THROUGHPUT PERFORMANCE EVALUATION AND ANALYSIS OF UNMODIFIED BLUETOOTH DEVICES

THESIS

Steven J. Taylor, Second Lieutenant, USAF

AFIT/GCS/ENG/04-20

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/04-20

THROUGHPUT PERFORMANCE EVALUATION AND ANALYSIS OF UNMODIFIED BLUETOOTH 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

Steven J. Taylor, BS

Second Lieutenant, USAF

March 2004

AFIT/GCS/ENG/04-20

THROUGHPUT PERFORMANCE EVALUATION AND ANALYSIS OF UNMODIFIED BLUETOOTH DEVICES

Steven J. Taylor, BS

Second Lieutenant, USAF

Approved:

/Signed/

_____ _____

Dr. Richard A. Raines Date
Thesis Advisor

/Signed/

_____ _____

Major Rusty O. Baldwin, Ph.D. Date
Committee Member

/Signed/

_____ _____

Dr. Michael A Temple Date
Committee Member

Acknowledgments

I would like to thank all the people who have helped at various times during this thesis process: those who have poked and prodded the work along, those who have endured my general demeanor during the long hours, those who have laboriously pored over every page of this document, and those who provided the much needed comic relief on those late night – all of which were necessary to get me towards graduation.

I would like to thank my thesis advisor, Dr. Richard Raines, and my committee members, Maj Rusty Baldwin and Dr. Michael Temple, without whose help none of this research would have been possible, let alone completed.

Steven J. Taylor

Table of Contents

Page

List of Figures

Page

List of Tables

Page

Abstract

The Air Force relies on the application of new technologies to support and execute its mission. As new technologies develop, the integration of that technology is studied to determine the costs and benefits it may provide to the war fighter. One such emergent technology is the Bluetooth wireless protocol, used to connect a small number of devices over a short distance. The short distance is a feature that makes using the protocol desirable. However short, there is still a vulnerability to interception.

This research identifies ranges at which several commercially available Bluetooth devices are usable. Various combinations of both distance and orientation are varied to determine a 360 degree map of the Bluetooth antenna. The map identifies distances at which certain throughput thresholds are available. This research shows that baseline 1 mW Bluetooth antennas are capable of throughput levels of 100 kbps at over 40 meters, which is four times the minimum distance specified in the protocol standard.

The 3Com PC card was the best performing PC card, capable of throughputs at or near 100 kbps out to 40 meters. The other PC Cards tested had similar performance. The Hawking USB dongle was the best USB antenna tested, achieving throughputs of over 200 kbps in three of the four orientation, and over 150 kbps at the fourth. The 3Com dongle was a close second, the Belkin dongle a distant third, while the DLink antenna was not able to achieve 100 kbps at any distance tested.

THROUGHPUT PERFORMANCE EVALUATION AND ANALYSIS OF UNMODIFIED BLUETOOTH DEVICES

I. Introduction

1.1 Introduction

More so than the other services, the Air Force relies on the application of new technologies to support and execute its mission. As new technologies develop, the possible integration of that technology is studied to determine the costs and benefits it may provide to the war fighter. One such emergent technology is the Bluetooth wireless system.

Bluetooth is a wireless computing protocol designed to integrate devices within a Personal Area Network (PAN). Created as a cable replacement technology, Bluetooth allows devices to communicate with one another wirelessly, eliminating the need for vendor specific cables and adapters. Being an open and public standard, Bluetooth can be incorporated by any manufacturer who wants to communicate with other devices wirelessly.

1.2 Background

As with any communications system, one of the chief concerns is the security of the system. When using a wireless communications system, the primary cause for security concerns are the possibility of signal interception by outside parties or unauthorized access of the system. While Bluetooth is designed to operate as a short range protocol, it is still vulnerable within that range.

Bluetooth implements many techniques to mitigate the possibility of interception, including frequency hopping and varying levels of encryption. Despite these efforts, it is still susceptible to attack. One way to eliminate the threat from outsiders is to field the system where the range of the network is enclosed within a secure area. To do so the transmission capabilities of Bluetooth must be determined.

1.3 Research Focus

The goal of this research is to determine the actual throughput capabilities of commercially available Bluetooth devices. By studying the performance of several antennas at varied distances and orientations, the performance can be generalized to an understanding of the capabilities of the Bluetooth wireless system as a whole.

The objective of this research is to develop a usability/vulnerability map for general Bluetooth devices. Identifying the distances and orientations for specific throughput levels will show both the capability of the Bluetooth system, as well as the range of possible signal exploitation.

To realize this objective, a study of the published material concerning the Bluetooth system and its performance forms a foundation for the research. With this knowledge, experiments are designed and conducted to determine the performance of assorted Bluetooth antennas. From that data a usability map is created to graphically display the capabilities of each system. Finally, results are compared to form a generalization of Bluetooth performance.

1.4 Summary

This study determines the capabilities of general, commercial Bluetooth systems, as an extension of the research conducted in [11]. The remainder of this document is organized as follows: Chapter 2 presents the relevant background on wireless computing, the Bluetooth standard, wireless security, and Bluetooth specific security issues. Chapter 3 details the experimental methodology guiding this research. Chapter 4 provides the results of the experiments and the analysis of that data. Finally Chapter 5 summarizes the research and discusses conclusions drawn from it.

2. Background

2.1 Introduction

This chapter contains the background information on Bluetooth communication devices. This chapter's information mirrors and extends previous work of [11]. It includes discussions of wireless computer communications, Bluetooth specific communications, wireless security issues, and Bluetooth specific security concerns.

2.2 Wireless Computer Communications

Wireless computer communications use electromagnetic radio waves to transmit information through the air. The signal's bandwidth capacity is a function of the frequency at which the antenna transmits. The higher the frequency of the signal, the larger the data load the signal can carry. However the higher capacity frequencies have a cost, namely the signal is more vulnerable to interference from atmospheric conditions. The choice of transmission frequencies is not completely open, as international and governmental agencies regulate frequency usage and allocation. In the United States, frequency usage is managed by the Federal Communication Commission.

2.2.1 Wireless Network Compositions

As the use of wireless communications has matured, it has evolved into several families of networks based upon the size and range of the network: local area networks (LAN), personal area networks (PAN), and metropolitan area networks (MAN).

2.2.2 Local Area Networks

Local area networks had their genesis in both industry and academia, possibly being the most researched topic in recent wireless communications. Wireless LANs have allowed business and students to be mobile within a campus area while still maintaining connectivity to the network. With laptops becoming a more popular platform in computing, mobile connectivity continues to grow in popularity. The ability of wireless technologies to achieve comparable data rates with wired networks has also fueled its acceptance.

2.2.3 The IEEE 802.11 Protocol Family

The Institute of Electrical and Electronics Engineers (IEEE) has developed the 802.11 family of specifications for wireless local area networks. All of the specifications in the 802.11 family "use the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance) for path sharing" [10].

802.11 was the first protocol in this family, formally specified in 1997 by IEEE. Using phase shift keying modulation, it broadcasts in the 2.4 GHz unlicensed ISM (Industrial, Scientific, and Medical) band using either Frequency Hopping Spread Spectrum (FHSS) or Direct Sequence Spread Spectrum (DSSS). This standard specified a data rate of 1 to 2 Mbps on the network.

The 802.11a protocol "applies to wireless ATM systems and is used in access hubs. 802.11a operates at radio frequencies between 5 GHz and 6 GHz. It uses a modulation scheme known as orthogonal frequency-division multiplexing (OFDM) that

makes possible data speeds as high as 54 Mbps, but most commonly, communications takes place at 6 Mbps, 12 Mbps, or 24 Mbps" [10].

The 802.11b standard is a backward compatible improvement upon the original 802.11. Also referred to as 'Wi-Fi,' 802.11b is the most common wireless protocol in commercial use today. It provides data rates of up to 11 Mbps, operating in the 2.4 GHz band. It modulates using complementary code keying (CCK) and broadcasts using DSSS.

The 802.11e standard was developed to provide a better level of Quality of Service (QoS) to the 802.11 family of protocols. The target of this standard is delay-sensitive applications, such as Voice over IP (VoIP) or other streaming data.

802.11g is the newest standard in the family, focusing on improving the data rates of 802.11b up to 54 Mbps in the same range as 802.11b. Like its predecessor, it also transmits in the 2.4 GHz band.

2.2.4 Personal Area Networks

The scope of a PAN is limited to a single office setting. PANs integrate low power devices within an office setting such as laptops, personal digital assistants (PDA), digital cameras, and other small digital devices. Using a common wireless solution, personal area networks can communicate without integrating various manufacturer cards, wires, and plugs to connect these items.

2.2.5 The IEEE 802.15 Protocol Family

IEEE 802.15.1 is the initial standard for wireless PAN implementation and the first in the 802.15 family. It is based on the Bluetooth v1.1 specification, which transmits in the 2.4 GHz band at rates up to 1 Mbps.

The 802.15.3 provides high data rates (20 Mbps and above) in the PAN arena while operating with low power, as a low cost solution.

802.15.4 differs from other standards in the family by providing a low bandwidth, personal area solution, with data rates near 20 kbps, 40 kbps, and 250 kbps. Like 802.15.3, it also focuses on "extra-low power MAC and physical layers" [15].

2.2.6 Metropolitan Area Networks and 802.16

Metropolitan Area Networks seek to connect both smaller LANs to larger networks and the Internet, as well as connect individual users. The goal is to wirelessly connect networks at ranges up to and beyond thirty miles. The 802.16 specification for Broadband Wireless Access (BWA) is still under development, but has several objectives.

The first is a wireless solution for replacing T1 lines in large areas. Many businesses have to wait for these lines to be installed in their buildings. A long-range, high bandwidth wireless solution could replace the need for expensive T1 lines, allowing much quicker access to high speed connections.

The next focus is on consumer network connectivity, that is cable-based connections and digital subscriber lines (DSL). A high rate wireless connection could help solve availability problems seen in this market.

Finally, a sub-group of the 802.16 committee is investigating mobile metropolitan connections: allowing individual users to remain connected to city wide networks as they travel within the MAN's broadcast range.

2.2.7 Transmission Methods

There are several different methods by which information can be transmitted over wireless networks. Each way has its set of benefits over the other methods, but also comes with its own deficiencies.

2.2.7.1 Narrow Band Radio

Narrow band radio transmissions occur within a specific frequency range. The transmitter and receiver are tuned to the same frequency and stay there for the duration of the connection. Because the signal is broadcast on that frequency, the possibility of interception and interference is high.

2.2.7.2 Spread Spectrum

Signals transmitted using spread spectrum broadcast the data across a large span of frequencies. Spread spectrum broadcasts are implemented using either Direct Sequence Spread Spectrum or Frequency Hopping Spread Spectrum.

2.2.7.2.1 Direct Sequence Spread Spectrum

In a direct sequence approach, each bit is spread over and transmitted on multiple frequencies. "Spread spectrum broadcasts in bands where noise is prominent, but does not rise above the noise" [14]. The data is spread across the frequencies based on a

pseudorandom key generated to modulate the data stream. That bit stream must be known by both parties, so they can both transmit and demodulate the signal.

2.2.7.2.2 Frequency Hopping Spread Spectrum

Unlike direct sequenced broadcasts, frequency hopping transmissions are sent on only one frequency at a time. However, they differ from narrow band transmissions, because the frequency changes multiple times over a given time period. Both the transmitter and receivers must be synchronized to the same hopping pattern to communicate. This reduces the chance of interference or interception by a third party.

2.3 Bluetooth

To "develop and promote a global solution for short-range wireless communication operating in the unlicensed 2.4 GHz ISM band," [4] Ericsson, IBM, Intel, Nokia, and Toshiba joined to form the Bluetooth Special Interest Group (SIG) in late 1998. To better market this technology, the SIG opted to make the specification open and royalty free, encouraging other companies to adopt it as a short range wireless solution.

The name Bluetooth comes from "the Danish King Harald Blatand (Bluetooth)," [3]. It was chosen because he is believed to have united the people of Denmark and Norway during the 10th Century. In that spirit of unity, Bluetooth was developed as a short-range network protocol designed to unite all the devices within a PAN.

The first version of the specification was made publicly available in the summer of 1999. The adopter members had access to the specification before it was made public,

so despite its seemingly initial incompleteness, there were working devices implementing the Bluetooth standard just as the documentation hit the public. The promoter group has grown since its inception to the size of nine, with 3Com, Lucent, Microsoft, and Motorola joining in late 1999. The adopter group has also grown to over 3000 companies worldwide, who have developed hundreds of Bluetooth devices. The specification is currently in version 1.1, with two distinct parts: "[t]he core specification defining the radio characteristics and the communication protocols for exchanging data between devices over Bluetooth radio links," [3] and "[t]he profile specification that defines how the Bluetooth protocols are to be used to realize a number of selected applications" [3].

The Bluetooth standard was developed to replace the vendor and protocol specific cables that run between different personal devices, such as PDAs, cellular phones, digital cameras, laptop computers, and other devices. Many of these devices have unique connectors that make integration a nightmare in a personal area network. Bluetooth hopes to eliminate the need for these connectors, by utilizing a common, open wireless standard to create these connections.

Devices adhering to the Bluetooth standard transmit in the 2.4 GHz ISM band, "employing frequency-hopping (FH) spread spectrum technology to reduce interference and fading" [16]. A time division duplex scheme is implemented, allowing for full duplex communications in a wireless personal area network, known as a piconet. A single piconet can support eight devices: one master and up to seven slaves. Bluetooth piconets can support asynchronous data links with each slave device and synchronous voice links with up to three slaves. The published range of a piconet is 10m when

transmitting at 1 mw EIRP. That range can be increased to 100m by increasing the transmission power. Bluetooth devices support transmissions on these links at rates up to 1 Mbps.

The ISM frequency band ranges from 2.400 MHz to 2483.5 MHz in most countries. Bluetooth operates in the 2402 MHz to 2480 MHz RF channels. Each channel in the range is 1 MHz wide, giving Bluetooth 79 channels in which to transmit. "Bluetooth radio hops from channel to channel at 1600 hops per second," [16] giving the network time slots of 625 microseconds. The sequence used in a piconet is unique to that piconet, being "determined using an algorithm based on the address (and clock) of the Bluetooth hub (master)" [16]. This hopping sequence is obtained by a slave once it has synchronized with the master of the piconet.

Bluetooth radios modulate using a binary system of Gaussian Frequency Shift Keying. It is utilized because of the better efficiency it provides above normal Frequency Key Shifting. This aids the device in maintaining the proper signal characteristics for Bluetooth transmissions. A simple comparison of Bluetooth and IEEE 802.11b can be seen in Table 1.

2.3.1 Protocols

There are two categories of protocols in the Bluetooth protocol stack: transport protocols and middleware protocols. These are not defined in the specification, but rather are natural groupings of the protocol stack. The protocols in the transport group are "developed exclusively for the Bluetooth wireless technology" [3]. All protocols transmitting over a Bluetooth link access these protocols to communicate. Middleware

protocols are those which support other protocols and applications, allowing old and new applications to use Bluetooth links to communicate, without knowledge of how the link itself works. This widens the area in which Bluetooth can be applied. This also allows "many applications already developed by vendors [to] take immediate advantage of hardware and software systems which are compliant to the (Bluetooth) specification" [12]. A diagram of the Bluetooth protocol stack is shown in Figure 1.

Table 1. IEEE 802.11 – Bluetooth comparison [16]

Comparison of IEEE 802.11 / 802.11b and Bluetooth Specifications		
Specification	IEEE 802.11 / 802.11b Wireless LAN	Bluetooth
Applications/Market	- Home - School - Enterprise - Campus-wide voice and data	- Cable replacement - Ad Hoc networking - Personal area voice and LAN access
Technology	- 2.4 GHZ ISM - Direct Sequence Spread Spectrum - Frequency Hopping Spread Spectrum	- 2.4 GHZ ISM - Frequency Hopping Spread Spread,Spectrum; 1600 hops per second
Data Rate	- Direct Sequence: 11 Mbps - Frequency Hopping: 1, 2 Mbps	- 1 Mbps
Power	20 dBm (typical)	0 dBm, 20 dBm
Range	100 M	1-10 M at 0 dBm; 100m at 20 dBm
Network Topology	Vendor dependent access points with client adapters; each access point supporting typically 128 devices	8 devices in a Piconet
Separate Voice Channel	Optional	Yes
Security	Optional Wireless Equivalent Protection (WEP)	Encryption, authentication

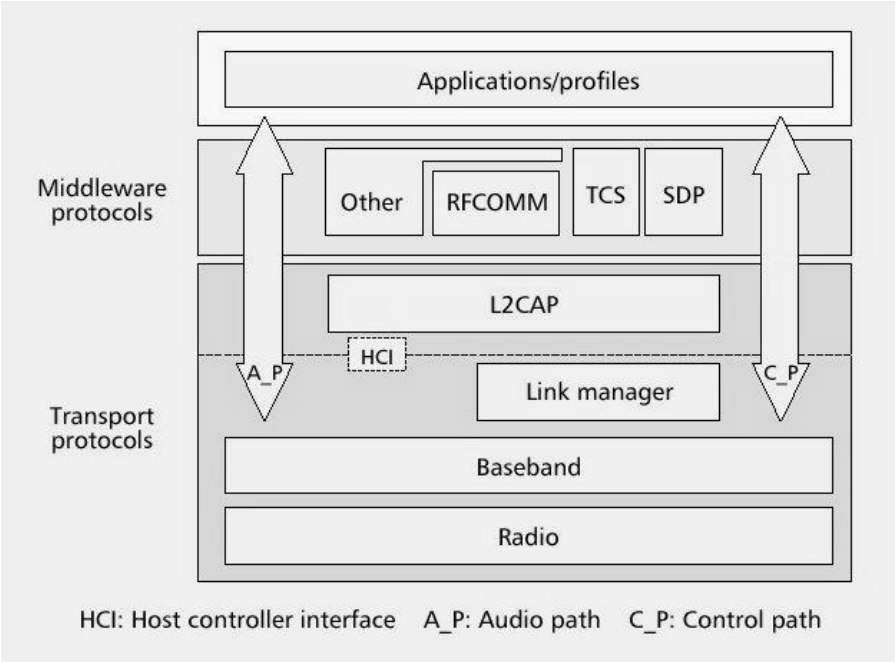

Figure 1. Bluetooth Protocol Stack [3]

2.3.2 Transport Protocols

2.3.2.1 Radio Layer

This layer is discussed in the preceding sections.

2.3.2.2 Baseband Layer

The essential, low level functions of a Bluetooth piconet are defined by the baseband layer. It controls the physical radio link of the device, piconet formation, transmission resource sharing, and low level packet types. The creation of piconets is managed in this layer through an inquiry and paging procedure that "synchronize[s] the transmission hopping frequency" [12].

For two Bluetooth devices to communicate, each must know two things: the other's Bluetooth device's address (BD_ADDR) and the master device's clock. The BD_ADDR is a unique 48 bit address that is imprinted when the device is manufactured. The BD_ADDR is "engraved on the Bluetooth hardware and it cannot be modified" [3]. The clock in each device is a 28 bit counter. The counter is incremented every 312.5 microseconds, "which corresponds to half the residence time in a frequency when the radio hops at the nominal rate of 1,600 hops/sec" [3]. Once a device knows these two pieces of data, it can communicate with the master and its piconet.

2.3.2.3 Piconet Formation

Bluetooth piconets exist in a truly ad hoc environment; there is no set infrastructure for the piconet. The duration of a piconet's existence is defined by the network's master and how long it deems a connection is necessary. Any given Bluetooth device "may serve either as master or slave at different times" [3]. Even though a piconet is comprised of up to seven slave devices, more than the seven slaves may be present within the physical range of the piconet. Those devices present but not active in the piconet are considered parked. Once a device has joined as a slave in a piconet, it may negotiate with the master to become the new master.

The master of a piconet assigns a locally unique active member address (AM_ADDR) to each active slave in the piconet. Those devices with the operating range, but not active (i.e., in parked mode) and those outside the operating range (stand-by mode) do not have AM_ADDRs. With this address, the master controls transmissions in the piconet. Two or more piconets may "exist in time and space independent of each

other" [3]. In fact, a single device may be a slave in more than one piconet at a time. The resulting topology is known as a scatternet. A Bluetooth device can accomplish this, provided its transmission slots from its first piconet do not overlap with its transmission slots in its second, and subsequent, piconets. An example of Bluetooth devices in a scatternet formation is shown in Figure 2.

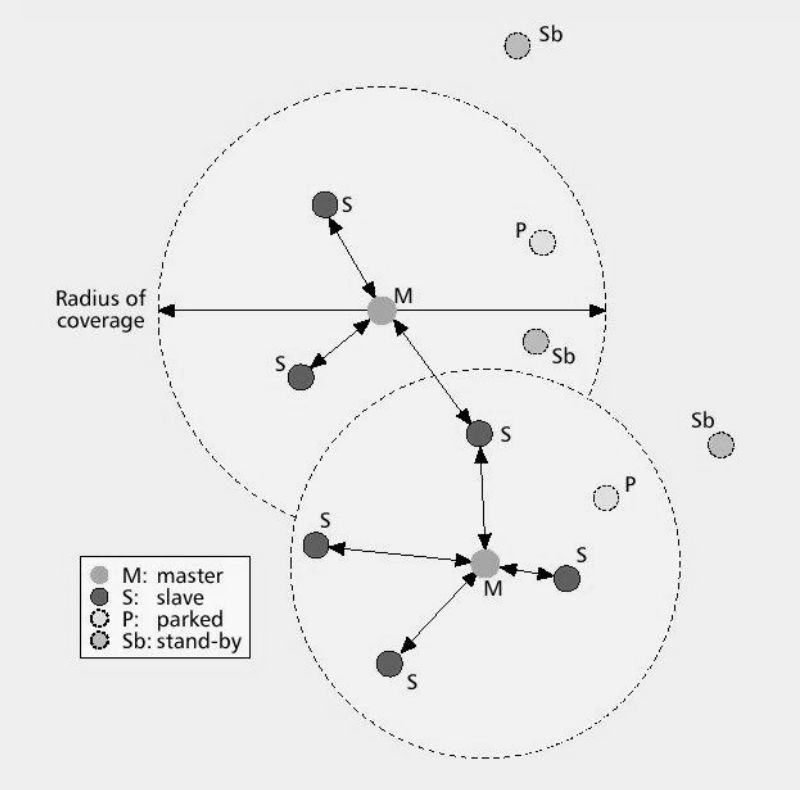

Figure 2. Bluetooth scatternet [3]

The devices in a piconet communicate by monitoring the sequence of frequency hops, synchronized with one another. The time slot in which each device transmits is 625 microseconds, which corresponds to 1600 hops/sec. Transmissions must begin and end

within that time slot. The exception to this rule is for "long packets," which can take three or five slots each. The hopping sequence is suspended during these transmissions, and then restarted where it would have been if only single slot packets were transmitted.

This frequency hopping sequence is based upon the master's BM_ADDR and clock. The master's clock identifies the frequency currently transmitting. Knowing these pieces of information, a slave can construct the hopping sequence for the piconet. Because it is the identifier for the piconet's hopping sequence, a master device can only exist in its own piconet, even when its slaves are in a scatternet formation.

The slaves in a piconet are synchronized by the master's clock. Each slave determines and stores "the offset time between their own Bluetooth clock and that of their master" [3] to keep synchronized to the master. The clock ticks twice per time slot, so the slot is determined by the second least significant bit. This bit classifies the time slot as even or odd, which determines whether it is the master's or a slave's turn to transmit.

This time division duplex (TDD) system alternates transmission authority between the master and slaves. "The master transmits on the even number slots…, while the slaves transmit on odd number slots" [3]. A slave must be contacted by the master in order to transmit in the piconet. Once the master has initiated contact, the slave may transmit in the next time slot. Any Bluetooth device can only transmit in one piconet at any given time, although deconflicted time slots may be used by devices to participate in several piconets.

Admission to a piconet is also controlled by the master. There is a two step process which the master uses to finds new devices (inquiry) and allow devices into the

piconet (paging). The master broadcasts an inquiry message within its transmission range to inform other Bluetooth devices of its presence. If any of those devices are running an inquiry scan (looking for a master in discovery mode), they respond with a packet containing that device's BD_ADDR.

Once informed of the willing devices available, the master explicitly invites devices to join the piconet by paging. During this transaction, the master gives the new slave the hopping sequence information along with the slave's AM_ADDR. If the master has prior knowledge of devices near it, then it may bypass the inquiry phase and just page those nearby components.

2.3.2.4 Connection Types

Bluetooth piconets allow both synchronous and asynchronous communications between its devices. The asynchronous connectionless (ACL) links are used for data traffic when the integrity of the data is important. The integrity is maintained "using retransmissions and sequence numbers, as well as forward error correction (FEC) if necessary" [3]. For synchronous traffic, up to three synchronous connection-oriented (SCO) links can be created in a piconet. SCO links are used primarily for supporting "periodic audio transmissions at 64 Kb/s in each direction" [3]. The integrity of these transmissions is slightly less, because retransmissions do not occur over SCO links. However, FEC mechanisms are used to recover from some identified errors.

2.3.2.5 Baseband Packets

There are five baseband packet types: Identification (ID), POLL/NULL, Frequency Hopping Sequence (FHS), ACL/SCO, and Data Voice (DV) packets as seen in Figure 3. Each packet type begins with "an access code (AC) field, which is used to distinguish transmissions in different piconets" [3]. Except for the ID packet, all of the packet types also contain a header block. The FHS, ACL/SCO, and DV packets contain a payload section.

The ID packet type is used during inquiry searches and synchronizations. The POLL packet is used when a slave needs to be contacted, but there is no payload to be delivered. The NULL packet type acts as a response when no payload is returned to the master. The FHS packet type is used during piconet creation, by which the master passes the appropriate BD_ADDR, AM_ADDR, and clock information to the new slave. The ACL packet type is used to pass asynchronous data. The SCO packet type is used to pass synchronous data. The DV packet type contains both ACL and SCO data, to be used when a SCO link also needs ACL type data transferred.

Each packet type contains multiple fields. The AM_ADDR field is used to identify "the destination slave of a master transmission or the source slave of a slave transmission" [3]. A Bluetooth master can broadcast messages to all of its slaves by setting the AM_ADDR to b'000'. The PDU_type field identifies the baseband packet type in which it is contained. The flags field is used in ACL packets to do flow control and retransmissions, using "a stop-and-go ARQ scheme and a 1-bit sequence number" [4]. The HEC provides a means to protect this header from errors in transit.

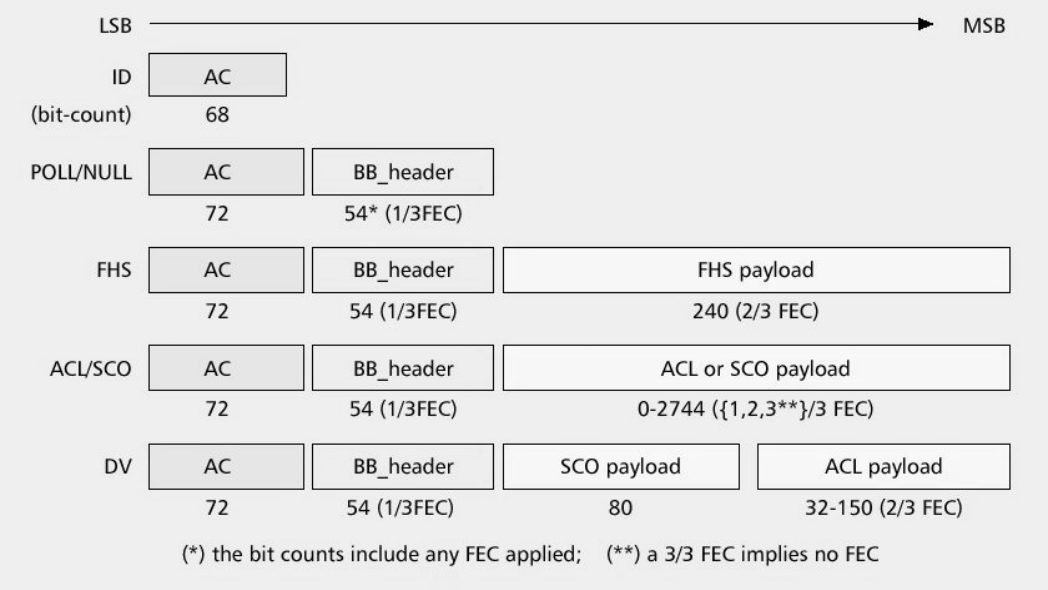

Figure 3. Baseband packet types [3]

The ACL payload is further decomposed into a header, a body, and a 16 bit CRC. The header has a logical channel field (L_CH) which routes the packet through the low levels of the protocol stack. When L_CH = b'11', the packet is used by the link manager to configue the piconet. When L_CH=b'01' or b'10', then L2CAP receives the packet.

2.3.2.6 Link Manager Protocol

The Link Manager Protocol (LMP) is a transactional protocol, responsible for setting up the properties of and controlling the Bluetooth link, to include authentication and encryption of the link. Bluetooth devices in a piconet can "authenticate another device through a challenge/response mechanism" [3], allowing the link to be encrypted once the connection is deemed authentic. The LMPs are responsible for negotiating amongst themselves, to determine which device provides what services.

LMP packets are transmitted in the ACL packet format. They are identified as such by the logical channel L_CH set to b'11' as seen in Figure 4. The LMP packet header is 8 bits long, with the first bit determining the packets sender. The transaction identifier (tr_ID) is '0,' the master sent the packet. If the tr_ID is '1,' then a slave sent the packet.

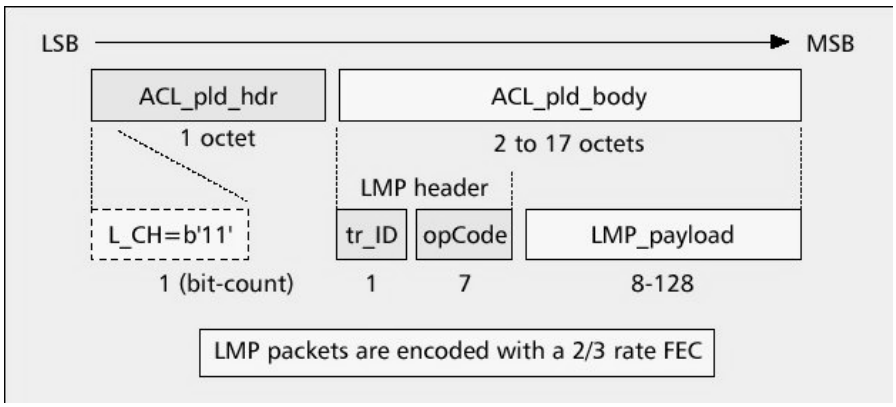

Figure 4. LMP packet type [3]

Authentication and encryption of Bluetooth connections is the responsibility of the LMP. The authentication protocol can be initiated by either device at any time during communication. The authentication procedure is "a challenge/response mechanism based on a commonly shared secret, a link key generated through a user-provided PIN" [3]. The process is begun by the challenger sending a challenge packet, which contains a random number. The claimant receives that packet and generates a response using a 128-bit authentication key. The claimant responds with the new number, where the challenger compares it to an expected result. A match confirms the identity of the claimant.

Once devices have authenticated, the encryption process may begin. Encryption on piconets covers both ACL and SCO links. Authenticated Bluetooth links generate a series of encryption keys from link key. These keys are controlled by the LMP, but SAFER+ algorithm is used in the baseband to encrypt the data. Along with the device's Bluetooth address and the master's clock, these keys are used to encrypt the body of the Bluetooth packets. This encryption runs in 3 modes. Mode 1 consists of no security at all. Mode 2 runs application level security/encryption of packets. Mode 3 hardware encrypts all traffic on link from the time the link is established.

The low power modes (sniff, hold, and park) of Bluetooth devices are controlled with LMP transactions. Sniff mode is when a Bluetooth device listens periodically for master transmissions per an agreement between the two devices. This agreement is decided through LMP interactions. Hold mode is a temporary pause in a slave's involvement in a piconet. This mode is activated when "a device agrees with its [master] to remain silent for a given amount of time" [3]. During this pause, the slave device still maintains its AM_ADDR.

In park mode, the AM_ADDR is surrendered by the slave. The slave remains silent until informed it can return to the piconet by the master device. A parked device may negotiate to return to the piconet prior to being invited back by the master. This is accomplished by replying to the master's beacon transmissions. Despite being in a low power mode, the Bluetooth device can still perform operations. Low power modes only affect a particular piconet. If the device is in a scatternet configuration, it can be active in one piconet and in a low power mode in another.

2.3.2.7 Host Controller Interface

The Host Controller Interface (HCI) is an abstraction layer in a Bluetooth device, not a protocol itself. Through the HCI, a host device communicates with its Bluetooth baseband layer. The HCI is "an interface for host devices to access the lower layers of the Bluetooth stack through a standardized interface" [3]. Through this interface, a host device can request to connect to a specific Bluetooth device, activate low power modes, initiate authentication, and other functions of the device. The capabilities of the Bluetooth card are limited to the HCI command set to which the host device has access.

2.3.2.8 Logical Link Control and Adaptation Protocol

To further abstract the hardware implementation details from the host device, the Logical Link Control and Adaptation Protocol (L2CAP) exists just above the Host Controller Interface. "The concepts of master and slave devices" no longer exist at the L2CAP level in the protocol stack [3]. The multiple channels of ACL links are multiplexed through the L2CAP layer for master devices. SCO links do not interact with the L2CAP, but rather are passed straight to the baseband layer.

L2CAP packets are often larger than the packet sizes supported by the lower levels. To account for this possible discrepancy, the L2CAP layer supports segmentation of its own packets. If the packet is segmented, the L_CH field in the ACL_pkt_hdr is set to b'10', identifying the packet as the first in the segmentation. In all following packets in that segmentation, the ACL_pkt_hdr is set to b'01'. L2CAP payloads can be configured as a signaling packet, a connection oriented payload, or a connectionless payload.

2.3.3 Middleware Protocols

2.3.3.1 Service Directory Protocol

Bluetooth was created to be wide-ranging wireless enabling standard with the ability to cover a large number of applications. To determine what applications or services a device can offer, Bluetooth provides the Service Directory Protocol (SDP). Through the SDP, devices can poll one another to establish which devices have what services to offer. The SDP does not provide the services itself; rather it is only a provider of information.

2.3.3.2 Radio Frequency Communication

To support serial communications protocols, Bluetooth devices have an RFCOMM emulator. The RFCOMM "emulates RS-232 control and data signals over the Bluetooth baseband" [12], emulating the ETSI 07.10 serial specification. With this middleware protocol, Bluetooth devices can support legacy serial communication applications without modifications of the legacy system.

2.3.3.3 Telephony Control Signaling

The Telephony Control Signaling (TCS) middleware protocol allows Bluetooth to access telephone applications. It consists of two command sets: the AT set (TCS-AT) and the binary set (TCS-BIN). The AT command set is run through RFCOMM, being a serial command set. The same commands can also control mobile phones and modems. The TCS-BIN command set is a binary encoding run on top of L2CAP, supporting

"normal telephony control functions such as placing and terminating a call, and sensing ring tones" [3]. TCS-BIN can also control broadcast, point-to-multipoint signals.

2.3.3.4 Adopted Protocols

Bluetooth also includes support for other common protocols, such as TCP/IP. Given this support for current and legacy applications, Bluetooth proves to be a flexible and formidable wireless communications standard.

2.3.4 Bluetooth Performance

Several studies have been conducted since the release of the Bluetooth specification seeking to evaluate and improve the technology and its capabilities. These studies have varied from antenna design and manufacturing [2] [18], to field environment tests [1], and performance analysis of the Bluetooth channel [9] [13] [17].

The Bluetooth specification shows that the selection of packet types greatly affects the throughput capabilities of Bluetooth communications. This variability is shown in Table 2. The Bluetooth devices determine the type of packets used in transmission based on a determination of the signal strength. Weaker signals outside the "golden range" of the device use packet types of smaller size and greater error correction. Stronger signals use packets of greater size and less error correction, on the presumption that the better signal is less likely to create errors. Studies have found throughput performance correlations between packet selection and both signal to noise ratio [17] and bit error rate [9].

Table 2. Packet type throughput variations [4]

Type	Payload Header (bytes)	User Payload (bytes)	FEC	CRC	Symmetric Max. Rate (kb/s)	Asymmetric Max. Rate (kb/s)	
						Forward	Reverse
DM1	1	0-17	2/3	yes	108.8	108.8	108.8
DH1	1	0-27	no	yes	172.8	172.8	172.8
DM3	2	0-121	2/3	yes	258.1	387.2	54.4
DH3	2	0-183	no	yes	390.4	585.6	86.4
DM5	2	0-224	2/3	yes	286.7	477.8	36.3
DH5	2	0-339	no	yes	433.9	723.2	57.6
AUX1	1	0-29	no	no	185.6	185.6	185.6

The throughput rates shown in Table 2 are maximums, assuming no retransmissions or uncorrectable errors in the system. The Bluetooth specification requires that the signal be receivable at ten meters. Throughput levels in excess of 300 kbps are possible at twenty meters and 200 kbps at thirty meters [11].

2.4 Wireless Security Issues

As in any trusted environment, the security of a computer network is an important factor in its design and implementation. The main areas of concern when securing a network are the authentication of the users, the availability of the network, and the confidentiality, integrity, and non-repudiation of the data.

- The *authentication* of users on a network ensures that only those people who should be on the network are on the network. Unauthorized access to a trusted network could enable an enemy to access sensitive information and/or systems.

- *Availability* of a network ensures that when the user needs the resources of the network, he can access them. Not only is the network available during normal usage, but also is survivable when under external stress, such as in a denial of service attack.
- *Confidentiality* of a network is necessary for the users to trust the system and one another. Without it, the data passed on the network may be acquired by unauthorized users.
- *Integrity* of the network's data ensures that the information has not been corrupted. Maintaining the integrity of the data involves both defending against malicious attacks as well as dealing with accidental failures of the system.
- *Non-repudiation* of the network's messages ensures that what happens on a network cannot be erased. A user sending a message cannot deny that the message was sent. This gives accountability to the system.

Computer networks operating in a wireless environment pose several security threats inherent to the transmission medium. The first of these is interference. A simple understanding of what transmission scheme is being used would allow an enemy to execute an effective jamming operation, denying access to the network. While spread spectrum technologies mitigate the likelihood of this, they do not defend against it completely.

Another vulnerability inherent to a wireless medium is signal interception, or eavesdropping. Unlike a traditional wired network where the transmission lines are fixed, a wireless network broadcasts over an area correlated to the transmitter's power

level. Any receiver in the coverage area can receive the signal. If the signal is not properly secured, an enemy could passively listen to the transmissions violating the network's confidentiality. Through various active attacks on the wireless network, an enemy could violate the network's availability, integrity, authentication, and nonrepudiation.

Many wireless networks are extensions of preexisting wired networks installed for the convenience of users. With this topology, the central access point is a large vulnerability, possibly being a single point of failure for the wireless portion of the network. While these wireless extended networks suffer from this weakness, ad hoc wireless networks do not. Being distributed in nature, these networks can often survive when a single node is brought down. This distribution of control helps ensure the survivability of the network.

Finally, the composition of wireless networks tends to be dynamic, even over short periods of time. Wireless networks are often implemented to give users mobility without losing connections. Because of the frequency of adding and dropping nodes in the network's topology, authentication becomes paramount in establishing and maintaining trust in the network. All of these factors must be considered when securing a wireless computer network.

2.5 Bluetooth Security Issues

Bluetooth enabled systems have some vulnerabilities that, if overlooked, could pose as a threat to the security of a piconet. These weaknesses can be classified into

several categories: eavesdropping and impersonation, location attacks, hopping attacks, cipher attacks, invalid states, and traffic exposure.

2.5.1 Eavesdropping and Impersonation

Eavesdropping and impersonation attacks require an attacker to acquire the initialization key of a Bluetooth device, which is used in the encryption process. This initialization key is derived from a PIN, a random number (computed from the device's authentication process), and the device's Bluetooth address (BD_ADDR). The last two can be intercepted easily, because they are broadcast in the clear. The PIN must be entered into both devices by their users. The first flaw is that the PIN has a default value of zero. If this is not changed, the initialization key can be easily determined and the link's encryption broken.

This PIN crunching can be used in two ways. In the first, an attacker must use an exhaustive search to guess all the possible PINs. From this list of possible PINs, the attacker attempts a verification process with the guessed PIN. This process is repeated until a successful verification is accomplished. This process is called "eavesdropping on the key establishment process" [8].

In the second scenario, the attacker takes a guessed PIN and tries to initialize a connection with the victim device by beginning the challenge-response protocol. Like the eavesdropping attack, this is repeated until a selected PIN returns a 'correct' response from the victim. This verified PIN is used to complete the key establishment protocol. To counter PIN guessing, Bluetooth devices use an exponential back-off process to delay the time between guesses allowed. While it may keep attacks at bay longer, it also allows

more time for the attacker to generate more PINs. This is called "stealing by participation" [8].

The link key and encryption keys are derived from the initialization key. Because of this, maintaining the secrecy of the device's PIN is essential. Once this is discovered, and enemy can impersonate that device. Having the initialization key, the attacker can contact other devices and acquire their links keys. By knowing the link keys, the attacker can impersonate these devices. A "man-in-the-middle" attack can be initiated by contacting two devices acting as one to the other. Both devices think that they are communicating with one another, and that the other has initiated the contact. Communications between the two now pass through the attacker, who can both read it and change it, if desired.

2.5.2 Location Attacks

Bluetooth devices that are in discovery mode respond to other devices with their Bluetooth address (BD_ADDR). Knowing this, an attacker can determine both the current location and the movements of a victim device. If the identity of the owner of the Bluetooth device is known, that connection can be used to track the owner. Because the BD_ADDR is an address permanently imprinted at the time of manufacturing, tracking a device and its associations cannot be prevented.

Changing power modes by a Bluetooth device can be controlled by the application layer of a device. Thus, malicious software can force a device into low power modes that scan for other devices in its area. The victim of such an attack will announce its presence which the attacker can track.

2.5.3 Hopping Along

The hopping pattern a Bluetooth device follows makes it difficult for an attacker to intercept Bluetooth transmissions. The attacker must either listen to all 79 channels simultaneously or hop along with the piconet master's sequence. To hop along with the master, an attacker must learn the pattern or the seed used to generate the hopping sequence.

The hopping sequence is determined by the clock and address of the master. When a device is in inquiry mode (not currently part of a piconet), the hopping sequence it uses is based on its own clock and a general inquiry access code which is common to all devices. During inquiry, a device transmits its clock and BD_ADDR. An attacker could scan the bands reserved for inquiry and eavesdrop. When the device is connected (part of a piconet), the hopping sequence is determined by the master, using both the master's BD_ADDR and clock. Piconet masters transmit their BD_ADDRs and clocks when they page devices. These transmissions could also be intercepted, giving the attacker the information necessary to follow the hopping sequence.

2.5.4 Cipher Attacks

Transmissions on a Bluetooth link can be encrypted. The basis for this encryption is "[an] encryption key K_C, the 48-bit BD_ADDR, the master clock bits $CLK_{26\text{-}1}$, and a 128-bit RAND value" [4]. From these four inputs, four linear feedback shift registers (LFSR) of size 25, 31, 33, and 39 bits are initialized to compute the encryption cipher.

To determine the encryption key, the inputs to the four LFSRs must be known. "An attacker can guess the content of the registers of the three smaller LFSRs and the

summation register with a probability of 2^{-93}" [8]. The contents of the largest LFSR can be determined from the outputs of the other LFSRs and the summation register. The output from the guess is compared to the actual transmission to determine the correctness of the guess. While this still a laborious process, it is considerably better than the 2^{128} required to exhaustively brute force through the encryption cipher.

2.5.5 Invalid States

The Bluetooth model has to guard against being caught in one of several possible invalid states found in various levels of the device. The link controller of a Bluetooth device can be in one of nine different states: one of two high level states or one of seven transitional states, as seen in Figure 5 [6].

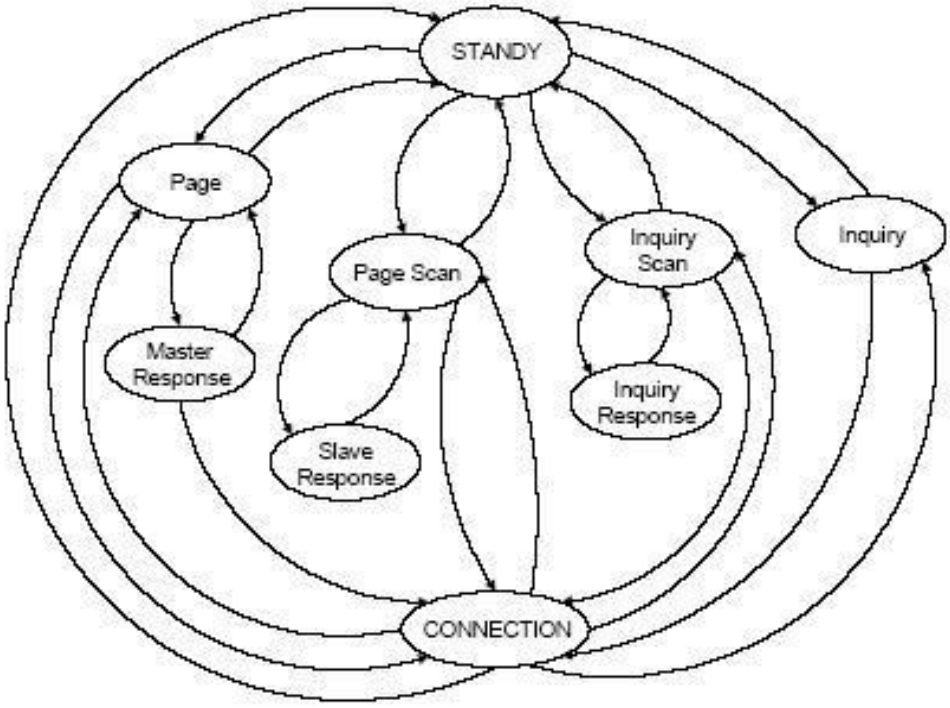

Figure 5. Link controller state diagram [6]

The two high level states can be determined by a single bit with no possible invalid states. However, three bits are needed to represent the seven transitional states. This leaves one state that needs to be guarded against. A manufacturer's design should be able to safely escape this state into a stable one to prevent unknown activity.

There are four possible states for the encryption of traffic. Hardware needs to avoid going into the invalid state of encrypted broadcast traffic and unencrypted unicast traffic. This would allow an outside device to listen to directed traffic while broadcast traffic is unavailable. The issue is not the encrypted broadcast data, but the availability of unicast data while some encryption is being used.

2.5.6 Traffic Exposure Issues

Data can be exposed to unauthorized parties when a slave and a master negotiate to change roles. This transfer time can leave data available to unwanted recipients, or even lost. If the master disables encryption during the switch, either traffic from the slave could be encrypted and received by no one, or unencrypted and readable by everyone. Either situation leaves the data in a situation not desired at the beginning of the transmission [6].

The link key scheme used by Bluetooth can also pose an exposure problem. The problem is illustrated in Figure 6. Device A uses its link as the basis for encryption for data passed between A and B. Device A uses that same link key to encrypt traffic between A and C. B can now listen to C's traffic, and even pose as C if it chose to do so

[16]. The solution is for A to have a better key management system, but this grows in complexity with the size of the piconet (or even worse for a scatternet).

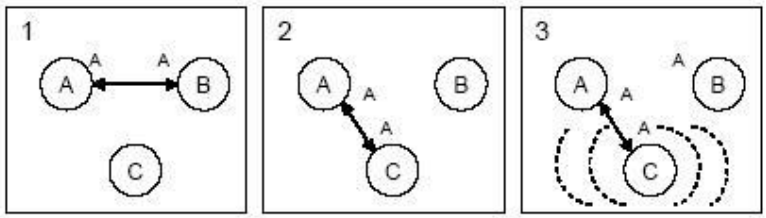

Figure 6. Link key traffic interception [6]

2.6 Summary

This chapter reviewed the topics necessary for understanding of Bluetooth wireless systems. First, wireless communications and the IEEE family of specifications governing it were discussed. Second, Bluetooth communications and its implementation were presented in detail. Third, security concerns in wireless communications were discussed. Finally, security vulnerabilities specific to Bluetooth systems were outlined. The next chapter presents the experimental methodology.

3. Methodology

3.1 Introduction

This chapter discusses the methods in the experiment, as well as how the data is collected and analyzed. This methodology parallels the work of Capt Tim Kneeland [11]. Doing this serves as both a validation of his work and extensions to that work, to further understand Bluetooth systems.

3.2 Problem Definition

The purpose of this study is to determine the effective range of Bluetooth wireless networks in an open air environment. This experiment evaluates several Bluetooth devices at various ranges and orientations to determine this distance.

3.2.1 Goals

This study develops a generic usability "map" for Bluetooth enabled systems. This map, similar to a physical topological map, identifies the maximum range of a Bluetooth transmitter-receiver pair. This not only indicates the maximum usable distance between the devices, but also the range at which the devices are vulnerable to interception.

3.2.2 Approach

The map is constructed by measuring the throughput capacity of pairs of various vendors' Bluetooth antennas. A systematic combination of several different vendor antennas, with throughput measured at various ranges and antenna orientations are used

to accumulate data on the capabilities of Bluetooth transceivers. The transmitting antenna, receiving antenna, distance between the two, and relative antenna orientation are varied. The data gathered from this sample of unmodified commercially available Bluetooth transceivers is used to infer the performance of Bluetooth systems as a whole.

3.3 System Boundaries

The System Under Test (SUT) is the Bluetooth channel, from transmitting antenna to receiving antenna, including the radio waves themselves. Within this system, the packets submitted to the Bluetooth protocol stack constitute the load offered to the system. All other components are either inputs or support elements to the SUT.

Within this SUT, the component under test (CUT) is the transmission capability of the transmitting antenna. The distance at which the Bluetooth antenna is able to transmit defines its usability/vulnerability range.

This experiment is designed to infer a maximum range at which two Bluetooth devices can communicate and are vulnerable to interception. The resulting distances are the best case for a piconet's transmissions. The addition of more devices to the piconet or the addition of barriers (as would be found in an office setting) will decrease the maximum range capability of the Bluetooth device.

3.4 System Services

The system provides the capability to transmit data wirelessly between two nodes. The system provides a successful transmission if the data is received with no errors, or if

the errors are correctable by the receiver. The system fails if either there is no data received or if there are errors that the receiver cannot.

Only successful trials of the system are considered in the data. A failure of the system is of no use in this study, with one exception. The failure that represents the antenna pair's inability to communicate over that distance or further is noted as that antenna pair's maximum distance.

3.5 Performance Metrics

The performance metric used to evaluate the system is throughput. Throughput, defined as the number of bits transmitted divided by the measurement period, measures the ability of the SUT to transmit data across the link. The amount of data successfully (errorless or corrected errors) transmitted per unit time is throughput. A failure of the system is identified by an unusually low throughput (high number of uncorrectable errors) or a zero throughput.

3.6 Parameters

This section describes the parameters involved in the experiment, both for the system and the workload.

3.6.1 System Parameters

- Antenna orientation – The radiation pattern of an antenna is not omni-directional, but varies according to the position of the receiver. Thus, the distance at which a signal is receivable will be affected by the position of the respective antennas.
- Antenna types – Different vendor antenna configurations are likely to produce variations in the performance of the Bluetooth link. The antenna shape,

encasing, and manufacturing could all affect the device's transmission capabilities.

- Distance – The distance between antennas will affect the throughput of the wireless system. With the power level fixed at 1 mW, there is a finite distance at which the signal is receivable. The strength and reliability of a wireless signal decreases proportionally to this distance.
- EM interference –Bluetooth devices operate in the unlicensed 2.4 GHz band. There are many other devices operating within these same frequencies and these devices could create scrambling or destructive interference of the Bluetooth signal. Errors caused by these transmissions will decrease the throughput of the Bluetooth transmission.
- Environmental Factors – Variations in barometric pressure, humidity, temperature, and other environmental factors can affect the Bluetooth signal by causing attenuation, path loss, or reflection of the signal.

3.6.2 Workload Parameters

- Packet Type – The antennas used in [11] came with software that conditioned the packet stream to use DM5 packets almost exclusively in their transmissions, through file transfer software included as part of the installation. Not all manufacturers use this software; most manufacturers force the use of Windows Explorer® to execute the transmissions. These signals vary in packet type, from DM1 to DH5 based upon the signal strength.

3.7 Factors

- Antenna orientation - (360, 90, 180, 270 degrees) – The levels for the antenna orientation were selected to cover 360 degrees around the transceiver. These levels are consistent with the previous work in [11]. The gain of most antennas is not uniform; therefore the antennas' orientation is expected to be a significant factor in the usable range of the device. The orientations of the two laptops relative to one another, along with the rotations of the transmitter, are shown in Figure 7.

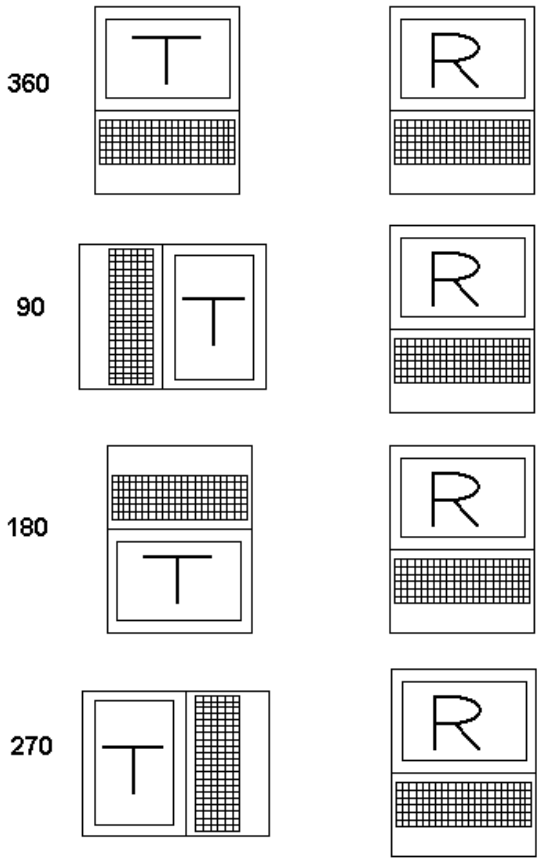

Figure 7. Transmitter/Receiver Laptop Orientations

- Distance – (five meter increments, one meter fine-tunings) – The five meter increments allow the expected range to be traversed rather quickly. The one meter refinements better define where the throughput levels pass certain thresholds (300, 200, 100 kbps, and failure). Due to path loss and signal attenuation, the distance between the two devices is expected to account for the largest percentage of variation in the experiment.
- Vendor Antennas – The different antennas represent a sample of the Bluetooth transceivers available commercially. The number of different devices generalizes these results to most Bluetooth devices. It is suspected that the device manufacturing has an effect upon the system's throughput capabilities and range. Specific details concerning the antennas used can be found in Appendix A.

The remaining parameters (possible electromagnetic interference and environmental-related factors) not varied are held as close to constant as possible. Being

environmental factors, they cannot truly be held constant without facilities well beyond the scope of this study. An effort is made to perform testing in conditions as close to constant as possible. It is expected that some of the resulting error is attributable to these environmental parameters.

3.8. Evaluation Technique

The evaluation technique used for this experiment is a direct measurement of the system. This evaluation technique is selected for several reasons. Since the true effect of the factors on the system's performance is unknown, a valid simulator for Bluetooth networks is unavailable. Direct measurement of a Bluetooth system correlates the factors to the performance metrics. This method is also valid because it is the best case scenario of an implemented Bluetooth network, which is the focus of this study.

3.9 Workload

The workload offered to the system is a 1000 KB text file. This has several advantages. The first is the ease of throughput calculations given a file of this size. This also allows the transfer to run long enough to achieve reliable results for the throughput measurement. The minimum amount of time needed to transmit the file is

$\frac{1001KB(\frac{8bits}{1byte})}{723.2kbps} = 11.07$ seconds, using solely DH5 packets. As the packet type varies, so will the best case throughput. As seen in Table 2, one-way throughput is highly dependent upon the packet type chosen by the transmitter. The best possible case throughput uses DH5 packets. This time represents the minimum necessary for a file to

be transmitted, and many of the trials are expected to take longer as the signal degrades. This workload is applied until the file transmission is complete.

3.10 Experimental Design

The experimental design for the throughput tests is a three factor, full factorial design with replications. A full factorial design with replications means the effect of each factor, effect of the interactions, and the effect due to experimental error can be separated from one another and be quantified. The number of trials for each orientation is variable, because each orientation is likely to fail at different distances. The best result is chosen from *r* iterations of experiment, to find the maximum range at which throughput level can be attained.

While the best case range is of primary interest, the mean of these replications is of interest to determine the statistical significance at each distance and orientation. Assuming a normal distribution of error and a 95% confidence ($z = 1.645$, $\alpha = 5$), the number of replications, *r*, required is given by $r = (\frac{164.5s}{5\bar{x}})^2$ [17], where *s* is the sample standard deviation and $\bar{x}$ is the mean of the sample. Each experiment is initially performed three times. From this sample, *r* is calculated and more replications are run until the desired confidence interval width is reached.

3.11 Experimental Setup

For each experiment, two laptops were arranged on wooden stools (0.6318 meters tall) in the orientations shown in Figure 7. A wooden stool was used to minimize

possible interference that metal stools may have produced. The distance between the laptops is measured and fixed for each experiment.

For each distance-orientation pair, the test file is transmitted at least three times. The packet level traffic for each successful transmission is captured by the CATC Merlin Protocol Analyzer [5]. This transmission sequence is analyzed to determine the throughput for the file transfer.

3.12 Results Analysis and Interpretation

The percentage that each factor contributes to the throughput can be determined from the data using analysis of variance (ANOVA). The mean square of each effect (MSx) is calculated from its sum of squares (SSx) and its degrees of freedom (v_x). The mean square of the error (MSE) is calculated the same way. The ratio of the two (MSx/MSE) is the computed F-value. If this value is greater than the F curve defined by $F(0.95, v_x, v_e)$, then factor x is significantly different than the error [7]. As mentioned above, the number of replications will be increased to ensure significance between levels of the experiment.

3.13 Summary

This chapter discussed the experimental methodology for testing the best case usable distance between two Bluetooth wireless devices. The goals and approach used in this experiment were presented, followed by a definition of the system and component under test. Next, a discussion of the parameters and factors varied in the experiment is

given. This is followed by a definition of the workload and experimental methodology. Finally, a description of the data analysis is presented.

4. Analysis and Results

4.1 Introduction

This chapter discusses the results from the throughput experiments performed on each of the antennas, as well as analysis of the data collected. This data is first generalized to each of the two general antenna types (PC Card and USB Dongle). Details of each individual antenna are then presented.

For all tests, a Dell Inspiron 8200 running Windows 2000 is the transmitting device. When facing this laptop, the PC cards extend from the right hand side of the keyboard. The USB dongle extends from the back of the laptop, on the left hand side. The receiving device is a Dell Latitude D600, also running Windows 2000. In this laptop, the PC card extends from the left hand side of the keyboard. The USB dongles extend from the back of the laptop, on the right hand edge.

The throughput levels are calculated by finding the time stamp on the first packet containing information from the test file, as well as the last. The size of the file is known, so the throughput is determined by simply dividing that size by the difference in time stamps of the last and first packets. The throughput calculator within Merlin is not used since it does not account for retransmissions of packets.

Throughput measurements are only performed out to 40 meters; a physical limitation of the indoor testing environment. Any cards whose thresholds for various throughput values exceeded this distance are noted in the analysis, but those lines are not shown in the maps presented.

4.2 Antenna Types

4.2.1 PC Cards

As a group, the PC cards performed quite similar to one another. Despite this similarity, the 3Com PC card performed the best. This may be due to the unique physical design of the 3Com antenna, which folds out of the plane of the card itself. However, the performance cannot be completely attributed to this physical difference, as the Belkin PC card (which does not have this antenna feature) performed almost as well as than the 3Com antenna. Both were able to transmit out to 40 meters, with 3Com's performance better at that distance. The Anycom antenna performed close to these two, but only had one orientation (360 degrees) that transmitted at 40 meters. The other orientations failed beyond 35 meters.

The amount of variance attributed to the manufacturer was only 0.1386%, and that was only significant to a 60% confidence. The majority of the variance was attributed to the distance (78.81%) and to the interaction between the distance and the manufacturer (11.00%). The orientation of the antenna only affected the variance when combined with the manufacturer and distance, and it was only 9.00% at that.

4.2.1.1 3Com PC Card

The 3Com PC card has an unusual feature; an antenna that flips up out of the plane of the card itself. It is possible that this feature is what contributed to the card's ability to transmit at over 100 kbps beyond 40 meters, the largest distance tested. Its transmission failure range is therefore unknown. The effect of the antenna extending to a

different plane than the other PC cards could be determined by running more tests, some where the antenna is extended and some where it is not.

The 90 degree orientation is the best at the 200 kbps level, successfully achieving that throughput at 20 meters. The 270 degree orientation is the best at the 100 kbps, with a distance of at least 40 meters. The specific data for each device can be found in Appendix A. For the 3Com PC card alone, the distance between the devices was the most significant factors, accounting for 84.5% of the variation. The interaction of the distance and orientation accounts for 6.3%, while the orientation alone accounts for 3.7%. Figure 8 below shows a graphical throughput representation for the different orientations.

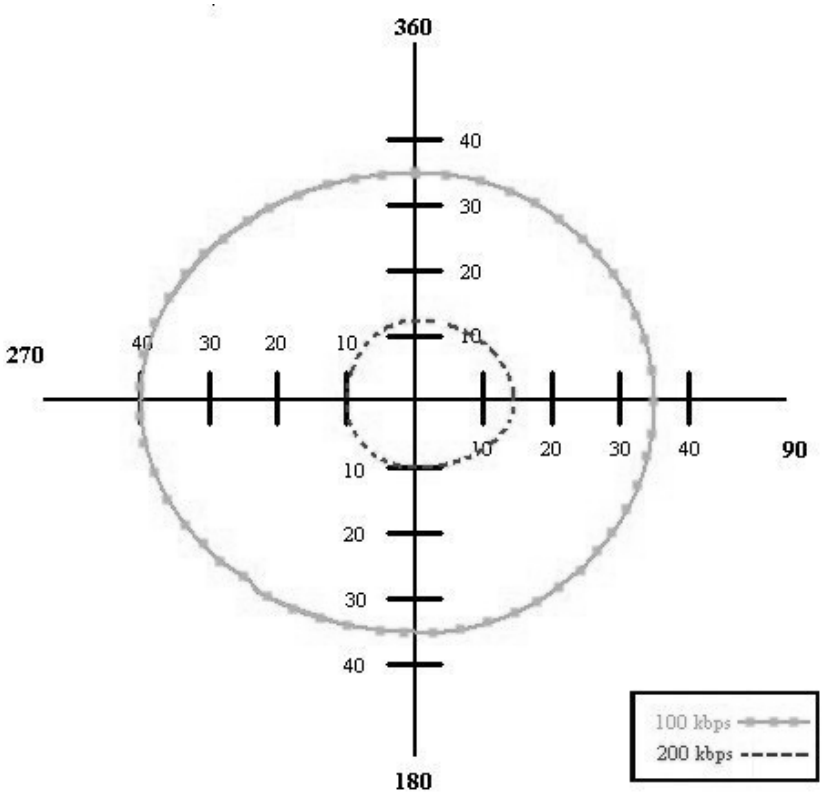

Figure 8. 3Com PC Card throughput ranges

4.2.1.2 Anycom PC Card

The Anycom PC card comes with a different software set than used by the other devices in this study. The file transfer software preconditions the packet stream for transmission. As a result, all the data packets broadcast have the DM5 packet type. This could affect the throughput levels because both the data block size and error correction level of this type packets are fixed. The distance at which the Anycom cards can successfully broadcast is shorter than the other two PC card antennas. Perhaps the retransmission of large blocks of data is the contributing factor, given that the number of packets with errors increases as the distance between the devices increases. Because the file transfer software for this card forces the data packets to be DM5s, this hypothesis cannot be tested without modifications to the software.

As shown in Figure 9, the 90 degree orientation is best at both the 300 and 100 kbps levels, producing ranges for each out to 10 and 30 meters, respectively. The 360 degree orientation is the best at the 200 kbps and failure levels. The 200 kbps level is possible at 25 meters, while the orientation fails out beyond 40 meters. Again, the distance between the devices is the dominating effect, causing 91.5% of the variation. The interaction between the distance and orientation accounts for 7.1% of the change, while the orientation alone accounts for less than one percent.

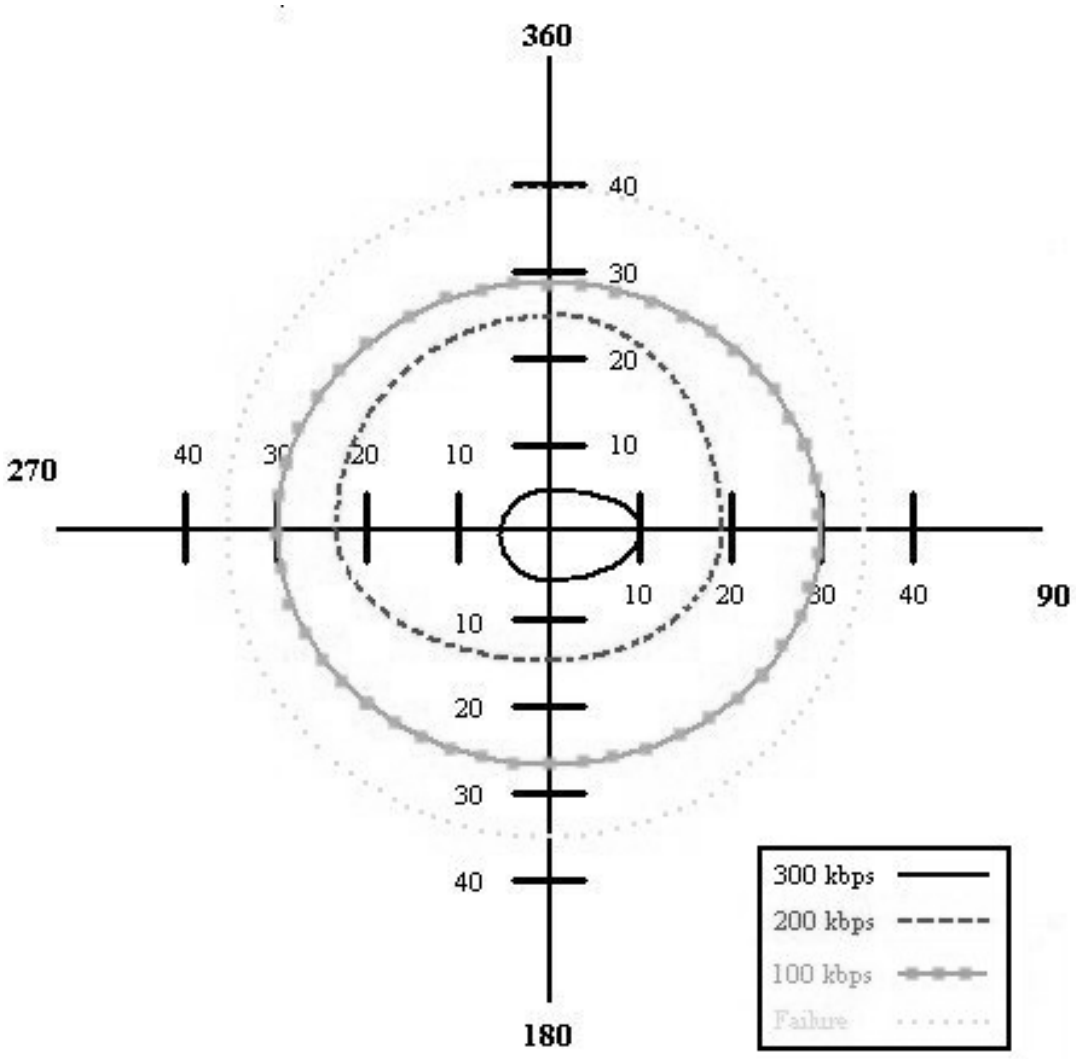

Figure 9. Anycom PC Card throughput ranges

4.2.1.3 Belkin PC Card

As shown in Figure 10 below, the 180 degree orientation is just slightly (less than 1 kbps) better than the 90 degree orientation, achieving the 300 kbps level at 10 meters. The 300 kbps line is flat for the 270 and 360 degree orientations because the antenna did not achieve throughputs of 300 kbps at any distance measured for those orientations.

This same anomaly occurs in the 3Com USB dongle's map. The 360 degree orientation is the best for the 200 and 100 kbps levels, transmitting at those levels at 25 and 30 meters, respectively. All orientations transmitted beyond the 40 meter mark, with the 90 degree orientation having the highest throughput at that distance. Similar to the 3Com antenna, the true failure distance is not known. Like the other two PC cards, the distance between the Belkin cards is the greatest contributor to the variation, accounting for 89.5% of it. Likewise the distance-orientation interaction and orientation itself followed suit, with allocations of 7.5% and 2.5%, respectively.

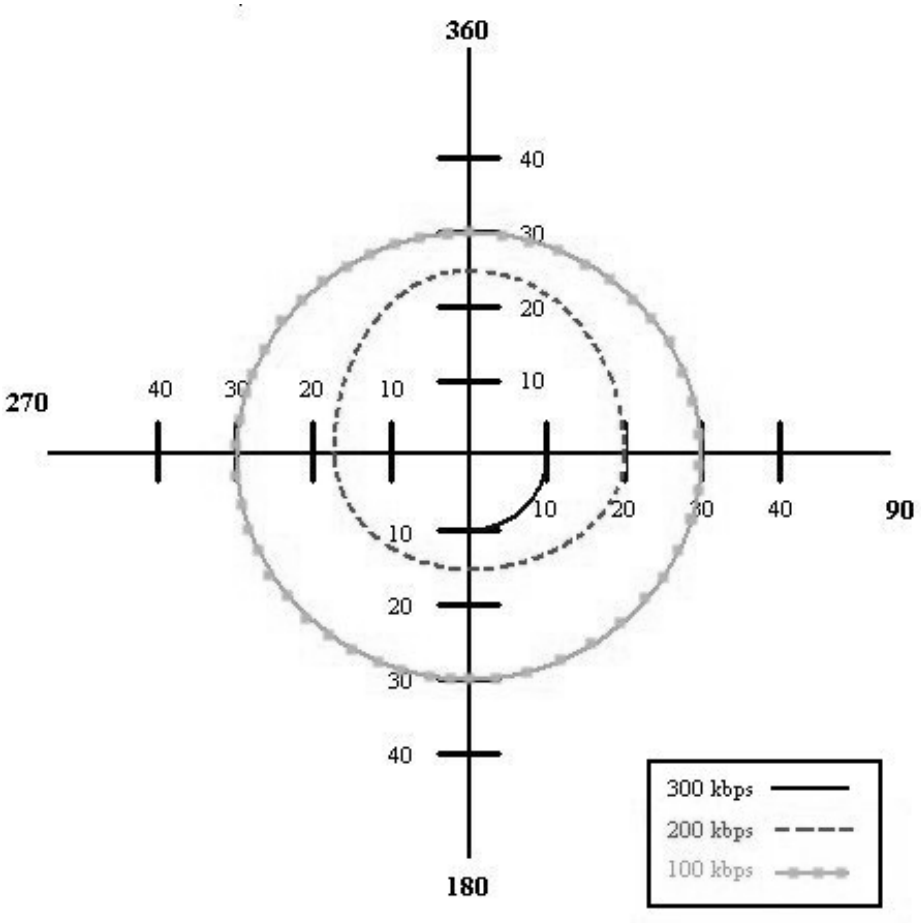

Figure 10. Belkin PC Card throughput ranges

4.2.2 USB Dongles

Unlike the PC cards, the USB dongles did not perform similarly to one another. There is a great difference between the top performer (Hawking) and the bottom performer (DLink). Some of this difference is likely attributable to the size of the dongles themselves, as the DLink antenna is considerably smaller than any of the other devices tested. The differences between the cards are easily distinguishable. The Hawking card is capable of over 200 kbps at 40 meters. The second best dongle (3Com) is capable of over 100 kbps at 40 meters. The Belkin device failed beyond 25 meters, and the DLink antenna was barely usable at 10 meters.

In fact, the manufacturer accounted for the majority of the variance (57.36%) in the USB group. After that, the variance ranks were comparable to the PC cards, with distance accounting for 22.87%, the manufacturer-distance combination accounting for 9.76%, and the orientation-manufacturer-distance grouping combining for just 7.67% of the variation.

4.2.2.1 3Com USB Dongle

The 360 orientation is slightly better than the 90 degree orientation for the 300 kbps level, both achieving it up to 11 meters (see Figure 11). The 270 degree orientation is also slightly better than the 180 degree orientation at the 200 kbps level, with both producing those results at 25 meters. All of the orientations are able to transmit above 100 kbps beyond 40 meters, so the distance to failure is unknown. The majority (73.6%) of the variance comes from the distance between the devices. The distance interacting

with the orientation accounts for 13.9% of the variation, while the orientation alone is again inconsequential, contributing to a miniscule 0.1835% of the change.

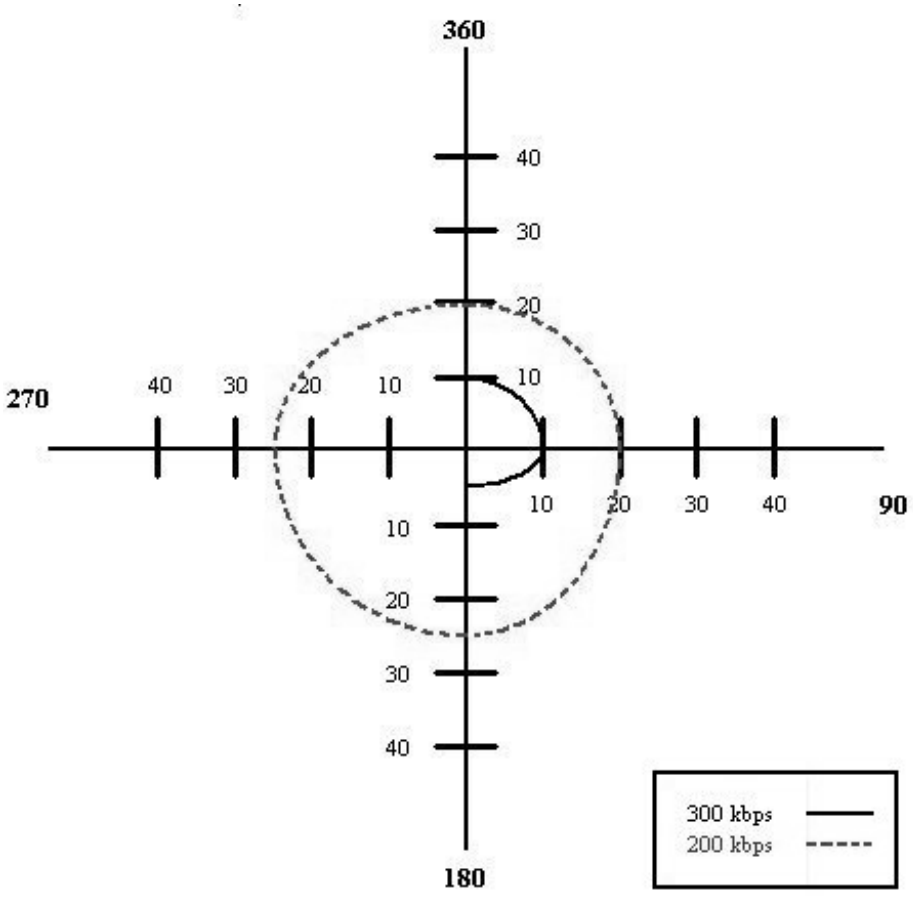

Figure 11. 3Com USB throughput ranges

4.2.2.2 Belkin USB Dongle

The 270 degree orientation, as shown in Figure 12, is the best here at the 300 kbps level, producing that throughput at 15 meters. It also dominates the 200 and 100 kbps levels, achieving each at 19 and 25 meters respectively. All of the orientations failed at 30 meters. The distance is slightly less of a factor, although still a considerable one,

accounting for 64.7% of the variation in the Belkin USB dongle. The distance-orientation interaction increased to fill that void, providing 27.4% of the variation.

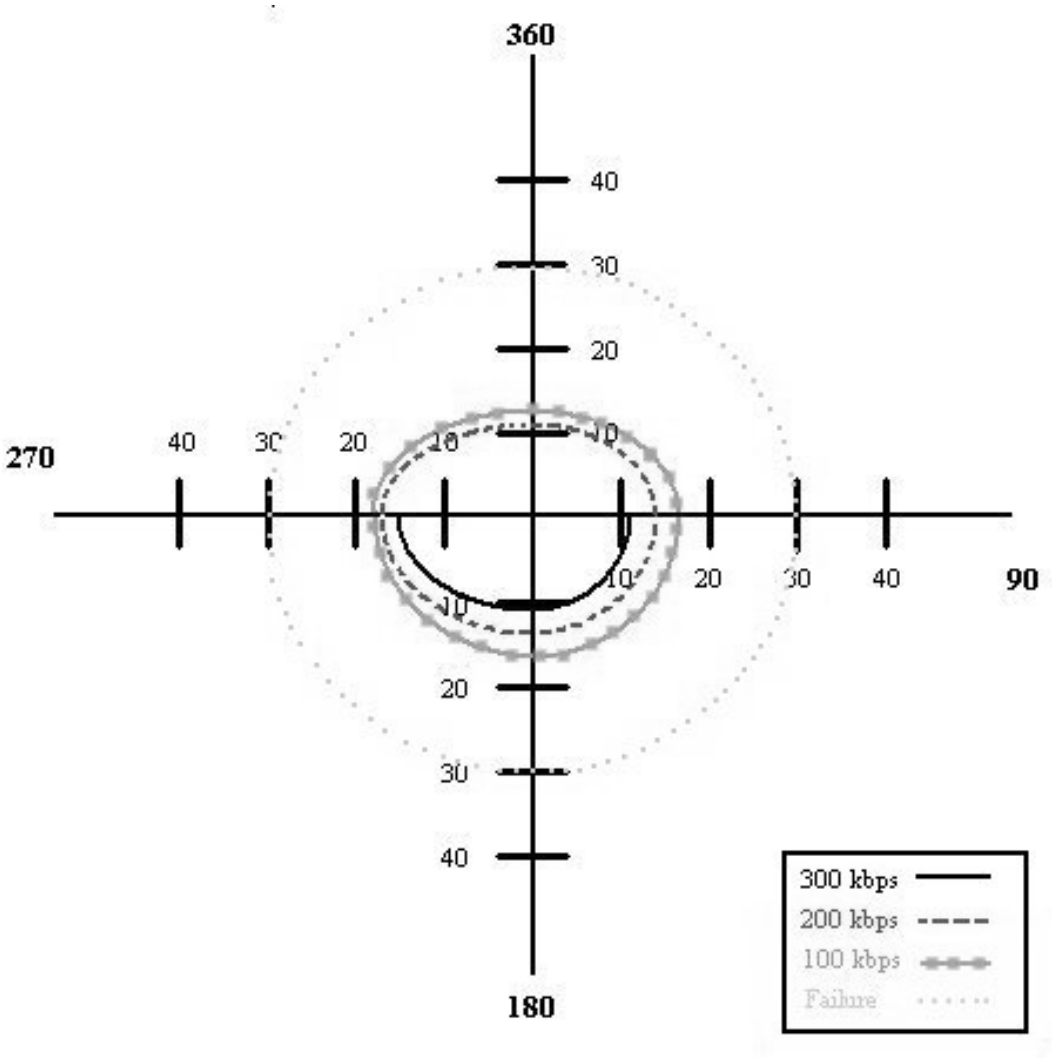

Figure 12. Belkin USB throughput ranges

4.2.2.3 DLink USB Dongle

The relatively abysmal performance (shown in Figure 13) of the DLink antenna is probably linked to the size of the device. The smallest of all the antennas, it is at least half the size of the rest of the USB devices. With this small antenna, the gain patterns for

both transmitting and receiving are diminished. This is likely the reason it was unable to transmit above 100 kbps, and why only one of the four orientations was successful beyond 15 meters. If DLink were to create a similar card, with only the antenna size changed, then this hypothesis could be tested.

The DLink card is unable to achieve throughputs of over 100 kbps at any distance measured. The only orientation of note is the 360 degree orientation, which has a usable signal out to 18 meters, whereas the other three orientations failed after 10 meters. Again, the distance between the devices accounted for the majority of the variation (74.1%). The distance-orientation interaction accounts for 17.5% of the variation, with the orientation alone having no significant effect at all on the throughput.

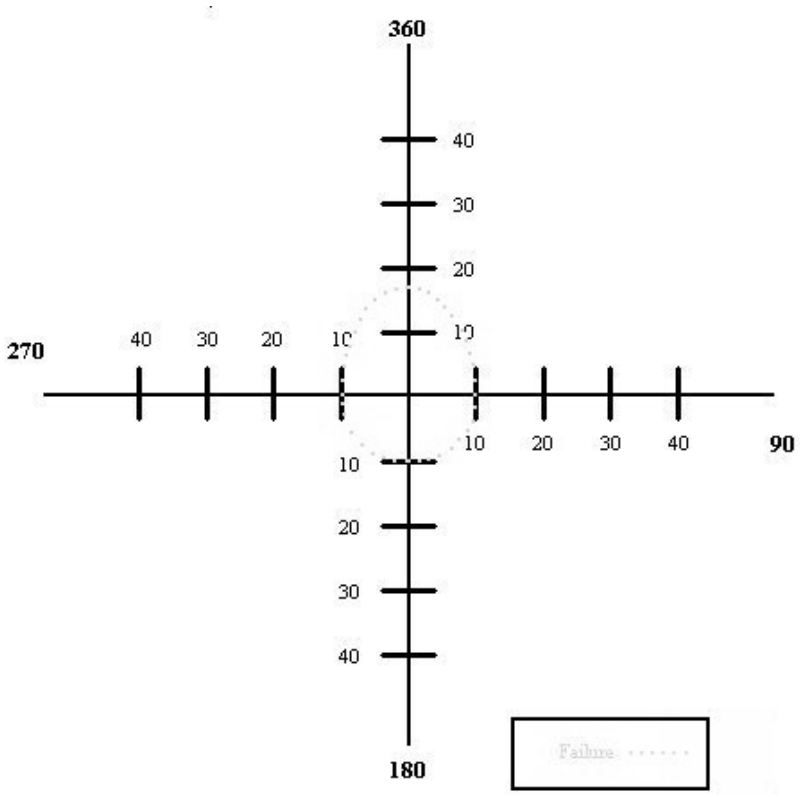

Figure 13. DLink USB throughput ranges

4.2.2.4 Hawking USB Dongle

Figure 14 reflects the throughput performance of this device. The 90 degree orientation is slightly better than the 270 degree orientation, both achieving the 300 kbps level at 24 meters. The 180 degree orientation is the only one not to transmit at the 200 kbps level at 40 meters. All four orientations are capable of at least 100 kbps beyond that distance; therefore the failure distance is unknown. For the Hawking antenna, 76.6 % of the variation is attributable to the distance between the devices. The interaction between the distance and orientation accounts for another 14.3% of the change. Again, the orientation alone has no effect on the variability.

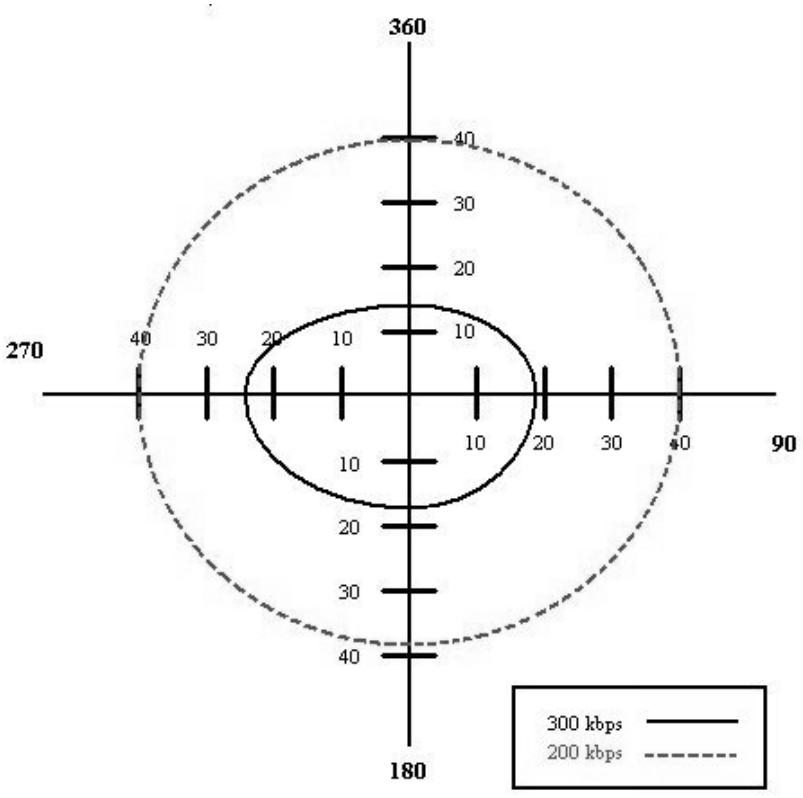

Figure 14. Hawking USB throughput ranges

4.3 Summary

This chapter presented the capabilities of seven different Bluetooth devices, giving both the results of the experiments and an explanation for those results. From these tests, it is shown that while performance does vary by manufacturer and antenna type, Bluetooth is capable of over 100 kbps at distances greater than 40 meters. The PC cards all preformed similarly, likely due to nearly identical size and manufacturing. The USB dongles varied considerably in performance, likely due to the same manufacturing differences. The larger dongles performed better while the smallest dongle (DLink) had the worst capability.

5. Conclusions and Recommendations

5.1 Chapter Overview

This chapter concludes the research presented in this thesis. A discussion of the outcome of each research objective is given. This is followed by recommendations for future work and a summary of the research.

5.2 Conclusions of Research

In developing these usability/vulnerability maps, it is found that for any given antenna, the distance between devices accounts for the greatest percentage of variation. This variation falls anywhere between roughly 60-90%. The manufacturing of the device also plays a significant role, as capabilities varied widely between all seven antennas tested.

Given that orientation by itself did not prove to be a significant factor for any of the devices, the usability/vulnerability range of Bluetooth devices appears to be based upon the distance from the transmitter. In some of these 1 mW devices, a throughput of over 100 kbps is attainable at distances exceeding 40 meters. This is much greater than the 10 meter range stated within the Bluetooth specification and advertised by the manufacturers themselves. Further study of higher power devices may prove this range to be even greater than reported here.

5.3 Recommendations for Future Research

This research accomplished an introductory study into the capabilities of commercially available Bluetooth devices, with their capabilities measured by the

throughput attainable at various distances and orientations. Possible further research topics in Bluetooth are:

- Full factorial analysis of antenna orientations, varying both the transmitter and the receiver positions.
- Heterogeneous pairing of antennas to determine if any variance can be attributed to transmitter/receiver differences.
- Performance evaluation of higher power (> 1 mW) Bluetooth devices
- Performance evaluation of Bluetooth access points
- Evaluation of Bluetooth enabled handheld devices (e.g. PDAs)

5.4 Summary

This research determined a usability/vulnerability range for seven commercially available Bluetooth devices. This information was derived from experiments varying the distance between and orientation of two Bluetooth antennas. These throughput maps provide a first step towards understanding the requirements for implementing a Bluetooth network in a secure environment, as well as laying a foundation for other research in this topic area.

Appendix A – Antenna specifics

This appendix contains the throughput tables and ANOVA charts for each of the antennas used in the experiment. The hardware details applicable to each antenna are also provided.

The ANOVA analysis for each card was limited to the distances at which measurements from each orientation were taken. A more precise analysis of variation could be possible if every orientation is measured at every distance.

1. 3Com PC Card

The 3Com PC card is operating on version 1.2.0.0 of its Bluetooth software.

Table 3. 3Com PC Card Best Case Throughput Data

Distance (m)	Orientation (degrees)			
	360	90	180	270
5	258.1503	259.3842	240.1674	245.3112
8	X	X	X	209.9062
9	X	X	X	205.6365
10	215.1285	240.8295	210.3961	211.5306
11	202.7748	X	195.5795	X
12	213.21	X	130.6046	X
15	152.0778	207.2215	160.4184	194.6324
16	X	192.9869	X	X
17	X	184.4927	X	X
20	181.8778	236.2174	115.7557	138.0750
25	161.7305	166.3749	114.0644	189.4269
30	145.1024	142.3006	133.5164	147.7197
35	104.6987	128.3680	101.6306	105.1203
40	89.4002	94.8932	98.0957	121.4639

Table 4. 3Com PC Card ANOVA

Analysis of Variance

Source	DF	SS	Mean Square	F Ratio	Prob > F
Distance	7	204496.5	29213.8	42.6207	<.0001
Orient	3	9568.093	3189.36	4.6530	0.0120
Distance*Orient	21	14394.16	685.436	4.4410	<.0001
Within	64	9877.915	154.342		
Total	95	238336.7	2508.81		

Variance Components

Component	Var Component	% of Total	Plot%	Sqrt(Var Comp)
Distance	2377.3630	84.511		48.758
Orient	104.3303	3.7088		10.214
Distance*Orient	177.0313	6.2932		13.305
Within	154.3424	5.4866		12.423
Total	2813.0671	100		53.038

2. Anycom PC Card

The Anycom PC card is configured as follows:

Table 5. Anycom PC Card Configuration

```
Installation Package
---------------------------------------------
System Release 2.14.221.31

Applications
---------------------------------------------
Bluetooth Wizard          - Version: 2.0.0.15
Bluetooth FileTransfer    - Version: 2.0.0.18
Bluetooth PhoneControl    - Version: 2.0.0.18
SppBridge.exe             - Version: 2.0.0.33
Bluetooth Printing        - Version: 2.0.0.22

Libraries
---------------------------------------------
hci.dll                   - Version: 2.0.0.27
l2cap.dll                 - Version: 2.0.0.7
obex.dll                  - Version: 2.0.0.10
phonecontrol.dll          - Version: 2.0.0.2
redmonnt.dll              - Version: 1.72.00
rfcomm.dll                - Version: 2.0.0.4
sdp.dll                   - Version: 2.0.0.9
wssbt.cpl                 - Version: 2.0.0.6

Other
---------------------------------------------
Serial Port Emulator (wss_spp.sys) 2.0.0.18
```

Table 6. Anycom PC Card Best Case Throughput Data

Distance (m)	Orientation 360	90	180	270
5	310.8796	312.2726	312.1685	311.7526
6	243.007	X	245.0786	258.2878
7	226.6161	X	230.897	236.9687
8	283.7363	X	222.6044	248.3123
9	285.868	X	244.7045	292.2025
10	298.609	308.6682	278.9408	298.6771
11	X	297.8212	272.6598	X
12	X	282.7078	187.6801	X
13	X	290.7888	265.5105	X
14	X	268.0415	237.3033	X
15	299.3483	281.0703	213.6675	257.0111
18	294.4746	239.6208	X	X
19	242.3778	241.0136	X	X
20	161.1558	195.0714	148.5022	260.1855
21	X	X	X	227.4422
22	X	X	X	211.3651
23	X	X	X	204.0767
24	X	X	X	188.1176
25	202.8758	183.8906	157.4685	167.4626
26	X	X	89.51811	140.4961
27	X	X	135.6525	141.3022
28	151.4826	X	X	152.0628
29	147.3432	X	X	121.2315
30	82.56734	152.3633	34.64043	100.1096
31	X	68.4913	X	X
32	X	62.1363	X	X
33	X	43.3275	X	X
34	X	49.787	X	X
35	53.27135	45.02945	80.86837	82.51223
40	39.58544	Fail	Fail	Fail

Table 7. Anycom PC Card ANOVA

Analysis of Variance

Source	DF	SS	Mean Square	F Ratio	Prob > F
Distance	7	1037623	148232	51.1523	<.0001
Orient	3	17084.15	5694.72	1.9651	0.1501
Distance*Orient	21	60854.95	2897.85	45.8714	<.0001
Within	64	4043.098	63.1734		
Total	95	1119606	11785.3		

Variance Components

Component	Var Component	% of Total	Plot%	Sqrt(Var Comp)
Distance	12111.172	91.5		110.05
Orient	116.536	0.8805		10.80
Distance*Orient	944.894	7.1		30.74
Within	63.173	0.4773		7.95
Total	13235.775	100.0		115.05

3. Belkin PC Card

The Belkin PC card operates on Bluetooth software version 1.2.1 and in the following hardware configuration:

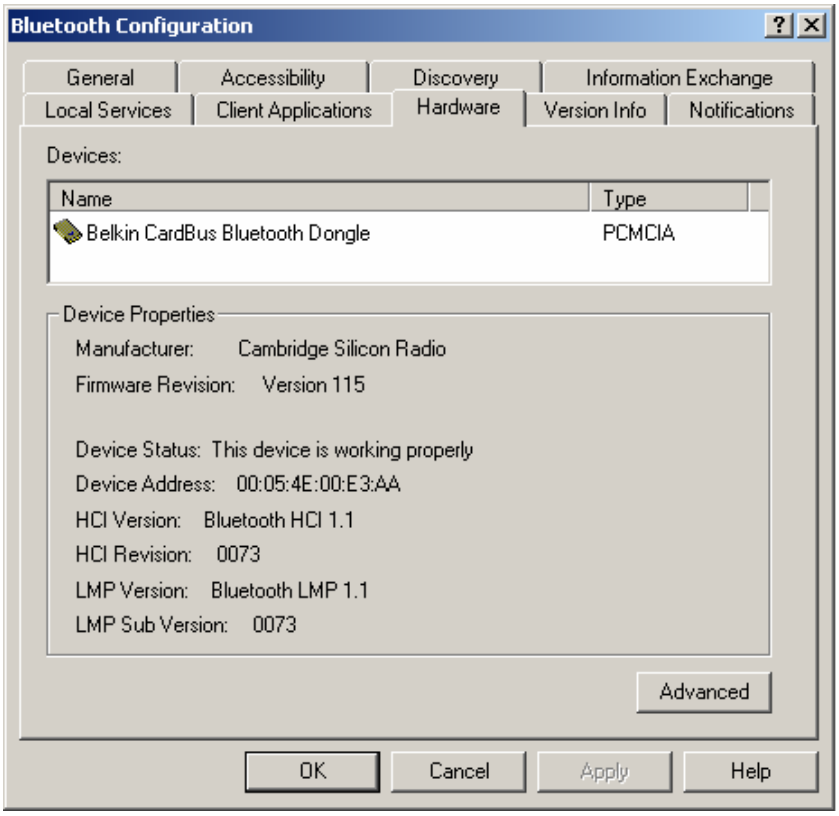

Figure 15. Belkin PC Card hardware configuration

Table 8. Belkin PC Card Best Case Throughput Data

Distance (m)	Orientation			
	360	90	180	270
5	295.1521	310.3502	304.6213	267.5716
10	283.6143	314.0172	314.4766	295.8986
15	290.7248	290.107	220.3812	219.2306
16	X	X	197.3695	210.6383
17	X	X	153.8683	204.3826
18	X	X	107.0329	189.7001
19	X	X	X	188.1151
20	262.6608	233.1074	141.6721	199.9294
21	X	64.4844	X	X
22	X	100.0395	X	X
23	X	122.6503	X	X
24	X	95.4178	X	X
25	218.9668	199.3818	150.3807	213.6679
26	123.3546	X	X	121.5646
27	93.71719	X	X	121.3193
28	121.9789	X	X	X
29	111.8363	X	X	X
30	181.4162	124.5304	107.3609	156.5348
35	72.176	86.2525	69.2656	58.939
40	65.7258	84.0386	43.6911	70.8047

Table 9. Belkin PC Card ANOVA

Analysis of Variance

Source	DF	SS	Mean Square	F Ratio	Prob > F
Distance	7	719774.9	102825	47.8435	<.0001
Orient	3	23652.7	7884.23	3.6685	0.0287
Distance*Orient	21	45133.13	2149.2	46.5930	<.0001
Within	64	2952.128	46.127		
Total	95	791512.9	8331.71		

Variance Components

Component	Var Component	% of Total	Plot%	Sqrt(Var Comp)
Distance	8389.6492	89.482		91.595
Orient	238.9599	2.5487		15.458
Distance*Orient	701.0232	7.477		26.477
Within	46.1270	0.492		6.792
Total	9375.7592	100		96.829

4. 3Com USB

The 3Com PC card is operating on version 1.2.0.0 of its Bluetooth software.

Table 10. 3Com USB Best Case Throughput Data

Distance (m)	Orientation			
	360	90	180	270
5	302.3882	309.2684	310.5731	278.1970
10	334.5866	300.4192	223.5487	273.4480
11	X	X	230.6585	251.3958
12	X	X	226.7077	221.0531
13	X	X	X	211.3359
14	X	X	X	223.9413
15	230.1000	258.1378	192.1216	173.8494
16	X	217.2722	X	X
17	X	209.5633	X	X
18	X	226.4022	X	X
19	X	207.4284	X	X
20	246.0953	238.9243	174.3963	175.8757
25	195.4834	198.7569	223.8112	254.7388
30	152.5373	186.9703	181.8987	173.0351
35	178.2483	169.5994	168.7867	138.1850
40	144.0456	141.5424	160.3589	130.9853

Table 11. 3Com USB ANOVA

Analysis of Variance

Source	DF	SS	Mean Square	F Ratio	Prob > F
Distance	7	218214.8	31173.5	17.3425	<.0001
Orient	3	5831.998	1944	1.0815	0.3785
Distance*Orient	21	37747.97	1797.52	4.3807	<.0001
Within	64	26260.71	410.324		
Total	95	288055.5	3032.16		

Variance Components

Component	Var Component	% of Total	Plot%	Sqrt(Var Comp)
Distance	2448.0019	73.6		49.477
Orient	6.1032	0.1835		2.470
Distance*Orient	462.3996	13.9		21.503
Within	410.3236	12.3		20.256
Total	3326.8283	100.0		57.679

5. Belkin USB

The Belkin USB dongle operates on Bluetooth software version 1.3.2.7 and in the following hardware configuration:

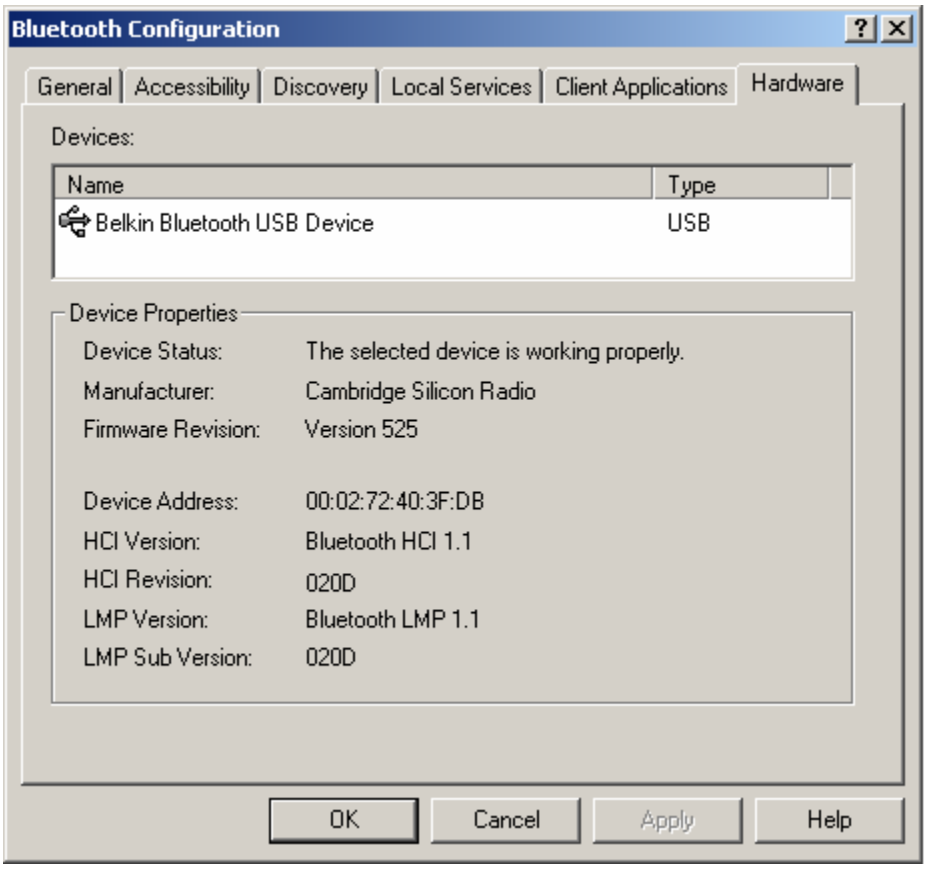

Figure 16. Belkin USB hardware configuration

Table 12. Belkin USB Best Case Throughput Data

Distance (m)	Orientation			
	360	90	180	270
5	299.4144	284.1751	337.0626	318.126
6	160.7332	301.1576	292.4248	X
7	259.321	284.2957	353.5038	X
8	154.8998	253.4432	378.1153	X
9	128.4706	332.7004	313.6787	X
10	164.645	362.6563	536.5242	277.0843
11	243.8308	313.6036	335.2519	X
12	121.2005	259.1673	271.9598	X
13	87.8603	238.8874	234.9804	X
14	90.4601	205.1956	113.5302	X
15	55.03324	135.325	147.0657	307.0196
16	X	118.8457	122.6434	227.9333
17	X	126.0265	59.5839	259.1159
18	X	76.1473	65.8017	196.2228
19	X	81.3496	81.4264	269.2253
20	33.79304	53.02871	32.41432	43.97504
25	18.61885	25.03195	47.46183	173.7474
30	Fail	Fail	Fail	Fail

Table 13. Belkin USB ANOVA

Analysis of Variance

Source	DF	SS	Mean Square	F Ratio	Prob > F
Distance	4	752701.8	188175	10.0411	0.0008
Orient	3	97821.12	32607	1.7399	0.2120
Distance*Orient	12	224885.2	18740.4	23.6858	<.0001
Within	40	31648.33	791.208		
Total	59	1107056	18763.7		

Variance Components

Component	Var Component	% of Total	Plot%	Sqrt(Var Comp)
Distance	14119.584	64.7		118.83
Orient	924.440	4.2		30.40
Distance*Orient	5983.076	27.4		77.35
Within	791.208	3.6		28.13
Total	21818.309	100.0		147.71

6. DLink USB

The DLink USB dongle operates on Bluetooth software version 1.2.2.15 and in the following hardware configuration:

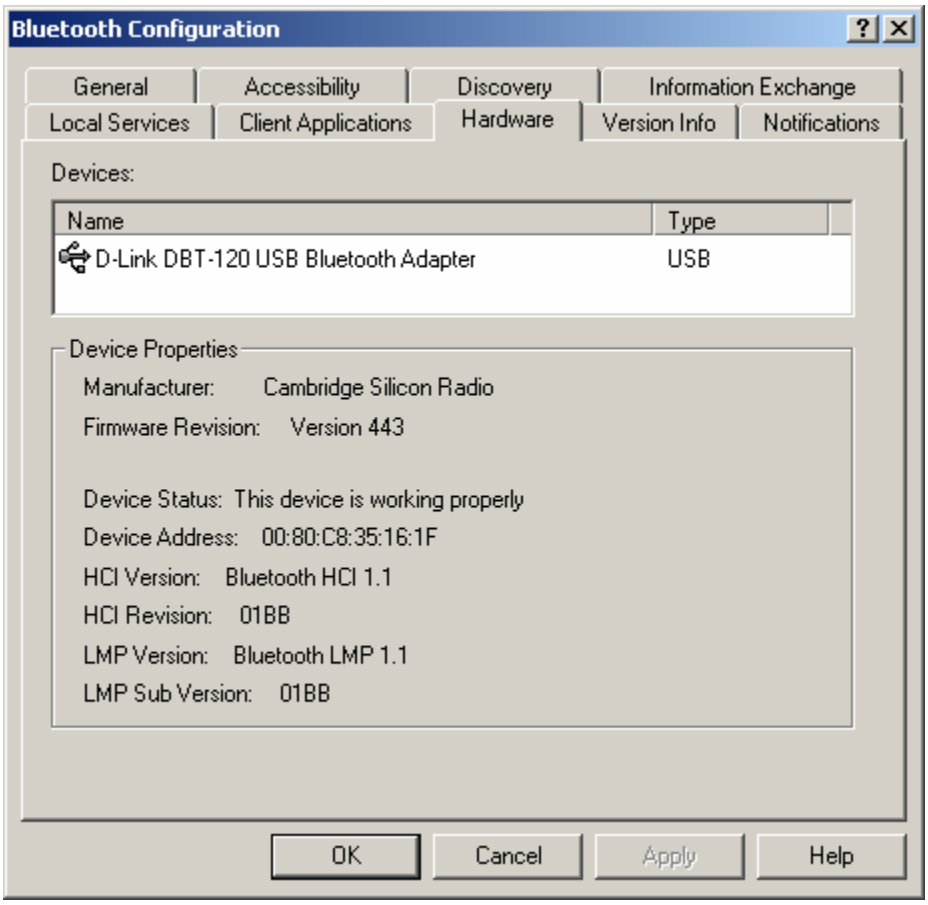

Figure 17. DLink USB hardware configuration

Table 14. DLink USB Best Case Throughput Data

Distance (m)	Orientation			
	360	90	180	270
5	43.39152	75.79362	68.14643	66.90015
10	60.87489	59.94364	47.82668	50.80767
15	27.23608	Fail	Fail	Fail
16	58.01765	X	X	X
17	37.2099	X	X	X
18	51.82118	X	X	X

Table 15. DLink USB ANOVA

Analysis of Variance

Source	DF	SS	Mean Square	F Ratio	Prob > F
Distance	2	16215.24	8107.62	15.5905	0.0042
Orient	3	173.5196	57.8399	0.1112	0.9504
Distance*Orient	6	3120.212	520.035	7.3007	0.0002
Within	24	1709.549	71.2312		
Total	35	21218.52	606.243		

Variance Components

Component	Var Component	% of Total	Plot%	Sqrt(Var Comp)
Distance	632.29867	74.115		25.146
Orient	0.00000	0		0.000
Distance*Orient	149.60135	17.536		12.231
Within	71.23123	8.3494		8.440
Total	853.13125	100		29.208

7. Hawking USB

The Hawking USB dongle operates on Bluetooth software version 1.2.2.18 and in the following hardware configuration:

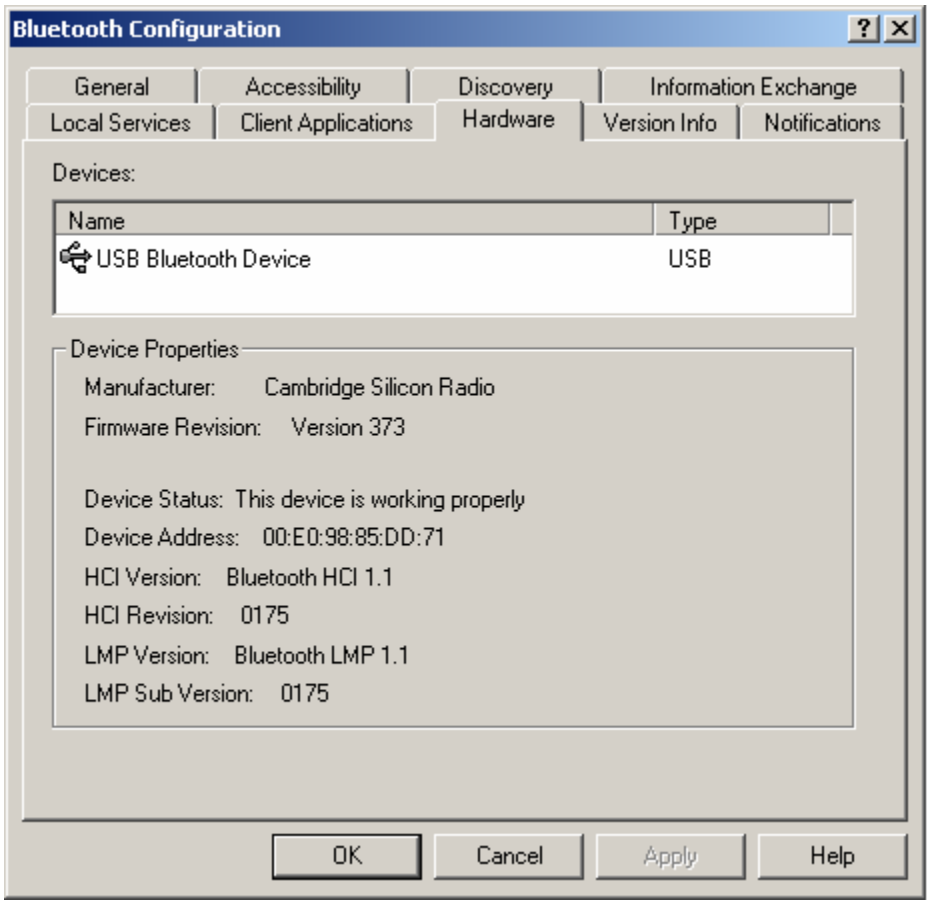

Figure 18. Hawking USB hardware configuration

Table 16. Hawking USB Best Case Throughput Data

Distance (m)	Orientation 360	90	180	270
5	503.4966	352.8667	482.6861	406.5817
10	491.7153	424.4977	500.9557	375.2075
11	328.8407	X	338.7356	X
12	325.9772	X	375.078	X
13	291.3198	X	343.1358	X
14	325.3945	X	344.3442	X
15	273.2397	320.9302	346.4961	313.9334
16	X	310.9543	332.935	X
17	X	333.4773	333.6981	X
18	X	334.6014	309.2662	X
19	X	326.3672	321.4038	X
20	270.644	297.2947	293.7065	316.054
21	X	X	X	293.368
22	X	X	X	327.362
23	X	227.1767	X	299.8671
24	X	329.9836	X	302.6235
25	236.115	205.3973	179.2193	266.7687
28	250.6789	X	258.2174	X
29	207.0178	X	224.6431	X
30	97.4692	225.7809	92.8612	263.6094
35	182.2338	177.4846	257.244	229.9656
36	X	X	117.6295	224.021
37	X	X	233.0498	258.5334
38	X	X	291.1436	201.4852
39	X	X	234.9721	277.8647
40	214.2752	244.6589	157.798	207.0786

Table 17. Hawking USB ANOVA

Analysis of Variance

Source	DF	SS	Mean Square	F Ratio	Prob > F
Distance	7	723496.8	103357	18.6854	<.0001
Orient	3	13143.24	4381.08	0.7920	0.5119
Distance*Orient	21	116159.7	5531.42	5.6505	<.0001
Within	64	62651.7	978.933		
Total	95	915451.5	9636.33		

Variance Components

Component	Var Component	% of Total	Plot%	Sqrt(Var Comp)
Distance	8152.106	76.6		90.29
Orient	0.000	0.0		0.00
Distance*Orient	1517.494	14.3		38.96
Within	978.933	9.2		31.29
Total	10648.534	100.0		103.19

Appendix B – Merlin Configuration

The following are screenshots of the recording options in Merlin:

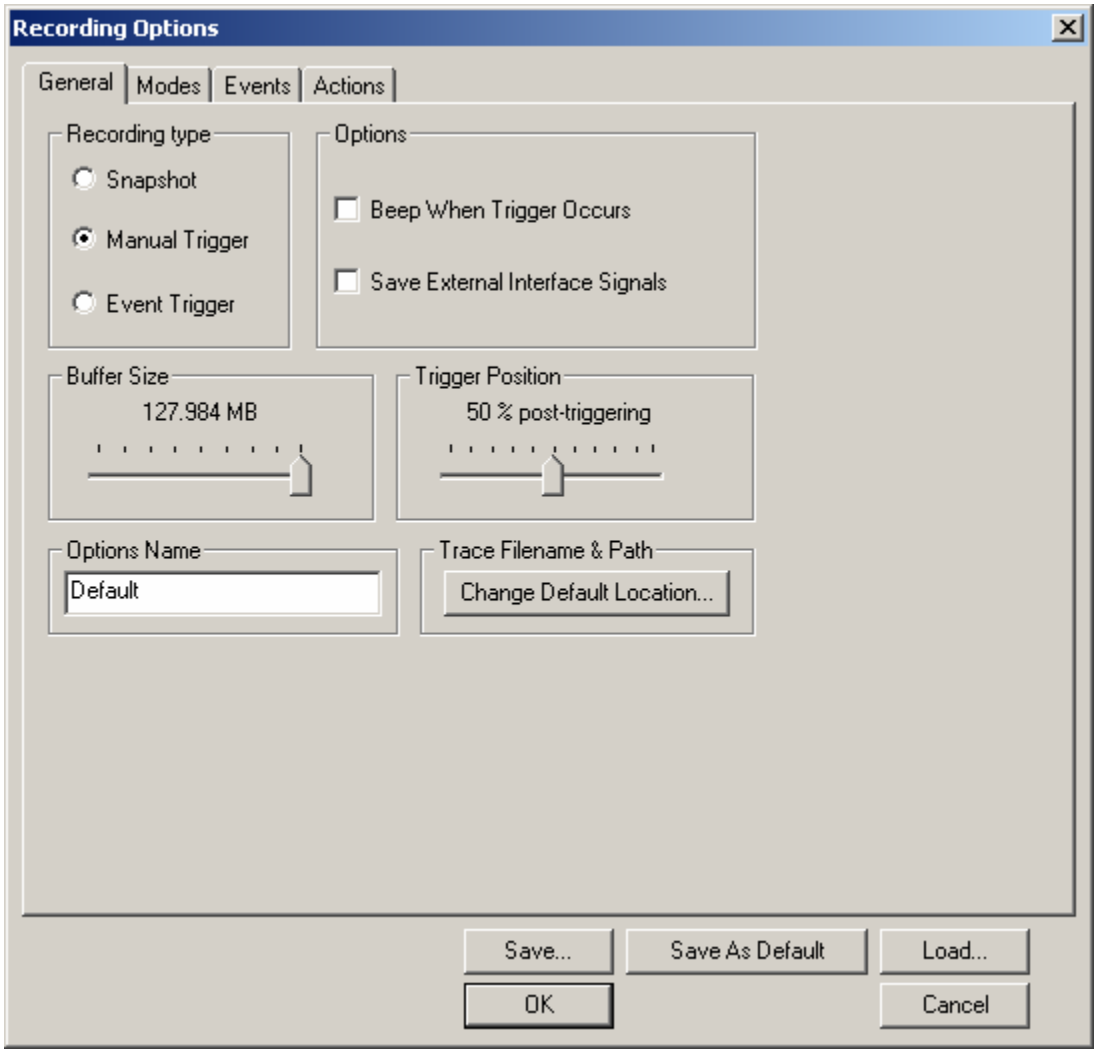

Figure 19. Merlin General Recording Options

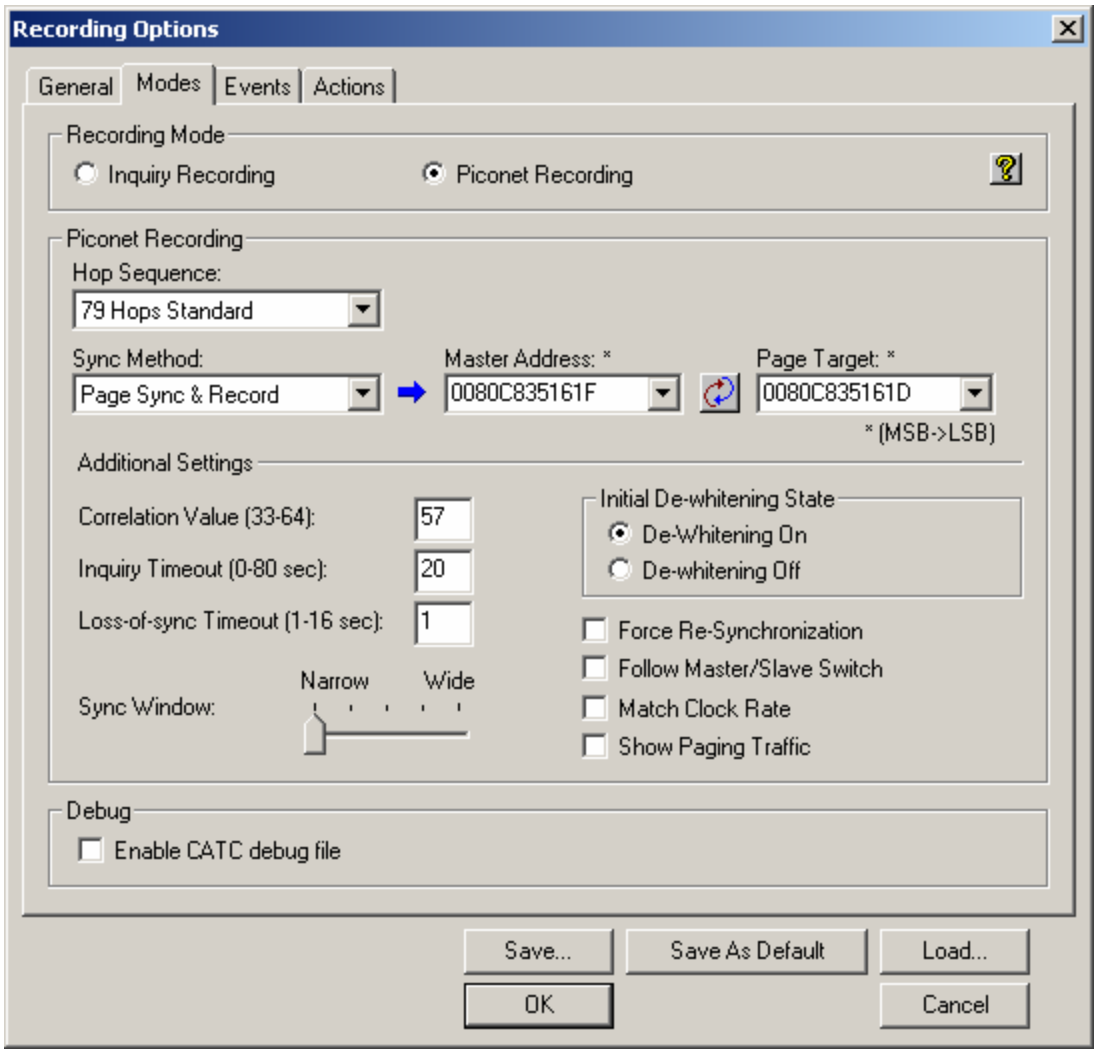

Figure 20. Merlin Modes Recording Options

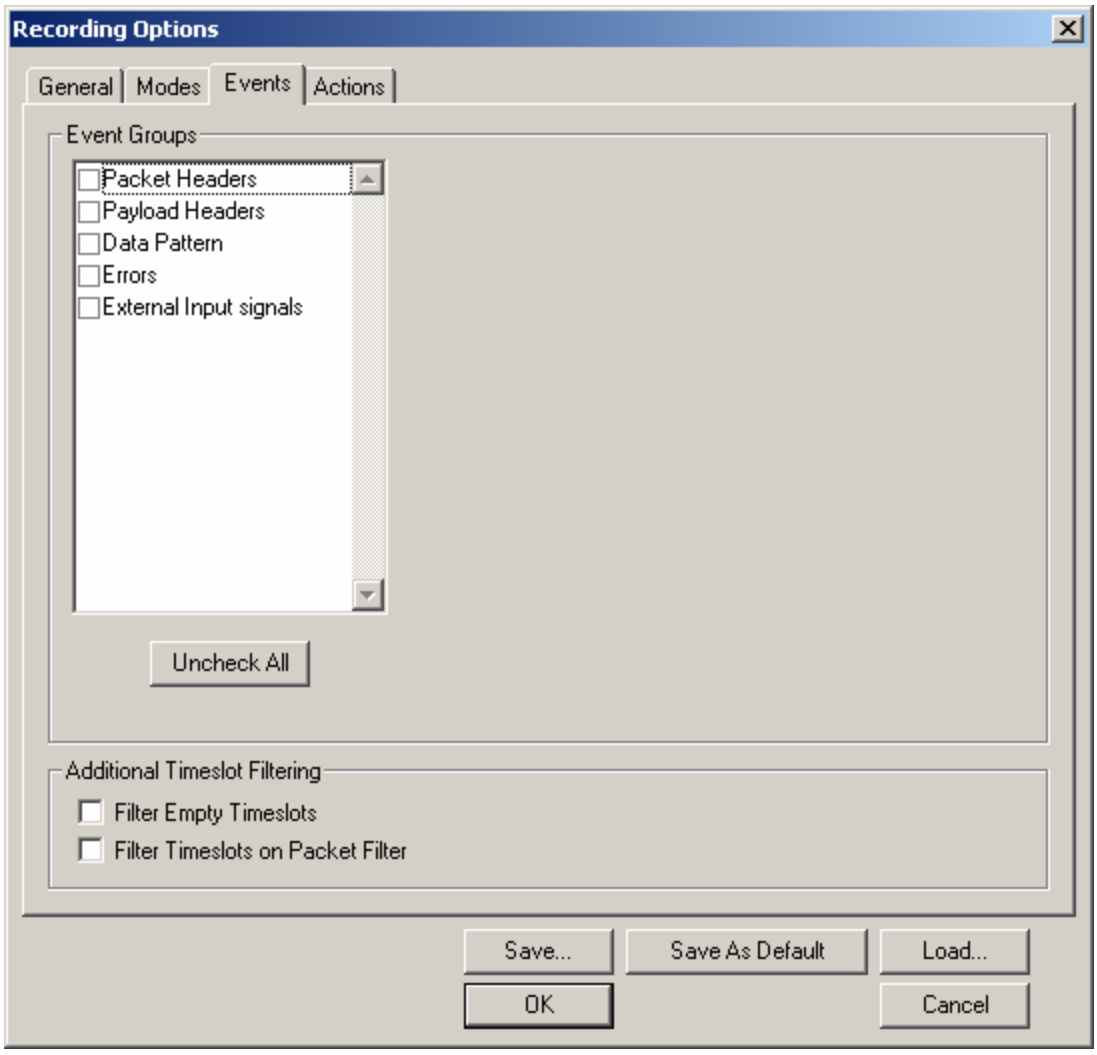

Figure 21. Merlin Events Recording Options

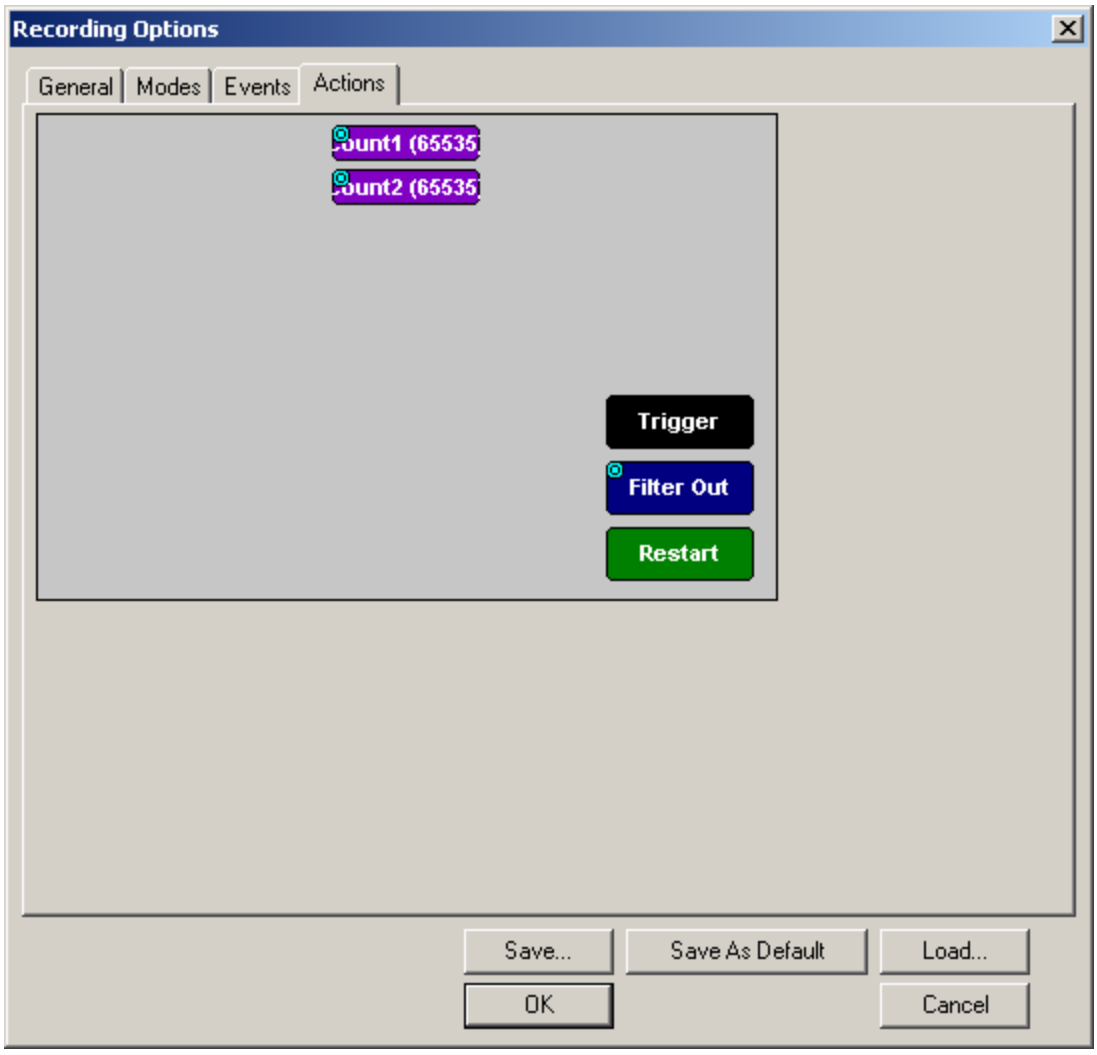

Figure 22. Merlin Actions Recording Options

Bibliography

[1] Banos, J., *Testing of Bluetooth Products in the Industrial Environment*, 28th Annual Conference of the Industrial Electronics Society, 2002.

[2] Betkas, F., et al, *Bluetooth Communication Employing Antenna Diversity*, 8th International Symposium on Computers and Communication, 2003.

[3] Bisdikian, C., *An Overview of the Bluetooth Wireless Technology*, IEEE Communications Magazine, Dec 2001.

[4] Bluetooth SIG, Specification of the Bluetooth System Version 1.1, http://www.bluetooth.org, 2001.

[5] Computer Access Technology Corporation, CATC Merlin, http://www.catc.com/products/merlin.html.

[6] Hager, Creighton and S. Midkiff, *An Analysis of Bluetooth Security Vulnerabilities*, Wireless Communications and Networking Conference, 2003.

[7] Jain, R., The Art of Computer Systems Performance Analysis, John Wiley & Sons, Inc., New York, 1991.

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

[9] Ju, M.C., et al, *Packet Selection Scheme Based on a Channel Quality Estimation for Bluetooth Systems*, 5th International Symposium on Wireless Personal Multimedia Communications, 2002.

[10] Kirk, M., *802.11*, SearchNetworking.com Definitions, http://searchnetworking.techtarget.com/sDefinition/, 2003.

[11] Kneeland, T. *Performance Evaluation of Effective Range and Data Throughput for Unmodified Bluetooth Communication Devices*, AFIT Thesis, 2003.

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

[13] Pedersen, Gert F., and P. Eggers, *Initial Investigations of the Bluetooth Link*, 52nd Vehicular Technology Conference, 2000.

[14] Sheldon, T., Encyclopedia of Networking & Telecommunications, McGraw Hill, New York, 2001.

[15] Singer, A., *802.15 aims to secure wireless PANs*, Network World Fusion, http://www.nwfusion.com/news/tech/2002/0311tech.html, 2002.

[16] Symbol Technologies, *Bluetooth: The Leading Edge in Wireless Personal Area Networking*, Technology Brief, April 2001.

[17] Valenti, M., et al, *On the Throughput of Bluetooth Data Transmissions*, Wireless Communications and Networking Conference, 2002.

[18] Yang, H.Y.D., *Printed Straight F Antennas for wLAN and Bluetooth*, Antennas and Propagation Society International Symposium, 2003.

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	March 2003 – March 2004

4. TITLE AND SUBTITLE

THROUGHPUT PERFORMANCE EVALUATION AND ANALYSIS OF UNMODIFIED BLUETOOTH DEVICES

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Taylor, Steven J., Second 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/04-20

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

Air Force Information Warfare Center
Attn: William Mueller, GG-13, Senior Engineer
404 Greig St, Bldg 178 DSN 925-1877
San Antonio, TX 78226-1844 e-mail: William.Mueller@lackland.af.mil

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

The Air Force relies on the application of new technologies to support and execute its mission. As new technologies develop, the integration of that technology is studied to determine the costs and benefits it may provide to the war fighter. One such emergent technology is the Bluetooth wireless protocol, used to connect a small number of devices over a short distance. The short distance is a feature that makes using the protocol desirable. However short, there is still a vulnerability to interception.

This research identifies ranges at which several commercially available Bluetooth devices are usable. Various combinations of both distance and orientation are varied to determine a 360 degree map of the Bluetooth antenna. The map identifies distances at which certain throughput thresholds are available. This research shows that baseline 1 mW Bluetooth antennas are capable of throughput levels of 100 kbps at over 40 meters, which is four times the minimum distance specified in the protocol standard.

The 3Com PC card was the best performing PC card, capable of throughputs at or near 100 kbps out to 40 meters. The other PC Cards tested had similar performance. The Hawking USB dongle was the best USB antenna tested, achieving throughputs of over 200 kbps in three of the four orientation, and over 150 kbps at the fourth. The 3Com dongle was a close second, the Belkin dongle a distant third, while the DLink antenna was not able to achieve 100 kbps at any distance tested.

15. SUBJECT TERMS

Computer Networks, Communications Protocols

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
U	U	U	UU	86	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