ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 3, pp: (373-378), Month: July - September 2015, Available at: www.researchpublish.com

Evaluation of Interferences in Medical Body Area Network

[1]Nirmal Kumar K, [2]Karthika A

[1, 2] PG SCHOLAR-II M.E (Applied Electronics)
[1, 2] NANDHA ENGINEERING COLLEGE, ERODE, TAMILNADU, INDIA

Abstract: **Cardiovascular diseases are the leading cause of death in all over the world. Advances in wireless technology have made possible the remote monitoring of a patient's heart sensors as part of a body area network. Some of these networks use a Bluetooth Low Energy (BLE) component to transmit the signal between the bio sensors and a smart phone. In wireless sensor networks the information carried in the data sensors is very important for everyone .This study investigates the impact of stray wireless transmissions from residential microwave ovens have on the BLE component of the body area network and also the security issues by using Bluetooth which acts as a intermediate between bio-sensors and smart phone. The results of this study may lead to improvements and widespread use of body area network medical systems.**

Keywords: **Body Area Network, Bluetooth Low Energy Component, Bio-Sensors.**

I. INTRODUCTION

Cardiovascular diseases are the leading cause of death for both men and women in the United States, and the cause for 25% of all deaths worldwide. Worldwide global deaths due to heart attacks and strokes are expected to increase by 15% in the next five years. 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.

The use of body area networks (BANs) 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 this patient centric paradigm, the focus changes to just-in-time intervention. Wearable heart sensors play a key role in continuous monitoring. With a medical sensor relaying heart data via Bluetooth to a smart phone, it is possible to track a patient anywhere a cellular signal is available.

Body area networks can provide real-time senor readings to a medical professional. However, these systems are only as effective as the data they provide. There are few, if any, studies using Bluetooth Low Energy (BLE). There is a need for research into the mobility issues related to the cost-effective non-proprietary devices that will be used to provide reliable BAN medical systems.

Remote monitoring sensors:

Physiological Sensors: To monitor basic physiological parameters such as heart rate, pulse rate, pH level, EEG, ECG, blood pressure, blood glucose, respiratory rate, physical activity level, weight, temperature, muscle tension sensing, sleep, sport training etc [35]. It can confirm the timings of the drug dosing and send the information to a mobile phone.

Environmental Sensors: To monitor the safety and well-being of an individual motion sensor, touch sensor, vision sensor, electronic nose etc.

II. BACKGROUND

A. Body Area Network:

At least 20 million people worldwide experience ***Non-fatal heart attacks and strokes every year. Many of these survivors require continuing medical care. New technologies allow wearable biomedical sensors that give patients the freedom to be mobile while still under continuous monitoring. With the increased use of wireless networks and rapid advancements in applications that run on smart phones, there has been increasing interest in BANs. Since a BAN is associated with wireless transmission of a user's personal data it is also called as wireless personal area network.***

The use of a Bluetooth-enabled remote monitoring system has to guarantee the integrity of the medical signal during the transmission process in order to provide an accurate diagnosis. It is known that the transmission of the medical signals may be affected by interference. In previous studies using the TCP/IP protocol stack to transmit the medical signals, data packets containing errors were not retransmitted but were shown in the monitoring process. Current protocols are not always well suited to support a BAN.

B. Bluetooth Technolog:

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. The technology operates in the unlicensed 2.402 GHz to 2.480 GHz Industrial Scientific Medical (ISM) band. 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.

Over 40 million Bluetooth enabled health and medical devices are already available on the market. Bluetooth enabled health and wellness devices already on the market are making it easier than ever to collect vital health information about people with a wide variety of medical conditions – even allowing healthcare providers to monitor patients while they're at home or on the go.

Bluetooth protocol standards through Bluetooth 3.0 are known as classic Bluetooth. Classic Bluetooth utilizes frequency hopping with terminals cycling through 79 channels at 1600 hops per second or 800 hops per second with Adaptive Frequency Hopping (AFH) enabled.

Bluetooth 4.0, also known as Bluetooth Low Energy (BLE) or Bluetooth Smart, is the latest version of the Bluetooth standard. The BLE standard builds off the previous releases and supports 800 hops per second at 200 kbps with AFH enabled. However, BLE was designed as a low energy technology. The smaller packets can be sent in one-tenth the time of classic Bluetooth. Subsequently, the BLE sensor does not need to send as much data. These changes were made to conserve energy which makes BLE a good choice for health-monitoring applications.

The BLE standard does include a couple additional differences. A BLE slave device is permitted to belong to only one piconet at a time and, unlike earlier releases, each BLE slave communicates on a separate physical channel in its communication with the master. Additionally, the BLE standard uses 40 equal size channels. Three of these channels are designated advertising channels. The advertising channels are not contiguous and are not included in the frequency hopping scheme. The other 37 channels use AFH. Adding to the resiliency of the Bluetooth communication, the BLE standard uses a 24-bit cyclic redundancy error check. If the verification of the packet fails, the receiver does not send an acknowledgement, and the sender will retransmit the packet.

C. Microwave Oven:

In the United States, approximately 85% of households have residential microwave ovens. These microwave ovens operate in the unlicensed ISM band. The relatively large power leakage from microwave ovens is a potential source of unintentional interference. 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.

D. Vulnerabilities in Bluetooth Security:

Bluetooth is extremely popular short-range, low-power wireless technology integrated into portable computing and communication devices and peripherals. Bluetooth connection has an advantage of being automatic but their data is

vulnerable to interception along with any other data sent on low-power radio waves. People may able to receive the sensitive information and also able to send files or viruses without any permission.

The strength of Bluetooth security relies on the length and randomness of the passkey used for Bluetooth pairing, during which devices mutually authenticate each other for the first time and set up a link key for later authentication and encryption. The weakest part of the Bluetooth protocol is during the initial stages to set up the connection, before encryption is fully utilized. Inquiry Scanning is a very vulnerable stage of the specification. The initial key exchange takes place over an unencrypted link, so it is especially vulnerable. If a hacker is able to discover the passkey, he can calculate possible initiation keys, and then from that, calculate the link key using a simple brute force attack.

A very well-understood and common Bluetooth attack takes advantage of the vulnerabilities in Discovery and Pairing processes. This attack focuses on forcing the devices to disconnect by flooding the channels with packets indicating the slave has lost the key. This forces the devices to redo the pairing process, which the attacker can then observe and obtain the link and encryption keys.

The BD_ADDR, like the MAC address of a computer, is supposed to be globally unique. However, in 2005, researchers at CSAIL found that this was not really the case. This is potentially huge security vulnerability. An attacker could assemble a list of commonly used BD_ADDR's use a device such as spoof tooth, which allows the attacker to change the BD_ ADDR of Bluetooth module. He could iterate through a list of commonly used BD_ADDR's until he starts finding packets. Now knowing the BD_ADDR of a device nearby, he can then proceed to launch attacks such as packet sniffing and packet injection. Vulnerable services do not require even pairing of the devices. NIST's National Vulnerability Database has listed 85 potential weaknesses in Bluetooth communication.

Some of the reported attacks on Bluetooth security are (1) MAC spoofing attack, (2) PIN cracking attack (3) Man in the Middle Attack, (4) Blue Jacking Attack,

(5) Blue Snarfing Attack, (6) Blue Bugging Attack,

(7) Blue Printing Attack, (8) Blue over Attack, (9) off line PIN recovery Attack, (10) Brute Force Attack, (11) Reflection Attack, (12) Backdoor Attack, (13) DOS Attack, (14) Cabir Attack, (15) Skulls Worm Attack, & (16) Lasco Worm Attack

E. Related Works:

Several studies have used residential microwave ovens to generate interference in classic Bluetooth piconets. The goal of these studies is to improve the availability of the network. A requirement of the BAN is that the BAN should be available even during jamming and denial-of-service attacks.

The fundamental issue with separate 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 and 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 because interferers lying in line-of-sight to the wanted piconets will have greater impact than those lying in non-line-of-sight positions.

Interference can be introduced by any of the electronics that surround everyone every day resulting in collisions. One way to simulate high latency, variable latency, limited packet rate, and packet loss is to use a residential microwave oven. For this reason, the common residential microwave oven is the most critical application to investigate with the goal of interference mitigation.

III. EXPERIMENTAL METHODOLOGY

A. Data Capture Tools:

The following tools and applications are necessary elements of the data collection process:

- Heart monitor. A heart monitor that implements BLE for wireless transmission is required. In this study the Polar H7 Bluetooth Smart Heart Rate Sensor was used.
- Smart phone device. For this study, an iPhone 5 running iOS 6 with the appropriate Polar heart monitor software app was used.

- Personal computer running the Back Track 5 Linux operating system with the Ubertooth One device and spectrum analyzer to perform real-time packet capturing. The spectrum analyzer was used to identify the pattern of interference generated by the microwave oven.
- Personal computer running Windows 7 with the Frontline ComProbe BPA LE Bluetooth protocol analyzer (ComProbe) and matching software. The ComProbe protocol analyzer was used to capture the channels and packet loss occurring in the Bluetooth piconet.
- A microwave oven rated at 1100 watts

B. Data Collection Approach:

Data was collected using a systematic approach. The Only variables manipulated were the distance from the microwave oven to the BLE component of the medical BAN system and the power level of the microwave oven. The distance between the BLE piconet and microwave oven was varied from 0.5 meters to 5.0 meters at 0.5 meter intervals. At each distance, five trials each at no power, low power, and high power are collected. The distance between the heart monitor and smart phone creating the BLE piconet was fixed at 0.5 meter with the smart phone being worn in a belt case on the right hip.

In order to test the null hypotheses associated with the research questions, the Pearson Product Movement Correlation Coefficient and Analysis of Variance (ANOVA) statistical techniques will be used. Microsoft Excel 2010's Data Analysis Toolkit was used for the analysis of these research questions. The data analysis was divided into three major parts. They are:

- To identify if a linear or non-linear correlation exists between the distance from the microwave oven, the power level setting of the microwave oven, and packet loss in the BLE piconet. The Pearson Product Movement Correlation Coefficient was used to test for correlation between two the variables.
- To test all channels are equally affected by the interference, an Analysis of Variance (ANOVA) single factor technique was used.
- Three predictive models were generated using multiple linear regression analysis. These models could be combined with AFH to create a modified protocol by the medical BAN system's Bluetooth component to avoid packet loss. In essence, as packet loss increases, the Bluetooth component will avoid the channel predicted to be most affected by the model.

C. Expected Results:

Previous studies have looked at packet loss in classic Bluetooth piconets due to interference from residential microwave ovens. Based on the results of these previous studies, similar results were expected with BLE, including:

- Significant packet loss in the 2430 to 2450 MHz frequency range (BLE channels 12 to 22)
- Correlation between distance from the oven and packet loss
- No correlation between the oven's power and the packet loss because it is expected that all ovens and power levels create very similar packet loss

IV. EXPERIMENTAL RESULTS

The experimental portion of the study collected data on packet loss caused by the interference generated by a residential microwave oven. The interference generated by the microwave oven is assumed to be randomly generated. The distance the piconet was from the microwave oven, and the power level of the microwave oven, are non-random. The control group was the piconet transmissions captured while the microwave oven was in an off state. The treatment was applied via the microwave oven in the low-power and high-power states.

The spectrum analyzer application data was captured to a text file. The arithmetic mean of the RSSI values captured for each channel was calculated by a Java program. It was observed that the detected signal strength seemed to increase when the piconet was in close proximity to the microwave oven running at the highest power level.

The ComProbe protocol analyzer collected the packet loss per channel. It was discovered that BLE is very resilient to interference. The percentage of packet loss per channel was much lower than was expected. However, the ComProbe software reported that channels 23, 29, 30, and 33 (frequencies 2452 MHz, 2464 MHz, 2466 MHz, and 2472 MHz respectively) were not available for most of the trials. It is unknown at this time why these channels would become unavailable, but it is assumed that AFH avoided the channels.

A. Correlation:

When the microwave oven was off, only 16 of the 37 data channels, and only one advertising channel, had any Packet loss. By contrast, the packet loss per channel with the microwave oven operating at the highest power level when the oven was only 0.5 meters from the piconet was 31 of the 37 data channels, and two of the advertising channels, experienced packet loss.

The correlation coefficient of packet loss and power level was 0.339. This weak to moderate correlation coefficient suggests there is sufficient evidence to suggest that an increase in the microwave oven's power level will contribute to packet loss.

B. Packet Loss by Channel:

Were all channels affected equally by the interference? The spectrum analyzer was used to measure the amount of interference on each channel at each distance and each power setting. Using an ANOVA text, the P-value of 0.343 suggests that there is not sufficient evidence to reject the null hypothesis that all channels are equally affected by interference. A two-sample T-Test assuming unequal variances was used to compare the upper and lower channels based on frequency to test if all channels were affected equally. Both the one-tail and two-tail P-values suggest that there is not sufficient evidence to reject the null hypothesis that all channels are affected equally.

The data collected in this study suggests that interference affects all channels equally. Based on the data collected, it must be concluded that the interference caused by the residential microwave oven is not clustered and equally affects all channels available to the BLE piconet.

C. Predictive Models:

Several multiple linear regression analyses were performed on the data. The variables used in all of these models is the level of interference created by the microwave oven as measured by the RSSI signal strength (R) captured by the spectrum analyzer, the distance in meters between the microwave oven and the BLE piconet (D), the percent of packets lost (L), the power level of the microwave oven (P), and the channel used (C).

The first model uses the signal strength of the interference as the dependent variable and the distance, packets lost, power level, and channel as the independent variables. The P-value for the independent variable channel suggested it did not contribute to the accuracy of the model. With channel removed, the model

$$R = 10.193 + 0.604(D) + 2.673(P) + 110.578(L) \qquad (1)$$

was statistically significant with a model P-value of 3.392×10^{-102} and an Adjusted R^2 value that suggests this model predicts 73.494 percent of the variation in the data points.

The next model uses the percent of packets lost as the dependent variable and the distance, signal strength of the interference, power level, and channel as the independent variables. The P-values for the independent variables channel and power level indicate that these two variables do not contribute to the accuracy of the model. These two variables were removed, and the regression was run again. The new model It is statistically a good predictor with a model P-value value of 8.47×10^{-17} but only explains 18.724% of data.

The final model was performed with the Channel as the dependent variable and the distance, power, signal strength, and packet loss as the independent variables. The P-value model was 0.3687. This high P-value indicates that the model is not a good predictor of the channel used. The regression was run again removing variables, but no configuration created a model that was a good predictor of the channel used.

The packet loss by itself is not a good predictor of the channel used. Another method of predicting the channel that will receive the interference needs to be identified before a model can be created that will be able to be used to avoid decreased throughput in the piconet.

V. CONCLUSION

This study provides a statistical analysis on how various configurations affect the number of lost packets. An analysis of the data by various factors will be conducted. The result of the research will lead to a better understanding of the causes and impact of data packet loss in BLE wireless personal area networks (WPANs) in a BAN. This data can be extrapolated to construct a set of guidelines that can be used when creating components for BLE-enabled BANs. This study is designed to predict the percent of packet loss caused by interference from a residential microwave oven based on the channel location, oven power level, and distance from the oven.

The AFH mapping function does not look ahead at what channels will be affected by interference. Instead, AFH simply keeps track of the channels that are in a used state and the channels in an unused state. Being able to predict the channels that will be affected before packets are lost would allow the piconet to avoid blocks of channels and decrease packet errors which will increase throughput.

This study is expected to be the first of a series of studies on different areas of medical BANs in common situations. Interference from a residential microwave oven was selected because this type of interference has been identified as causing packet loss in other networks. Future experiments will study the effects of interference generated by industrial equipment that may be common in some work environments. None of these advances in BAN medical systems are feasible if common workplace interference can cause the BAN system to administer an incorrect treatment that may be more dangerous than the illness.

REFERENCES

[1] Centers for Disease Control and Prevention. Heart Disease Facts. 2014 [cited 2014 May 8]; Available from: http://www.cdc.gov/heartdisease/facts.htm.

[2] B. Latre, B. Braem, I. Moerman, C. Blondia, and P. Demeester, A Survey on Wireless Body Area Networks. Wireless Networks, 2011. 17(1): p. 18.

[3] B. Johny and A. Anpalagan, Body Area Sensor Networks: Requirements, Operations, and Challenges. Potentials, IEEE, 2014. 33(2): p. 5.

[4] M. Zhang, A. Raghunathan, and N.K. Jha. Towards Trustworthy Medical Devices and Body Area Networks. in DAC '13: Proceedings of the 50th Annual Design Automation Conference. 2013. Austin, TX: ACM.

[5] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V. Leung, Body Area Networks: A Survey. Mobile Networks and Applications, 2011. 16(2): p. 23.

[6] A. Alesanco, and J. Garc´ıa, Clinical Assessment of Wireless ECG Transmission in Real-Time Cardiac Telemonitoring. IEEE Transactions on Information Technology in Biomedicine, 2010. 14(5): p. 9.

[7] T. W. Rondeau, 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.

[8] Bluetooth SIG Inc. Bluetooth Technology Creating Huge Opportunities in Health & Wellness. 2012 [cited 2012 July 30]; Available from: http://www.bluetooth.com/Pages/Health-Wellness-Market.aspx.

[9] Home Appliances Characteristics by Type of Housing Unit. 2005 [cited 2010 February 28]

[10] T.M. Taher, M. Misurac, J. LoCicero, and D. Ucci, Microwave Oven Signal Modeling. in WCNC 2008 IEEE Wireless Communications and Networking Conference. 2008. Las Vegas, NV: IEEE.

[11] A. Sikora and V.F. Groza. Coexistence of IEEE 802.15.4 with other Systems in the 2.4 GHz-ISM-Band. in IMTC 2005 - Instrumentation and Measurement Technology Conference. 2005. Ottawa, Canada: IEEE.

[12] K.R. Chowdhury and I.F. Akyildiz. Interferer Classification, Channel Selection and Transmission Adaptation for Wireless Sensor Networks. in Communications, 2009. ICC '09. IEEE International Conference on. 2009. Dresden: IEEE.

[13] H. Huo, Y. Xu, M. Gidlund, and H. Zhang, Coexistence of 2.4 GHz Sensor Networks in Home Environment. The Journal of China Universities of Posts and Telecommunications, 2010. 17(1): p. 10.