Communication Devices

Neal A. Watts

PACKET ANALYSIS OF UNMODIFIED BLUETOOTH COMMUNICATION DEVICES

THESIS

Neal A. Watts, 1st Lieutenant, USAF

AFIT/GCS/ENG/04-22

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government.

AFIT/GCS/ENG/04-22

PACKET ANALYSIS OF UNMODIFIED BLUETOOTH COMMUNICATION DEVICES

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Computer Science

Neal A. Watts, BS

1st Lieutenant, USAF

March 2004

AFIT/GCS/ENG/04-22

PACKET ANALYSIS OF UNMODIFIED BLUETOOTH COMMUNICATION DEVICES

Neal A. Watts, BS

1st Lieutenant, USAF

Approved:

/signed/	9 Mar 2004
_____	_____
Dr. Richard A Raines Thesis Advisor	Date
/signed/	9 Mar 2004
_____	_____
Major Rusty O. Baldwin, Ph.D. Committee Member	Date
/signed/	9 Mar 2004
_____	_____
Dr. Michael A. Temple Committee Member	Date

Acknowledgments

I would like to express my sincere appreciation to my faculty advisor, Dr. Richard Raines, for his guidance and support throughout the course of this thesis effort. The insight and experience was certainly appreciated. I would, also, like to thank my committee members, Maj. Rusty Baldwin and Dr. Michael Temple.

Neal A. Watts

Table of Contents

Page

List of Figures

Page

List of Tables

Page

Abstract

Bluetooth technology has potential for widespread use within the Department of Defense and the Air Force. An office environment using Bluetooth technology can wirelessly connect computers, printers, and other office equipment in order to share information over short distances. The clutter and annoyance of cables connecting equipment can be eliminated. Bluetooth provides a standard interface for connection, as opposed to many different proprietary cables.

The research is conducted indoors in a climate controlled environment, with minimal obstructions, to closely follow free-space signal propagation. Four different antenna orientations are used. The factors varied are the distance between devices, and the antenna orientation.

This research determined that two of the four cards tested have a specific distance where a change from Data High rate packets and Data Medium rate are used. The change occurs at two meters for one and three meters for the other. This research also shows that manufacturers transmit identical data in identical formats. Also, this research shows that antenna orientation, and receiver signal strength indicator values have no predictive value in determining packet type used for transmission.

PACKET ANALYSIS OF UNMODIFIED BLUETOOTH COMMUNICATION DEVICES

1. Introduction

1.1 Introduction

Bluetooth technology has potential for widespread use within the Department of Defense and the Air Force. An office environment using Bluetooth technology can wirelessly connect computers, printers and other office equipment in order to share information over short distances. The clutter and annoyance of cables connecting equipment can be eliminated. Bluetooth provides a standard interface for connection, as opposed to many different proprietary cables.

As with any new technology, especially wireless technology, there is a potential for misuse and possible security implications. Bluetooth provides support for encryption and frequency hopping to increase its security. One aspect of Bluetooth technology that has not been explored is how much information can be determined about a user, their data, or equipment just by examining the packet type.

1.2 Background

Wireless technology has a great potential for widespread use in the DoD. However, all wireless transmissions are vulnerable to interception and recording. Since capturing and recording wireless traffic is not very difficult, how much information could

a potential attack gain by analyzing Bluetooth traffic? Data analysis on packet traffic might expose some security risk that has not been discovered yet.

1.3 Research Focus

The focus of this research is to determine what kind of information can be determined using packet analysis. The two aspects being researched are the ability to determine the distance between users based on the type of packets being transmitted, and whether a specific manufacturer of Bluetooth cards can be identified by packet analysis. The ability to identify a specific manufacturer of Bluetooth devices might allow a potential attacker to exploit a possible weakness in that device. The ability to determine the distance between users could link a Bluetooth identity to a person's real identity. A Bluetooth user would not be able to remain anonymous.

Special hardware or software for the Bluetooth cards is not used. All cards used in this investigation are unmodified, commercially available, off-the-shelf devices. The use of unmodified devices helps determine how much information can be gained and exploited by someone with the ability to electronically sniff packets. Recording packets on a Bluetooth transmission is not a difficult task. It is possible and common for anyone to have the ability to capture and record a Bluetooth link.

1.3.1 Objectives

This research has two main objectives. The first objective is to determine if there are any differences in the way various manufacturers of Bluetooth devices transmit the

same data. If there are any variations, are they significant enough to determine a specific manufacturer?

The second objective is to determine if the distance between users can be determined based on the type of packets being transmitted between the pair. If the distance between users can be determined, then more research into the direction of the users can be done in the future. This research does not take direction into account, only distance.

1.3.2 Approach

This research follows a particular process to accomplish the above objectives. First, currently published research associated with Bluetooth technology is reviewed. Also covered is the Bluetooth core specification. An overview of the available Bluetooth sniffing applications is covered. Bluetooth Receiver Signal Strength Indicator (RSSI) values are recorded for various distances and antenna orientations. The RSSI metric is collected because it is the only signal power function provided in the Bluetooth specification. This data is analyzed to determine any statistical significance. The final step in data collection transfers a file between two laptops at various distances and antenna orientation to record the packet transmissions. This information is analyzed.

1.4 Summary

The primary focus of this research is to determine any differences in manufacturer implementations of the Bluetooth specification, and to determine if the distance between Bluetooth devices can be determined based on the type of packets being transmitted.

This research is restricted to commercially available hardware in a specific environment. It provides a foundation for further research.

The rest of the document is presented as follows. Chapter 2 provides an overview of Bluetooth research, literature and specification. This chapter also addresses some of the known security issues with Bluetooth technology. Chapter 3 describes the methodology for accomplishing the objectives of this research. Chapter 4 discusses the experiments conducted, the data collection and the data analysis. Chapter 5 contains a summary of the research, and presents the conclusions of this research.

2. Literature Review

2.1 Introduction

This chapter provides background information used as the basis for the research. Areas covered include an overview of wireless computing, the Bluetooth protocol, Bluetooth security and Bluetooth performance.

2.2 Overview of wireless computing in general

Wireless computing can be a great benefit to the computer user. Using one universal protocol to connect together a wide range of peripherals can make for a very clean workspace. The military applications of this technology are easy to see. Short range applications of wireless mice, keyboards and speakers make for a cleaner workspace. Medium range wireless networks for the office environment can eliminate the need to run new networking cable in an old building. The Army is even using long range wireless networks to enable soldiers to travel freely in the battlefield, yet still be in constant contact.

2.3 Overview of Bluetooth

The Bluetooth idea was launched by Ericsson in 1994 [Blu01]. The original intention was to make a wireless connection between an earphone or cordless headset and the wireless phone. Ericsson determined that a low power radio frequency technology was a feasible approach. In early 1998, Ericsson, IBM, Intel, Nokia, and Toshiba formed the Bluetooth Special Interests Group (SIG) [Blu01]. The purpose of the Bluetooth SIG is to “develop, publish and promote the preferred short-range wireless

specification for connecting mobile products, and to administer a qualification program that fosters interoperability for a positive user experience" [Blu01]. The SIG's goal is to have open licensed, free specifications and protocols, and to encourage other companies to join the SIG. Free access to the specification and protocols allows products to be interoperable and grow the Bluetooth market share. As of three years ago, there were over 2000 members in the SIG [Blu01].

In May 1998, the Bluetooth SIG officially announced the Bluetooth technology. A little over a year later in July 1999, the Bluetooth version 1.0 specification was released. This specification was updated to version 1.1 in February 2001. The most current version (1.2) was adopted November 2003. Version 1.2 implements Advanced Frequency Hopping, enhances voice processing, faster connection setup and is backward compatible with pervious versions. Version 2.0 is currently under development, but there is no date when it is scheduled to be released. [Blu01]

The name for Bluetooth was chosen by Ericsson, named after the king of Denmark, *Harald Blåtand*. *Blåtand* translates literally into "Blue Tooth" (king of Denmark from 940-981 [DeS03]. Blue Tooth did not have blue teeth, but had dark hair and a dark complexion. He earned his place in history by unifying Denmark under Christianity and conquering Norway and uniting the two nations. Following this uniting theme, the Bluetooth name was chosen to signify uniting the world of telecom and computers.

2.3.1 Technology Description

Bluetooth wireless technology is a short range wireless protocol designed as a cable replacement technology for desktop computers. It has since been expanded to include many more applications including keyboards, mice, phones, PDA's, digital cameras, and other portable electronic devices. Traditionally, these devices have used a proprietary cable that makes interconnection difficult which leads to a cluttered work space. If a user loses or breaks a cable, a replacement may be hard to find.

Bluetooth operates in the 2.402 to 2.480 GHz ISM (industrial, scientific, and medical) band and uses a fast frequency hopping spread spectrum (FHSS) technique. FHSS enables multiple access to the channel, reduces the amount of interference, and allows synchronized Bluetooth receivers to access the data. Bluetooth uses 79 different channels, 1 MHz per channel, and changes frequency 1600 times per second [Blu01]. If there is interference on one frequency only that transmission is lost. A limited number of errors caused by interference can be corrected by an Error Correction Code (ECC).

2.3.2 Description of the Bluetooth Protocol Stack

The Bluetooth protocol stack is shown in Figure 1. The goal of the protocol stack is to make it possible for different applications to communicate through a common interface. The common parts of the stack all applications use is the Bluetooth data link and physical layer. Some will use a vertical slice of the protocol stack. The Bluetooth protocol was designed so that it does not change any of the higher level protocols such as TCP/UDP and OBEX. Since the Bluetooth specification is an open specification, any vendor can incorporate proprietary protocols into the generic Bluetooth stack.

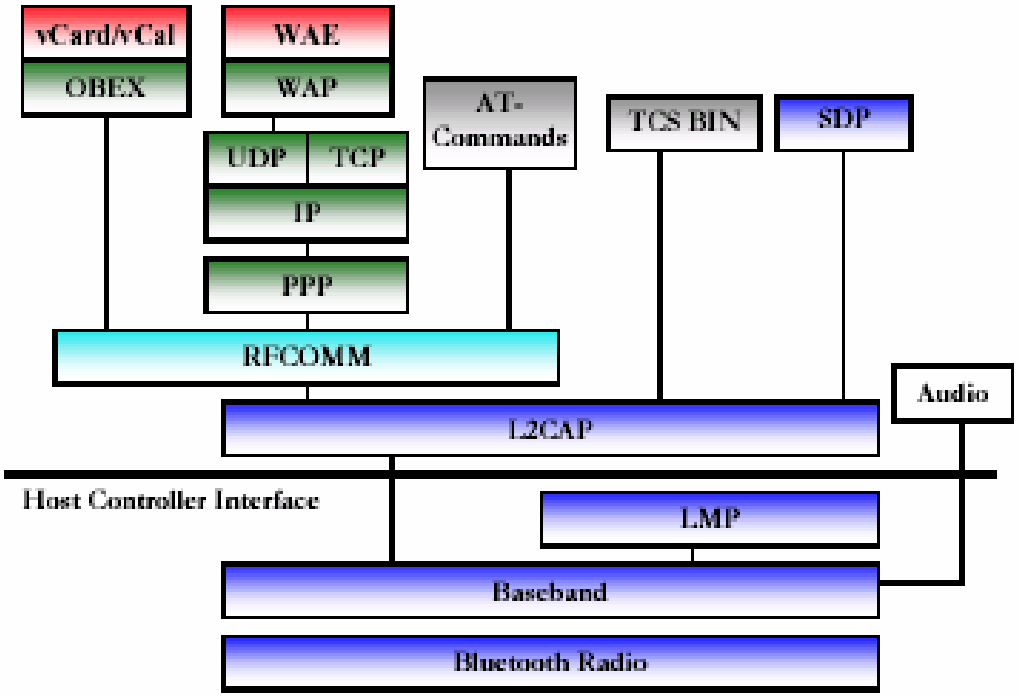


Figure 1 The Bluetooth Protocol Stack [Ana01]

The Bluetooth protocol has four major areas: the Bluetooth core protocol, cable replacement protocol, telephony control protocols, and adopted protocols. A simpler division is has only two layers the transport layers and the middleware layers [Bis01].

2.3.2.1 Bluetooth Transport Layers

The following briefly describes the Transport layers radio, baseband, link manager (LM), host controller interface (HCI) and the logical link control and adaptation protocol (L2CAP) [Bis01].

2.3.2.1.1 Radio Layer

The Bluetooth radio specifications describe the physical characteristics of the Bluetooth signal. The physical characteristics are important because this research focuses on the low level details of the Bluetooth signal.

2.3.2.1.2 Baseband Layer

The baseband layer defines how piconets are created and the physical RF transmission link. Two parameters are required for Bluetooth devices to talk to each other. One is the 48-bit devices address determined at the manufacture time (BD_ADDR). The second piece of information is the free running 28-bit clock. The clock advances once every 312.5 μseconds, corresponding to half the dwell time at a hop rate of 1,600 hops/sec [Bis01]. These two parameters form the basis for the protocol authentication and authorization functions.

2.3.2.2.1 Formation of Piconet and Scatternet

A piconet is a Bluetooth term for the network formed by two to eight Bluetooth nodes. A piconet is a short-range ad hoc network containing wireless links. Piconets have master/slave topology; each piconet can have only one master but up to seven active slaves. Each slave is given a temporary unique identifier called an active member

address (AM_ADDR). Other slaves can be synchronized with the master, but must be in the parked mode only (non-active).

Overlapping piconets form a scatternet. Scatternets extend the range of a device and allow it to communicate with multiple devices. A master in one piconet can be a slave in another piconet.

The hopping sequence is coordinated with the master device in the piconet. The time slot for a hop is 625 microseconds. Each baseband transmission lasts only one slot, but some packets can occupy three or five time slots. In the multi-slot packet, the frequency is not changed for those time slots. The hopping sequence resumes where it would have been if the device had used a single time slot.

There are two main types of transmission packets; asynchronous connectionless link (ACL), and synchronous connection-oriented links (SCO). The SCO link is used mainly for audio transmissions, and has a 64 kbps bi-directional data rate. The SCO link does not support retransmission if an error occurs but attempts to recover from the error using a forward error correction mechanism. "The ACL link is a best effort link appropriate for asynchronous data transmission" [Bis01]. The ACL does support retransmission, sequence number, and forward error correction.

2.3.2.1.3 Link Manager Protocol

The Link Manager Protocol (LMP) is used to set up the properties of the Bluetooth link between devices. The LMP coordinates all authorization, authentication, and encryption messages. LMP messages are also used to determine what kind of link is

established between devices (ACL or SCO) and the power modes of the devices. For SCO connections, the poll interval and the packet size are handled with LMP messages.

2.3.2.1.4 Host Controller Interface Protocol

The host controller interface in not a protocol. Its role is to act as a standard interface to the lower layers of the Bluetooth stack. “A host may instruct its baseband to create a link to a specific Bluetooth device, execute inquiries, request authentication, pass a link key to the baseband, request activating a low power mode etc”[Bis01].

2.3.2.1.5 Logical Link Control and Adaptation Protocol

The logical link control and adaptation protocol (L2CAP) “supports higher level protocol multiplexing, packet segmentation and reassembly, and the conveying of quality of service information.” [Blu01] The L2CAP “hides” the specifics of the lower layers and provides a packet interface to the higher layers.

At this level of the protocol the master/slave concept no longer exists. The L2CAP multiplexes channels over the devices’ ACL links. Each slave has only one ACL link, while the master has an ACL link for each slave. Packets are no longer limited to a one transmission time slot, they can be much larger. The segmentation and reassembly for transmission over the air are handled by the L2CAP.

2.3.2.2 The Middleware Protocols

The middleware protocols are the radio frequency communication (RFCOMM), service discovery protocol (SDP), and the telephony control signaling protocol (TCS).

These protocols are used as a link to bridge the Bluetooth protocols and make them compatible with existing protocols, like TCP/IP. Not all of the middleware protocols are used in a communication application. Each session may use different parts of the middleware protocols. The two middleware protocols most applicable to this research are discussed below.

2.3.2.2.1 Service Discovery Protocol

The Service Discovery Protocol (SDP) supports a wide range of Bluetooth equipped devices. When a Bluetooth device needs to service query another Bluetooth device the SDP is used. The SDP provides information about the services, but does not provide access to them. Access to the services is accomplished through different means once the device learns about them.

2.3.2.2.2 Radio Frequency Communication Protocol

The Radio Frequency Communication (RFCOMM) protocol is "used as to expose a serial interface to the packet-based Bluetooth protocol layers" [Bis01]. The RFCOMM emulates the signals of an RS-232 cable. It is based on the ETSI standard TS0 7.10 [Blu01]. The RFCOMM is useful because it permits legacy serial applications to be compatible with the Bluetooth link without any modification. The RFCOMM can "support up to 60 simultaneous connections between two Bluetooth devices [Blu01]."

2.4 Known Security Vulnerabilities of Bluetooth wireless technology

Bluetooth wireless technology is primarily designed as a cable replacement technology, not as an alternative to medium range wireless protocols such as IEEE 802.11. With short range, limited power output, and a constantly changing network, the security issues facing the designers are different from those encountered by an IEEE 802.11 wireless network. One of the bigger obstacles for a Bluetooth network is determining what devices are allowed to communicate with each other and how to prevent other devices from listening in. Establishing an ad hoc network is done with a combination of authentication and encryption, but both have their weakness. The Bluetooth protocol has specific weaknesses including eavesdropping and impersonation attack, location and identity attack, and a weakness in the encryption algorithm used. All of these are explained below.

2.4.1 Eavesdropping and Impersonation

In an eavesdropping attack, an attacker intercepts traffic between other Bluetooth nodes. In an impersonation attack, the attacking Bluetooth device hijacks another device's identity and pretends to be that device; a traditional man-in-the-middle type of attack. Man-in-the-middle attacks are not unique to Bluetooth but are a vulnerability common to many protocols.

There are two approaches to carrying out these types of attacks. The first approach is to determine the key being used. The second is to steal the initialization keys by actively participating in the authentication process. In the first type, the attacking device is in a receive-only mode; it does not transmit anything to the device it is

attacking. The attacking device generates all the keys up to a certain length. It then performs the "verification step in the initialization key protocol based on his guess, and the random strings communicated in the clear"[JaW01]. If the guess is correct, the results will be correct. Now the attacker can listen undetected on the other device's traffic.

2.4.2 Location and Identity Attack

In a location and identity attack, the goal is to associate a person's identity with the Bluetooth identity. Linking a Bluetooth identity to a person's identity can be used to track movements and habits. Identity matching attacks are easy to carry out as long as the victim's device is in the discovery mode. When a Bluetooth device is in discovery mode, it responds to discovery inquiries. The attacker presents his Bluetooth device to connect to the victim's device, which responds with its Bluetooth identity. An identity for a Bluetooth device is unique, thus it is easy to track.

Even a device is not in discovery mode, it can still be tracked. Tracking is done using the channel access code (CAC). The CAC is computed using the unique Bluetooth device identifier of the master device. Bits 39-62 of the CAC are bits 1-24 of the Bluetooth device address. Each message transmitted contains the CAC. Therefore, it is a pretty simple matter to determine the Bluetooth device address and keep track of them. This attack is made more difficult because the attacking device must be modified to extract the CAC from the messages being transmitted. In a normal Bluetooth device, the CAC is not reported to the application layer, and is hidden from the user.

2.4.3 Weakness of the Encryption Cipher

Bluetooth has the ability to encrypt the data being sent. "The Bluetooth specification 1.0 describes the link encryption algorithm as a stream cipher using 4 LFSR (linear feedback shift registers)"[Tra01] with a key length of between 8 and 128 bits. Note that none of the transmissions dealing with authentication and authorization are encrypted. A brute force attack takes at most 2^{128} operations to break the encryption. Jakobsson and Wetzel have shown that it can be broken with 2^{100} operations [JaW01]. Golic has shown that the cipher can be broken with a time and space complexity of 2^{66} [Gol97].

To carry out the attack an attacker guesses the first 93 bits of the cipher. Bluetooth uses four linear feedback shift registers (LFSR) for data encryption. The four LFSR total 128 bits, but are each sized differently. The LFSRs are 25 bits for the first, 31 bits for the second, 33 bits for the third and 39 bits for the fourth. The 93 bit size is chosen because that represents the size of the first three LFSRs. The last 39 bits, or the fourth LFSR, are computed based on the previous 93 bits and the contents of the summation register. The attacker can verify if the guess is correct by "comparing a string of the actual output to the generated output"[JaW01]. At least 128 bits of ciphertext and known plaintext are needed to verify the guess. The verification operations take on the order of 2^7 operations. This yields a total complexity of 2^{100} operations. Note that is attack must be carried out twice to be successful. The first time the attack is successful, it will yield the key used for one frame. It must be carried out a second time to get the master key.

The second attack described by Golic [Gol97] is even more efficient, because most of the work is done ahead of time. In this attack, the attacker chooses at random N states of the cipher, and computes the output key steam. This information is stored in a database for later use. Then the attacker observes M bits of the keystream. "If M*N > 2^{132} on expects to see a collision between the actual keystream and a keystream in the database" [JaW01]. By choosing N=M=2^{66}, the cipher can be broken in time and space complexity of 2^{66}.

2.5 Key Transmissions in the Clear

The first four of the five steps in the initialization process, as described in Section 2.6, are transmitted unencrypted. The initialization key is not a security concern because it is discarded. The link key is transmitted in the clear too. The link key is important to protect, since it is used in the generation of the encryption key.

2.6 Key Exchange

The Bluetooth specification defines the steps for key generation and management. There are a several kinds of keys used in Bluetooth, but the most important is the link key. This key is used for authentication between Bluetooth devices and is also used in the encryption process. In addition to the link key, there is an initialization key and an encryption key. All three keys are used in a five step process to establish secure Bluetooth communications. The five steps, as defined in the Bluetooth specification [Blu01] are:

1. Generation of initialization key
2. Generation of link key
3. Link key exchange
4. Authentication
5. Generation of the encryption key (optional)

The E_{22} algorithm [Blu01] derives the 128 bit initialization key, which is used to create the link key. The link key is created from a Bluetooth device address (BD_ADDR), a PIN, the length of the PIN, and a random number (IN_RAND). After the link keys are exchanged, the initialization key is discarded.

Authentication is based on a challenge-response scheme where the key is checked by using a 2-move protocol using symmetric secret keys. The authentication procedure can be done with either stored link keys or by pairing devices and entering a personal identification number (PIN). The link manager coordinates the actions between the two devices. The link key procedure is depicted in Figure 2.

The challenger sends the responder a random number, the device's address of the responding node and the link key. This is submitted to the E1 algorithm which calculates a signed response (SRES) value [Can01]. The responder sends the SRES value back to the challenger. If the two values are the same, authentication has been successful. If mutual authentication is required, then the responder and challenger change roles, which is coordinated through the Link Manager.

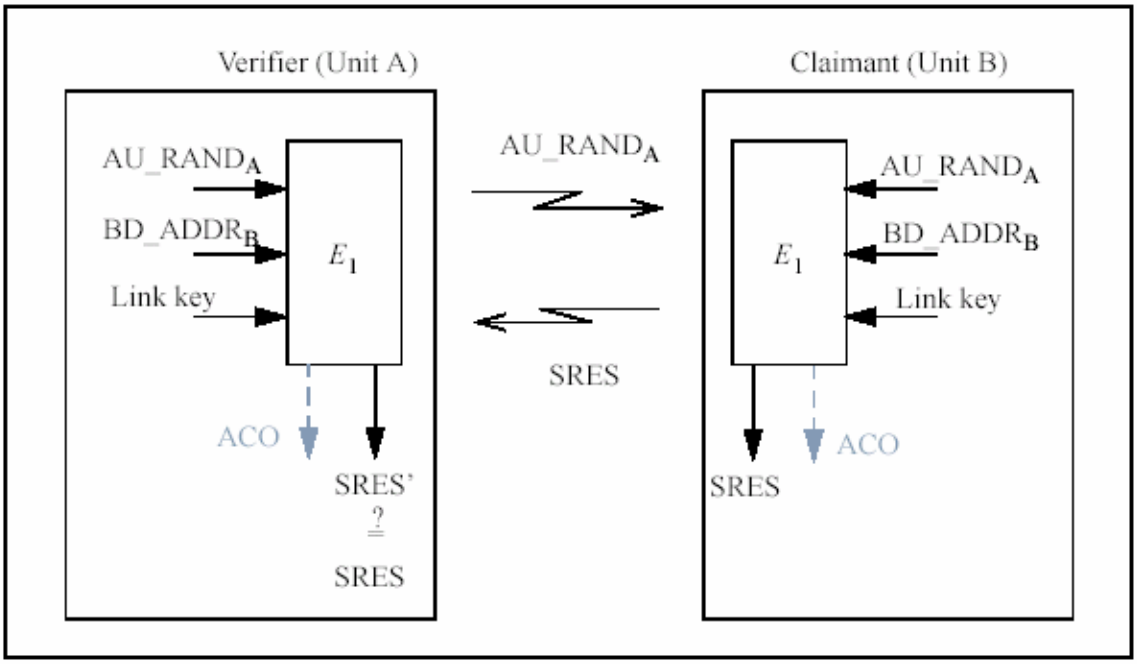


Figure 2 Challenge-Response for Bluetooth [Tra00]

If authentication fails, the SRES values do not match, and a random amount of time elapses until a new authentication attempt is made. The length of time between attempts is exponentially increases for each repeated failure to authenticate. This prevents an attacker from trying a large number of keys over a short period of time.

The encryption step is optional, however, if used, the key is between 8 and 128 its. The encryption key is composed of a 128-bit current link key, a 128-bit random number (EN_RAND), and a 96-bit ciphering offset number (COF). It is created using the 8-round SAFER+ encryption algorithm [Blu01]. The 96-bit COF is derived from either the master Bluetooth device address or the ACO value calculated from the authentication procedure.

2.7 Bluetooth Packet Format

The Bluetooth specification [Blu01] gives a general description of a Bluetooth packet. The packet is in little endian format, with the least significant bit sent over the air first. A typical packet consists of three main parts; the access header, the header and the payload. The access header is a fixed size of 72 bytes, the header is a fixed size of 54 bytes, and the payload can range from 0 to 2745 bytes. This is the general format for all Bluetooth packets. The payload portion varies according to the specific packet type the transmission is being used for. The specific packet types are frequency hop synchronization (FHS) packets for synchronization, HV packets for voice transmission, DV packets for a combination voice and data packet, and DM or DH packet types for asynchronous connections-less data transfer. The RS-232, RFCOMM, and Telephony Control Protocol (TCS) packet are all formatted different, but are not used in this research which focuses on baseband DM and DH packet types.

The DH*x*(*x*:1,2,3) use only a 16 bit CRC at the end of the payload to verify for data integrity. The DM*x*(*x*:1,2,3) use a 2/3 FEC coding that can correct 1 bit error out of 15 [JuP02]. The DM*x* packets are more likely to be used in a lower quality Bluetooth channel because it can correct errors without retransmission. The DH*x* packets are more likely to be used when the probability of transmission error is very low.

Table 1 Describing ACL Packet Types [Jup02]

	Payload Data Size(Bytes)	Maximum Packet Size(bits)	No. of Slots	FEC
DM1	0~ 17	240	1	2/3
DH1	0~ 27	240	1	No
DM3	0~ 121	1500	3	2/3
DH3	0~ 183	1496	3	No
DM5	0~ 224	2745	5	2/3
DH5	0~ 339	2744	5	No

The access header packet is used for synchronization, DC offset compensation, and identification. The first 4-bits are the preamble, the next 64-bits are the sync word, and there is an option 4-bit trailer at the end. The extra 4-bits are used only if a packet header follows the access header packet.

The packet header consists of six fields:

- AM_ADDR 3-bit active member address
- TYPE 4-bit type code
- FLOW 1-bit flow control
- ARQN 1-bit acknowledge indication
- SEQN 1-bit sequence number
- HEC 8-bit header error check

The total header length is 54-bits, consisting of these 18-bits repeated three times for error correction purposes.

The Bluetooth specification lists five common packet types; ID, POLL, NULL, FHS, and DM. The ID packet is 68-bits and is used in paging, inquiry and response routines. The POLL packet is 126-bits and is used by the master in a piconet to poll the slaves. A POLL packet forces the slaves to respond, even if the slave has no information to send. The NULL packet is 126-bits and carries no payload. It is used to respond to ARQN and FLOW packets. The frequency hop synchronization (FHS) packet is 240-bits, with a 144 information bits. It is a special control packet revealing the Bluetooth device address and the clock of the sender, among other things. The DM1 packet is used to support control messages or it can be used to carry regular user data.

2.7.1 Data Whitening

The Bluetooth specification describes how a simple form of bit scrambling is performed on packets before they are transmitted. *Data whitening* is randomizes redundant patterns. Whitening is not a form of encryption, but rather a very simple way to randomize the packet data. It is accomplished using a linear feedback shift register, the master clock and the packet. Both the packet header and the payload are scrambled.

2.8 Previous Related Work

Previous work related to Bluetooth has been done at AFIT by Captain Tim Kneeland and Lt Randal Noel [Kne03, Noe03]. Captain Kneeland's thesis investigated transmission range and data throughput for Bluetooth devices; Lt. Noel's thesis was on performance of Bluetooth while operating in 802.11 interference environment.

Captain Kneeland's thesis [Kne03] has some important implications for this research. His thesis found that is was possible to get reliable transmission up to 30 meters under ideal conditions while using Bluetooth devices designed for 10 meters. The main factor in determining range of transmission is the orientation of the antenna relative to each other. Antenna orientation impacts the signal quality and therefore the transmission range. The antenna orientation is a parameter that will be addressed.

Lt Noel's thesis [Noe03] found that Bluetooth throughput was unaffected while operating in an interference environment with IEEE 802.11 and provided good background information on how Bluetooth operates.

2.8.1 Channel Quality and Packet Type

There is a relationship between channel quality and the packet type for a Bluetooth network [JuP02]. "The selection of packet types can be determined using the original frequency hop sequence and the RF channel quality indicated in the frequency table, which is controlled by the link manager (LM) and the link controller (LC) of Bluetooth units." [JuP02]. The manufacturer of the Bluetooth card can determine the quality of the Bluetooth signal and the corresponding packet type to use. It is highly unlikely that the user will be able to control what kind of packets will be used for transmission.

Figure 4 shows the various levels of tolerance to error that the different packet types have. As expected, it shows that the DM1 packet is the most error tolerant, while the DH5 packet is the least error tolerant. Signal quality is the main factor in determining what type of packet is used for transmission.

2.8.2 Packet Types and Throughput

Previous work [Val02] has examined the relationship between packet type and throughput. This research is done with the six Asynchronous Connection Link packets that are used for data transfer. The six packets types are DM1, DH1, DM3, DH3, DM5 and DH5. Tests were conducted in high signal to noise ratio channels and low signal to noise ratio channels. The most important conclusion is that "the DH1 and DH3 packets never achieve maximum throughput" [Val02]. The research suggests that these packets should only be used if latency or data-length requirements require their use. It was also found that the "DM 1 frames are of limited utility and should be reserved only for the harshest of channel conditions" [Val02].

2.9 Summary

This chapter reviewed several topics necessary for a fundamental understanding of Bluetooth. First, an overview of wireless computing was covered. Next, the Bluetooth protocol was described. Additionally, Bluetooth security issues and performance were discussed. The next chapter defines the experimental methodology of this investigation.

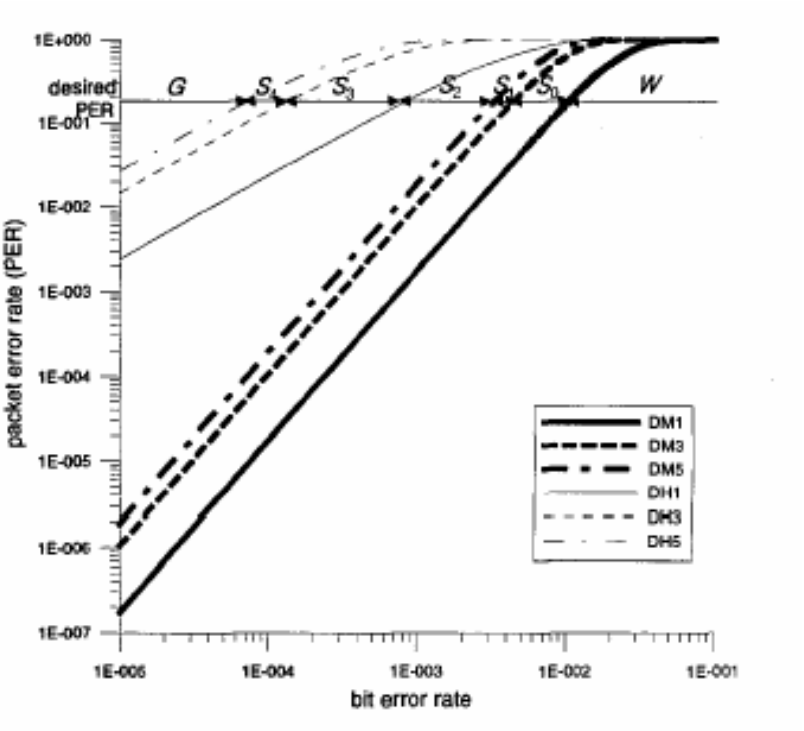


Figure 3. PER versus BER for ACL packets. [JuP02]

3. Methodology

3.1 Introduction

This chapter discusses the problem definition, specific research objectives, and a solution methodology. The problem definition explains the problem under study. Secondly, the objectives are discussed. Finally, the solution methodology is presented in detail to include system boundaries, parameters, factors, evaluation technique and experimental design and validation.

3.2 Problem Definition

The Air Force continually encourages the use of new technologies. New technology can reduce cost, manpower, and increase productivity. However, new technology often means new security risks. One of these new technologies is the Bluetooth wireless networking protocol. As with many new technologies, most security aspects have been examined, but maybe not every aspect. One aspect that has not been explored is how much information can be determined by the type of packet used for transmission. Another interesting aspect to explore is if the distance between users can be identified by the type of packet being transmitted between two devices.

3.3.1 Research Objectives

The research objectives of this study consist of four parts:

1. To determine if Bluetooth devices from different manufacturers of transmit data in identical ways.

2. If there is a difference in the way manufacturers format a Bluetooth packet, are there any security implications that can be determined?
3. Determine if a correlation exists between RSSI values, distance, antenna orientation, and manufacturer.
4. Determine the distance between users by examining packet type.

It is expected that there will be a difference in the way that different manufacturers transmit the same data over a Bluetooth link. The difference is expected because of vendor specific implementations of the Bluetooth protocol. One vendor may have a more efficient way of transmitting the data on the packet level compared to another vendor. Different hardware chipsets used by manufacturers may have some impact on the data transmissions. Further, manufacturers use different antenna configurations that may work better than others.

To achieve the research goal the main investigative tool used will be Merlin, manufactured by Computer Access Technology Corporation. Merlin is a packet capture device for recording and analyzing packets in a Bluetooth piconet. Merlin is connected to a computer via a USB connector and has a software interface. Merlin is a passive device in a piconet, it does not transmit any Bluetooth packets, it only receives and records packets.

One research objective is to determine how various manufacturers of Bluetooth devices format a Bluetooth packet for transmission of identical data. If specific fields within a Bluetooth packet can be changed by a manufacturer, are there any security

weaknesses that can possibly be exploited? Does one manufacturer make a more secure Bluetooth card than another manufacturer? All manufacturers must pass certain test criteria to sell a network card that carries the Bluetooth name. However, each manufacturer is free to design and manufacture network cards. As long as the network card meets the Bluetooth specification, and passes the Bluetooth test, the card can be sold as a Bluetooth networking card.

It is expected that most of the fields in the packet will remain unchanged from vendor to vendor. Some fields will change, because the device clock and the Bluetooth address will be different for each card.

Another question being examined in this research is if the distance between users can be determined by the type of packet being transmitted. To accomplish the goal of determining distance, research on what factors determine the difference between DH and DM packets.

The Bluetooth specification does not specify the conditions when DM or DH packets are used. The specification only says "quality measurements in the receiver of one device can be used to dynamically control the packet type transmitted from the remote device for optimization of the data throughput" [Blu01]. There is no reference as to the input factors for "quality measurements". Prior research [BaP99] has suggested that the bit error rate of the RF channel is the primary factor for packet type. However, the factors that influence the RF channel quality are not known. The RF quality between different manufacturers may be attributed to antenna designs or other hardware that offer

better reception of the RF signal. The channel bit error rate information is not available to the user.

3.3.2 System Boundaries

The System Under Test consists of all components required for Bluetooth communication. Two system components are used. One is used for file transfer. It is composed of two Dell Inspiron 8200 laptops with Bluetooth NIC's and Windows 2000. The second system is one Dell Inspiron 8200 running Red Hat 8.0 Linux and one Dell Inspiron 8200 running Windows 2000 operating system. These computers are used for the RSSI portion of the testing. No files are transferred between the two laptops, only the signal strength between the two Bluetooth NIC's is measured. For each vendor's Bluetooth card, the corresponding software package is also installed on the laptops. The software is needed to be able to transfer files between the two laptops. All the Bluetooth cards used in this research meet the Bluetooth specifications Version 1.1.

The Component Under Test is the Bluetooth NIC that connects to the laptop. These Bluetooth cards are tested in pairs, both cards being from the same manufacturer and model. Testing the cards in identical pairs is done to eliminate errors caused by different manufacturers.

3.3.3 Testing

Testing consists of verification, file size, file type, and repeatability. Verification is needed to be sure that the entire file was transferred and not only part of it. A text file

is used for this reason because it is easy to see in the packet payload where the text begins and ends in order to verify complete file transmission. The file size for testing is a 1000 KB file. The 1000 KB file creates enough packets so that there are a large number of packets to analyze. The file is also convenient to use because it is already on hand. Also, using the same file every time ensures that the transmission payload is the same every time.

The Bluetooth protocol supports other high-level networking protocols such as TCP/IP and FTP. To test all the high-level protocols is impractical and beyond the scope of this research. This experiment is limited to File Transport Protocol (FTP) traffic using whatever packet type the vendor card chooses to transmit. FTP was chosen because it is a common method of transferring files between computers. FTP is a method of file transfer that Windows 2000 uses to transfer files. The DM5 (Data Medium rate 5) and DH5 packet types are expected to be the most common packet types because they have the largest payloads for transmitting data. Higher throughput is achieved by using the longest time slot with the largest payload.

3.3.4 Physical Setup

The physical setup of the experiment is designed to minimize interference. The experiment is performed indoors in a large 500 seat auditorium. The experiment is set up on a stage 12 meters wide and 7 meters deep is surrounded on three sides by walls. The stage floor is a carpet. The ceiling is approximately 10 meters tall.

The laptops are set on wooden stools that are 97.248 centimeters high. Wooden stools were used to minimize interference with the RF signal. All distances are measured from the back of one laptop to the back of the second laptop. Merlin sits on a cart. Merlin is physically located within 0.75 meters of the master laptop of the piconet. This distance was chosen because the USB cord connecting Merlin to the laptop is only 0.75 meters long. Merlin is located 1 meter off the floor sitting on a cart. The recordings from Merlin are the same whether it is connected to the master or the slave of the piconet, but for consistency, Merlin is always connected to the master. The choice of master or slave is made via software in the initial setup wizard in Merlin.

The network cards used in this experiment are all Bluetooth USB cards. The USB cards are connected directly to the laptops. The USB cards are mounted in the top USB port, and the USB cable for Merlin is located in the bottom port. The USB ports are located on the back left of the Dell Inspiron 8200 laptop, and on the back right of the Dell Latitude D600 laptop.

The Bluetooth specification defines three power levels for Bluetooth cards. The different power levels have different transmission ranges. Table 2 below describes the power levels and transmission ranges for differing power class. All the Bluetooth cards used in this experiment are Power Class 3 cards designed for maximum transmission range of 10 meters.

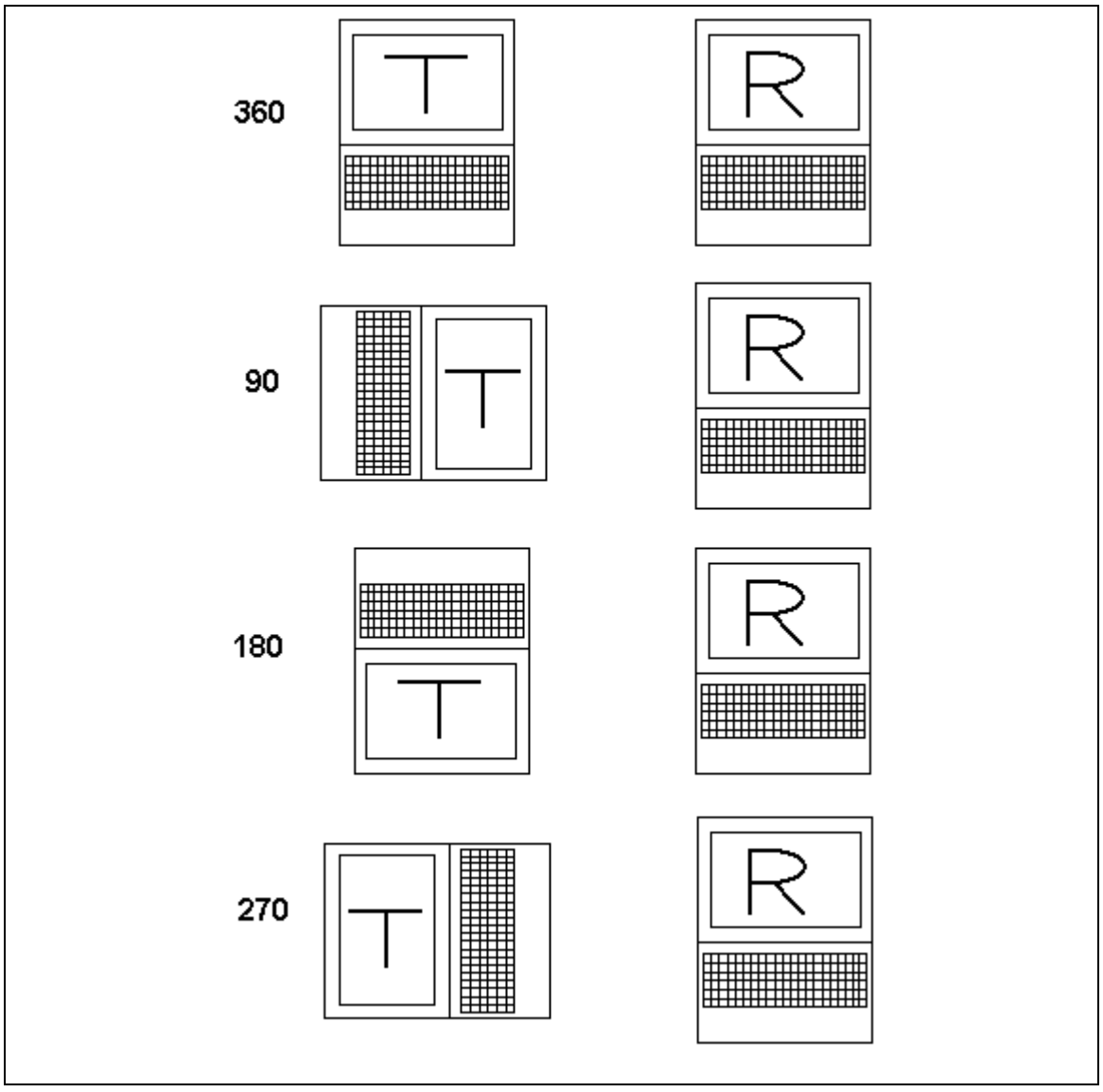
Table 2 Power Classes [Blu01]

Power Class	Maximum Output Power (Pmax)	Nominal Output Power	Minimum Output Power[1)]	Power Control
1	100 mW (20 dBm)	N/A	1 mW (0 dBm)	Pmin<+4 dBm to Pmax Optional: Pmin[2)] to Pmax
2	2.5 mW (4 dBm)	1 mW (0 dBm)	0.25 mW (-6 dBm)	Optional: Pmin[2)] to Pmax
3	1 mW (0 dBm)	N/A	N/A	Optional: Pmin[2)] to Pmax

One of the parameters for this research is the pair-wise antenna orientation. One antenna (located in the laptop) is rotated in 90 degree increments, and the other antenna (located in the other laptop) remains stationary. For this research, the master of the piconet is the antenna that is rotated. The slave is the laptop that is moved further away from the master as the distance increased. The master laptop is never moved, it is only rotated.

For this research, four antenna orientations are used and described as; 360 degrees, 90 degrees, 180 degrees and 270 degrees. When both antennas are pointing in the same direction, this is defined as the 360 degree orientation. When the transmitter is pointing at the receiver, is the 90 degree orientation. The 180 degree orientation is when the two antennas are pointing in opposite directions, and the 270 degree orientation is when the transmitter is pointing away from the receiver. Figure 4 below gives a graphical description of the antenna orientation setup.

Figure 4 Antenna Orientations [Tay04]



3.3.5 Performance Metrics

Possible relationships between RSSI value, distance, antenna orientation and Bluetooth device manufacturer are investigated to predict the packet type transmitted.

One of the research goals is to determine the signal strength threshold value as indicated by the RSSI value that causes a packet switch from the DH type packet to the DM type packet.

The performance metrics used in this research are the distance and RSSI signal strength values which cause a switch between DH and DM type packets. Both distance and signal strength are expected to be different for each card manufacturer because of different antenna designs and the type of chipsets used in the hardware.

The RSSI value is determined by three factors: distance, antenna orientation, and the network card manufacturer. The packet type has no impact on the RSSI value. The factors that influence packet type are the signal strength, distance, antenna orientation and the manufacturer of the network card and the corresponding software.

The performance metric used to evaluate the packet type experiment is the percentage of DH packets compared to the total number of data packets. The null and hop packets are a significant amount of packets transmitted, and are of no use in this research. The null and hop packets are not used for any evaluation metric, and are ignored. A sharp drop in the percentage of DH packets at a given distance would be a useful pattern to recognize. Observing the distance at which a change in packet type occurs could allow an observer to make an educated guess at the distance between Bluetooth devices.

3.3.6 Parameters

The parameters for this experiment are as follows:

- Packet Type – The signal quality and corresponding bit error rates are determining factors in the type of packets transmitted. The user has no control over which type of packet are used for transmission.
- Method of file transfer – Each manufacturer supplies software with the card. However, an alternate method for transferring files is to use the Windows Explorer and drag and drop the file from one laptop to the other. Both versions use FTP as the underlying protocol, but the user interface is different.
- The manufacturer's software – Each manufacturer supplies their own software for use with their Bluetooth card. Using the appropriate software is important to make sure the device is operating as intended by the manufacturer.
- Environmental conditions – Temperature and humidity can impact RF signal quality. The effects of these two parameters are mitigated by testing indoors in a climate controlled environment. All tests are done under similar conditions.

3.3.7 Factors

The factors for this experiment are:

- The manufacturer of the Bluetooth network card. This experiment uses the following Bluetooth Card: Epox BT-DG02 USB, D-Link DBT-120

USB, Hawking Technology H-BT10U USB, Belkin F8T003 USB. These cards are a representative sample of industry standards.

- Distance between laptops – The distance between Bluetooth devices can have an impact on performance. Beyond the protocol's 10 meter limit, numerous packet errors can occur. The experimental starting distance is 0 meters apart, and increases in 1 meter increments out to 10 meters.
- Antenna Orientation – This may have some impact on the error transmission rates. It will have an impact on the transmission range, as noted by Kneeland [Kne03]. Antenna orientation is varied in 90 degree increments on only one machine.

3.4.1 Evaluation Technique

For this research, direct measurement is used. This approach was chosen because it would be impractical to create a simulation for the system under test. It is much easier and very practical to run the experiment in a live environment. While testing in a real life environment may introduce some errors, it is a very good representation of how the system may be used outside of an academic study. Direct measurement is also the simplest means to determine the correlation between network card manufacturer and packet type.

3.4.2 Experimental Design

The experimental design for this research has multiple steps. The first step is to get the RSSI values at various distances for different pairs of manufacturer cards. The second step is to transfer data between two laptops and record the packet transmissions. Once the two steps are accomplished, the relationship between distance, signal strength, manufacturer and packet type can be determined.

3.4.3 Settings on Merlin

All the testing is performed using the Merlin recording wizard. Screen shots of the settings used with Merlin are provided in Appendix A. The only change made to the default settings is to increase the buffer size to 128 MB from the default of 1 MB. Increasing the buffer size is required to capture the entire file transfer data packets. The extra buffer space that is not used is discarded at the end of the recording.

Merlin records all the packets transmitted from the time the piconet is first established until the piconet is destroyed, or until the buffer on Merlin is full. The packets that are of most interest are the packets used to transmit data, and the link manager protocol packets. Many packets recorded in Merlin are the polling packets between the master and slave. The polling packets are of little use in this experiment and are ignored. Another large number of packets are for the hopping frequency, and are of limited use in this research. Merlin has a setting that hides the null and poll packets, only data packets and link manager protocol packets remain. Hiding the null and poll packets is a useful feature to see where the data transmission begins and ends.

3.4.4 Signal Strength

Some Bluetooth cards have the ability to read the Receiver Signal Strength Indicator (RSSI) value. This is accessed through the Host Controller Interface (HCI) software. All transceivers supporting variable power transmission links make use of the RSSI value. The RSSI feature is an optional item that some Bluetooth manufacturers choose to support. The Bluetooth specification gives a brief description of how the RSSI value is calculated and used. "The RSSI measurement compares the received signal power with two threshold levels, which define the Golden Receive Power Range. The lower threshold level corresponds to a received power between -56 dB and 6 dB above the actual receiver sensitivity. The upper threshold level is 20 dB above the lower threshold to an accuracy of +/- 6 dB" [Blu01]. Figure 5 gives a graphical representation of the above description.

3.5 Summary

The experiment outlined in this chapter is intended to determine if there are any differences in the way Bluetooth cards from different manufacturers transmit data. Based on differences established between manufacturers, Chapter 4 describes the approach taken to determine which one is more efficient and if there are any security implications between the vendors. Also being examined is if the distance between users can be determined by the packet type that is being transmitted.

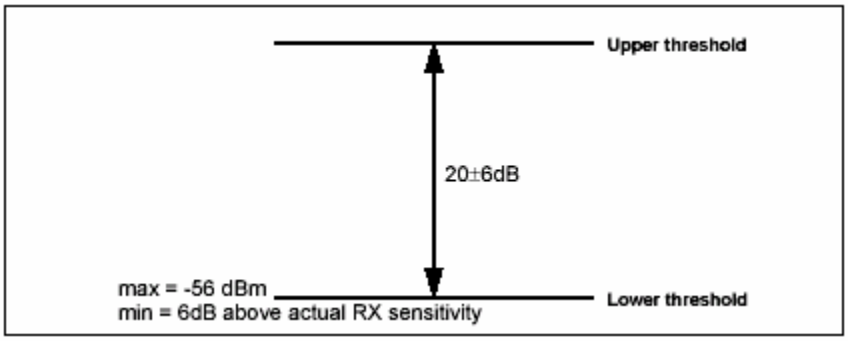


Figure 5. RSSI Range and Accuracy [Blu01]

4. Experiments, Data, and Analysis

4.1 Introduction

This chapter discusses orientation and packet type experiments using commercial off-the-shelf Bluetooth USB cards. First, a test is performed to see if data is transmitted differently by manufacturers. Second, the antenna orientation experiment is discussed along with the data collected and data analysis. Third, the distance and packet type experiment is discussed along with the data collected and the data analysis.

Analysis for each card pair is performed separately. Each card is examined separately because the data collected for each card is very different. To aid in the analysis of research results, JMP version 5.0.1.2 is used. JMP is a statistical analysis program produced by SAS institute Inc.

4.2 Supported Features

Of the four cards tested, the DLink, Hawking, and Belkin cards all support the full range of features. The Epox cards tested support all features of the other three with the exception of power control, i.e., the Epox card transmits at one fixed power output level. The transmit power on a card is adjusted based on the RSSI value of the device. "If the RSSI value differs too much from the preferred value of a Bluetooth device, it can request an increase or a decrease of the other device's TX power" [Blu02].

4.2 Manufacturer Differences

The first test performed is to determine if there are any differences in the way various manufacturers transmit the same data. The approach is to record all the packets

used for transmitting the test file, and then examine the packets to see if there are any unique characteristics that can be noted. Upon examination of various aspects of the recording, it was determined that there are no significant differences in the way the four different manufacturers transmit the test file.

The areas that are examined are how the initial link pair between the two devices is set up, the Link Manager Protocol messages used, and the payloads of the data packets. All the manufacturers take the same steps to set up the link, the LMP message are virtually identical, and very little data is sent before the actual file. The only difference is the packet type used for transmission of the test file. However, packet type is dependent upon the link quality and other factors, not determined by manufacturer of the card. The uniformity of the initial transmission does not contain any unique identifiers to be able to identify a specific manufacturer. The only time there could be a fingerprint of a manufacturer is during the initial set up. Once the file transfer begins, the only data being transmitted it the test file and occasionally some information in the Link Manager Protocol packets.

4.3 Antenna Orientation

For the antenna orientation experiment, the objective is to collect data on the distance and antenna orientation and the corresponding RSSI values. The RSSI value metric would then be combined to see if there is a relationship between distance and RSSI and what impact, if any, may result from antenna orientation. Also being examined is if there is a specific RSSI threshold value that determines packet type. A 90% confidence interval is used for the antenna orientation and RSSI value tests. A 90%

confidence was chosen because of the inherent inaccuracy of the RSSI measurement (+/- 6 dB).

The RSSI values for the Epox card are the highest of the four cards at 18 dB, but falling to zero dB at distances just over one meter. Table 3 below shows the RSSI values with respect to distance for the Epox card.

Table 3. RSSI Values for Epox (dB)

Distance (meters)	Orientation (degrees) 90	180	270	360
0	18	18	10.17	15.18
1	4.04	11	6.95	0.07
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0

The ANOVA analysis from JMP showed that the only significant factor was distance. The Table 5 shows the ANOVA results. The majority of the variation (87.3%) is due to distance. This is expected because of path loss. The antenna orientation was not a factor, and did not have any impact in the ANOVA. The combination of distance and orientation accounted for 12.6% of the variance.

Table 4. ANOVA for Epox RSSI Values

Variability Chart for Average RSSI Value

Analysis of Variance

Source	DF	SS	Mean Square	F Ratio	Prob > F
Distance	10	2713.493	271.349	28.6866	<.0001
Antenna	3	30.84858	10.2829	1.0871	0.3696
Distance*Antenna	30	283.7727	9.45909	.	.
Within	88	0	0		
Total	131	3028.114	23.1154		

Variance Components

Component	Var Component	% of Total	Plot%	Sqrt(Var Comp)
Distance	21.824185	87.3		4.6716
Antenna	0.024963	0.1		0.1580
Distance*Antenna	3.153030	12.6		1.7757
Within	0.000000	0.0		0.0000
Total	25.002178	100.0		5.0002

The RSSI values for the Hawking card are much different. Table 6 below shows the RSSI values for the Hawking card. Most of the values of RSSI values were negative, but did not seem to drop very dramatically as distance increased.

Table 5. Hawking Technologies RSSI Values (dB)

		Orientation (degrees)			
		90	**180**	**270**	**360**
Distance (meters)	**0**	0	0.81	-2.66	0
	1	0	0	0	0
	2	-1.67	-0.35	0	-0.34
	3	-3.38	-2.36	-2.21	-3.9
	4	-2	-0.19	0	-5.43
	5	-4.1	-1.88	-2.26	-6.34
	6	-4.15	-3.02	-3.2	-1.61
	7	-3.58	-7.92	-6.03	-3.55
	8	-8.61	-5.1	-4.72	-7.16
	9	-9.05	-4.95	-2.58	-3.15
	10	-5.62	-3.19	-4.59	-7.23

The ANOVA analysis from JMP is shown in Table 7 below. The only significant factor is distance, and it makes up 56.4% of the variation. Antenna orientation was not a significant factor, and only had minimal impact in the variation at 2.2%. The interaction of the distance and orientation is not a significant factor. However, they did make up 41.4% of the variability.

Table 6. ANOVA for Hawking Technologies RSSI Values

Variability Chart for Average RSSI Value

Analysis of Variance

Source	DF	SS	Mean Square	F Ratio	Prob > F
Distance	10	573.4915	57.3491	6.45076	<.0001
Antenna	3	42.4504	14.1501	1.59164	0.2120
Distance*Antenna	30	266.7088	8.89029	.	.
Within	88	0	0		
Total	131	882.6507	6.73779		

Variance Components

Component	Var Component	% of Total	Plot%	Sqrt(Var Comp)
Distance	4.0382377	56.4		2.0095
Antenna	0.1593891	2.2		0.3992
Distance*Antenna	2.9634314	41.4		1.7215
Within	0.0000000	0.0		0.0000
Total	7.1610582	100.0		2.6760

The data for the Belkin card looks very similar to that of the Hawking card. The card starts off right at zero dB for close distances and gradually drops to – 8 dB as distance increases. The table below shows the data collected for the RSSI experiment.

Table 7. Belkin RSSI Values (dB)

Distance (meters)	Orientation (degrees) 90	180	270	360
0	0	0.07	-0.41	-0.05
1	0	0	0	0
2	0	0	0	-6
3	-3.32	0	-1.61	-6.71
4	-8.87	-1.45	0	-4.02
5	-9.12	-4.68	-4.16	-6.93
6	-9.93	-9.44	-8.02	-9
7	-9	-8.78	-7.86	-8.98
8	-6.06	-6.38	-4.63	-8.6
9	-5.89	-7.22	-5.23	-8
10	-5.89	-7.22	-5.23	-8

The ANOVA analysis from JMP shows that the significant factors were distance and antenna orientation. The results are shown in Table 9 below. The significant factors for the Belkin card are both distance and antenna orientation. Distance is 70.5% of the total variance, and antenna orientation is 8.1%. Antenna orientation is much higher compared to the other three cards tested. The interaction of distance and orientation accounts for 21.3% of the variance. This is rather high percentage of variance for a second level interaction. This is most likely due to the inherent inaccuracy of the RSSI value measurement.

The DLink card appeared to fare the worst in the RSSI testing. Table 10 below shows the data collected for the DLink card. It appears as if the lowest RSSI value the hardware supports is -10 dB. This lower threshold is reached in only three meters. The RSSI values drop very rapidly with distance.

Table 8. ANOVA for Belkin RSSI Values

Variability Chart for Average RSSI Value

Analysis of Variance

Source	DF	SS	Mean Square	F Ratio	Prob > F
Distance	10	1239.802	123.98	14.2139	<.0001
Antenna	3	135.6887	45.2296	5.1854	0.0053
Distance*Antenna	30	261.6731	8.72244	.	.
Within	88	0	0		
Total	131	1637.164	12.4974		

Variance Components

Component	Var Component	% of Total	Plot%	Sqrt(Var Comp)
Distance	9.604815	70.5		3.0992
Antenna	1.106276	8.1		1.0518
Distance*Antenna	2.907479	21.3		1.7051
Within	0.000000	0.0		0.0000
Total	13.618570	100.0		3.6903

Table 3. DLink RSSI Values (dB)

		Orientation (degrees)			
		90	**180**	**270**	**360**
Distance (Meters)	**0**	0	2.6	-0.2	0
	1	-9	-5.85	-0.046	-6
	2	-7.21	-5.28	-3.97	-7.35
	3	-10	-9.81	-8.42	-9.2
	4	-7.64	-3.43	-6.84	-9
	5	-10	-9.74	-10	-10
	6	-8.53	-9.35	-10	-10
	7	-10	-10	-10	-9.73
	8	-10	-3.57	-8.67	-10
	9	-4.64	-10	-10	-9.72
	10	-10	-9.52	-9.2	-10

The ANOVA analysis is shown in the Table 11 below. The significant factors are only distance. The distance accounts for 70.5% of the variance. Antenna orientation accounts for only 1.6% of the variance. The combination of the two accounts for 27.9% of the variance.

Table 4. ANOVA for DLink RSSI Values

Variability Chart for Average RSSI Value

Analysis of Variance

Source	DF	SS	Mean Square	F Ratio	Prob > F
Distance	10	1190.527	119.053	11.1046	<.0001
Antenna	3	52.42627	17.4754	1.6300	0.2032
Distance*Antenna	30	321.6321	10.7211	.	.
Within	88	0	0		
Total	131	1564.586	11.9434		

Variance Components

Component	Var Component	% of Total	Plot%	Sqrt(Var Comp)
Distance	9.027639	70.5		3.0046
Antenna	0.204677	1.6		0.4524
Distance*Antenna	3.573690	27.9		1.8904
Within	0.000000	0.0		0.0000
Total	12.806006	100.0		3.5785

4.4 Distance and Packet Type

As previously mentioned, most of the packets observed in transmission are for the hop frequency and the null packet. As transmissions times increase, so does the number of hop packets. The increased number of hop packets is because the hop frequency changes every 625 microseconds. A typical number of packets needed to transmit the test file are around 28,000 total packets. However, this can vary considerably. The DLink card, at longer distances, requires over 800,000 packets to transmit the test file. This is an exception case.

The second goal of this research is to determine at what distance a manufacturer switches from using a DH packet to a DM packet. Each card is evaluated separately. The performance metric used to make this determination is the percentage of DH type packets compared to the total number of data packets (comprised of both the DM and DH packet type). In cases where the DH type packet is used, there are usually an equal number of DM1 packets compared to DH packets. The large numbers of DM1 packets

are observed because Bluetooth uses the DM1 packet for L2CAP message. DM1 packets are also used where only a small amount of data needs to transmitted.

For all the cards tested, a complete ANOVA is performed using JMP for each packet type. Each card is analyzed separately because it allows for examination of the significant factors of each manufacturer. The complete ANOVA tables are located in Appendix E-H, but only the important highlights are discussed within the thesis. A confidence interval of 95% is used to determine significant factors.

4.4.1 D-Link DBT-120 USB

The DLink card has the most clear-cut definition between the DH and DM packets. At the zero and one meter distance, the DH packet type comprises between 0.5% and 55% of the total data packets. All the distances past two meters exclusively use the DM packet. Past two meters, the DH packet type was almost never used. Table 11 shows the percentage of DH type packets with respect to distance.

The DM1 packet is used more as the distance increases. From three meters to ten meters, the DM1 packet accounts for nearly 100% of the data packets. The DM5 packet was not used after five meters. It is known that the DM1 packet is used most often when the signal quality is very poor. Also, the extremely large number of packets transmitted with errors provides evidence of poor signal quality. Given the Merlin test configuration, there is no way to record the channel bit error rate to determine what constitutes a poor quality signal.

It is important to note that the DLink card was physically the smallest of the four cards tested and seemed to have problems transmitting at distances past five meters. Common problems encountered are failure to send the file, failure to locate the other laptop, errors in the packets that were transmitted, and very low throughput.

The variability charts for all the cards shows the percentage of DH type packets used in transmission. What is expected is the DH type used at short ranges, then not be used at all at longer ranges. When no DH packets are used, then the DM packet type is used. Ideally there is a distinct break at certain distances where the packet type switch occurs. In Figure 6, the DH packet is used for the zero and one meter distance.

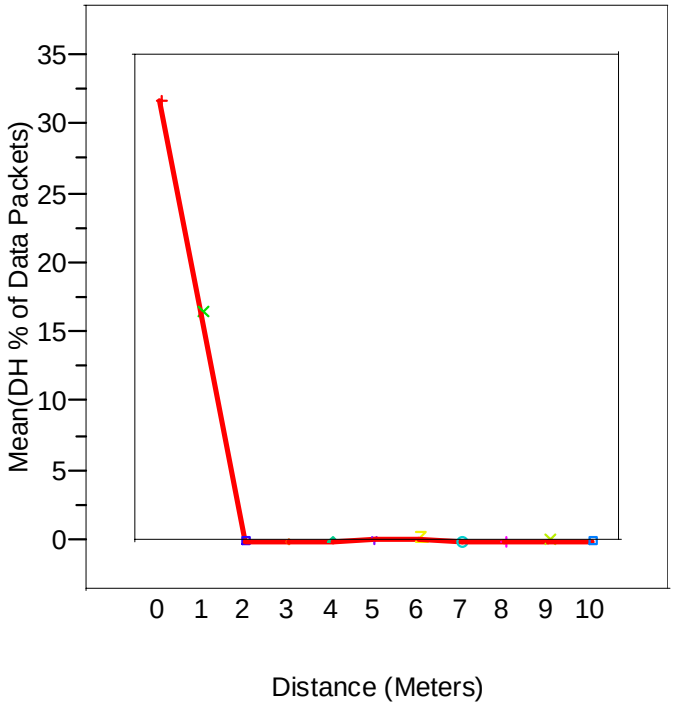


Figure 4 DH packet type at distance for DLink

The ANOVA from JMP shows the significant factors to be distance and distance with orientation. Of these factors, distance accounts for 49.8 % of the variance, and

distance and antenna orientation account for 32.9%. The repetitions of each file transfer combined with distance and orientation account for only 13.2%. This lower percentage can be attributed to the transmissions having very similar characteristics between each repetition.

4.4.2 Epox USB BT-DG02 USB

The Epox card was the hardest to analyze. There is no significant change in packet type as distance increases. Also, the RSSI values are the same from two to ten meters, at a value of zero dB. The lack of change over distance or RSSI value makes it impossible to predict the packet type with respect to distance.

The percentage of DH packets ranges from 52% down to almost 0%. This is a very wide range to try and analyze. At a distance of one meter, 51.6% of the data packets are the DH type for all antenna orientations. At a distance of ten meters, and the 90 degree antenna orientation, 52.6% of the packets are the DH type. At ten meters and 180 degrees orientation, between 1% and 18% of the packets are DH type. It would appear that at longer ranges, antenna orientation does have an impact on the packet type.

A significant number of DH type packets are present at all ranges that were tested. There is no distance where an abrupt change in packet type occurs. The DH packet type is used in significant number at all distances. So, for the Epox card tested, there is no way to determine a specific distance that a certain packet type will be used. Figure 6 illustrates the variability in the use of the DH type packet over the transmission ranges. Even at the maximum distance of ten meters, the DH type packet is used in 25% of the

transmission, roughly the same amount that occurs at four meters. Similar frequency of DH packets at different distances for the Epox card means that there is no distinct distance where a packet type change occurs.

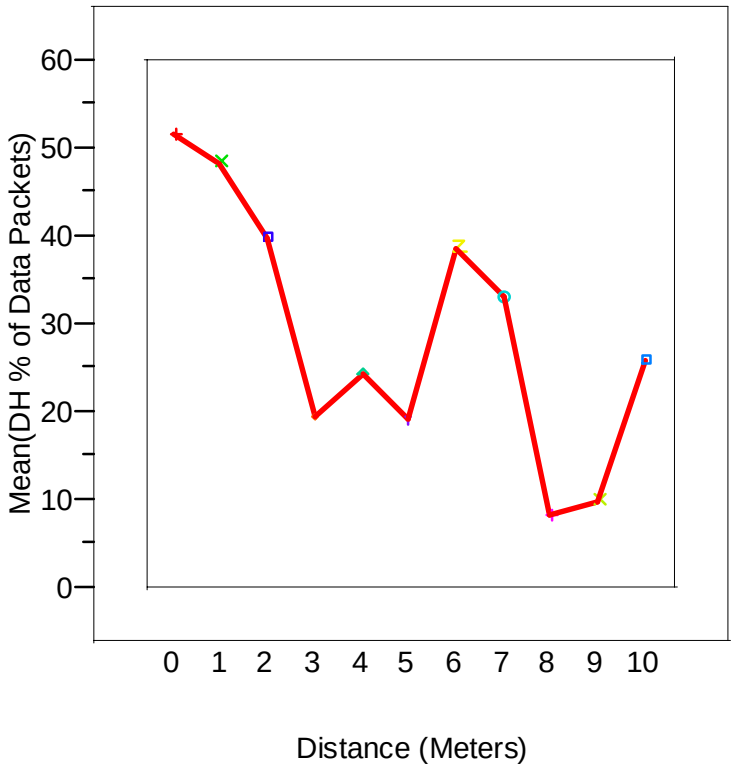


Figure 5 DH packet type at distance for Epox

The ANOVA from JMP shows two significant factors for the Epox card, distance and distance with orientation. The components of the variance are distance with orientation (38.3%), distance (33.9%), and repetitions of distance and orientation (27.9%).

4.4.3 Hawking Technology H-BT10U USB

The third card analyzed is the Hawking card. This is also a difficult card to analyze with no apparent pattern. There is no clearly observable change in packet type with an increase in distance. From zero to two meters, the DH5 packet type is the most used packet type. The DH type packets account for 51% of the total data packets. However, from three meters to eight meters, the DH packet type is still used, but it is not very common. Its percentages drop to between 1% and 10%. However, there are several exceptional cases where it varies between 35% to 45%. The packet type varies widely between repetitions at these distances. In some repetitions, the DH packet type is used, and in other repetitions of the same distance and antenna orientation, the DH packet type is not used. Figure 7 shows the wide variations in the percentages of DH type packets. Initially the use of DH type packets drops off with distance out to seven meters. The DH packet type then is used more frequently at the eight meter to ten meter distance. This is completely unexpected to see the DH packets used at longer ranges.

The ANOVA from JMP of the Hawking card shows the same significant factors as the other cards, distance and distance with antenna orientation. The variance due to distance is 43.3%, the repetitions of distance with orientation is 39.1%, and distance with orientation is17.6%

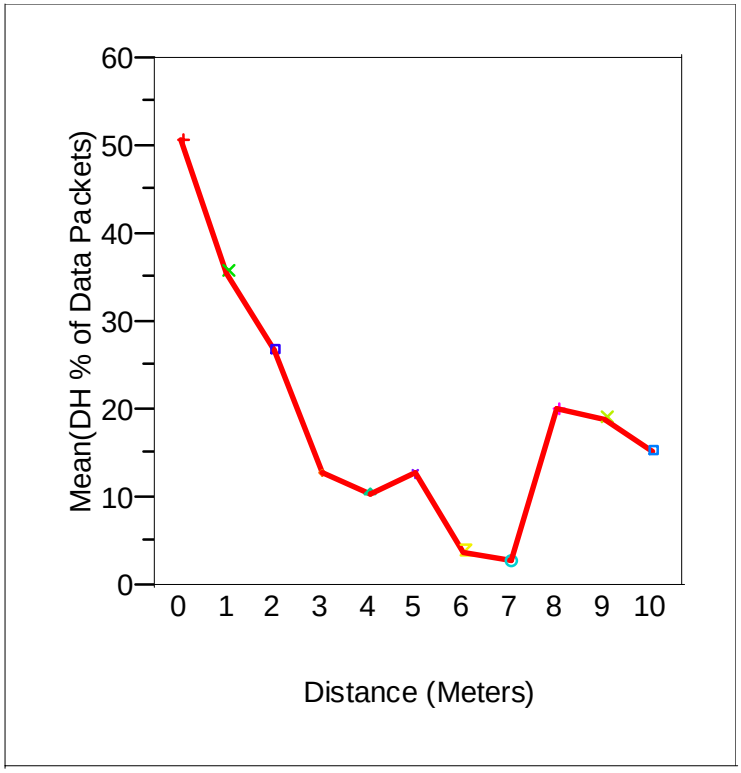


Figure 6 DH packet type at distance for Hawking

4.4.4 Belkin F8T003 USB

The fourth card analyzed is the Belkin card. This card also has a distinct pattern of packet type and distance. As expected, at short distances the DH5 packet type is the most common. At one meter or less, the DH packet type is 78% of the data packets. There are also a very low number of DM1 packets. Distance increases cause a change in packet type. The packet type change occurs at the three meter mark. Beyond the three meter distance, the percentage of DH packets drops to 0-5% of the data packets. The

small rise at 10 meters is not enough to be statistically significant. Figure 8 below shows the percentages of DH packets at all distances.

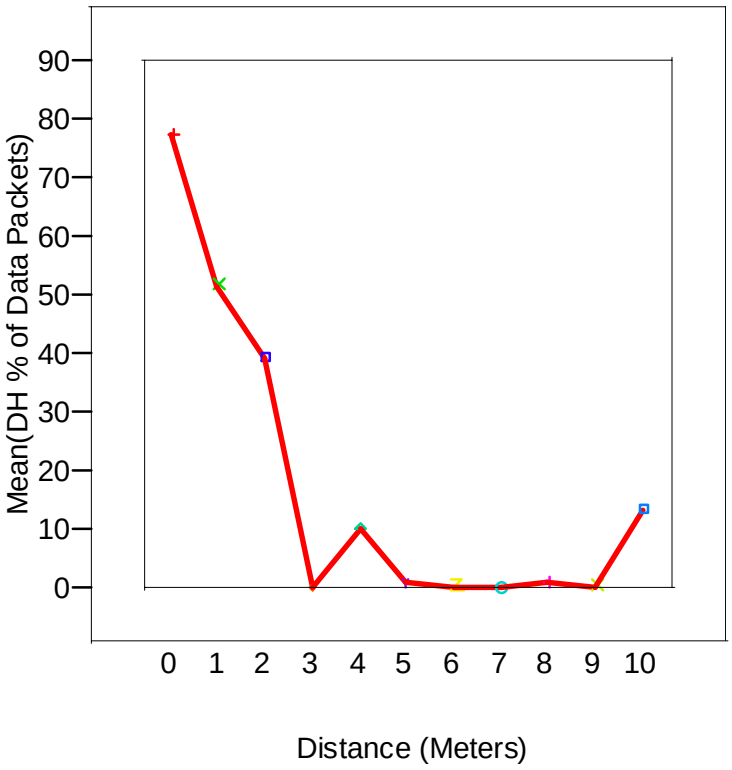


Figure 7 DH packet type at distance for Belkin

The ANOVA for the Belkin card is similar to the other three cards tested. The significant factors are distance, and distance with orientation. The variation of each component was slightly different than the rest. Distance, at 63.1%, accounts for the vast majority of the variation. The rest of the variation is distance with orientation at 22.3%, repetitions of distance with orientation at 8.8% and finally antenna orientation alone at 5.8%.

4.5 Common Observations

During the conduct of this research, several observations were noted. These are observations that seem to hold true, but there are no statistics or metrics to back up the claims. The first observation was related to the power levels used in transmission. Of the three cards that did support variable power transmission, all the cards used maximum power, even at the closest distance. The cards did not start out transmitting at maximum power, but within a few thousand packets, LMP messages were sent to increase power. There are no errors in the packets being transmitted to indicate the link is poor quality. The fact that all the cards eventually transmitted at max power, even at close distances, suggests that power control is not a very important feature for a Bluetooth card to support. The one card that did not support variable levels of power transmission, Epox, did not have any trouble transmitting the test file to a maximum distance of ten meters. Not supporting variable power transmission is not detrimental to the card.

The second common aspect observed in the testing was when LMP messages were sent to change between the non-FEC packet type, DH, and the FEC packet type, DM. There is no pattern for the number of packets having correctable or uncorrectable errors before a switch of packet type. In looking at the data recordings, there is no real pattern of when a packet type was changed. However, both the master and the slave make the change at the same time.

The third observation was the number and type of packets transmitted. The three most frequently observed packet types are the DM1, DM5 and DH5. The DM3 is seen less often then the main three. The ratio of DM3 packets varies slightly by manufacturer,

but they typically account for between 5%-8% of the total number of data packets. The Belkin card at distances past four meters has the highest level of DM3 packets at 35%-55% of the total data packets. The last two packet types, DH1 and DH3, are only very rarely observed. Out of a typical 30,000 packet transmissions, it is common to see fewer than ten packets of DH1 or DH3 type. These packets are only very rarely used. The reason for the infrequent use of the DH1 and DH3 might be related to the research by Valenti [Val02]. The Valenti research shows that the DH1 and DH3 packet type never achieve maximum throughput for any signal to noise ratio.

Another attributes that all the cards share is the manufacture of both the hardware and the software. All the hardware chipsets are produced by Cambridge Silicon Radio (CSR). Each Bluetooth card uses a slightly different hardware version, they are all made by CSR. No information can be found on the differences between the CSR chipsets. The software is also produced by a common manufacturer, Widcomm. Like the hardware, three cards use a slightly different version of the software, but it is all produced by the same company. The Belkin card is the only one to use a different software package. It looks like this software is developed specifically for the Belkin cards.

The primary limitation for this research is the highly variable nature of the RF signal used for transmission. The RF signal can be influenced by temperature, humidity, the physical layout of the room, microwaves and other electronic interference. A room with cubicle walls and lots of people can reduce the signal strength of the Bluetooth signal. However, actually measuring the quality of the Bluetooth signal and the associated degrading factors would be very useful, but beyond the scope of this research.

Manufacturer	Hardware	Software	Power Control
Dlink	CSR 443	Widcomm 1.2.2.15	Yes
Belkin	CSR 525	Belkin 1.3.2.7	Yes
Hawking	CSR 373	Widcomm 1.2.2.18	Yes
Epox	CSR 272	Widcomm 1.2.2.9	No

Figure 8 Specific Properties

4.6 Summary

This chapter discussed the antenna orientation and packet type experiments performed, the data collected and the data analysis. The antenna orientation experiments showed that certain orientation of the Bluetooth device antenna received stronger signals that others and that orientation of the antenna is a statistically significant factor in three of the four cards. However, antenna orientation or signal strength had no impact on the packet type used for transmission. The manufacture tests showed that there is not enough information to identify a manufacturer based solely on observing the packets being transmitted. There are no unique signatures that can be observed by looking at the packets transmitted.

The goal of using packet type to determine the distance between transmitter and receiver is only partially successful. Distance between transmitter and receiver can be determined for the DLink and Belkin cards. The distance between transmitter and receiver for the Epox and Hawking can not be determined. The RSSI value has no

predictive value of what kind of packet used in transmission. There is not enough evidence to support a conclusion for a general Bluetooth case. Each manufacturer has a different RSSI value, and different mix of DM and DH packets.

5. Conclusions and Recommendations

5.1 Introduction

This chapter reviews and summarizes research accomplishments and objectives. First, the impact of the research is discussed and the implications for Bluetooth devices within the DoD. Second, the experimental objectives and results are reviewed along with conclusions drawn. Last, the areas for further study are proposed.

5.2 Research Impact

Overall, the RSSI values provide no benefit in predicting packet type for equipment tested from all manufacturers tested. Previous research performed by Captain Tim Kneeland [Kne02] has shown the very limited use of RSSI values in predicting throughput. The RSSI value reported by a card is only accurate within +/-6 dB according to the Bluetooth specification. [Blu02]

The ability to covertly monitor Bluetooth packets and determine a user's location would be useful. If this can be done, it would be one more security risk that may need addressing within the DoD prior to large scale use. Determining the distance between users could be the first step to linking a Bluetooth identity to a real identity. While this might not be a big issue on an installation, it might be something to consider when using Bluetooth in public areas, like an airport or a restaurant.

5.3 Outlines of Future Work

This research provides a preliminary look at trying to determine the distance between users based solely on packet type. Based on the limited success of the work

done so far, it does not seem to warrant further exploration. There is not enough information available to an outside observer looking solely at packet information to make reliable distance estimates. The issue of distance with direction, needed to determine a user's actual location, has not been explored. The most practical way to determine a user's location would be the use of specialized hardware. I would not recommend any more research down this path.

There has been some indication the Bluetooth SIG is adding a user location feature in the next release of the Bluetooth specification for pervasive computing purposes. However, the Bluetooth specification version 2.0 released in November 2003 has no support.

For this research to have more impact, the ability to record or determine the bit error rate of the Bluetooth link would be very useful. If the bit error rate of the signal can be determined, the crossover points for different packet types may be determined and better distance estimates determined.

Another possible topic to explore is to try to determine the higher level protocol used above Bluetooth. For example, does FTP traffic generate different packet pattern than HTTP traffic? Can one determine what type of application is running on the Bluetooth device solely by looking at the type of packets being transmitted? Some related work is already being done using the 802.11 wireless networking protocols with some success. Bluetooth might be another wireless protocol to examine.

5.4 Summary

This research determined if it is possible to estimate the distance between users based on packet type and signal strength. The antenna orientation experiments determined the significance of antenna orientation on RSSI values. The packet type experiment generated an estimate of expected packet type for a specific distances and manufacturers. Together, these provide a first look study investigating the possibility of using Bluetooth technology to locate Bluetooth users.

Appendix A
Merlin Bluetooth Packet Analyzer Settings

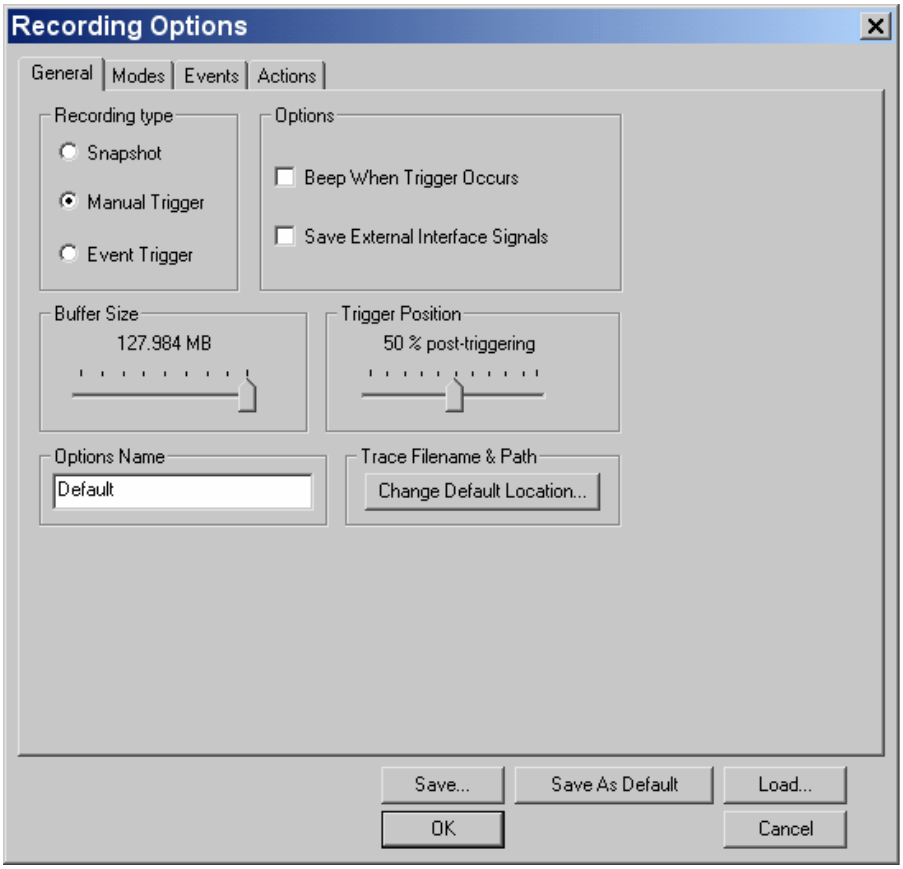


Figure 9. Merlin General Recording Options

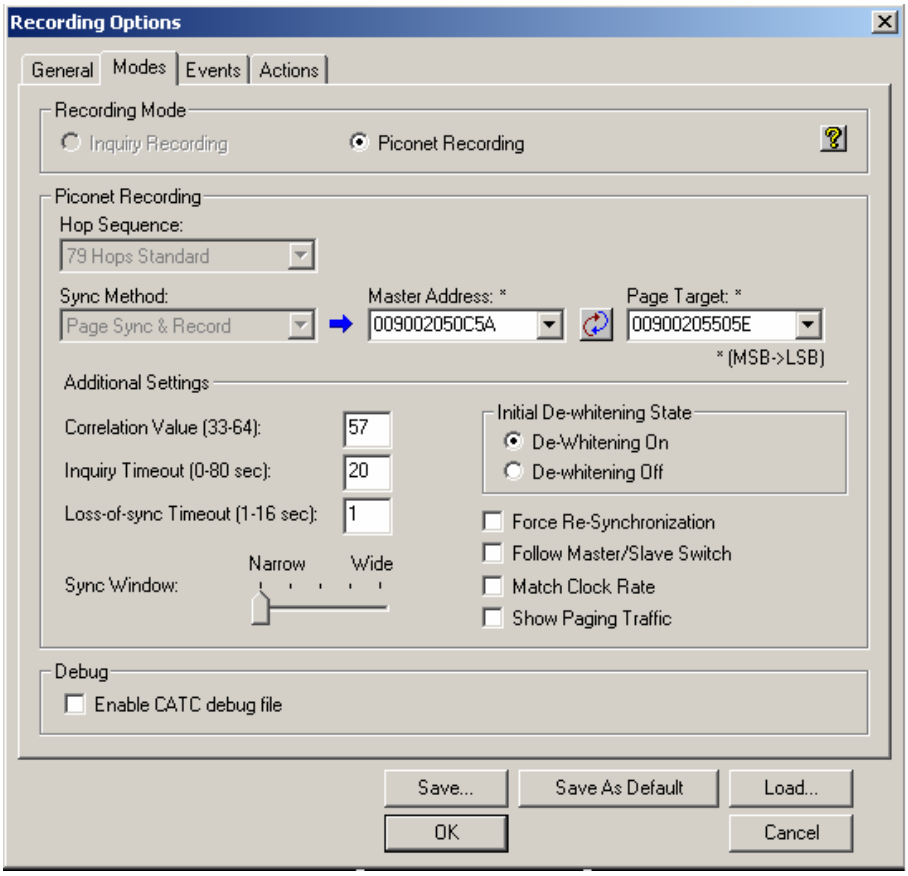


Figure 10. Merlin Modes Recording Options

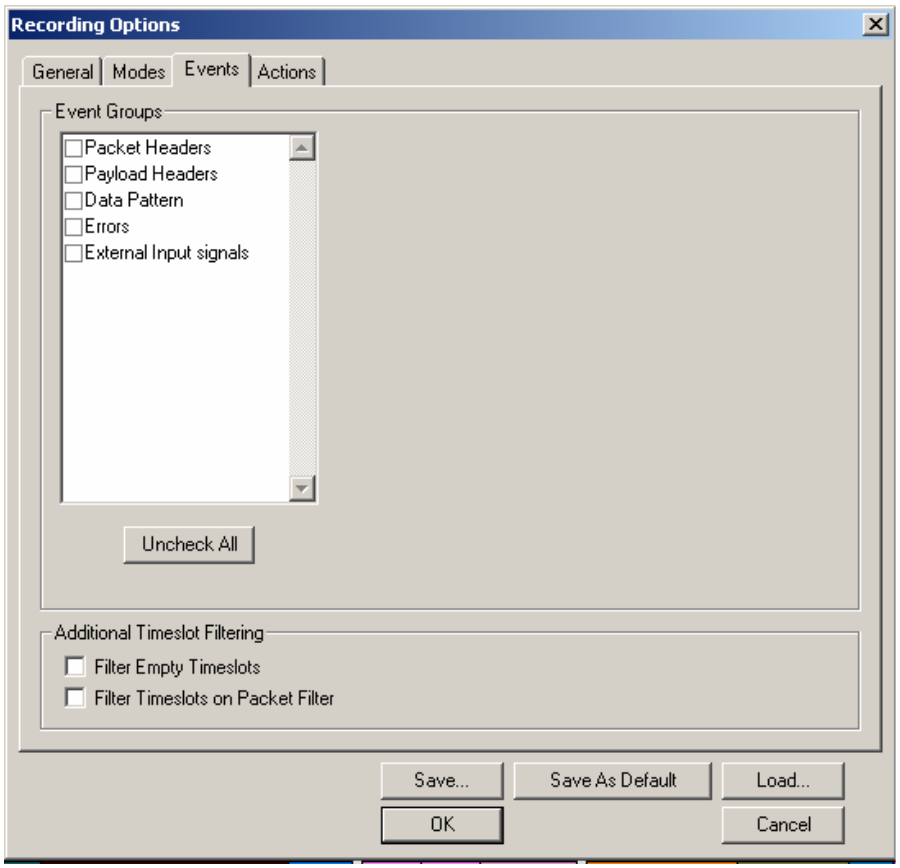


Figure 11. Merlin Events Recordings Options

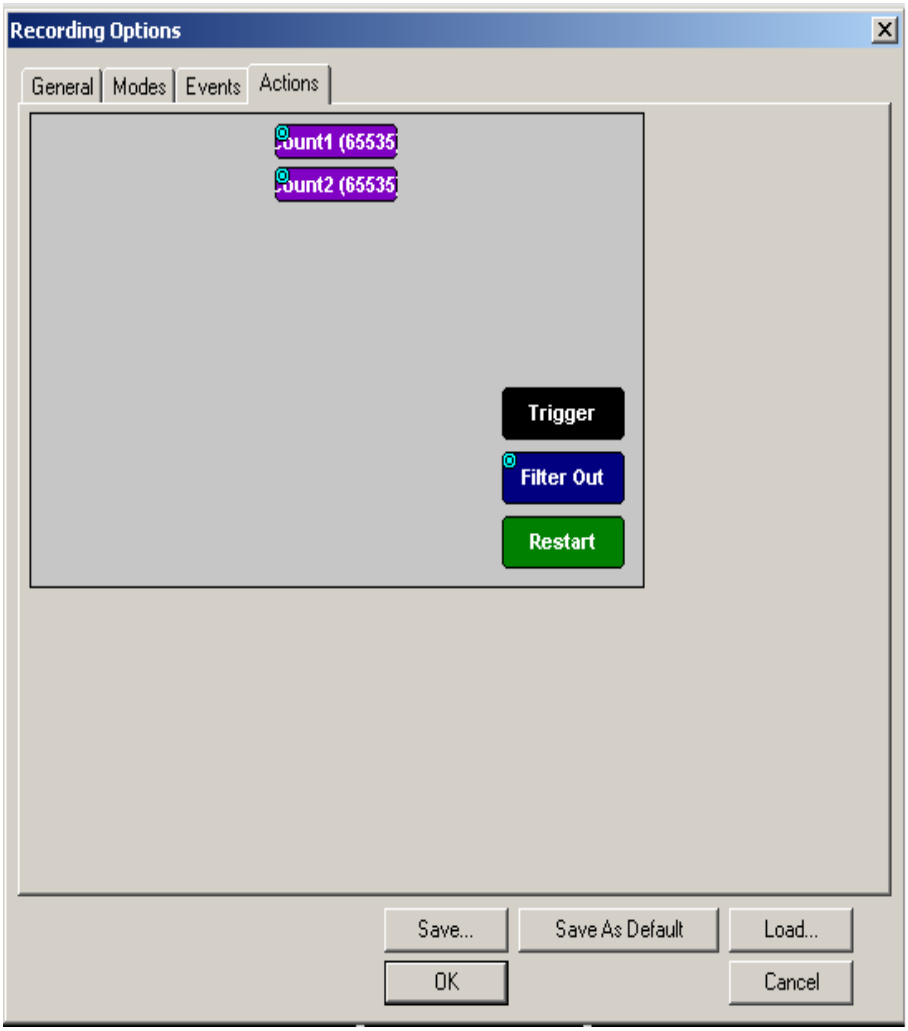


Figure 12. Merlin Actions Recording Options

Appendix B

Receiver Signal Strength Indicator Sampler Script for Linux

```
# RSSI Sampler by Tim Kneeland
# Last updated Dec 2, 2002
# This script samples Receiver Signal Strength Indicator values and outputs
# them to a file.  A connection must be established first with a transmitter
# using "hcitool cc <BD_ADDR>".  Script execution requires three command line
# arguments following script name. First argument is the BD_ADDR of the
# transmitter a connection is established with.  Second argument is the name
# of the output file to append the data too.  Third argument is the number of
# RSSI samples to take for each orientation and distance measurement.  Script
# will promt for distance in meters (integer values only) and promt to change
# orientation of receiver.  Script is exited inputing a distance of 99.

# Output the date to file
date >> $2

# A distance of 99 will exit the script
distance=0
while [ $distance -le 99 ]
do
  # Prompt for distance
  echo -n "Input distance between transmitter and receiver in meters: "
  read distance
  if [ $distance -eq 99 ]
  then
    exit 1
  fi
  # Output distance to file
  echo "Distance in meters: $distance" >> $2
  # Four different orientations
  for iteration in 1 2 3 4
  do
    # Prompt for proper orientation of receiver
    echo -n "Place receiver at `expr 90 \* $iteration` degrees and hit enter."
    read z
    echo "Orientation in degrees: `expr 90 \* $iteration`" >> $2
    # Sample RSSI the number of times specified by the third argument
    x=1
    while [ $x -le $3 ]
    do
          hcitool rssi $1 >> $2
          x=`expr $x + 1`
    done
  done
done
```

Appendix C
Bluetooth Manufacture Hardware Versions

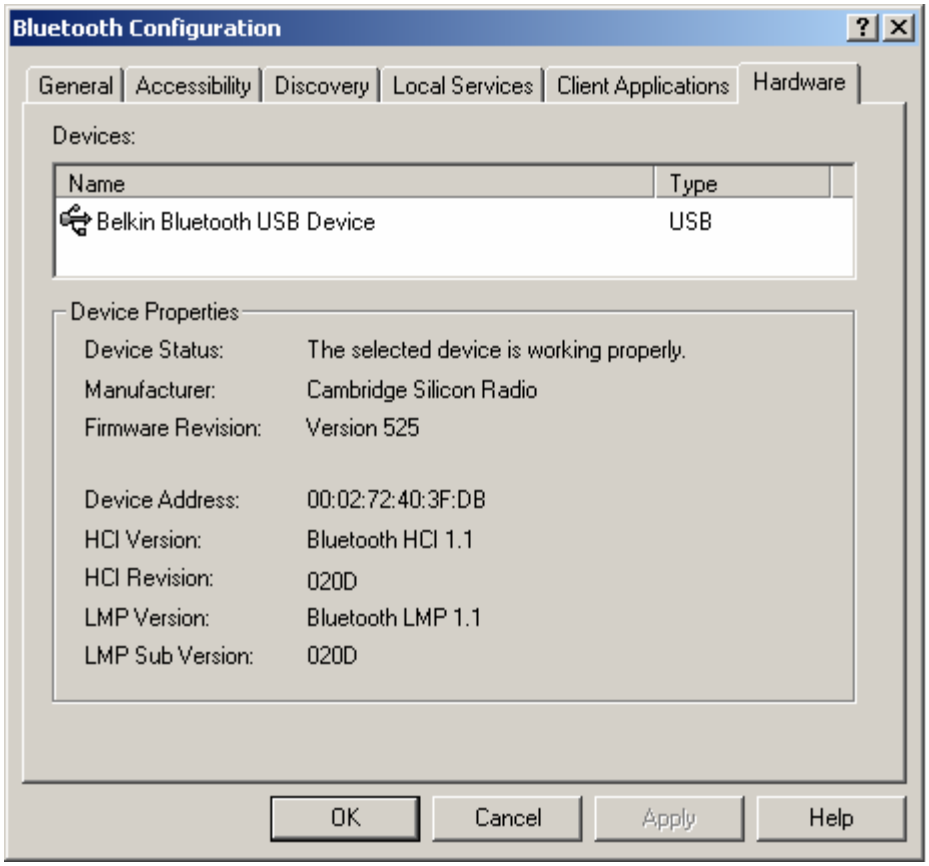


Figure 13. Belkin F8T003 USB Hardware

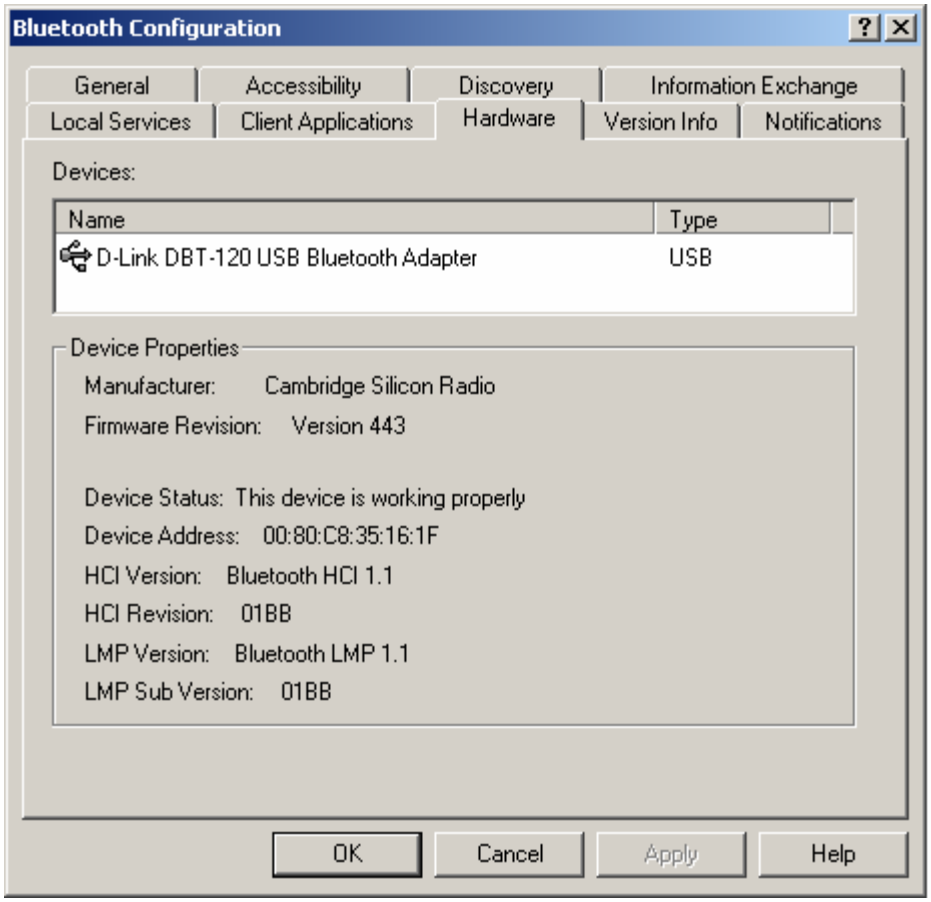


Figure 14. D-Link DBT-120 USB Hardware

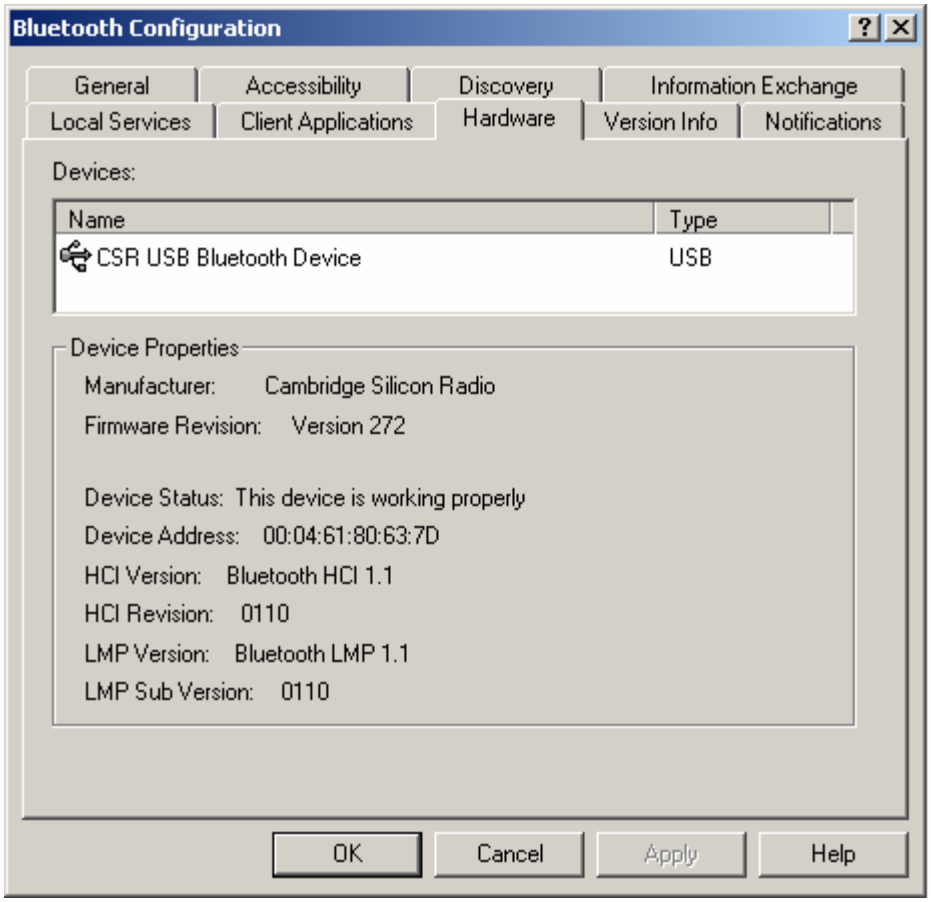


Figure 15. Epox BT-DG02 USB Hardware

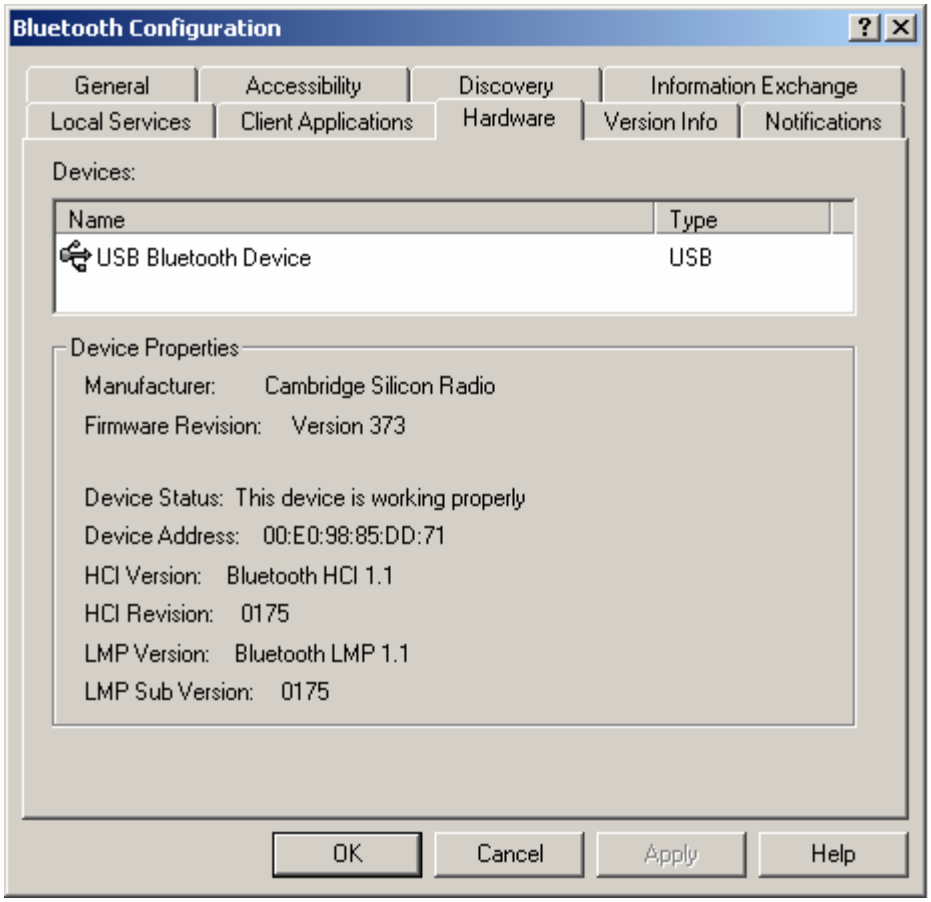


Figure 16. Hawking Technology H-BT10U USB Hardware

Appendix D

Bluetooth Manufacture Software Versions

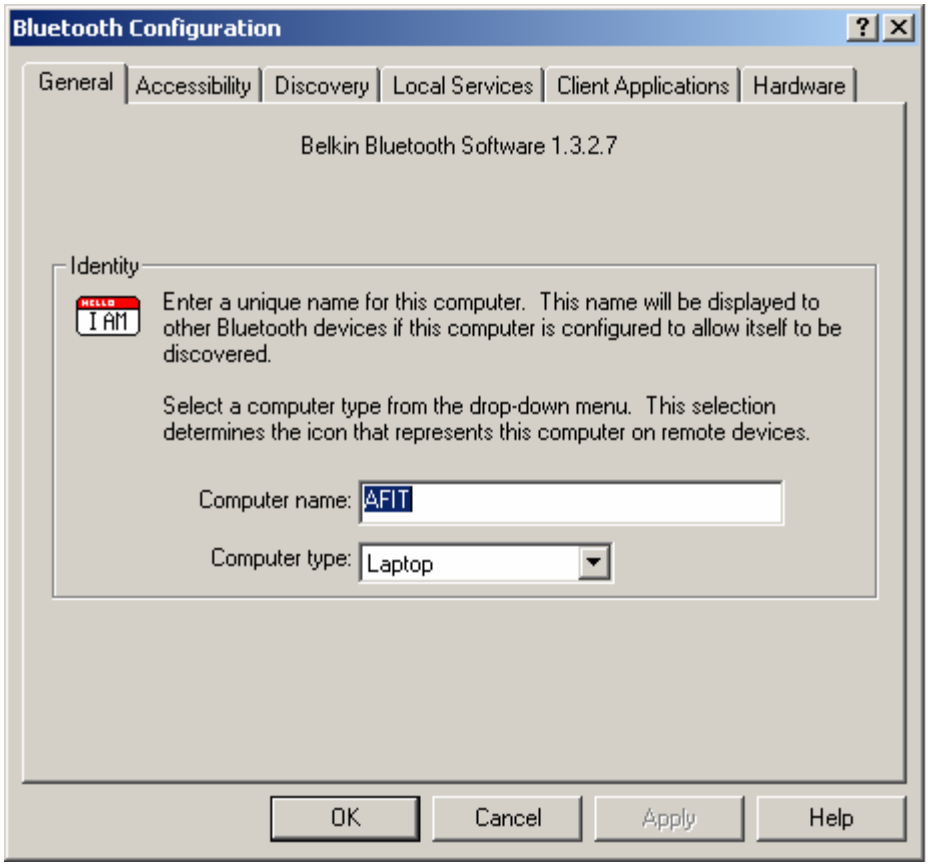


Figure 17. Belkin F87003 USB Software

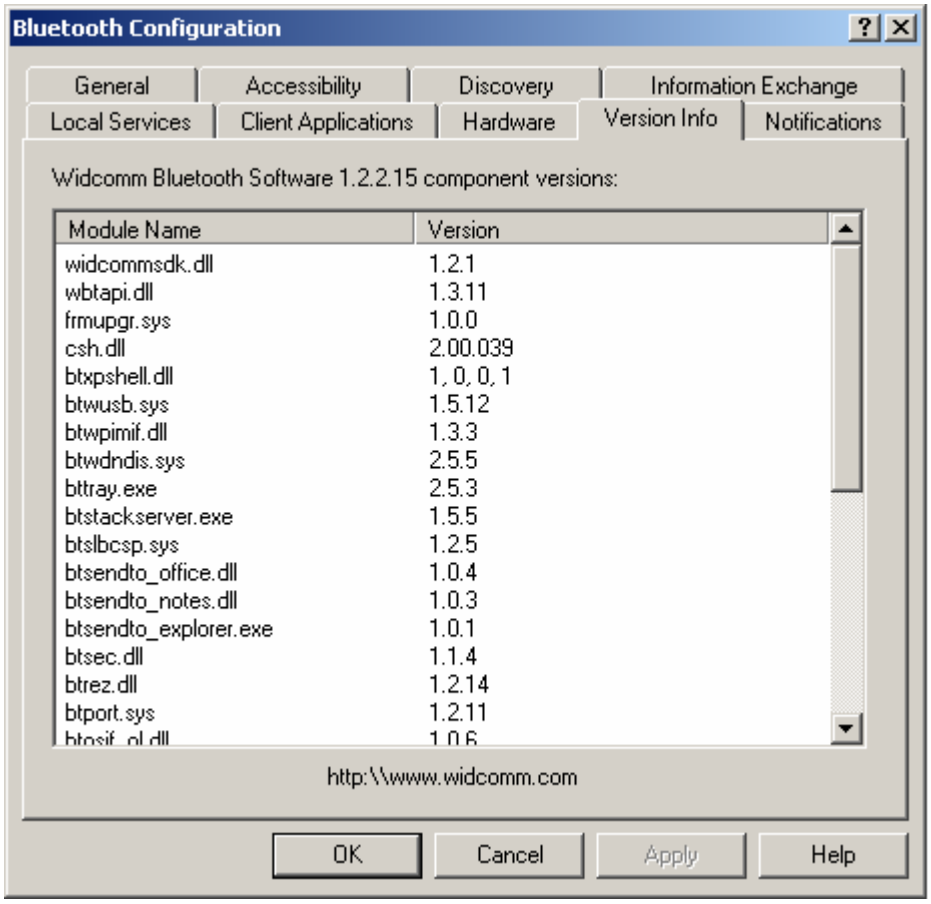


Figure 18. D-Link DBT-120 USB Software page 1

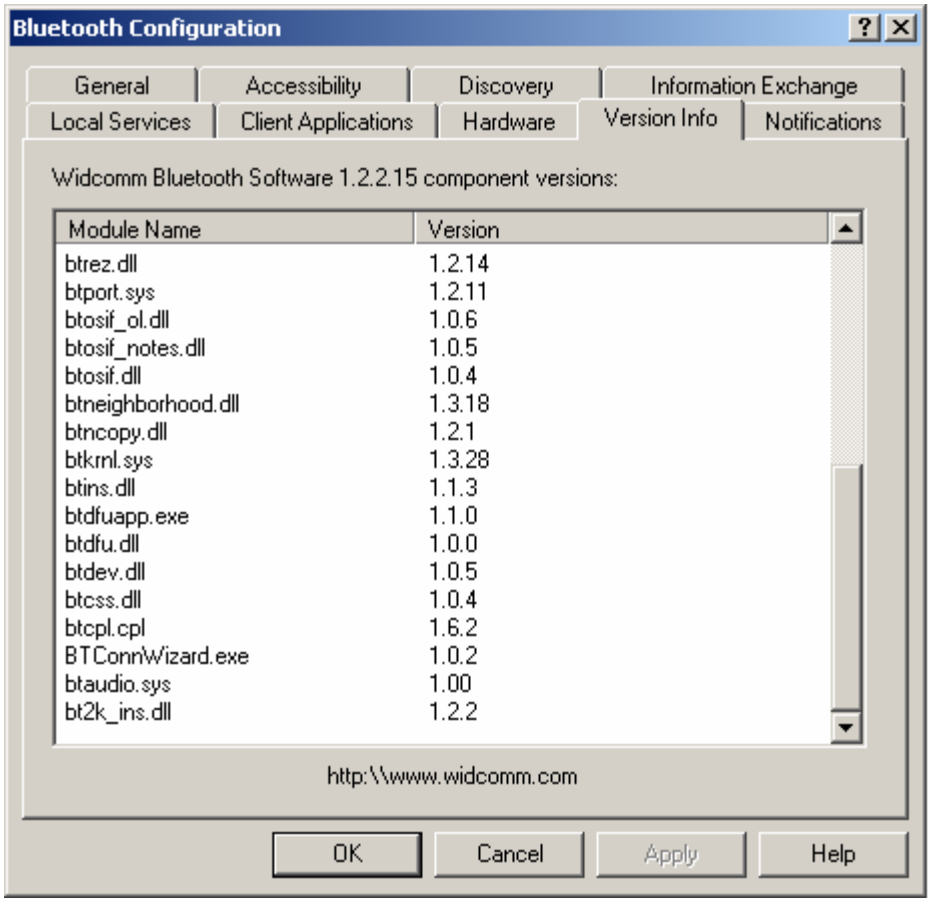


Figure 19. D-Link DBT-120 USB Software page 2

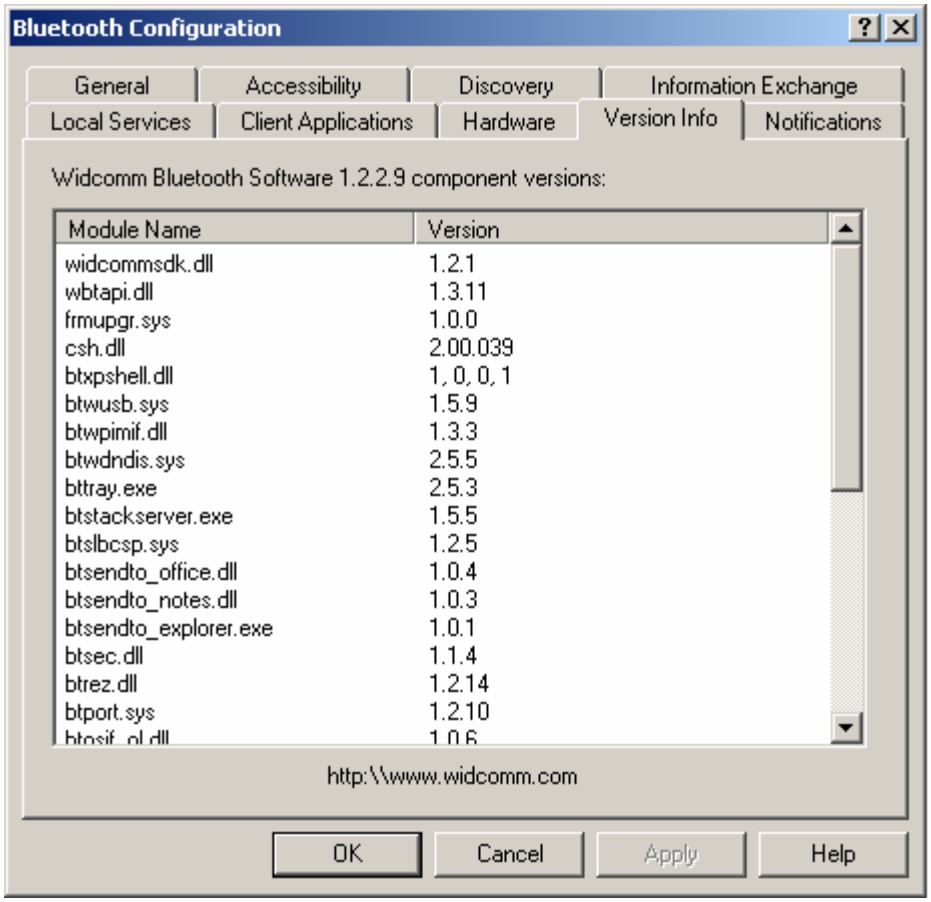


Figure 20. Epox BT-DG02 USB Software page 1

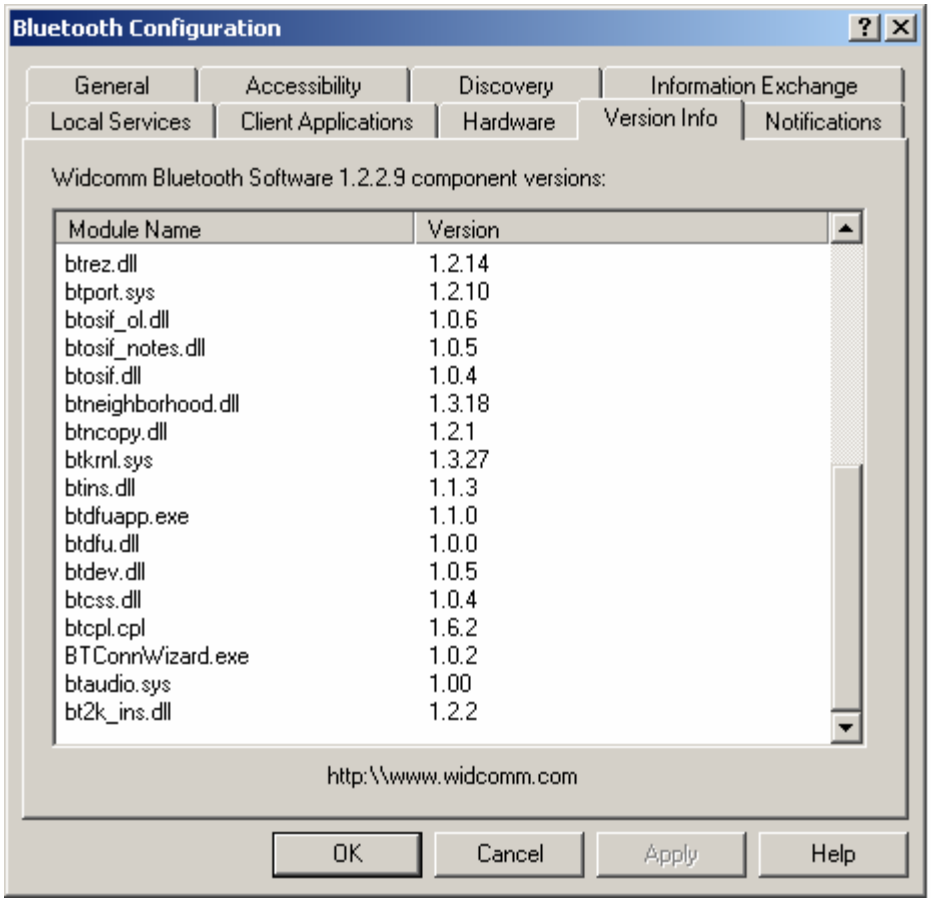


Figure 21. Epox BT-DG-2 USB Software page 2

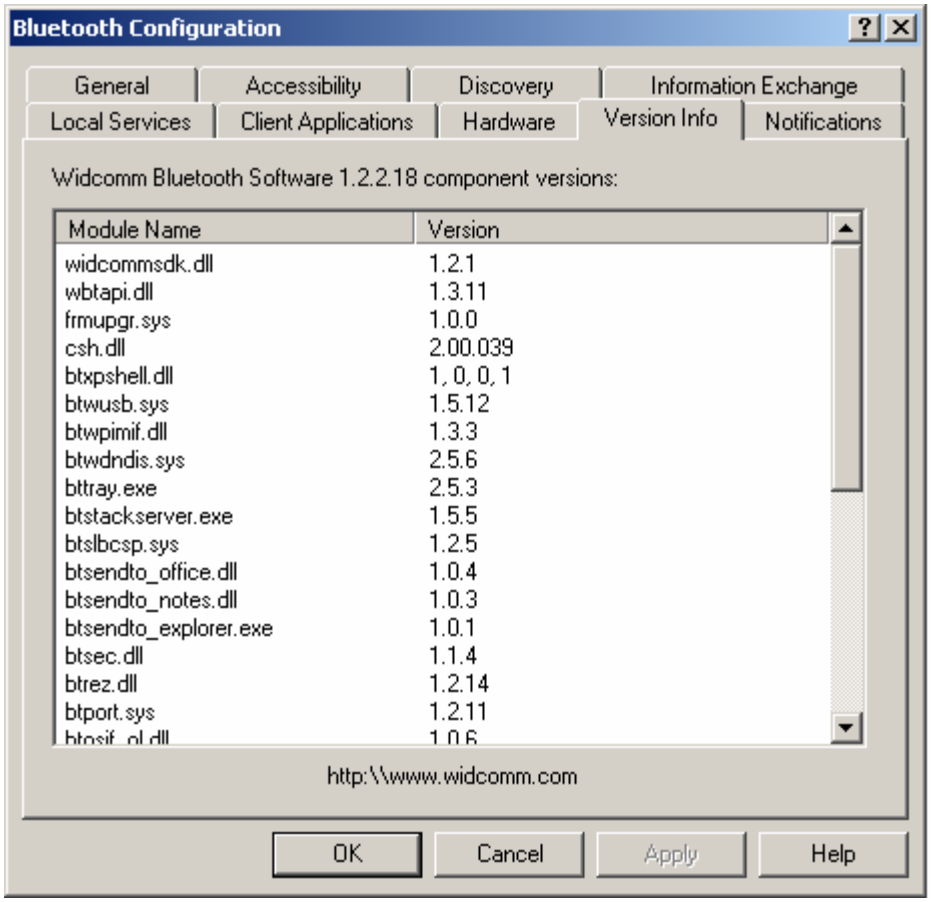


Figure 22. Hawking Technology H-BT10U USB Software page 1

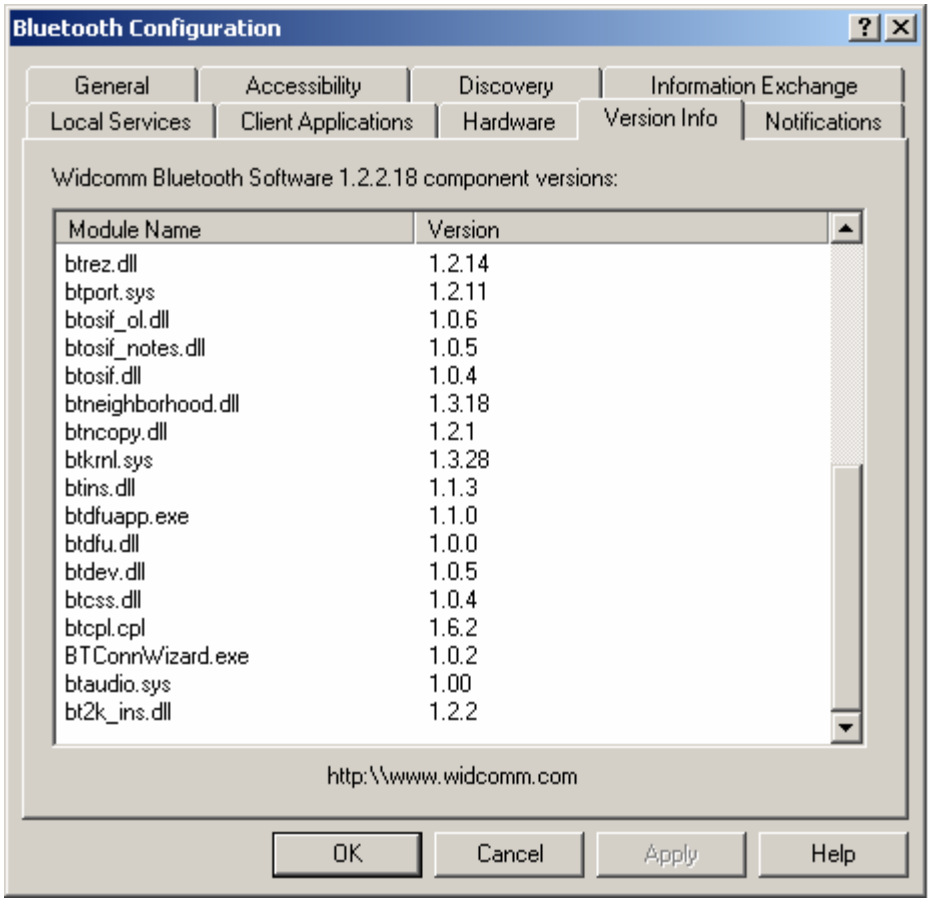


Figure 23. Hawking Technology H-BT10U USB Software page 2

Appendix E

Features Supported for Bluetooth Cards

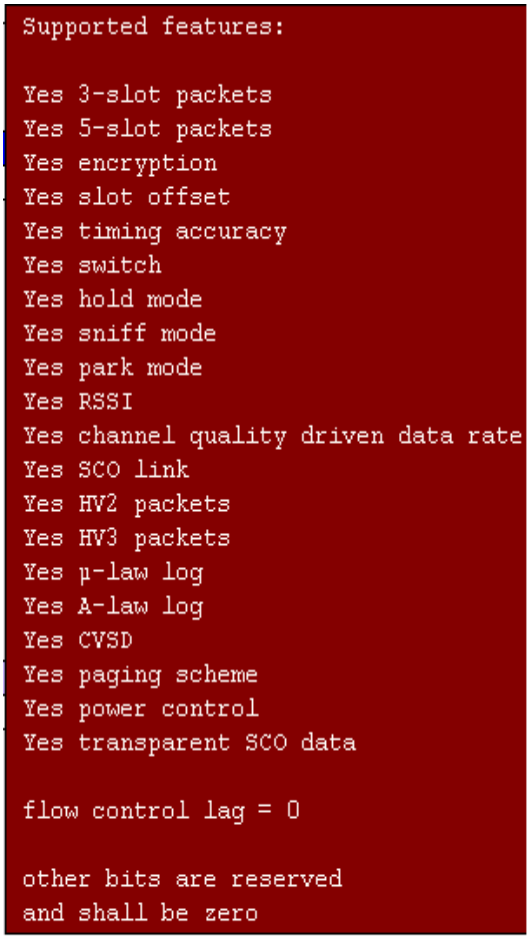


Figure 24. Features Supported on DLink, Hawking and Belkin cards

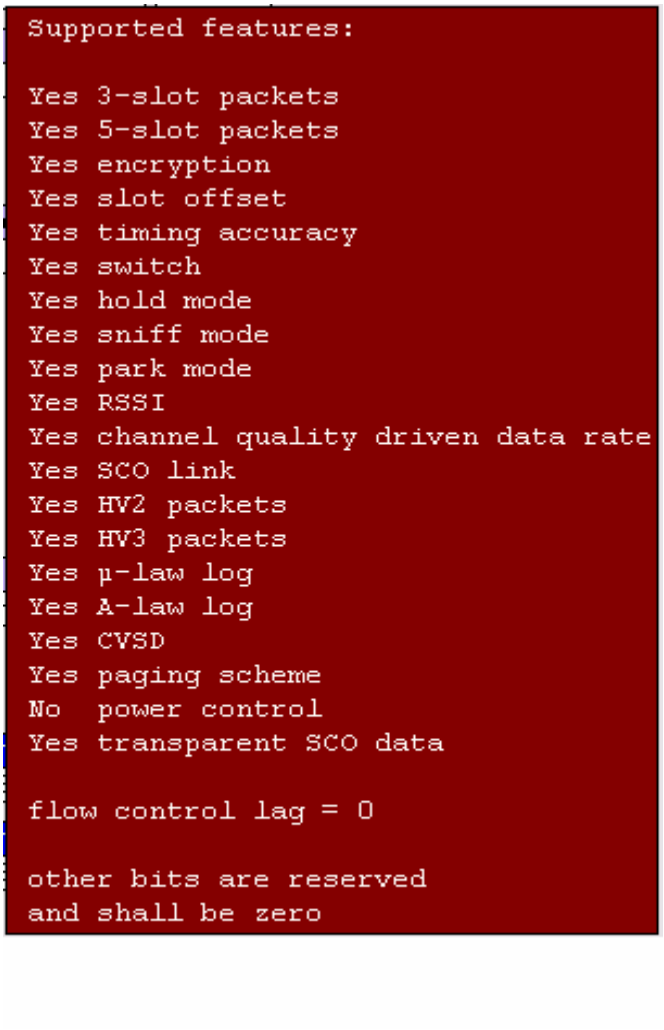
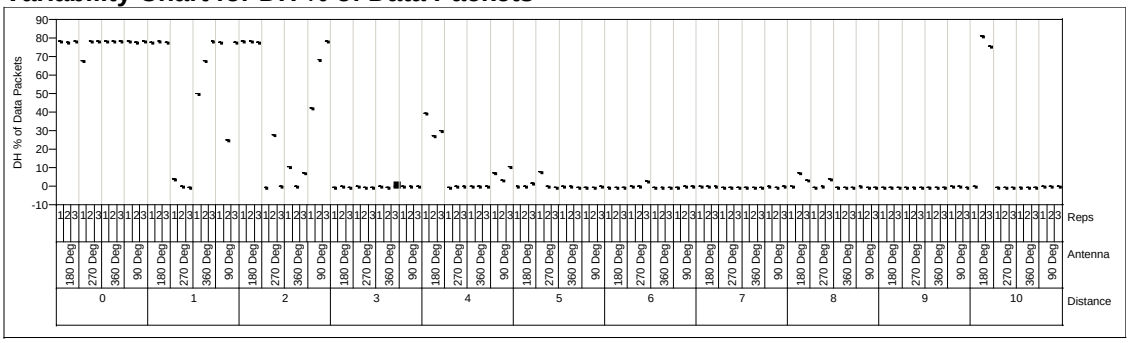


Figure 25 Features Supported on Epox Card (No power control)

Appendix F
ANOVA for Belkin F8T003 USB

Variability Chart for DH % of Data Packets



Analysis of Variance

Source	DF	SS	Mean Square	F Ratio	Prob > F
Distance	10	84739.08	8473.91	11.0218	<.0001
Antenna	3	8110.045	2703.35	3.5162	0.0269
Distance*Antenna	30	23064.9	768.83	8.5691	<.0001
Reps[Distance,Antenna]	88	7895.477	89.7213	.	.
Within	0	1.16e-10	0		
Total	131	123809.5	945.111		

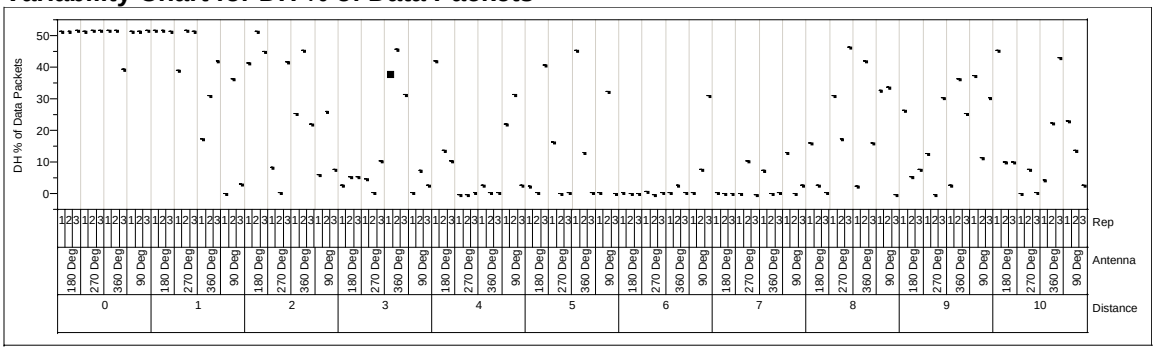
Variance Components

Component	Var Component	% of Total	Plot%	Sqrt(Var Comp)
Distance	642.0899	63.1		25.339
Antenna	58.6218	5.8		7.656
Distance*Antenna	226.3695	22.3		15.046
Reps[Distance,Antenna]	89.7213	8.8		9.472
Within	0.0000	0.0		0.000
Total	1016.8025	100.0		31.887

Appendix G

ANOVA Charts for Hawking Technology H-10BTU USB

Variability Chart for DH % of Data Packets



Analysis of Variance

Source	DF	SS	Mean Square	F Ratio	Prob > F
Distance	10	23898.07	2389.81	6.66449	<.0001
Antenna	3	682.8965	227.632	0.63480	0.5984
Distance*Antenna	30	10757.64	358.588	2.34700	0.0011
Rep[Distance,Antenna]	88	13445.15	152.786	.	.
Within	0	0	0		
Total	131	48783.75	372.395		

Variance Components

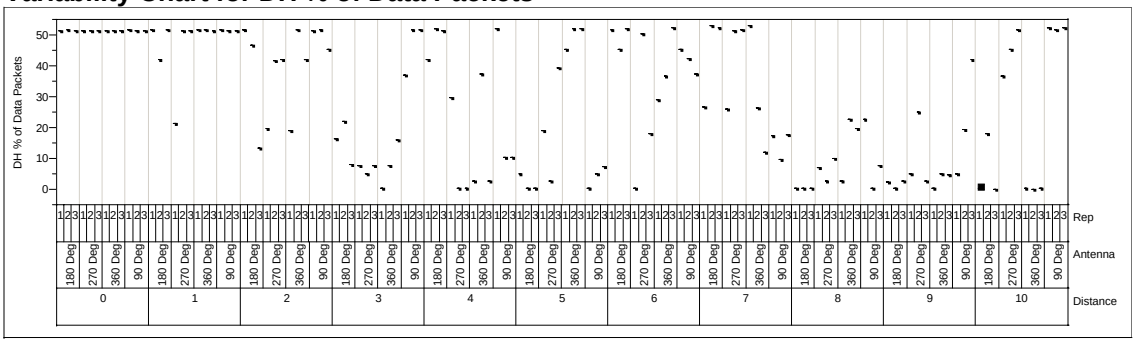
Component	Var Component	% of Total	Plot%	Sqrt(Var Comp)
Distance	169.26823	43.3		13.010
Antenna	0.00000	0.0		0.000
Distance*Antenna	68.60073	17.6		8.283
Rep[Distance,Antenna]	152.78577	39.1		12.361
Within	0.00000	0.0		0.000
Total	390.65473	100.0		19.765

Negative Variance Components were set to zero

Appendix H

ANOVA Charts for Epox BT-DG02 USB

Variability Chart for DH % of Data Packets



Analysis of Variance

Source	DF	SS	Mean Square	F Ratio	Prob > F
Distance	10	25614.08	2561.41	3.84860	0.0020
Antenna	3	1013.669	337.89	0.50769	0.6800
Distance*Antenna	30	19966.27	665.542	5.11679	<.0001
Rep[Distance,Antenna]	88	11446.18	130.07	.	.
Within	0	0	0		
Total	131	58040.19	443.055		

Variance Components

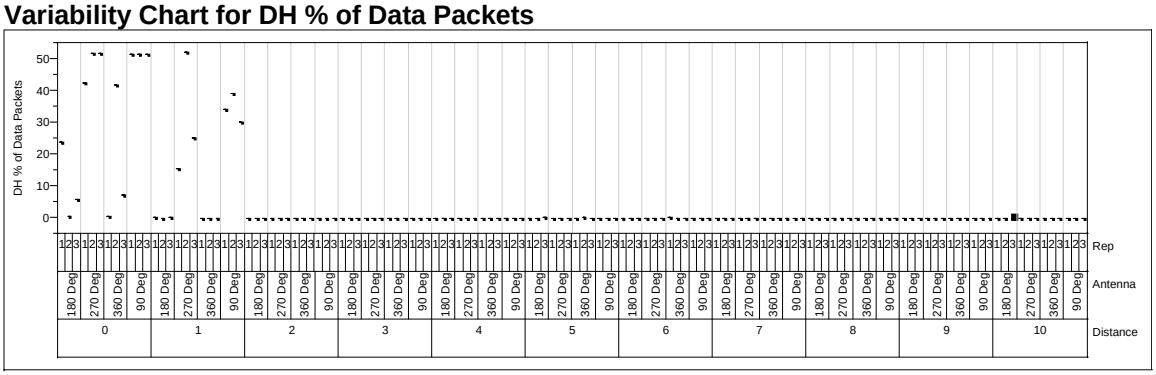
Component	Var Component	% of Total	Plot%	Sqrt(Var Comp)
Distance	157.98882	33.9		12.569
Antenna	0.00000	0.0		0.000
Distance*Antenna	178.49071	38.3		13.360
Rep[Distance,Antenna]	130.07018	27.9		11.405
Within	0.00000	0.0		0.000
Total	466.54970	100.0		21.600

Negative Variance Components were set to zero

Appendix I

ANOVA Charts for D-Link DBT-120 USB

Variability Chart for DH % of Data Packets



Analysis of Variance

Source	DF	SS	Mean Square	F Ratio	Prob > F
Distance	10	12773.8	1277.38	6.34663	<.0001
Antenna	3	1329.438	443.146	2.20176	0.1084
Distance*Antenna	30	6038.071	201.269	8.43997	<.0001
Rep[Distance,Antenna]	88	2098.547	23.8471	.	.
Within	0	0	0		
Total	131	22239.85	169.77		

Variance Components

Component	Var Component	% of Total	Plot%	Sqrt(Var Comp)
Distance	89.67587	49.8		9.470
Antenna	7.32960	4.1		2.707
Distance*Antenna	59.14064	32.9		7.690
Rep[Distance,Antenna]	23.84713	13.2		4.883
Within	0.00000	0.0		0.000
Total	179.99324	100.0		13.416

Bibliography

[Ana01] Anand N., *An Overview of Bluetooth Security*, SANS Institute, 2001

[Bis01] Bisdikian, C., *An Overview of the Bluetooth Wireless Technology*, IBM Research Report, June 2001.

[Blu01] Bluetooth SIG, *Specification of the Bluetooth System Version 1.1*, https://www.bluetooth.org, 2001

[Can01] Candolin, C., *Security Issues for Wearable Computing and Bluetooth Technology*, Helsinki University of Technology, 2001.

[DeS03] DeSchryver, D., *What is Bluetooth and Why Care?*, The Doyle Report, http://www.thedoylereport.com/spotlight?object=archive%5B%5D&content_id=3860 , August 2003.

[Geh02] Gehrmann, C., *Bluetooth Security White Paper*, Ericsson Mobile Phones, 2002.

[Gol97] Golic, J., *Cryptanalysis of Alleged A5 Stream Cipher*, Proceedings of Eurocrypt '97, Springer LNCS 1233, 1997.

[JaW01] Jakobsson, M. and Wetzel, S., *Security Weaknesses in Bluetooth*, Lucent Technologies and Bell Labs, Murray Hill, NJ 2001.

[JuP02] Ju, M., C. Park, D. Hong, K. Youn, J. Cho, *Packet Selection Scheme Based on a Channel Quality Estimation for Bluetooth Systems*, Wireless Personal Multimedia Communications, 2002.

[Kne03] Kneeland, T., *Performance Evaluation and Analysis of Effective Range and Data Throughput for Unmodified Bluetooth Communication Devices*, Masters Thesis, Air Force Institute of Technology, 2003.

[Met99] Mettala R., *Bluetooth Protocol Architecture, Version 1.0*, Bluetooth White Paper, Nokia Mobile Phones, 1999.

[Noe03] Noel, R., *WLAN CSMA/CA Performance in a Bluetooth Interference Environment*, Masters Thesis, Air Force Institute of Technology, 2003.

[Tay04] Taylor, S., *Throughput Performance Evaluation and Analysis of Unmodified Bluetooth Devices*, Masters Thesis, Air Force Institute of Technology, 2004.

[Tra00] Traskback, M., *Security of Bluetooth: An Overview of Bluetooth Security*, Helsinki University of Technology, 2000.

[Val02] Valenti, M., *On the Throughput of Bluetooth Data Transmissions*, IEEE, 2002.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
23-03-2004	Master's Thesis	August 2003 – March 2004

4. TITLE AND SUBTITLE

PACKET ANALYSIS OF UNMODIFIED BLUETOOTH COMMUNICATION DEVICES

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Watts, Neal A., 1st Lieutenant, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way, Building 640
WPAFB OH 45433-8865

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GCS/ENG/04-22

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Mr. Bill Kroah
National Security Agency
NSA/R5
Ft. George G. Meade, MD 20755-6000

(301)688-0348

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Bluetooth technology has potential for widespread use within the Department of Defense and the Air Force. An office environment using Bluetooth technology can wirelessly connect computers, printers, and other office equipment in order to share information over short distances. The clutter and annoyance of cables connecting equipment can be eliminated. Bluetooth provides a standard interface for connection, as opposed to many different proprietary cables.

The research is conducted indoors in a climate controlled environment, with minimal obstructions, to closely follow free-space signal propagation. Four different antenna orientations are used. The factors varied are the distance between devices, and the antenna orientation.

This research determined that two of the four cards tested have a specific distance where a change from Data High rate packets and Data Medium rate are used. The change occurs at 2 meters for one and 3 meters for the other. This research also shows that manufacturers transmit identical data in identical formats. Also, this research shows that antenna orientation, and receiver signal strength indicator values have no predictive value in determining packet type used for transmission.

15. SUBJECT TERMS

Radio Communications Systems and Wireless Communications

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Richard A. Raines, AD-23, DAF
U	U	U	UU	99	19b. TELEPHONE NUMBER *(Include area code)* (937) 255-6565, ext 4278 (Richard.raines@afit.edu)

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18