A STUDY OF PACKET LOSS CAUSED BY INTERFERENCE BETWEEN THE BLUETOOTH COMPONENT OF A TELECARDIOLOGY SYSTEM AND RESIDENTIAL MICROWAVE OVENS

William C. Barge

Indiana State University
Terre Haute, USA

Abstract

Cardiovascular diseases are the leading cause of death in the United States. Advances in wireless technology have introduced telecardiology, the remote monitoring of a patient's electrocardiograph (ECG) sensors via cellular telephony. Some of these telecardiology systems use a Bluetooth component to send the ECG signal between the bio sensors and the cellular phone. Several previous studies have suggested that stray wireless transmissions in the ISM band cause interference resulting in packet loss in Bluetooth piconets. While the Bluetooth devices in a telecardiology system are usually less than half a meter apart, patients using these systems are exposed to wireless signals from various sources, including other Bluetooth devices, Wi-Fi networks, and even microwave ovens. This study investigates the impact that wireless transmissions from residential microwave ovens may have on the Bluetooth component of the telecardiology systems.

I. INTRODUCTION

Cardiovascular diseases are the leading cause of death for both men and women in the United States [1]. Characterized by arrhythmia, most ischemic episodes take place during daily activities. Because survival is dependent on timely access to emergency care, early detection of this type of abnormal heartbeat is very important [2].

The availability of broadband wireless services and handheld technology has provided the opportunity for wearable personal health devices. This new wireless healthcare allows for early disease detection via real-time patient monitoring. Using low-cost sensors and wireless systems, it is now possible for primary care physicians to monitor patients at home, work, and in conventional point-of-care environments [3].

Telecardiology, the ability to monitor a patient's heart rate remotely, is being explored as a tool to save lives and reduce medical related in-hospital monitoring. With a medical sensor relaying electrocardiograph (ECG) data via Bluetooth to a smart phone, it is possible to track a patient anywhere a cellular signal is available [4]. The Bluetooth module is configured as a slave and the smart phone is considered to be functioning as a master. The signal acquisition unit sends data to the Bluetooth module, which transmits data continuously, in blocks of ECG samples plus temperature readings and blood pressure [2, 3].

The users of telecardiology systems are mobile, so maintain connectivity among Bluetooth devices may pose some challenges [5]. Due to the absence of coordination between independent masters while accessing the wireless medium, devices will encounter high packet interference if several piconets are simultaneously operating in the same area. Additional sources of interference are non-communications devices including residential microwave ovens. The power leakage from these devices is limited by concerns about user safety rather than limiting interference. The study of packet loss due to interference is importance because it affects our knowledge of the throughput of a piconet and, consequently, the effectiveness of the telecardiology system [6].

II. BACKGROUND

A. Telecardiology Systems

Cardiac disease is the single leading cause of death in the United States. According to the American Heart Association, approximately 265,000 incidents of out-of-hospital cardiac arrests occur annually [7]. Studies have found that early detection and defibrillation is critical for survival. Treating a patient who is experiencing ventricular fibrillation during the first 12 minutes of cardiac arrest achieves survival rates of up to 75 percent. Survival with treatment after 12 minutes drops to four percent [8].

Cardiovascular disease is usually characterized by arrhythmia, making it important to detect this kind of abnormal heartbeat [2]. In addition, most ischemic episodes leading to a heart attack take place during daily activities rather than in the hospital. The ability to implement real-time remote monitoring of a cardiologic patient's heart during daily activity can reduce the delay in administering emergency care and increase the chances of patient survival [9].

Remote monitoring systems can consist of two components: a data analysis system and a client program connecting the mobile device to a remote database [3]. Communication can be Bluetooth, Wi-Fi, or 3G networks. Telecardiology is being explored as a tool to save lives and reduce medical costs related to in-hospital monitoring. Although these remote monitoring systems can take many forms, they all are functionally divided into four subsystems: electrocardiograph (ECG) sensors, data sampling, wireless transmission, and host interface [10].

The ECG sensors are worn on the body and transmit the continuous electrical signals from the heart. These signals must be periodically sampled in order to be digitized. The sampling frequency and digitization method play a critical role in determining the characteristics of the digital signal [8, 11]. Fig. 1 demonstrates the conversion process. Part (a) represents the analog heart beat which is sampled at discrete intervals as represented by (b). The sampling interval is obtained from standard databases or developed by the sensor manufacturer and is beyond the scope of this study. The digital signal is then packetized into a frame to be transmitted wirelessly to the host. To provide portability to the patient, this wireless transmission is often accomplished via a cellular connection between the patient and the medical provider. Because it is unrealistic to establish a full-time cellular connection, an additional component is often included to buffer the data.

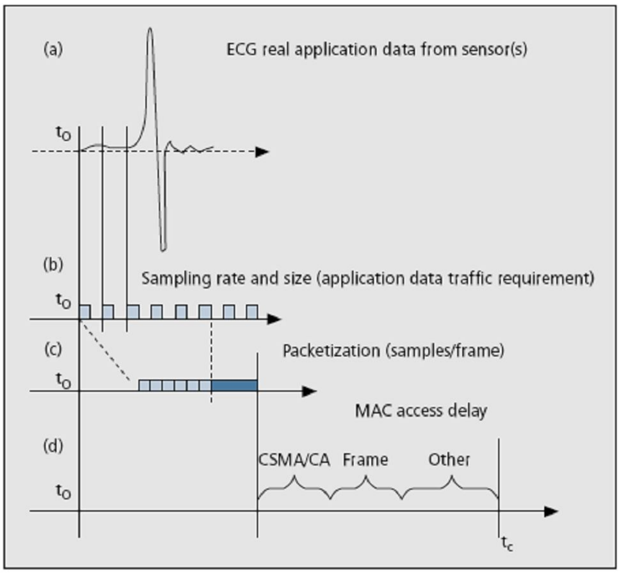


Fig. 1: From heart beats to digital bits [11]

The IEEE 1073 Medical Device Communications standards organization is responsible for developing specifications for wireless interface communication. The main objective is to develop universal and interoperable medical equipment interfaces that are easy to use and quickly reconfigured [11–13]. While radio frequency (RF), Wi-Fi, and Zigbee are mentioned in the literature, Bluetooth offers the additional benefits of an embedded base, reliable data transfer, and device compatibility between different vendors.

As diagramed in Fig. 2, the Bluetooth component sits between the data sampling and wireless transmission subsystems. The ECG sensors include a Bluetooth module that is configured as a slave. The cellular smart phone functions as the master. The ECG sensors' Bluetooth module transmits data continually in blocks of ECG samples. Mobile application software is run on the smart phone. The phone's Bluetooth module stores the transmitted data in the buffer. The mobile application reads data from the buffer and transmits this data to a remote medical facility via the cellular connection. The software can transmit data at set intervals or when the data measurements are beyond a preset value. In addition to ECG samples, body temperature, blood pressure, and GPS coordinates can be sent. The transferred data is sent to a medical provider who can examine and manage the patient's status. If the patient's measurements are out of range, emergency care can be dispatched to the patient's location [2, 12].

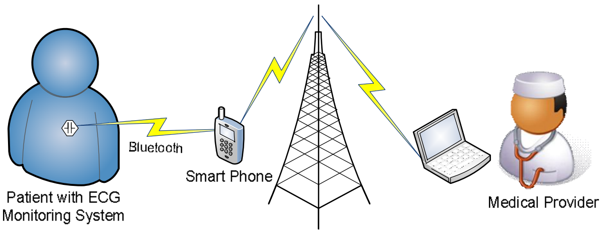


Fig. 2: Telecardiology system using Bluetooth and smart phone technology

With a medical sensor relaying ECG data via a cellular phone, it is possible to track a patient at home or anywhere a cell phone signal is available [4]. However, because the ECG component is more sensitive to time delays than to packet loss, the unacknowledged data service is used [11].

B. Bluetooth Technology

Bluetooth was one of the first IEEE 802.15 protocols. It is a single-hop, point-to-multipoint technology designed for ad-hoc, short-range wireless applications [14]. Bluetooth is a low cost and low power wireless interface for ubiquitous connectivity in the area of Personal Area Networks (PAN) covering distances of 10 meters or less. The technology operates in the unlicensed 2.402 GHz to 2.480 GHz Industrial Scientific Medical (ISM) band and utilizes frequency hopping with terminals cycling through 79 channels at 1600 hops per second [15, 16]. In Bluetooth, each packet is transmitted or received on a different channel. The Bluetooth standard is maintained by the Bluetooth Special Interest Group (SIG) and operates under Title 47 of the Federal Communication Commission's Code of Federal Regulation: Part 15 – Radio Frequency Devices which stipulates that the wireless devices must not give interference and must take any interference received [16].

Over two billion Bluetooth devices are available, with more than nine new Bluetooth enabled products being certified every day [17]. In addition to headsets used with cellular phones, companies are rolling out Bluetooth-enabled medical devices, consumer appliances, and office technology [18]. Bluetooth currently supports low data rates for data transfer, but announced in April 2009, that Bluetooth 3.0 will provide increased throughput with data transfer rates of 24 Mbps and interconnection with IEEE 802.11 Wi-Fi networks [17].

Piconets and Scatternets. Bluetooth is a transmission standard designed to support ad-hoc connectivity in a local area. When Bluetooth devices are within range, they can cluster into ad-hoc networks called piconets and temporarily designate one device to act as the master unit to coordinate transmissions with up to seven slave units. The slaves in a piconet can only have links to the master. Slaves cannot directly transmit data to one another. All packets have to be passed to the master when inter-slave communication is necessary. In effect, the master acts as a switch for the piconet and all traffic must pass through the master. Any device can be either a master or a slave within a piconet, and the device can change roles at any point in a connection when a slave wants to take over a master's role. At any given moment, there can be up to 7 active slaves in a piconet but only one master. [5, 14].

When two or more independent, non-synchronized Bluetooth piconets overlap, a scatternet is formed in a seamless, ad-hoc fashion allowing inter-piconet communication. While the Bluetooth specification stipulates the use of time-division multiplexing (TDM) for enabling concurrent participation by a device in multiple piconets, it leaves the choice of actual mechanisms and algorithms for achieving this functionality open to developers [19].

Bluetooth is based on packet transmission and frequency hopping (FH) technologies to provide channelization among different piconets within the same area. Terminals belonging to the same piconet communicate over the channel identified by a frequency hopping code. According to the Bluetooth standard, terminals are allowed to hop within 79 frequency bands, or channels, in the unlicensed 2.4 GHz ISM band [20].

Based on different FH code patterns, several piconets can coexist in the same area, regardless of whether or not they link to form a scatternet. Within scatternets, packet collisions can occur with significant probability and this kind of interference degrades link performance [20].

The frequency hop spread spectrum (FHSS) system reduces Bluetooth’s ability to produce interference to other ISM band devices by spreading the power throughout the spectrum. In addition, FHSS provides the ability to reduce the effects of interference from other sources. If another device is using a portion of the ISM band and packets are lost, the Bluetooth device will retransmit unacknowledged packets on a different channel than they were originally sent. However, the FHSS is pseudorandom. There is no intelligence in the FHSS to avoid hopping onto certain channels. Even with the pseudorandom FHSS sequence, interference from other devices may still produce significant packet errors and reduce throughput [16].

In a Bluetooth piconet, the master controls the channel. Due to an absence of coordination between the independent masters while accessing a wireless medium, devices may encounter high packet interferences if several piconets are simultaneously operating in the same area. A pair of packets transmitted in two piconets are said to interfere with each other if the packets are transmitted on the same frequency and the two packets overlap. Because of the popularity of Bluetooth devices, it may not be unusual to find tens of independent piconets in a crowded place [6].

Fig. 3 diagrams three different Bluetooth configurations. The first piconet, labeled P_1, has one master, A, and three slaves, B, C, and D. The second piconet, P_2, is a peer-to-peer network with C acting as the master and H as the slave. The third piconet, P_3, has E as the master and D, and F as slaves. Together these three piconets form a scatternet. The two connections in the scatternet are C and D. Node C acts as a slave in P_1 but as the master in P_2. Node D acts a slave in both P_1 and P_3.

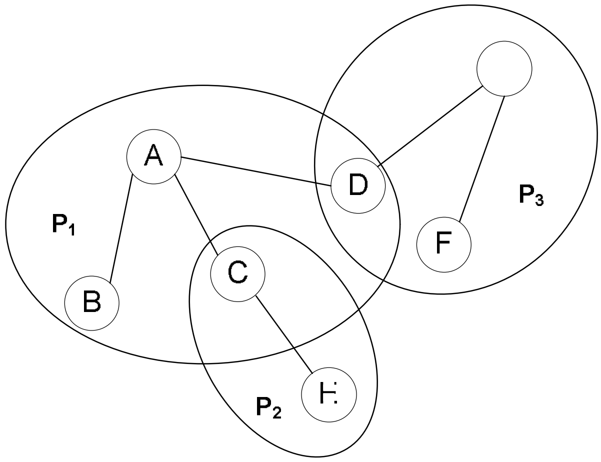


Fig. 3: Example Bluetooth topology [19]

Using the example scatternet in Fig. 3, assume piconet P_2 represents a telecardiology system with the ECG sensors being represented by node H and the smart phone represented by node C. Next assume piconet P_1 represents a network where node A is a Bluetooth-enabled PC and nodes B and D are other Bluetooth-enabled devices. In this example, the smart phone, node C, belongs to two piconets. Node C acts as the master when communicating with node H. There may be a reason to transfer the ECG data to a PC, such as when the patient visits the physician. At these times, the smart phone may act as a slave in the other piconet. However, node C cannot simultaneously act as a master and a slave, rather it must oscillate between these two functions. When polled by node A, it acts as a slave; otherwise it acts as the master for node H. In this way, data from node H may be transferred to node A via node C.

Messages sent through the scatternet "meander" from device to device until they arrive at the destination [21]. When a device is not active in a piconet, the messages may be rerouted to an alternate path, if one is available. Sometimes wireless devices drop packets that should have been forwarded to other devices in order to save their own resources [22].

Bluetooth is based on packet transmission and frequency hopping (FH) technologies to provide channelization among different piconets within the same area. Nodes belonging to the same piconet communicate over the channel identified by the frequency hopping code.

Frequency Hopping. The most important aspects of a Bluetooth device for an interference study are its frequency and power output. The Frequency Hopping Spread Spectrum (FHSS) technique employed by Bluetooth implements stop-and-wait Automatic Repeat request (ARQ), Cyclic Redundancy Check (CRC), and Forward Error Correction (FEC) functions to ensure that the wireless links are reliable. As a result, the FHSS is said to alleviate interference caused by other radio technologies in the ISM band [23].

The FHSS employed by Bluetooth uses 79 channels each 1 MHz wide with a hopping rate of 1600 channels per second. Bluetooth communication is also time division duplex (TDD) where between two entities on the same Bluetooth piconets, one device transmits in a period followed by another device's transmission. With more than two members of a piconets, the master controls the transmission sequence by polling each slave sequentially to indicate when it may transmit [16].

Distinguishing and isolating one piconet from another is the frequency hopping sequence. Two types of links are allowed. Synchronous connection-oriented (SCO) links support symmetrical circuit-switched connections and are expected to be used for voice traffic. Asynchronous connectionless (ACL) links are used for bursty data transmissions. The master controls the allocation of the ACL link bandwidth to each slave [24]. The connection speed can be as high as 721 Kbps in one direction and 57.6 Kbps the other way in an asymmetrical configuration or 432.6 Kbps in each direction in a symmetrical configuration [25]. Data traffic in a piconet is said to be symmetric if both the master and slave transmit at the same rate [6].

Bluetooth Communication Structure. The Bluetooth communication structure is based on an ad-hoc network. All Bluetooth units within a piconet share the same channel and hop using the same hop pattern defined by the Bluetooth device address (BD-ADDR) and current value of the system clock (CLK) of the master. Because each piconet contains a master with unique BD-ADDR and a different CLK, the hop pattern varies from one piconet to another [15].

Consider a Bluetooth piconet with a single slave, such as in a telecardiology system. The master of the piconet transmits packets to the slave using frequency hopping. The master can choose from three different packet lengths: 366 (DH1), 1622 (DH3), and 2870 bits (DH5) with payloads of 216, 1464, and 2712 bits, respectively. These packets occupy one, three, or five Bluetooth slots; each slot is of length 625 microseconds (μs).

When a slave receives a packet, it sends a one slot acknowledgement packet of 126 bits. A packet and the acknowledgement packet together consume two, four, or six slots. Every data and acknowledgement packet has 18 bits in the header that are 1/3 FEC protected; that is, each such bit is repeated three times [24].

A slave can transmit only if the master has addressed it in the previous slot. The master transmits in the even-numbered slots and a slave transmits in the odd-numbered slots. Packets must occupy an odd number of slots. Each packet spans one, three, or five slots and is transmitted on a single channel in a single frequency band. After each packet is transmitted, the devices retune their radios to the next frequency in the sequence. The sequence involves all 79 channels [24].

Regardless of the length of the packet, the entire packet is sent on the same channel. A new channel is used only for the next packet. Throughput can be significantly increased by selecting appropriate packet lengths [24].

The FHSS used in Bluetooth has 79 channels, each of which has 1 MHz of bandwidth. The center frequencies of the 79 channels, in MHz, are $f = 2402 + k$; where $k = 0, 1, 2, \ldots, 78$.

The frequency hopping sequence is determined by a hopping kernel. In each round, the hopping kernel first selects a segment of 64 adjacent channels and then hops to 32 of them at random without repetition. Next, a different 32-hop sequence is selected from another segment of 64 adjacent channels, and the process is repeated. In this way, a pseudo-random sequence of frequency hopping slides as the hopping kernel passes through the 79 available channels [23]. Fig. 4 illustrates the sequence selection of 62 adjacent channels. As can be seen in segments 2 and 3, if a channel selection segment starts at a channel number greater than 15, the segment will wrap around to channel 0 and continue the segment.

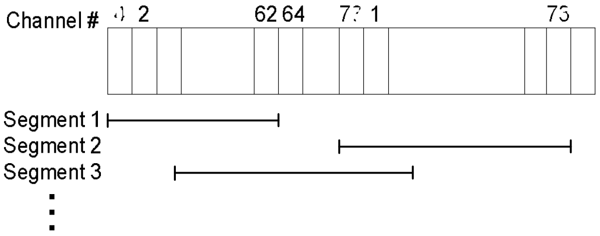


Fig. 4: An example of sequence selection
in Bluetooth frequency hopping [23]

The Adaptive Frequency Hopping (AFH) scheme was implemented in the Bluetooth Spec v1.2. In the AFH scheme, the slave devices measure the quality of the 79 Bluetooth channels in the Channel Classification phase. The slave devices then send their measurement results to the master device so that its AFH hopping kernel can determine the appropriate hopping sequence. More precisely, the AFH scheme classifies the 79 Bluetooth channels into two groups: unused and used. The former should not be used because the unused may have heavy interference, but the latter are suitable for transmission. The AFH scheme then employs a mapping function to uniformly map the unused channels to the used channels. As a result, the scheme can avoid the channels affected by heavy interference, and thereby improve data throughput [23].

In a study of interference in Bluetooth networks, Hung and Chen (2008) proposed that the expected number of used channels can be derived by

$$N_{good} = \sum_{i=1}^{79} P_g^{(i)} ,$$

where $P_g^{(i)}$ is the probability that the i^{th} channel will be marked as used. The IEEE 802.15.2 standard specifies two operating modes: $N_{good} \geq N_{min}$ (i.e., Mode L) and $N_{good} < N_{min}$ (i.e., Mode H). Suppose $\delta(i)$ is a function that indicates whether the i^{th} channel is used or unused. The two operating modes can be described by the step function

$$\delta(i) = \begin{cases} 0 & \textit{if the } i^{th} \textit{ channel is unused} \\ 1 & \textit{if the } i^{th} \textit{ channel is used} \end{cases}$$

Mode L is used when N_{good} is equal to or larger than N_{min}. A mapping function is then employed by AFH to uniformly map unused channels to the used channels. Therefore, the classified N_{good} channels will be the reduced hopping set. The probability that the channels will be in the good state is derived by

$$P_g' = \frac{1}{N_{good}} \sum_{i=1}^{79} P_g^{(i)} \times \delta(i)$$

Mode H is used when N_{good} is less than N_{min}. The hopping sequence is divided into R_g consecutive good slots and R_b consecutive bad slots alternately. Although the values of R_g and R_b are determined by the traffic type required by the application, to preserve the frequency diversity, $R_g + R_b$ must not be less than N_{min}. All used channels are uniformly mapped into the good slots and unused channels are uniformly mapped into the bad slots. Therefore under the AFH mechanism, P'_g can be obtained by

$$P_g' = \frac{R_g}{R_g + R_b} \times \frac{\sum_{i=1}^{79} P_g^{(i)} \delta(i)}{N_{good}} + \frac{R_b}{R_g + R_b} \times \frac{\sum_{i=1}^{79} P_g^{(i)} \left(1 - \delta(i)\right)}{79 - N_{good}}$$

In the Bluetooth system, a slotted channel is used for transmission with each slot spanning 625 µs. User data is transmitted through packets which normally span a single time slot but can be extended to up to five time slots. In single time slot packet transmission, the fraction of time that the system is in an active state, or duty cycle, is 366 µs. The rest of the time (259 µs) is used for transient time-setting. In three and five time slot packet transmissions, the duty cycle is 1.616 µs and 2.866 µs respectively. For full duplex transmission, a Time Division Duplex (TDD) scheme is used. Each single time slot packet is transmitted on a different hop frequency as opposed to a single hop frequency is used for the entire span of a multi time slot packet. The hop frequency in the first time slot after a multi time slot packet uses the frequency determined by the current Bluetooth clock value [15].

In Bluetooth, six symmetric asynchronous data link (ACL) packets are defined. These include three medium data rate packets (DM 1, 3, and 5) and three high data rate packets (DH 1, 3, and 5) [15].

Packet Loss and Collisions. Packet collisions take place when two or more piconets simultaneously transmit over the same frequency slot. The distance between piconets influences the interference effects due to packet collision. Frequency-hopping (FH) patterns of different piconets can be represented through statistically independent time-discrete random processes. A study found that packet loss probability increased proportionally to the number of piconets in the area [20].

Based on different FH code patterns, several piconets can coexist in the same area. In situations where a large number of people gather, the Bluetooth devices can form a large number of piconets with different number of slaves per piconet. In such a dense piconet area, packet collisions can occur with significant probability causing degrading link performance and reducing the overall throughput [5, 26].

Inherent to the wireless technology characteristics, a device can appear anytime, anywhere. These unpredictable appearances present a challenge when compared to a preplanned wireless network configuration. One growing area of study is determining how well Bluetooth devices are able to operate in close proximity to each other. Bluetooth uses a frequency-hopping technique, and a Bluetooth device's FH spans the entire frequency band. Overlapping between Bluetooth channels on different wireless networks is inevitable [11].

Several studies have investigated different aspects of Bluetooth packet loss. One study looked at packet loss at the MAC sublayer and monitored performance [11]. The study suggested that as distance between Bluetooth piconets decreased, the packet loss increased. At a very close range of 0.5 meter, packet loss was up to 60 percent. As the distance between piconets was increased to 2 meters, packet loss decreased to 18 percent. The unexpected appearances of wireless devices can severely impact the existing surrounding wireless environment [11].

Handover may also cause degradation in an application's performance by introducing delay or packet loss. These degradations may have different impacts according to the requirements of the application. Some of them are managed by the corresponding MAC sublayer via retransmission. For real-time applications, or very sensitive data transfers, delay or packet loss may have dramatic consequences [11].

Another study looked at the distance between piconets members and the distance to an external source of interference, which in this study was a microwave oven. The closer the Bluetooth piconet member was to the oven, the greater the effect of the interference. However, in this study, the Bluetooth devices maintained connection and usable throughput even in extreme situations [16].

The fundamental issue with Bluetooth piconets operating within the same environment is that they are not time synchronized to each other, causing collisions to occur in both time and frequency. As a result, unwanted data signals can interfere with the data transmissions on a wanted piconet. Consequently, the requirement to retransmit packets will increase, reducing the overall data throughput. The frequency of collisions was found to depend on the proximity of piconets within the environment [15].

This third study calculated the number of frequency collisions that occurred in the downlink direction between a single wanted piconet and up to four unwanted piconet/interferers when they are transmitting. Downlink transmissions, from the master to the slave, occupy even numbered time slots whereas uplink transmissions occupy odd numbered time slots [15].

The study found degradation is more significant for multi-slot packet transmission in Bluetooth. The author expected this result because the entire packet spanning 3 or 5 time slots will be retransmitted if it is corrupted. As a result, the data throughput of the system is reduced, especially when a large number of interferers are present [15].

The effects of frequency collisions depend largely on the proximity of piconets within the environment. The location of piconets within the environment is a crucial factor since interferers lying in line-of-sight to the wanted piconets will have greater impact than those lying in non-line-of-sight positions [15].

A fourth study concluded that the delay-throughput characteristic of a Bluetooth-based PAN is exponential regardless of types and size of files within its transmission range. The delay also increases with increase in file sizes for a non line-of-sight propagation. This exponential characteristic is also evident in the communication using different types of Bluetooth devices [27].

A fifth study confirmed that within a piconet, different slaves may experience different bit success rates, even though the same frequency is used for all slaves. Interference can be location-dependent where errors in wireless networks are caused because one slave may be near an external wireless device while the master and other slaves may be away from the source of interference [24].

Packet Loss Probability. The FH patterns assigned to the different piconets can be modeled as statistically independent time-discrete random sequences assuming values in the set $\{f_0, f_1, \ldots, f_{N_f-1}\}$. The N_f frequencies f_i are the carrier frequencies used for hopping. Assuming each Bluetooth unit transmits with the same power level W_T (i.e., absence of power control) and that each interference power, I_M, due to M active piconets is

$$I_M = \sum_{m=1}^{M} \chi_m Y_m \ ,$$

where χ_m, $m = 1, \ldots, M$, are independent, identically distributed binary random variables accounting for the occurrence of the frequency-collision events, and Y_m is the power received due to a transmitter belonging to the m^th^ piconet [26].

Mazzenga (2004) continues by developing a function to estimate the packet loss probability due to M, the number of active piconets in the area. The packet loss probability can be expressed as

$$P_{LP}(M) = \sum_{m=1}^{M} \binom{M}{m} q^{M-m} p^m \beta_m$$

where p is given by

$$p = \begin{cases} \dfrac{1}{N_f} & \textit{synchronized piconets} \\ 1 - (1 - N_f)^2 & \textit{unsyncronized piconets} \end{cases}$$

and $q = 1 - p$. The N_f frequencies f_i are the carrier frequencies used for hopping. The coefficients β_m are

$$\beta_m = \int_{-\infty}^{0} g_m(x) \otimes f_c(x) dx \,,$$

where $g_m(x) = \rho_o^{-m} f_{Y_1}(-x/\rho_0) \otimes \cdots \otimes f_{Y_m}(-x/\rho_0)$ for $m = 1, 2, \ldots, M$ and $g_0(x) = \delta(x)$.

The author does make a few assumptions, primarily that $f_Y(x)$ and $f_c(x)$ and are known. Note that $\otimes$ denotes convolution, $f_Y(x)$ is the probability density function of Y and $f_c(x)$ is the probability density function of C, the received power.

As validation for the packet loss probability function, the authors performed a Monte Carlo simulation with M masters uniformly located in a a circular area 20 meters in diameter. Each master formed a piconet with N_s active slaves where N_s was a random number, uniformly distributed between 1 to 7. Both C and Y were assumed to be discrete probability density functions. The study concluded that the packet loss probability changes with changes in the receiver's position.

Bluetooth Quality of Service. Quality of service is an important issue when dealing with any communications link. The Bluetooth specification provides Quality of Service (QoS) configuration according to the requirements of higher layer applications or protocols. The properties that can be configured depend on the application QoS requirements, data rate, buffer storage, peak bandwidth, delay requirements and delay variations. For example, an application transferring compressed video streams may want a link that is not "bursty", and may be able to miss a few packets as long as the delay on the link is not too high [27].

C. Microwave Ovens and Bluetooth

In the United States, approximately 85% of households have a residential microwave oven [28]. These microwave ovens operate in the ISM band. The relatively large power leakage from microwave ovens is a potential source of interference to unlicensed Federal Communications Commission (FCC) Part 15 communication devices. Because of the disproportionately large power output of microwave ovens compared to the low powered Bluetooth devices, studies have suggested that microwave oven interference can greatly reduce the data throughput of Bluetooth networks, which can severely impair operation and usability [16].

The magnetron tubes used to generate microwave energy in a microwave oven generate a continuous wave centered at 2.45 GHz which is in the middle of the ISM band. At full-power operation, a microwave oven usually has an output spectrum about 2 MHz wide, but during the start-up and shutdown cycles, the spectrum can be as wide as 20 MHz. Residential microwave ovens generate power output from 400 to 800 watts.

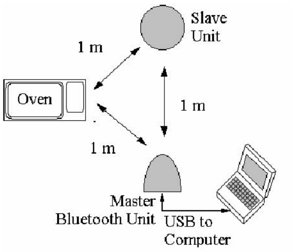
In the 2004 study, Rondeau analyzed the interference effects of microwave ovens on Bluetooth networks. A Bluetooth protocol analyzer was used to capture all of the data packets during a transmission. Each of the five tests used a USB Bluetooth module connected to a notebook computer. This USB module acted as the master in the piconet. The distance between the Bluetooth slave device and the master was varied, as was the distance between the oven and the master and slave device.

Each test consisted of a 30 second transmission where a total of 24,000 packets were transmitted by both the master and the slave. All tests followed the same procedure. To start each test, the oven was warmed up for 30 seconds, and then the computer controlled spectrum analyzer captured the oven spectrum for 30 seconds. After the spectrum capture was completed, the Bluetooth devices were connected and the protocol analyzer began to capture all traffic for 30 seconds.

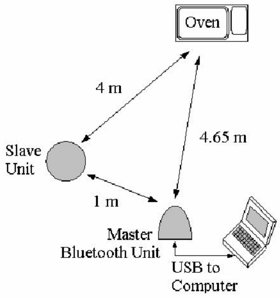
Three different environments were used for the tests. The first environment was a modular building identified in Figure 5 was Bluetooth Lab. The second environment was an office setting. The third environment was outdoors using a line-of-sight path.

Fig. 5 illustrates the five experimental setups used by Rondeau. Note that setup (e) actually identifies two scenarios. First the piconet members were 30 meters apart. Then the experiment was repeated with the piconet members 72 meters apart.

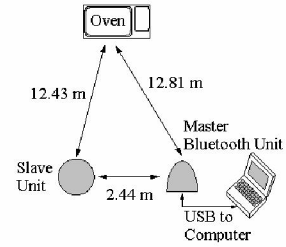
In setup (a), all packets transmitted at the 2.440 GHz frequency were lost due to the extremely high interference. Packets were also lost in adjacent channels on frequencies 2.439 and 2.441 GHz. As the oven was moved further from the piconet, fewer packets were lost. Table 1 lists the packet transmission rates and percentage of the maximum transmission data rates for each of the five experimental scenerios. As can be seen in the data, the distance between the piconet members and the distance to the microwave oven determines the extent to which the microwave oven affects the Bluetooth network. The closer the oven was to the piconet, the greater the effect of the interference.



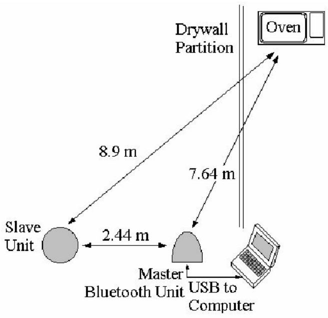
(a) Piconet 1 m from oven (Bluetooth Lab)



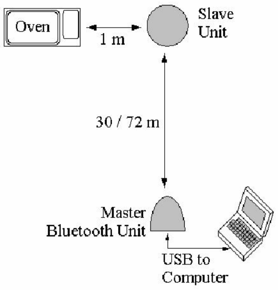
(b) Piconet 5 m from oven (Bluetooth Lab)



(c) Piconet 12.5 m from oven (Bluetooth Lab)



(d) Piconet 8 m from oven through drywall (office)



(e) Outdoor test setup

Fig. 5: Experimental Test Setups [16]

Table 1

Bluetooth Data Rates in Interference Environments [16]

Experimental Scenarios	DM1 packet transmission (kbps)	Percent of Max	DH1 packet transmission (kbps)	Percent of Max
Maximum Data Rate	108.8	100.0	172.8	100.0
a. Piconet 1 m from oven – Without oven on	108.4	99.6	166.3	96.2
a. Piconet 1 m from oven – With oven on	75.3	69.2	99.9	57.8
b. Piconet 5 m from oven	85.2	78.3	149.6	86.6
c. Piconet 12.5 m from oven	105.4	96.9	163.7	94.7
d. Piconet 8 m from oven through drywall	103.9	95.5	160.7	93.0
e. Outside – 30 m master/slave separation	25.1	23.1	68.4	39.6
e. Outside – 72 m master/slave separation	38.5	35.4	38.4	22.2

Several other studies investigate the interference of microwave ovens on Bluetooth networks. The first study compared the effects of interference from IEEE 802.11 b and the interference from microwave ovens on a Bluetooth piconet [29]. This study varied the distance between the Bluetooth links from 0.5 meters to 5 meters and the distance from the interference source from 0.1 meters to 10 meters. Just as in Rondeau's study, Matheus and Magnusson found microwave oven interference to be very frequency dependent. Although the study found no significant difference in interference between IEEE 802.11b and microwave oven interference, the results of the study do suggest that the affects of the interference are dependent on the distance between the interference source and the piconet.

In yet another study, the interference of another Bluetooth piconet was compared to the interference caused by an IEEE 802.11b network [30]. The results of the study were similar to the previously mentioned studies; however, this study found the probability of a Bluetooth packet collision is the joint probability of packet overlap in both time and frequency. The study also showed that the Bluetooth performance packet loss was dependent on signal power, path conditions, available channels, packet size, master-slave distance, and piconet density.

A final study on Bluetooth channel error rates in the presence of microwave ovens found that the interference created by microwave ovens can be treated as non-coherent noise [31]. In the study, the line-of-sight distance between the microwave oven and the piconet was varied between 1.5 and 10 meters as the oven heated a cup of water. The data collected in each 2 minute trial of this study found that channels 60 through 70 were most subjected to high interference from the microwave oven. The study also found the probability of retransmission by a Bluetooth receiver is given by

$$P_r(\gamma) = 1 - P(\overline{A})P(\overline{B})P(\overline{C})P(\overline{D})P(\overline{E}),$$

where A, B, C, D, and E are the events:

A: the 72-bit synchronization of the forward channel fails;

B: the header frame error rate (FEC) of the forward channel fails;

C: the Hamming code protecting the payload of the forward transmission fails;

D: the 72-bit synchronization of the reverse packet fails;

E: the header FEC of the reverse packet fails.

III. DISCUSSION

The IEEE 1073 Medical Device Communications standards organization is developing specifications for wireless interface communication. The group is focusing on using available and emerging technologies to transmit the medical data. All of these technologies operate in the unlicensed 2.4 GHz Industrial Scientific Medical (ISM) band which is also occupied by non-communications devices including residential microwave ovens.

While Bluetooth is said to be resilient to interference with moderate bandwidth, maintaining connectivity among Bluetooth devices in a telecardiology system piconet may pose some challenges. Stray wireless signals can interfere with the wanted data transmission causing frequency collisions. The proximity of the piconets within the environment has a direct effect on frequency collisions and the resulting packet loss.

Studies of interference from residential microwave ovens on Bluetooth piconets have found that there is an indirect relationship between distance from the microwave oven and packet loss. As the distance between the oven and the piconet decreases, the amount of interference increases, resulting in an increased packet loss and decreased piconet throughput.

With 85 percent of U.S. household having a microwave oven, it is reasonable to assume that a patient wearing a telecardiology system may stand within a meter of an operating microwave oven. It has been shown that the stray interference generated by the microwave oven can decrease throughput of the Bluetooth piconet by up to 60 percent. When a reliable transmission protocol is used, lost packets are detected and resent at the expense of overall data throughput. However, due to the sensitivity to time delays, the ECG component of the telecardiology system uses an unacknowledged data service. In these systems, packet loss may have dramatic consequences.

It has also been shown that not all Bluetooth channels are affected by this stray interference. In a study varying distance between the piconet and microwave oven, it was found that channels 60 through 70 were most affected by the interference from the microwave oven. While Bluetooth's AFH has the ability to identify channels affected by heavy interference, the selection of start channel is a function of the current clock value.

Given that different slaves may experience different bit success rates even on the same frequency and the ECG component is time sensitive, it is not known if this hop scheme is sufficient to avoid lost data in time-sensitive remote monitoring using telecardiology systems.

IV. CONCLUSION AND FUTURE WORK

Telecardiology systems can provide real-time ECG readings to a medical professional. However, these systems are only as effective as the data they provide. It is known that for real-time applications, delay or packet loss may have dramatic consequences. In addition, telecardiology systems may be more sensitive to packet loss due to the fact that they use unacknowledged data service used because the ECG component is more sensitive to time delays than to packet loss.

Previous studies have looked at packet loss in Bluetooth piconets due to interference from residential microwave ovens and have found (1) loss of all packets in the 2.43 to 2.45 GHz frequency range, (2) correlation between distance from the oven and packet loss, and (3) unequal channel interference by power and distance with channels 60 through 70 being most affected.

While this study is specific to the Bluetooth component of a telecardiology system and interference caused by the stray signals transmitted by residential microwave ovens, the results of the study can have a broad impact in the field of digital communication and telemedicine. As was identified in other studies, packet loss in Bluetooth piconets can be caused by other Bluetooth piconets, IEEE 802.11b/g/n networks, and stray signals transmitted by microwave ovens and some forms of lighting. Even though not all of these common causes of interference affect Bluetooth piconets in the same way, the affects may be similar enough that a modified-AFH protocol may be needed to effectively reduce packet loss when the piconet is subject to the various forms for interference. Further studies of the impact of stray wireless signals on the emerging wireless healthcare devices are needed to determine the feasibility of widespread use of these devices.

REFERENCES

[1] *Heart Disease Facts and Statistics*. 2009 [cited 2009 October 15]; Available from: http://www.cdc.gov/heartdisease/statistics.htm.

[2] Belgacem, N. and S. Boumerdassi, *Mobile Personal Electrocardiogram Monitoring System with Patient Location* Proceedings of the 1st ACM International Workshop on Medical-Grade Wireless Networks, 2009: p. 3.

[3] Hu, Y., et al., *Providing a Cushion for Wireless Healthcare Application Development.* Potentials, IEEE 2010. 29(1): p. 5.

[4] Proulx, J., et al., *Development and Evaluation of a Bluetooth EKG Monitoring Sensor.* Computer-Based Medical Systems, 2006. CBMS 2006. 19th IEEE International Symposium on, 2006: p. 5.

[5] Chang, A.C., *Connectivity, Mobility, and Security Supports for Wireless Personal Area Networks and HealthNet*. 2008, University of California: Los Angeles. p. 207.

[6] Naik, K., et al., *Analysis of Packet Interference and Aggregated Throughput in a Cluster of Bluetooth Piconets Under Different Traffic Conditions.* Selected Areas in Communications, IEEE Journal on, 2005. 23(6): p. 14.

[7] *Out-of-Hospital Cardiac Arrest — Statistics*. 2009 [cited 2009 November 10]; Available from: http://www.americanheart.org/downloadable/heart/1236978541670OUT_OF_HOSP.pdf.

[8] Shih, E., et al., *Continuous Medical Monitoring Using Wireless Microsensors.* Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems (ACM), 2004: p. 1.

[9] Gonçalves, B., et al., *ECG Data Provisioning for Telehomecare Monitoring.* Proceedings of the 2008 ACM Symposium on Applied Computing, 2008: p. 6.

[10] Park, C., et al. *An Ultra-Wearable, Wireless, Low Power ECG Monitoring System*. n.d. [cited 2009 October 5]; Available from: http://www.ece.uci.edu/~chou/biocas06-ECG.pdf.

[11] Cypher, D., et al., *Prevailing Over Wires in Healthcare Environments: Benefits and Challenges.* Communications Magazine, IEEE, 2006. 44(4): p. 8.

[12] Yao, J., R. Schmitz, and S. Warren, *A Wearable Point-of-Care System for Home Use that Incorporates Plug-and-Play and Wireless Standards.* Information Technology in Biomedicine, IEEE Transactions on, 2005. 9(3): p. 9.

[13] Kennelly, R.J., *The IEEE 1073 Standard for Medical Device Communications.* AUTOTESTCON '98. IEEE Systems Readiness Technology Conference., 1998 IEEE, 1998: p. 2.

[14] Dideles, M., *Bluetooth: A Technical Overview.* ACM: Crossroads, 2003. 9(4).

[15] Arumugam, A.K., et al., *Scenario Driven Evaluation and Interference Mitigation Proposals for Bluetooth and High Data Rate Bluetooth Enabled Consumer Electronic Devices.* Consumer Electronics, IEEE Transactions on, 2002. 48(3): p. 11.

[16] Rondeau, T.W., M.F. D'Souza, and D.G. Sweeney, *Residential Microwave Oven Interference on Bluetooth Data Performance.* Consumer Electronics, IEEE Transactions on, 2004. 50(3): p. 8.

[17] Bluetooth SIG Inc. *Bluetooth Technology Gets Faster with Bluetooth 3.0*. 2009 [cited 2009 September 12]; Available from: http://www.bluetooth.com/bluetooth/press/sig/ibluetoothi_technology_gets_faster_with_ibluetoothi_30.htm.

[18] Piazza, P., *From Bluetooth to RedFang*, in *Security Management*. 2005. p. 10.

[19] *Scatternet - Part 1: Baseband vs. Host Stack Implementation*. 2004 [cited 2009 October 31]; Available from: http://www.bluetooth.com/NR/rdonlyres/090D96C0-5396-45F7-BDFD-2B7C70AF5E59/0/Scatternet_Part_1_Baseband_vs_Host_Stack_Implementation.pdf.

[20] Mazzenga, F., et al., *Evaluation of Packet Loss Probability in Bluetooth Networks.* Communications, 2002. ICC 2002. IEEE International Conference on, 2002. 1: p. 5.

[21] Wang, S., *EDITORIAL: Wireless Networks and Their Applications in Building Automation Systems.* HVAC&R Research, 2008. 14(4): p. 5.

[22] Li, H., *Design of a Secure, Trustworthy, and Scalable Network Architecture for Wireless Ad Hoc Networks*. 2006, University of Kentucky. p. 117.

[23] Hung, H.-H. and L.-J. Chen, *An Analytical Study of Wireless Error Models for Bluetooth Networks.* Advanced Information Networking and Applications - Workshops, 2008. AINAW 2008. 22nd International Conference on, 2008: p. 6.

[24] Sarkar, S., F. Anjum, and R. Guha, *Optimal Communication in Bluetooth Piconets.* Vehicular Technology, IEEE Transactions on, 2005. 54(2): p. 13.

[25] Dhawan, S., *Analogy of Promising Wireless Technologies on Different Frequencies: Bluetooth, WiFi, and WiMAX.* Wireless Broadband and Ultra Wideband Communications, 2007. AusWireless 2007. The 2nd International Conference on, 2007: p. 9.

[26] Mazzenga, F., et al., *Performance Evaluation in Bluetooth Dense Piconet Areas.* Wireless Communications, IEEE Transactions on, 2004. 3(6): p. 12.

[27] Rashid, R.A. and R. Yusoff, *Bluetooth Performance Analysis in Personal Area Network (PAN).* RF and Microwave Conference, 2006. RFM 2006. International, 2006: p. 5.

[28] *Home Appliances Characteristics by Type of Housing Unit, 2005*. 2005 [cited 2010 February 28]; Available from: http://www.eia.doe.gov/emeu/recs/recs2005/hc2005_tables/hc9homeappliance/pdf/tablehc2.9.pdf.

[29] Matheus, K. and S. Magnusson, *Bluetooth Radio Network Performance: Measurement Results and Simulation Models.* Wireless Ad-Hoc Networks, 2004 International Workshop on, 2004: p. 5.

[30] Zhen, B., Y. Kim, and K. Jang, *The Analysis of Coexistence Mechanisms of Bluetooth.* Vehicular Technology Conference, 2002. VTC Spring 2002. IEEE 55th, 2002. 1: p. 5.

[31] Krishnamoorthy, S., et al., *Channel Frame Error Rate for Bluetooth in the Presence of Microwave Ovens.* Vehicular Technology Conference, 2002. Proceedings. VTC 2002-Fall. 2002 IEEE 56th, 2002. 2: p. 5.