International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 3 (2015) pp. 6581-6600
© Research India Publications
http://www.ripublication.com

An Attack Perceptive Approach for Reliable and Secure Wireless Connectivity between Medical Devices in Public Environment

Ananthanarayanan.V[1], Rajeswari.A[2,]GouthamKashyap. P[3], Sharad S.[4]

1, 4. Dept. of CSE, Amrita Vishwa Vidyapeetham, Coimbatore,
2. Dept. of ECE Coimbatore Institute of Technology, Coimbatore,
3. Dept. of ECE, Amrita Vishwa Vidyapeetham, Coimbatore.

Abstract

Implementation of wireless sensors in Personal Medical Devices (PMDs) results in wire-free communication between the medical devices on the patients' body and provides mobility to the patients. In such health applications more importance has to be given to data reliability and security of PMDs. In this research work, wireless co-existence of a wireless insulin pump was experimentally investigated. An empirical study was carried out to prove that RSSI and LQI parameters are not sufficient to validate the wireless co-existence of the insulin pump. As a solution, an Attack Perceptive Algorithm (APA) was proposed and in the wireless insulin pump, operating in 2.4 GHz ISM band. It was tested along with a Wireless Local Area Network (WLAN) in an indoor environment. Results prove that implementation of APA assures invulnerability to the insulin pump from the Electromagnetic Interference (EMI) caused by the co-existing WLAN and ensures data reliability and security. This fact is supported by attacks carried out by an intruder with various key operational parameters. Thus, an expression for the total attacks to be done by the intruder to become a receiver is calculated.

Keywords: Wireless Co-existence, RSSI, LQI, Personal Medical Data, Wireless Sensor Networks (WSNs), APA, EMI, Security.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) that operate in the ISM band can be used in the medical devices for constant observation of patients' health condition. Wireless transmission of medical data like temperature, blood pressure, sugar, etc., from the sensor on the patients' body to the monitoring systems facilitates mobility to the patients. Such WSNs also help in automating some of the common treatments like injection of insulin, intravenous therapies, etc.

Three US agencies, Federal Communication Commission (FCC), Food and Drug Administration (FDA) and Center for Medicare and Medicaid Services (CMS) play a crucial role in setting standards and certifying the Wireless Personal Medical Devices (WPMDs). These WPMDs range from heart rate monitors for measuring individual performance in sports to wearable blood glucose meters. Food and Drug Administration (FDA), USA [1] has approved the usage of Bluetooth - Powered Blood Glucose Meter Insulin Pump Combo Systems for monitoring the blood glucose level. Since these devices involve communication of critical data, more focus is required on data accuracy and privacy.

Further, the guidance document drafted by FDA [2] on design of RF wireless devices in medical devices and International Electro technical Commission's (IEC) document[3] on necessary tests to reduce electromagnetic disturbances also highlight the risks associated with the wireless data transmission in medical devices and the Electromagnetic Compatibility (EMC) of the wireless devices particularly in the ISM band. But the provisioning of system security has been mentioned as a feature and not as a requirement.

The organization of this paper is as follows: Section 2 discusses the advantages and disadvantages of using 2.4 GHz ISM band in WPMDs. Section 3 furnishes the evidences of attacks on the WPMDs in the recent past. Section 4 provides background information about Wireless Co-existence and factors on which it depends. Section 5 describes the experimental setup and the preliminary test to determine the maximum spatial range of WPMDs. Section 6 proves the insufficiency of using RSSI and LQI as decision parameters' in Wireless Co-existence testing. Section 7 proposes the Attack Perceptive Algorithm (APA) and Section 8 describes the Wireless Co-existence test on the WPMD. Section 9 gives the results obtained and validates the proposed method. Section 10 gives the results of the Attack Scenarios for the proposed model. Section 11 gives the Attack Probability expression and result .Section 12 provides the conclusion and discusses the future scope.

2. A 2.4GHZ ISM BAND INWPMDS [21-22]

Of the two universally available unlicensed ISM bands - 2.4 9GHz and 433MHz, the later has better propagation effects and communication range than the former. However, the antenna size is a major constraint for 433MHz as the usage of large antenna in WPMDs makes the devices bulky and difficult to be placed on patients' body. Further the coherence bandwidth [20] is larger than that of the bandwidth of the entire band. Hence all the channels in the band are highly correlated and the effects due to multipath propagation cannot be minimized. Although 2.4GHz ISM band suffers more loss due to propagation and diffraction, the compact size of the antenna makes the device handy. Also the coherence bandwidth is much smaller than that of the entire 2.4GHz band's bandwidth and all the channels in the band are frequency selective. Thus channel hopping in WPMDs is realizable and would help combating the effects due to multipath propagation.

On comparison, 2.4GHz ISM band is better suited for WPMDs to the 433MHz band. But the deployment of Wireless devices operating in the limited 2.4GHz ISM

band for commercial purposes has also drastically increased in the last few years. The presence of ISM band standards like IEEE802.11 (WLAN), IEEE802.15.1 (Bluetooth), ZigBee (IEEE802.15.4), microwave oven, cordless phones in the hospital/home environment has also become indispensable. Instances of cyber-attack that gained control over the wireless heart defibrillators have been reported [4]. Hence it is important to investigate the wireless co-existence of the WPMDs to ensure reliability and security to the personal medical data.

3. ATTACKS ON WPMDS

The adversaries attacking the medical system can be classified into active and passive attackers. Active attackers have the capability to eavesdrop on traffic between the devices, network controller and the supervisor, inject messages, replay old messages, spoof, and ultimately compromise the integrity of device operation. Active attackers, if successful, can not only invade a patient's privacy but can also suppress legitimate data or insert false data into the network leading to unwanted actions or prevent legitimate actions. Faulty data received at the monitoring terminal may lead to wrong treatment and may leave the patient's life at high risk. Passive attackers, on the other hand, do not try to interfere with the operation of the medical devices.

In 2008, Professor Kevin Fu, a computer scientist at the University of Massachusetts Amherst, found that by capturing a signal, hackers can gain control of an implanted heart defibrillator with a wireless outlet. Fu found that implanted defibrillators are tested using a specific radio signal when been fitted inside a patient, and because the signal turns the device on and off, capturing and rebroadcasting the signal would switch the device off [4].

In August 2011, Jerome Radcliffe stood onstage at the Black Hat Technical Security Conference in Las Vegas, hacked into the popular Medtronics' wireless insulin pump that was affixed to his abdomen by a thin tube, and completely disabled it[10][11][12]. According to Radcliffe, an attacker could intercept wireless signals and then broadcast a stronger signal to change the blood-sugar level readout on an insulin pump so that the person wearing the pump would adjust their insulin dosage. If done repeatedly, it could kill a person [5].

Radcliffe suggested scenarios where an attacker could be within a couple hundred feet of a victim, like being on the same venue or on the same hospital floor, and then launch a wireless attack against the medical device. He added that with a powerful enough antenna, the malicious party could launch an attack from up to a half mile away. The only thing needed to launch an attack is the serial number of the device to be able to communicate with it. That serial number for his model is only six digits long, and Radcliffe wrote a computer program that was able to scan all potential combinations until it found the right one

Another hacker, Barnaby Jack, who works for antivirus vendor McAfee, had also demonstrated problems with some of Wireless Personal Medical Devices, taking Radcliffe's findings a step further by showing how to use an antenna to scan public places and attack pumps from up to 300 feet away without knowing the serial number of the device [6].

Hence, there arises an increasing concern on the security and privacy aspects of the WPMD related to medical data such as data collection, data transfer and processing and maintaining electronic medical health records. By and large, security is not added to wireless medical devices, due to its limited battery life and memory, thus giving way to such vulnerabilities. The lack of security not only affects patients' privacy but may also cause harm to the patient by allowing adversaries to interject spurious data ensuing in erroneous treatments. Furthermore, too much of security also causes problem to patient during emergency situations. Without the key, access will not be granted to the implanted devices putting the patient's life at stake. So, there is always a trade-off between security and safety of the WPMD.

4. WIRELESS CO-EXISTENCE

Wireless co-existence is the ability of a wireless system to communicate in an environment where other devices may or may not be using the same protocol and wireless access technologies can also perform their tasks [2]. The system has to perform flawlessly without being susceptible to the Electromagnetic Interference [EMI] caused by other devices. [7]And[15] use RSSI and LQI as the two basic parameters to validate the wireless co-existence of a WSN and to assure credibility to the data transmitted.

4.1. RSSI and LQI

Received Signal Strength Indication (RSSI) [8] quantifies the power of the signal at the receiver before demodulation. It is proportional to the logarithmic ratio of power of the received signal (P_r) to the reference power (P_{ref}) considered.

$$RSSI \propto \log\left(\frac{P_r}{P_{ref}}\right) \ldots\ldots \quad (1)$$

By Friis' free space transmission equation,

$$P_r = P_t G_t G_r (\lambda/4\pi d)^2 \quad \ldots\ldots \quad (2)$$

Where

P_t - Power transmitted,

G_t- Gain of the transmitting antenna,

G_r- Gain of the receiving antenna,

λ- Wavelength of the signal,

d - Distance between the transmitter and the receiver

Hence,

$$RSSI \propto \log\frac{P_t G_t G_r (\lambda/4\pi d)^2}{P_{ref}} \quad \ldots\ldots \quad (3)$$

Thus RSSI also depends on the power transmitted, frequency of operation and the distance between the transmitter and the receiver. However RSSI does not provide information about the correctness of the data received and indicates only the received signal power.

LQI (Link Quality Indicator) [9] is a metric of the current quality of the received signal. The LQI gives an estimate of how easily a received signal can be demodulated by accumulating the magnitude of the error between ideal constellations and the received signal over the 64 symbols immediately following the sync word.

LQI is best used as a relative measurement of the link quality. Lower the value of LQI, lower the deviation which indicates a better link. Higher values of LQI, indicate the presence of interference. In other words, LQI qualifies the correctness of data received and is not an indication of the received signal strength. However LQI is dependent on RSSI since the strength of the transmitted signal also determines the quality of data received.

4.2. Multipath Fading and Channel Hopping

The received signal is affected by the external factors [7] like multipath fading, radio channel characteristics, attenuation due to the transmission medium, temperature and co-channel and adjacent channel interferences. Among these, the effect due to multipath fading makes the received signal power probabilistic [20]. Especially, in an indoor environment, the multipath reflections are high as every object behaves as an obstacle or a reflector to the signal. Hence there are larger number of potential signal paths and the power received at the receiver is the algebraic sum of the multipath reflections along with the Line of Sight [LOS] signal.

$$P_r = \cos\left(2\pi ft + \frac{2\pi d}{\lambda}\right) + \cos\left(2\pi ft + \frac{2\pi d}{\lambda} + \phi_1\right) + .. + \cos\left(2\pi ft + \frac{2\pi d}{\lambda} + \phi_n\right) + ... \quad ... (4)$$

Where

f - the frequency of the signal,

t -Time, *d* is the distance,

λ -The wavelength and

ϕ_n-The phase shift incurred due to n^{th} multipath reflection.

The first term on the RHS of the equation (4) is due to LOS and rest are due to multipath reflections. The RSSI depends on the phase of the multipath signals and the received signal power is difficult to predict. Thus the parameters RSSI and LQI (which depends on RSSI) are not sufficient to validate the wireless co-existence of WSNs. Mitigating multipath fading through multi hopping [20]proposes how a channel hopping MAC protocol can combat multipath fading. Packets are transmitted in different frequencies so that the receiver can shift from one channel frequency to another for packet reception. This reduces the packet loss considerably and the interference in any of the operating channels results in loss of the corresponding data only in that channel and can ensure wireless co-existence. But sending copies of same data in multiple channel utilizes more bandwidth.

4.3. Fragmentation and Transmitter Power

WSNs have to be configured such that they are less sensitive to the interference from other devices. Data can be fragmented into packets improving the bandwidth efficiency. Fragmentationmitigates interference and lowers the probability of collision. Increasing the fragments increases the overhead time. Also if the interference is at the center frequency of the operating bandwidth the entire data is lost. The transmitted power [13] can be controlled based on the interference present in the environment. But the power transmitted should neither affect the Electromagnetic Compatibility (EMC) nor the wireless co-existence of the system.

5. EXPERIMENTAL SETUP AND PRELIMINARY TEST

5.1. Device Parameters

The experimental setup [14] consists of a Glucose Monitoring System (GMS) that is interfaced with a Texas Instruments' MSP430 microcontroller. The microcontroller receives the patient's blood glucose value from the GMS and transmits it to another MSP430 microcontroller placed few meters away and drives a specially designed micro pump for injecting insulin to the patient. The communication of glucose value from GMS to the infusion pump is done by a pair of Texas Instruments' CC2500 motes. The entire system is automated to provide continuous observation and medication. The setup is shown in Figure 1 and Figure 2. In order to study the data received at the Infusion Pump an RS232 communication is established between the receiver and a desktop computer. TeraTerm 4.75 virtual terminal displays the data received. The entire setup is set in an indoor environment at room temperature.[15] Shows a similar experimental setup for BAN using IEEE802.15.4. IEEE802.15.4 has 16 channels with 2MHz bandwidth in the ISM band.

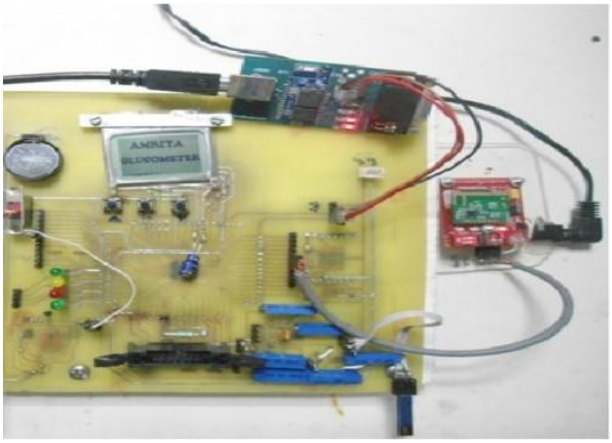

Figure 1: Glucose Monitoring System

Figure 2: Infusion Pump interfaced with MSP430

Texas Instruments' CC2500 transceiver mote is a Short Range Device (SRD) [16] operating in the ISM band with the frequency range between 2.4GHz - 2.4835GHz. There are 256 highly frequency selective channels of operation with configurable bandwidth, base frequency and device address. The base frequency of the transceiver motes is set to 2.432GHz with 200 KHz as the bandwidth per channel. Modulation format is 2-FSK and the data rate is 29.953kBaud per second. The power transmitted is set to 1dBm at the transmitter [16]. The transceiver pairs linking the GMS and the insulin pump are kept few meters apart in a noise free indoor environment. The radio module used in this research work has 26MHz and so we had avoided channels with carrier frequencies of 2405, 2418, 2431, 2444, 2457, 2470 and 2483 MHz to avoid spurioussignals [16].

5.2. Spatial Characteristics of Signal Strength and Packet Delivery

Before conducting the wireless co-existence experiment, a preliminary experiment has to be made to decide the spatial range [20] up to which the GMS and the insulin pump can be separated so that the received signal strength and the errorless packet delivery can be maximum. An 8 byte test data is transmitted and the distance between the GMS and the insulin pump is increased gradually by a step of 1m. At each step the RSSI level and the data received were recorded for a period of 5 minutes. Figures 3 and 4 plot the average RSSI and Error-free Packet Delivery Rate (PDR) as a function of distance.

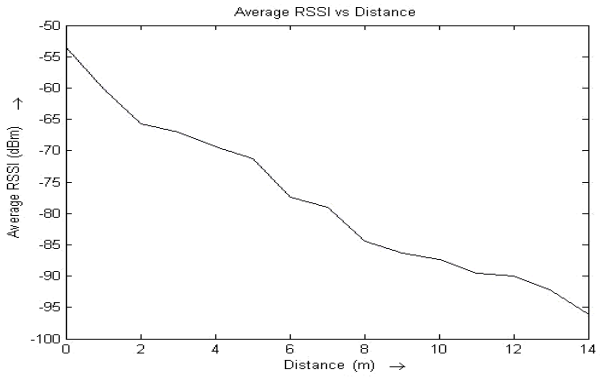

Figure 3: Average Received Signal Strength versus Distance

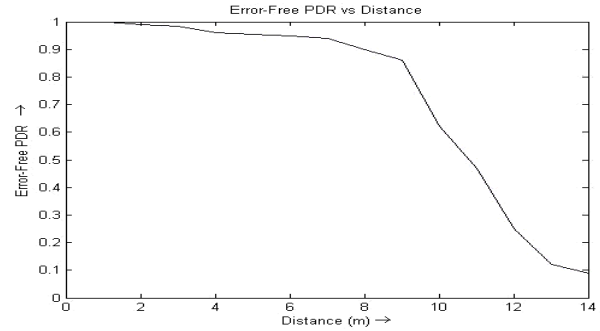

Figure 4: Error-Free PDR versus Distance

As the distance increases the average RSSI decreases. As the distance increases beyond 8 m the Error-Free PDR decreases below 0.9. The power due to multipath reflections and scattering become predominant over the power due to LOS signal. When placed further away the LOS signal is weaker and the reception rates depend on the accurate position of the nodes. Hence the maximum distance for error-free communication between the GMS and insulin pump in the indoor environment is 8 m. It also minimizes the effects due to multipath reflections.

6. RSSI AND LQI CREDIBILITY TEST

The GMS and the insulin pump are placed 5m apart in a noise free environment. An 8 byte test data is transmitted via channel 10 from GMS to the insulin pump along with date and time each, 3 bytes each, and with 1 byte of Device ID. RSSI and LQI values are recorded. The following result was obtained from the experiment:

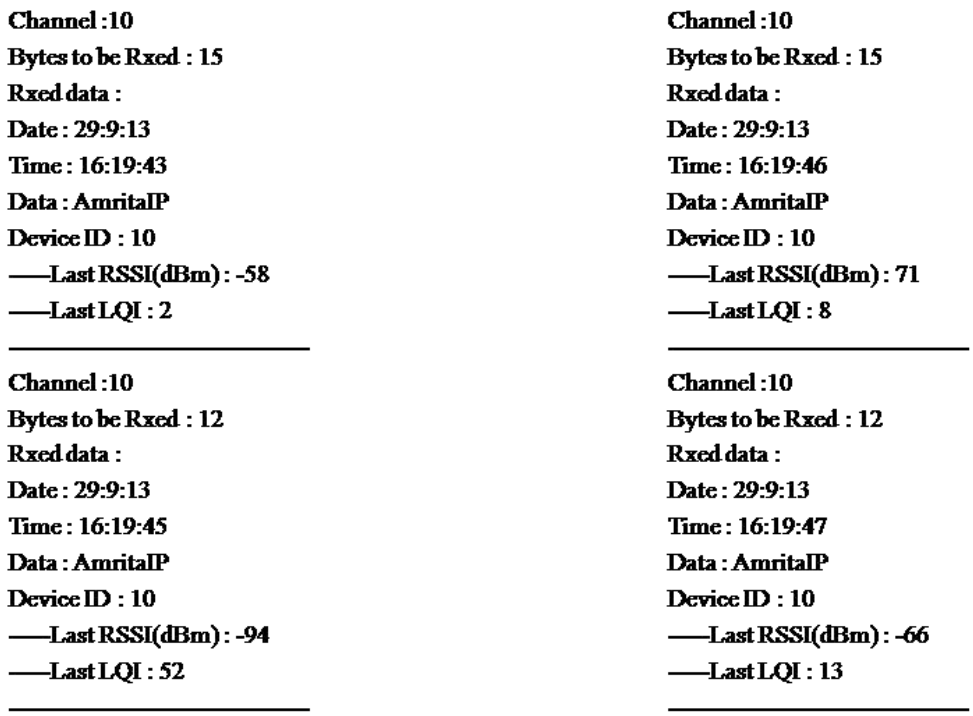

Figure 5: RSSI and LQI validation

From Figure 5 it can be observed that the RSSI value reaches -94 dBm for the second set of received data while it doesn't fall below -71 dBm for the remaining 3 sets of received data. The sudden decrease in the RSSI value is clearly due to multipath reflections. The message has suffered more attenuation due to self-interference and deflection of pulse shape due to reflections and scattering. The receiver has demodulated the data which suffers more deviation from the ideal signal

constellation and has resulted in a high value of LQI. However, the data received is error free. It is difficult to interpret whether the low RSSI value is due to EMI or multipath fading. A threshold value of RSSI cannot be fixed to discern between the presence and the absence of EMI. Hence, it is impractical to use RSSI and LQI values as decision parameters to check the wireless co-existence of WPMDs. Since WPMDs involve automation with highly critical data, more accuracy and prompt decision making is necessary. It would be better if the data received can be used as the decision parameter for the wireless co-existence test.

7. ATTACK PERCEPTIVE APPROACH

7.1. Data Fragmentation and Checksum Calculation

The 8 byte medical data is fragmented into 4 parts, each containing 2 bytes of data, and each fragment is appended with 1 byte of Device ID and 3 bytes of Date and Time. A checksum is calculated from each fragment and the checksum value is appended at the end of each fragment.

7.2. XTEA Encryption

Extended Tiny Encryption Algorithm [17] (XTEA) is a block ciphering encryption technique. It is a 64-bit block Feistel network with a 128-bit key and a suggested 64 rounds. To provide security, each fragment is XTEA encrypted before transmission.

The 128-bit key can generate 2^{128}-1 different combinations out of which only one code is implemented. Hence it reduces the probability of the risk of attack to $(1-2^{128})^{-1}$. XTEA takes few bytes of memory for both encryption and decryption when run on a microcontroller. The existing security algorithm used in Bluetooth and ZigBee is AES-128 cipher but it is computationally complex with P-boxes and S-boxes and it consumes more power, cannot be used for securing medical devices. Whereas, XTEA is computationally simple, consumes less memory and proves to be better in terms of power and space constraints for WPMDs.

7.3. Channel Selection and Synchronization

Four different channels are selected to communicate individual encrypted fragments and channel hopping technique is deployed. Channels are chosen such that they are wide apart to minimize the packet loss due to interference from wireless devices operating in the same frequency spectrum. The transmitter is set to hop to the next channel for every 1500ms and the receiver scans for the data for 200ms in a channel and hops to the next channel. The time required for calibration during frequency hopping is 721µs [16] and the remaining time is sufficient for the receiver for packet reception. Thus the operating channel between the transmitter and the receiver synchronizes for data communication.

After XTEA decryption, the checksum is re-calculated with the data received from each fragment and verified with the checksum appended at the end of each fragment. If the checksum values match, then the communication was successful and there are no interfering devices operating in the vicinity. If the checksum doesn't match then WLAN's signal has interfered with the CC2500's operating channel. At

this juncture the CC2500's current operating channel overlaps with WLAN's operating channel bandwidth and is not further suitable for communication. CC2500's transceiver pairs shift the data communication from the interfered channel to a predefined backup channel which doesn't overlap with the operating bandwidth of WLAN. The data lost due to interference is again re-transmitted in the new operating channel. Implementation of data fragmentation and channel hopping techniques makes optimum utilization of bandwidth. In APA, sending fragmented messages in 4 different channels reduces the risk of complete data loss. Even if there is a presence of data loss due to EMI in a particular channel, only a part of data is lost which can be overcome by changing the operating channel.

7.4. ATTACK PERCEPTIVE ALGORITHM

7.4.1 ATTACK PERCEPTIVE ALGORITHM AT THE TRANSMITTER

The following are the steps followed by the attack perceptive algorithm at the Transmitter:

1) Wakeup the CC2500 from the Sleep mode.
2) Perform the Frequency Synthesizer Calibration. Configure the device as a transmitter along with the Device Address. Select 4 channels for hopping.
3) Set the transmit time to zero and select the first channel.
4) Read the GMS value and convert it to 8 bytes of data.
5) Fragment the data into 4 fragments each having 2 bytes appended with 3 bytes of dateand time. Calculate the checksum for each fragment and append it at the end of the respective fragment.
6) Encrypt the packet using Extended Tiny Encryption Algorithm (XTEA) and append it with 1 byte of receiver's device address.
7) Set the channel time to zero
8) Transmit the packet.
9) Check for the transmit time and channel time.
10) If transmit time < 6000ms, go to Step12.
11) Else go to Step14.
12) If channel time < 1500ms, go to Step8 (Perform communication in the same channel).
13) Else hop to the next channel and go to Step7 (To send a new packet in the next channel).
14) Wait for the acknowledgement from the receiver.
15) If Positive acknowledgement is received, go to Step17.
16) If Negative acknowledgement is received or if acknowledgement is timed out, switch to a predefined backup channel. Go to Step 7 and retransmit the same packet.
17) Transmission is over and switch to sleep mode.

7.4.2. Attack Perceptive Algorithm at the Receiver

The following are the steps followed by the attack perceptive algorithm at the Receiver:

1) Wakeup the CC2500 from the Sleep mode.

2) Perform the Frequency Synthesizer Calibration. Configure the device as a receiver along with the Device Address. Select the 4 channels for hopping same as that of the transmitter.
3) Set the packet search time to zero. Enable the receiver and select the first channel.
4) Set the channel time to zero.
5) Scan for the packet.
6) If the packet is received, XTEA decrypt the data and calculate the checksum. Display the packet received, calculated checksum on the desktop.
7) If checksum calculated is equal to the checksum received, send a Positive acknowledgement to the transmitter module
8) Else send a Negative acknowledgement to the transmitter and switch to the predefined backup channel. Go to Step 4.
9) Check the packet search time.
10) If packet search time < 6000ms, go to Step12.
11) Else go to Step15.
12) Check for the channel time.
13) If channel time < 200ms, go to Step5.
14) Else hop to the next channel and go to Step4.
15) Reception is over and switch to sleep mode.

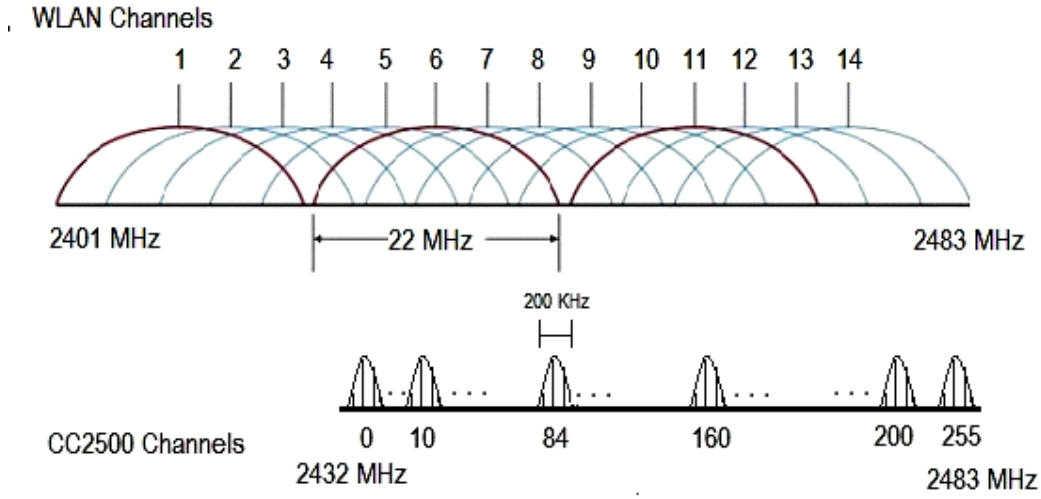

Figure6: Overlapping Channels of WLAN and CC2500

8. WIRELESS CO-EXISTENCE TEST WITH WLAN

In order to assess the wireless co-existence of wireless insulin pump, the distance between the CC2500 transceivers of GMS and the insulin pump is fixed as 5m. A WLAN that is located 2m from the CC2500 receiver is switched on to attack the transceiver pair. Channels 10, 84, 160 and 200 are chosen for operation. The frequencies of operation of channels in the insulin pump are chosen in such a way that

they overlap with all possible WLAN's channels as shown in Figure 6. Wireless co-existence test is carried out for the entire wireless insulin pump's and WLAN's frequency overlapping spectrum. Table 1 lists the WLAN channels along with their frequency of operation.

TABLE 1: WLAN Channels and their Bandwidth

Channel ID	Center Frequency (MHz)	Operating Bandwidth (MHz)
1	2412 MHz	2401 – 2423
2	2417 MHz	2406 – 2428
3	2422 MHz	2411 – 2433
4	2427 MHz	2416 - 2438
5	2432 MHz	2421 – 2443
6	2437 MHz	2426 – 2448
7	2442 MHz	2431 – 2453
8	2447 MHz	2436 – 2458
9	2452 MHz	2441 - 2463
10	2457 MHz	2446 – 2468
11	2462 MHz	2451 – 2473

TABLE 2: CC2500 and WLAN Channels Operating with Common Frequencies and CC2500's backup channels

CC2500's Operating Channels	CC2500 Channel's Center Frequency (MHz)	WLAN Operating Channels	CC2500 Backup Channel	Back up channel's operating frequency (MHz)
10	2434.9994 MHz	4, 5, 6, 7	210	2474.9896 MHz
84	2449.7958 MHz	7, 8, 9, 10	225	2477.9889 MHz
160	2462.9920 MHz	10, 11	15	2435.9992 MHz
200	2472.9900 MHz	-	25	2437.9998 MHz

Table 2 shows that WLAN's channels 4 to 11 overlap with the CC2500's operating channels - 10, 84 and 160. CC2500's channel 200 overlaps with none of the WLAN's channels. The channels of WLAN are turned on one by one for a constant time period and the data received along with the checksum, RSSI and LQI values at the CC2500 receiver are recorded.

9. RESULTS

The packets received, by the CC2500 receiver interfaced with the insulin pump, were error free when WLAN channels 1, 2 and 3 were functioning. None of the CC2500's channels overlap with WLAN's channels 1, 2 and 3 and hence there was no packet

loss due to interference. The calculated checksum values matched with the received checksum values. Figure 7 shows a sample of packets received when WLAN's channels 1, 2 and 3 were under operation.

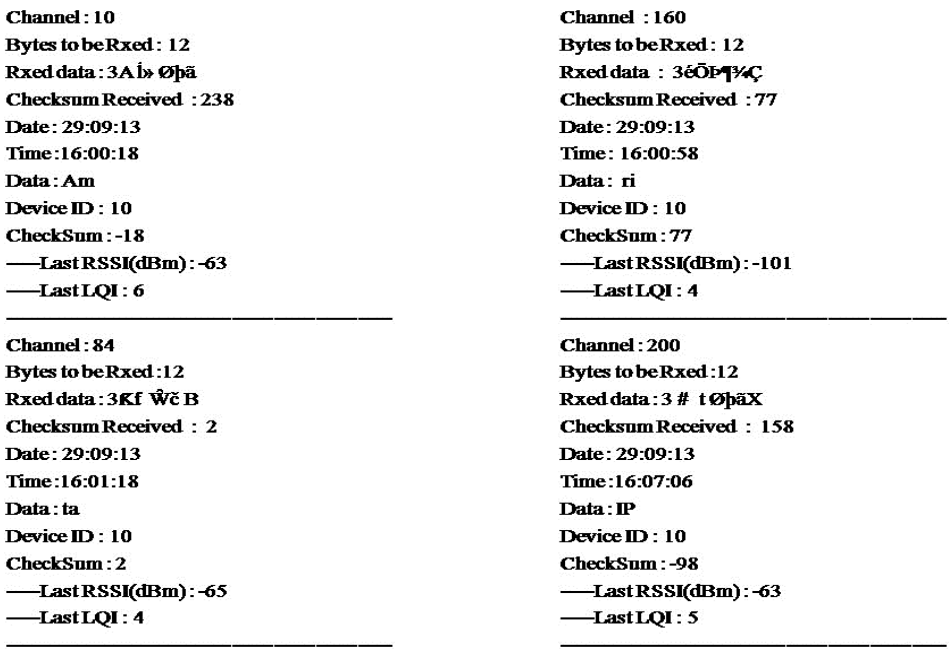

Figure 7: No data loss in CC2500's channels; WLAN's operating channels 1, 2 and 3

Figure 8 shows a sample of received error prone packet in channel 10 due to WLAN channel 4. The checksum value calculated doesn't match with the value received. This indicates the presence of interference at channel10. The receiver sends a negative acknowledgement to the transmitter. The transmitter pairs switch from channel 10 to a predefined backup channel 210. The data was retransmitted, by the CC2500 transceiver connected to the GMS, through the backup channel and the received data was error free. The channels 84, 160 and 200 do not overlap with the WLAN channel's operating bandwidth and were not affected by the EMI. The matching of the checksum values in the respective channels proves the above result. A similar result was observed due to WLAN's channels 5 and 6.

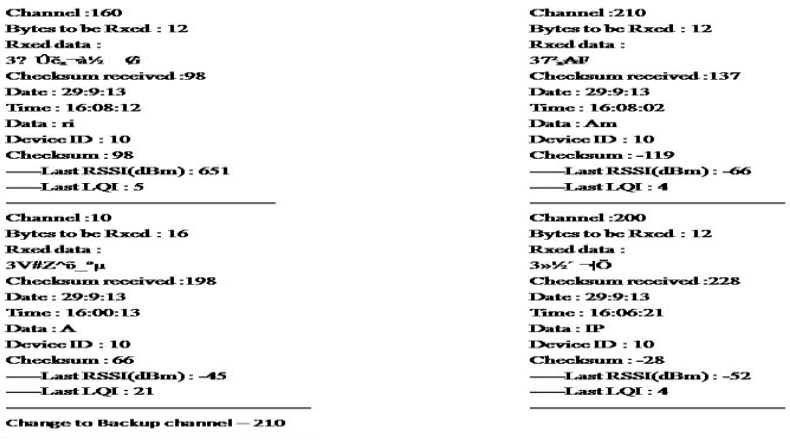

Figure 8: Sample of data loss in CC2500's channel 10; WLAN's operating channel 4

When WLAN's channel 7 was under operation, packets loss was observed in CC2500's channels 10 and 84 as both of them overlap with the WLAN's operational bandwidth. The data transmitted in both the channels were shifted to the backup channels 210 and 225 respectively for further communication. The remaining channels 160 and 200 were operating unaffected. Figure 9 shows packet loss in channel 84 due to interference of WLAN channel 8. The backup channel was predefined to be 225 and the communication was shifted to it. A similar case was observed when WLAN's channel 9 was under operation. Channels 84 and 160 were attacked when WLAN's channel 10 was coexisting. Figure 10 displays the output due to WLAN's channel 10.

Channel 160 alone was interfered when WLAN's channel 11 was under operation and the CC2500's channel operation was shifted to channel 15. The data in remaining channels were error free.

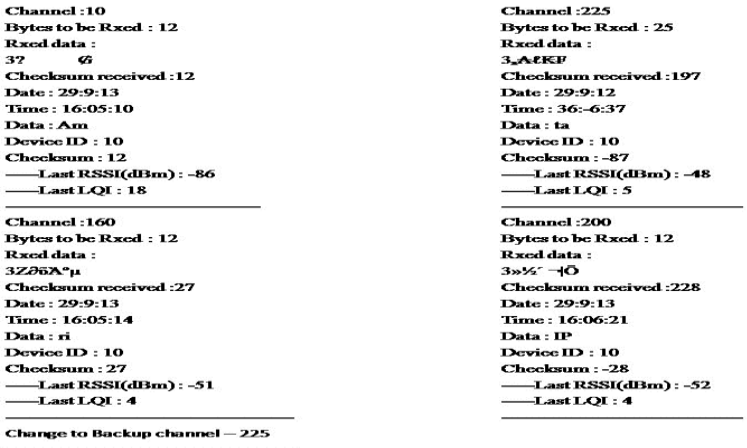

Figure 9: Sample of data loss in CC2500's channel 84; WLAN's operating channel 8

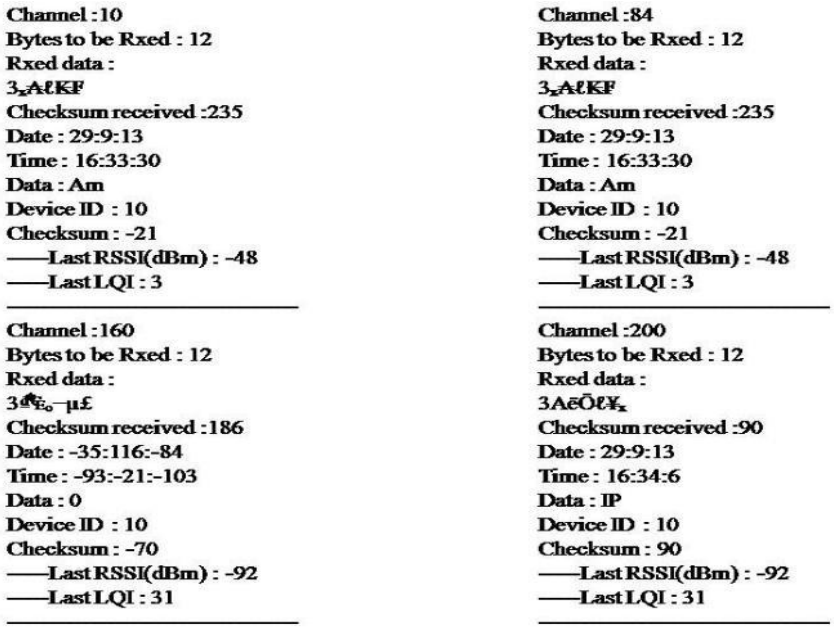

Figure 10: Sample of data loss in CC2500's channels 84 and 160; WLAN's operating channel 10

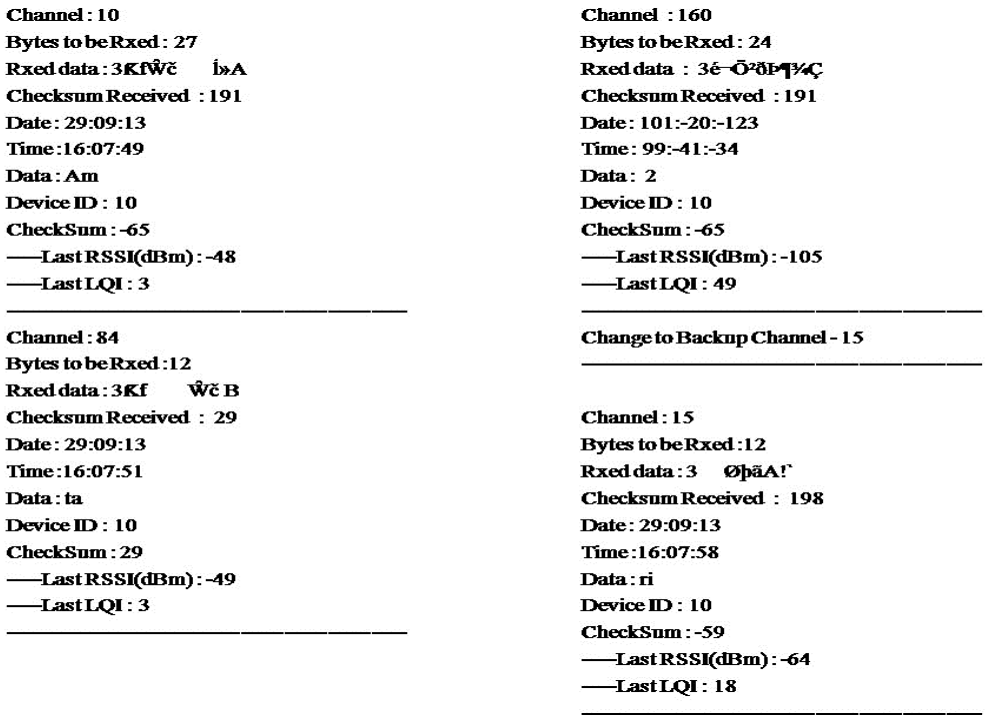

Figure 11: Sample of data loss in CC2500's channel 160; WLAN's operating channel 11

Channel 200 of CC2500 is unaffected by the interference in the entire experiment as its operating bandwidth overlaps with none of the WLAN's channels.

Based on our studies, it is recommended to adopt the following solutions to react to the attack detected. It is observed from our experimentation that the recommended solution (APA) identifies and handles possible attacks and interference.When the acknowledgement is negative or the acknowledgement is timed out, the operating channel should be shifted to a new channel that is free from the WLAN's interference. If still not possible to get positive acknowledgement, the infusion pump activities will be temporarily withheld and a warning will be issued to the patient and the doctor to take necessary actions. APA provides wireless co-existence to the GMS - insulin pump device with the WLAN.

10. ATTACK SCENARIOS

In this section, the various attacks that was carried out on the CC2500 modules are discussed. These attacks was done by an intruder (also a CC2500 module). The aim is to provethat the data sent and received is secured and reliable. The attacks are done on the essential operation parameters such as Device ID, Operating Frequencies and Encryption Keys.

10.1. Intruder with Unknown Device ID

In this attack, the intruder module does not know the Device ID of the transmitting module. Here, the intruder will need to try all the possible Device IDs before being able to know the exact Device ID. Until then, there will be no packets received by the intruder, as shown in figure 12.

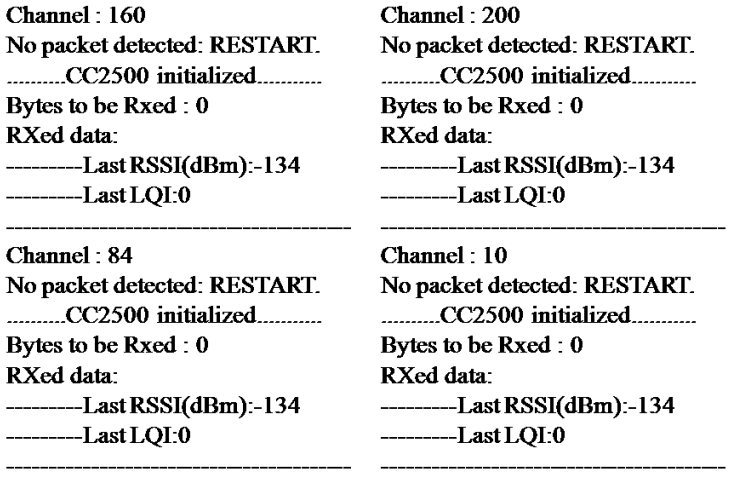

Figure 12: Sample of No packets detected across all channels in CC2500; Operating with unknown Device ID

10.2. Intruder with Unknown Frequencies of Operation

This attack has two perspectives:

- The intruder is aware of the device ID but is unaware of the operating

frequencies in which the communication takes place between the sender and the receiver. Thus, in this case the result will be "no packets detected".

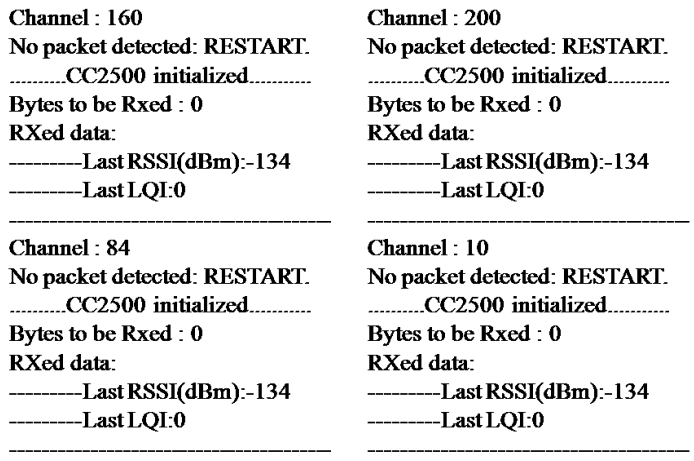

Figure 13: Sample of No packets detected across all channels in CC2500; Operating with unknown Operational Frequencies

- The intruder is now aware of the device ID and also one of the operating frequencies in which the communication takes place between the sender and the receiver. Thus, in this case the intruder receives data only from that channel, which gives it only a part of the original plain text. As only one quarter of the data that is sent is received, the security is maintained and the data received here is not reliable as the checksum may (or) may not satisfied.

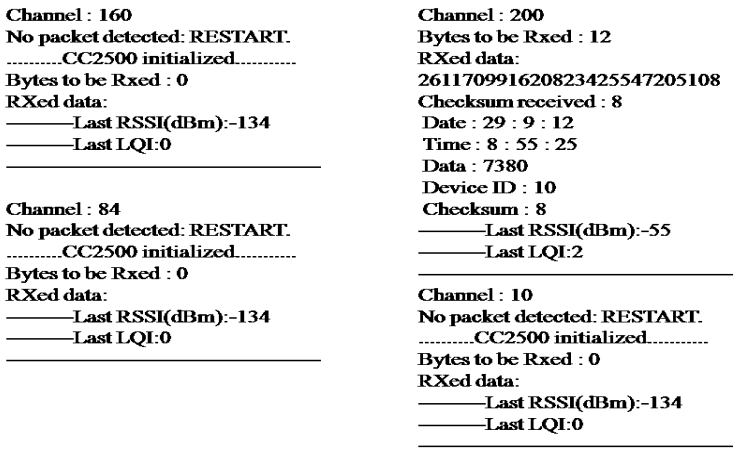

Figure 14: Sample of No packets detected across all channels in CC2500; Operating with one known Operational Frequencies

10.3. Intruder with Unknown Encryption Key

In this attack environment, the intruder has figured out the correct Device Id and the Operating Frequency but does not know the key with which data is encrypted by

XTEA, a block cipher with a key size of 128 bits. So, the intruder tries all the possibilities to get the message from the sender. The following is the output:

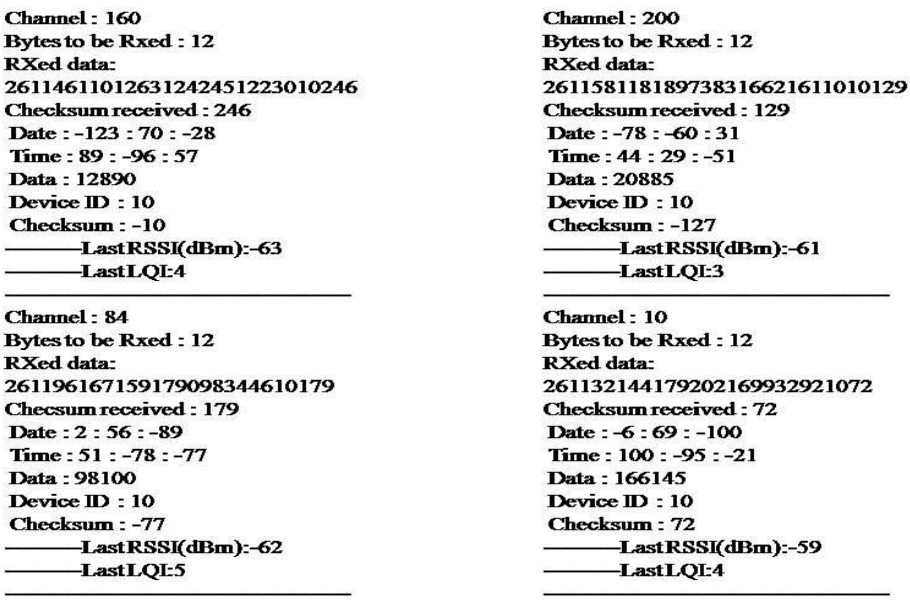

Figure 15: Sample of packets received across all channels in CC2500; Operating with unknown Encryption Key

11. ATTACK PROBABILITY

Based on the tabulated result, we can calculate the time taken for the intruder to become aproper receiver. This depends on the value that is stored in the device configure registers along with the encryption key length. It is found that there are 200 usable possibilities including the hardware restrictions. The generalized expression to calculate the number of trials needed by an intruder to become a receiver is expressedas:

$$\text{No. of Trials} = 2^{\text{nba}} * {}^{2^{\text{nbf}}}_{4}C * 2^{128}$$

Where:
nba =no. of bits in Device ID Register =8
nbf =no. of bits in Channel Register =8
And 128 is the no. of bits in encryption key.
Thus, from the results we found the time for the intruder to be:

$$\text{No. of Trials} = 2^{8} * {}^{2^{8}}_{4}C * 2^{128}$$

The approximate number of trials needed for the intruder with 200 possible Device ID and Choosing the correct Operating Frequencies from the 200 existing choices to become a receiver is **64,684,950.**

12. CONCLUSION

From the experiment it can be substantiated that the wireless personal medical devices are prone to intentional or unintentional interferences in public environment. It is not a viable

solution to use RSSI and LQI as decision parameters in Wireless Co-existence test. The implementation of APA adds intelligence to WPMDs in overcoming the data loss due to such wireless attacks and ensures Wireless Co-existence of the WPMDs in the WLAN environment providing data reliability. However, APA is effective only when the transceiver pairs are placed within the range (< 8m) wherein the measured PDR in the noise-free environment is above 0.9. Since the transceiver pairs are placed on the human body, the range is < 8m and PDR > 0.9 and hence APA is effective. As a future scope, a study on the selection of appropriate predefined backup switching channel could enhance APA. Ciphering the transmitted medical data using XTEA enables secured medical data communication with additional overhead in time delay which is also well within the acceptable range for wireless personal medical devices. The attacks by an intruder carried out on the modules, establishes the fact that the medical data that is communicated is reliable and secure.

ACKNOWLEDGMENT

The authors would like to thank the authorities of AMBE Research Center, and Mobile & Wireless Networks Research Lab of the Department of CSE, Amrita Vishwa Vidyapeetham,and Coimbatore for providing all the facilities for developing this system for the benefit of society.

REFERENCES

[1] Wouter Stomp,"ACCU-CHEK Bluetooth-Powered Blood Glucose Meter Insulin Pump Combo System Receives FDA Approval", Jul. 2012,[Online] Available:http://medgadget.com/2012/07/accu-chek-bluetooth-powered-blood-glucose-meter-insulin-pump-combo-system-receives-fda-approval.html.

[2] FDA Guidance Document,Jul. 2012, Available: http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077210.htm.

[3] International Electrotechnical Commission. Medical electrical equipment—Part 1: General requirements for basic safety and essential performance. Part2: Collateral standard: Electromagnetic disturbances—Requirements and tests. IEC 62A/746/CD, draft Edition 4 of IEC 60601-1-2. Geneva (Switzerland): IEC, 2011.

[4] Barnaby.J Feder, " A Heart Device is Found Vulnerable to Hacker Attacks",Mar,2008,[Online]Available:http://www.nytimes.com/2008/03/12/business/12heart-web.html?_r=0.

[5] Darlene Storm , "Black Hat: Lethal Hack and wireless attack on insulin pumps to kill people", Aug,2011, [Online] Available: http://blogs.computerworld.com/18744/black_hat_lethal_hack_and_wireless_attack_on_insulin_pumps_to_kill_people

[6] Dan Goodin, " Insulin pump hack delivers fatal dosage over the air",Oct,2011,[Online]Available:http://www.theregister.co.uk/2011/10/27/fatal_insulin_pump_attack/

[7] Nur Hija Mahalin, H. S. Sharifah, S. K. Syed Yusof, N. Fisal, R. A. Rashid, "RSSI Measurements for Enabling IEEE802.15.4 Co-existence with IEEE802.11 b/g", TENCON 2009, IEEE Region 10 Conference, 2009, pp.1-4.

[8] Ralf Grossmann, Jan Blumenthal, Frank Golatowski, Dirk Timmermann, "Weighted Centroid Localization in ZigBee based Sensor Networks", IEEE International Symposium on Intelligent Signal Processing - WISP, Oct. 2007 pp. 1-6.

[9] Calculation and usage of RSSI and LQI, [Online] Available:http://e2e.ti.com/support/low_power_rf/w/design_notes/calculation-and-usage-of-lqi-and-rssi.aspx.

[10] Tiffany Kaiser, "Insulin Pumps Susceptible to Wireless Attacks", Aug, 2011.[Online]Available:http://www.dailytech.com/Insulin+PumpsGlucose+Monitors+Susceptible+to+Wireless+Hacking+Overdosing/article22365.htm

[11] Jordan Roberston, "Medtronics insulin pump vulnerable to attack", Feb. 2012. [Online] Available: http://www.bloomberg.com/news/2012-02-29/mcafee-hacker-says-medtronic-insulin-pumps-vulnerable-to-attack.html

[12] Jim Finkle, "Medtronic probes insulin pump risk", Oct. 2011 [Online] Available: http://www.reuters.com/article/2011/10/25/us-medtronic-cybersecurity-idUSTRE79O8EP20111025

[13] Mathew B. Shoemake, "Wi-Fi (IEEE 802.11b) and Bluetooth Co-existence Issues and Solutions for the 2.4 GHz ISM Band", Texas Instruments White Paper, Version 1.1, Feb. 2001. [Online]Available: www.focus.ti.com/pdfs/vf/bband/co-existence.pdf.

[14] Ananthanarayanan V, Mithun Haridass TP, Naveen.R, Rajeswari A "Reliable and Affordable Embedded System Solution for Continuous Blood Glucose Maintaining System with Wireless Connectivity to Blood Glucose Measuring System", IJCA Proc., Amrita International Conference of Women in Computing, Jan. 2013 pp. 36-43.

[15] Jan-Hinrich Hauer, Vlado Handziski, Adam Wolisz, "Experimental Study of the Impact of WLAN Interference on IEEE 802.15.4 Body Area Networks", European Conference on Wireless Sensor Networks, Feb. 2009 pp. 17 - 32.

[16] CC2500 datasheet [Online]Available:www.ti.com/lit/ds/symlink/cc2500.pdf

[17] Wheeler, David J. and Needham, Roger M. "TEA Extensions". Computer Laboratory, Cambridge University, England. Oct. 1997.

[18] Morten Engjom, "Practical Sensitivity Testing", Design Note DN002, Texas Instruments [Online]Availablehttp://www.ti.com/lit/an/swra097/swra097.pdf

[19] "IEEE Standard for Local and metropolitan area networks— Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)", 2010. [Available:]http://standards.ieee.org/getieee802/download/802.15.4-2011.pdf.

[20] Watteyne T, Lanziseram S, Mehta A, Pister K. Mitigating Multipath Fading Through Channel Hopping in Wireless Sensor Networks, in*IEEE International Conference on Communications (ICC)*, Cape Town, South Africa, 2010.

[21] Rappaport, Wireless Communications: Principles and Practice, Pearson Education India, 2009

[22] Constantine A. Balanis, Antenna Theory: Analysis and Design, 2nd ed., John Wiley and Sons, Inc., New York, Reprint 2009.