**Chapter 14. Implantable Medical Devices: Architecture and Design**

Fei Hu Qingquan Sun Yeqing Wu Mengcheng Guo Jiang Lu

Jiayin Li, Daniel Justin Gay, Justin K. Garner, Anthony L. Poellnitz,

Electrical and Computer Engineering, The University of Alabama, Tuscaloosa, AL, USA

**1. Introduction**

D

ue to the great improvement of MicroSystems Technology (MST), the implantable medical devices (IMDs) are substantially developed recently [1]. There are many active IMDs that are commonly used today. These include devices such as pacemakers, implantable cardioverter defibrillators, wireless capsule endoscopes, etc. IMDs such as pacemakers are some of the original implantable devices that doctors began using to regulate medical conditions. And they are becoming more and more prevalent. Research shows that there are nearly 1 million pacemakers alone implanted each year throughout the world. The wide use and implementation of pacemakers produces over $5 billion per year in sales.

IMDs include various devices such as stents, bio-implants, valves, and joint-replacements, etc. These are all referred to as passive IMDs, which are of the more simplistic variety. These are other more complex and involving examples including IMDs such as pacemakers, implantable cardioverter defibrillators (ICDs), neurostimulators, programmable drug pumps, and other devices of this sort. These are called active IMDs. These IMDs are of the more refined and sophisticated sort. It usually requires more effort and research to design such intricate devices as these.

IMDs such as pacemakers are some of the original implantable devices that doctors began using to regulate medical conditions. However, over time, the need to have more functionality has increased. Scientist began looking for ways to have implantable devices that would record data as well as regulate functions without having to constantly invade a person’s body. The progress in wireless communication technology has made this dream a reality. With standards such as Zigbee, developers have created devices that monitor pressure, temperature, and other rates in the body. These devices are able to send out signals of the data that it collects. Whether patients are in their homes or in health care facilities, wireless communication is allowing for data to be collected by implantable devices and uploaded to the physician’s personal logs. A physician can be alerted in case of an emergency sensed by the IMDs. The patient’s implant sends a signal to an external monitor which in turn sends data to a secure server. Doctors receive alerts of changes in their patients care immediately and are able to respond quicker if necessary, by actually alerting patients that they need to come to the hospital. There are various ways to collect this data as discussed throughout this paper. Battery life, body interference, signal strength, magnetic interference must all be considered as factors when creating IMDs and their counterparts that will receive and analyze the data signals.

IMDs are changing the way that doctors practice medicine in the twenty-first century. The progress in wireless communication systems has allowed for the creation of smaller, safer devices with better wireless telemetry. Because of these new developments, the range of patients using wireless monitoring devices has expanded beyond its largest holder, cardiac patients. In former times, pacemakers were the main IMDs, but now wireless IMDs can send signals that include measurement and recording of physiological parameters using high frequency electromagnetic signals.

This chapter will cover developments in IMDs starting with examples of different IMDs and their characteristics. Following this will be sections that discuss wireless communication, security, and power consideration within an IMD. Developments within IMDs will be presented within each of these categories in order to give the reader a look at unique developments within the IMD research community. This chapter will conclude with a discussion of some reliability and compatibility concerns about IMDs and their widespread implementation.

**2. IMDs Examples**

One of the first IMDs created was the external pacemaker. At their initial conception these were fairly simplistic devices. They contained no real sensing, processing, nor communication capabilities. They were utilized to control the rhythm of the heart without any feedback. When their battery life expired, they were simply recharged and recalibrated for the particular person. This recalibration was simply altering the pacing rate. This was usually repeated every few years to ensure that the device continued to work properly and that there was no malfunction in the device thus preventing serious health issues to the user due to device failure. Approximately a decade after the invention of the first external pacemakers, Medtronic (a notable IMD research agency) began to work toward and produce the first models of the implantable pacemaker. This was greatly sparked by the development of wireless techniques for communication. This enabled scientists and researchers to implement these ideas into the design of IMDs thus leading to the development of the implantable pacemaker. Through this technology pacemakers were eventually designed to be reactive, or "responsive", to their environment. This enabled the pacemakers to be able to change the pacing rate according to the activity level of the user. This was a notable breakthrough for the time. IMDs have evolved greatly from these discoveries. Modern pacemakers are responsive to many environmental characteristics. Many modern pacemakers and other IMDs have the competence to involve considerable processing to facilitate sensing, monitoring, detecting, responding, communicating, and several other activities. This enables the typical pacemaker user to interact much like any other human being without severe danger or hazard. These more modern devices also have the advantage of being able to download software code that can run in addition to or as a replacement for the existing code. This downloadable code is often simply referred to as "downloadable firmware."

Another device that is often implanted into patients is the SynchroMed IITM (S2) implantable drug pump [2]. The implantable drug pump seems to be very technologically advanced and complex. The drug pump consists of many sensors and gadgets that allow it to pretty much be self-governed. Once this device is completely assembled and configured, the S2 is communicated with wirelessly. This is done by sending signals to the device informing it to configure itself to the particular patient and to perform diagnostics to determine what dosage of medication should be administered and when and various other variables that should be considered when the S2 is implanted into the patient. Next a clean-room worker will put the implant into a sterile package that will hold the device until it is removed in the operating room and inserted directly into the patient. Once the actual implant takes place, the doctor instructs the programmer to program the implant so that it senses that it is now inside of an actual human and to react accordingly. The drug pump is capable of initialization, diagnostics, and even logging itself all within minutes. It is also able to communicate wirelessly, sound an audible alarm, and even begin to pump the desired drug and sense its capability to do so. Eventually the device will indicate that it should be replaced via a device known as an Elective Replacement Indicator (ERI) and often times change its performance if it is allowed to reach the end of its lifetime often known as the end of service point (EOS). This is a very large step from the external pacemaker that we discussed previously. Once this is assessed the device will be removed and discarded or it will be returned to Medtronic for analysis.

These IMDs have many sensors that enable them to react and work appropriately to complete the task of which they are employed. These sensors often simply react to their environment and respond in a way that seems most fitting. This is prevalent in the S2 device that we mentioned earlier. This device is able to sense its electromagnetic environment and monitor it for the presence of wireless telemetry communications. This device also monitors itself and checks for stall, measures its battery voltage or charge, tracks the passage of time, and also diagnoses several other issues or occurrences that may occur over time. Not only is it capable of monitoring and measuring these things but it is also able to proactively take steps to the correction and remedying of these actions. This device is able to do all this by examining its environment and comprehending its capabilities, status, history, and configuration. The S2 pump has been proven to react and correct itself when some malfunctions occur. If the pump were to malfunction due to the presence of a strong magnet, a damaged port, or some other technical difficulties, the will detect its malfunction. It will sound an audible alarm and indicate this error in the next telemetry communication session. Another example of the S2 pump being able to correct itself deals with the amount or volume of fluid (medication) the pump has displaced into the patient's body. The pump monitors the amount of fluid it dislodges and if it senses that it has released too much, it will sound an audible alarm and consider itself in the ERI or EOS state. One problem resulting from this method is that the error can be the result of a variety of different, non-related circumstances. The error could result from something as simple as a temporary drop in battery voltage. This action would create a condition where the device becomes unresponsive even to the operator or physician thus requiring the physician to surgically remove and correct or replace the device in the patient. This is good in the aspect that it is reactive and able to fix problems but can also become a nuisance when it happens repeatedly; forcing numerous surgeries in order to fix a problem that is otherwise non-existent. While all this may seem rather complex and involving, the S2 is considered to be relatively sensor poor compared to many other modern day IMDs.

Another case where an IMD shows superior sensory activity is shown in the case of the cardiac pacemaker [3]. The cardiac pacemaker makes use of sensors to determine patient activity. The various characteristics of the patient (posture, activity, etc) is determined using several different procedures, such as using 1, 2, or 3 axis accelerometers in a range of devices such as the Medtronic Kappa 900TM. In addition to these characteristics, cardiac devices monitor the electrical activity of the heart using leads to propagate the signals. Now some devices such as the Medtronic's RevealTM Insertable Loop Recorder and Reveal Plus have enabled "leadless" or subcutaneous sensing of the ECG. Some other cardiac devices sense other characteristics such as oxygen, pressure, or other levels. There are also several other characteristics and traits that are now traceable by neurostimulators and IMDs. These devices are being spread to treat several other parts of the body. One of these in particular is the NeuroPace Responsive NeuroStimulatorTM (RNS). This device measures the electrical activity of the brain (EEG). This information and technology is used to detect epileptic seizures. Another device that has been utilized is the temperature sensor. These are often used to address tissue heating during recharge of the IMD to ensure that no overheating occurs. Yet another form of a sensor is used to simplify patient communication. One example of this is the use accelerometers to detect physical tampering to the device. This can be something as minute as a patient tapping on the device or as crucial as the presence of a magnet. Discoveries are being made and research is being conducted that may one day lead to direct "Brain Computer Interfaces". Scientists are predicting that sometime in the near future, IMD sensors will sense a new range of characteristics such as "hormone levels, anesthetic agents, and other factors within the human body such as drugs."

**3. IMD Communication System**

**3.1 Transceivers**

The use of IMDs has been increasing over the past decade and with the rapid development of new technology, will continue to increase over the next several years. Many of the devices are custom made, having their own protocols and frequencies. Having this independence usually enables the device to optimize the amount of power it consumes as well minimize the amount of space it must take up in the body. However, when there is more than one implantable device in the body, it becomes difficult to sync the wireless network of implanted sensors to an external base. Therefore, a predetermined communication standard is needed for wireless communication of implantable devices.

 There are three low power wireless communication solutions to this problem: Ultra Wide Band, Bluetooth, and Zigbee. The Ultra Wide Band (Wi-Fi), like the others runs on the IEEE 802.15 standard [1]. Wi-Fi is able to achieve extremely large data rates but has higher power consumption rates. Most medical devices are collecting only small bits of data at a time and therefore the large data rate of Wi-Fi is unnecessary. Since the large data throughput is not necessarily needed, Wi-Fi devices have been abandoned for smaller more efficient devices. Bluetooth is also able to achieve a high data rate. However, continuous data transfer is required which diminishes the life of the power source in the implanted medical device. Though Bluetooth eliminates the need for cable operations and works well in rechargeable devices such as cell phones and PDA’s, it is not feasible for IMDs. Since, neither of these solutions provides optimal use for the IMD’s, several electronic companies created an alliance known as ZigBee [4]. The ZigBee protocol attempts to create a standard with ultra low power consumption, cost, and complexity at low data rates. Therefore, it is suitable for wireless transmission of IMDs such as the monitoring of ECG waveforms which has a high sampling rate [5]. While the amount of power used during transmission is almost equal for ZigBee and Bluetooth, ZigBee uses almost no power during its sleep mode is in only awake for a short period of time. This ability allows the batteries to last for several years before a replacement is needed, a grand breakthrough since most people do not desire to be encroached. ZigBee also allows over 65,000 devices to connect to the same network, enabling the interaction of devices and providing a way for more implantable devices and networks to communicate as new devices are developed. The large number of nodes on the Zigbee standard allows for the monitoring of several parameters at once. One node can monitor body temperature, another heart rate, and so on and so forth from sensors inside of implantable devices. New digital and programmable intelligence allows the implementation of a standard approach to the telemetric link. The Analog Front End (AFE) is capable of multiplexing diverse inputs from the sensors. Since signal condition parameters can be selected by the user in real time through the telemetric link, the sensing part of the remote board can be off during inactivity in order to preserve power.

Sensor Module

Sensor Module

Reconfigurable Analogical Front End

Mux

Switch

PIC Micro Controller

ZigBee

Transceiver

Chipon

CC2420

Power

Figure 1: Block diagram of the implantable unit [1]

 In [1] an implantable digital microcontroller was tested using the Zigbee standard, which evaluates the performance of the device during data transmission in an in vivo setting. The platform for this system consists of the implantable unit, the receiving unit, and the graphical user interface. In Figure 2, a block diagram of the implantable unit is shown. Various types of sensors can be attached to the system and operated by the microcontroller which controls the configuration of the Analog Front End through an electrical switching system.

The CC2420 chip shown in Figure 1, is the transceiver for the implanted and host units because it implements the ZigBee standard particularly because the physical layer is embedded in the hardware along features from the MAC layer for error detection. The PIC microcontroller is chosen because loop antenna in the Pixie module work better than dipole antenna because of radiation.

 In the electronic design of the Analog Front End main stage, the gain is represented by the following equation

 (1)

where R1 can be programmed through a 100kΩ potentiometer, creating

 (2)

where N is an 8 bit number located in the register and R2 is 470Ω.

Because of the switching architecture, different AFE configurations can be obtained and the subsystem can be shut down to save battery life. To correctly test these performances two sensors were chosen, a thermistor and a pressure transducer. This firmware was developed to complete features implemented by the hardware so that the ZigBee standard could be properly implemented in the microcontroller. Although only a reduced version of ZigBee was implemented, the C-code is compatible and easily integrated using full ZigBee. The firmware is organized in a manner to establish communication only when necessary and for a small amount of time for power management purposes. As shown in Figure 2 below, communication is always established by the implanted unit which controls when transceiver is in operation or not. After the initialization, a command is sent and an acknowledgement is received. As seen in the flowchart, the four commands that can be sent are, modify AFE parameters, perform calibration, define transmission power, and modify the length of the sleep state.

Init

Cmd\_Req

Received

Menu

Main (Cycle)

Send

Receiving

Parameters sensor

Calibration sensor

TX Power

Wake Up

Figure 2: Flow Diagram of the implantable unit firmware [1]

The main state consists of a loop which switches the system on and off again after it obtains data and stores it. Once the memory is full, it transmits the data. Since this can take a long time, the transceivers may be turned off for days at a time. However, if the data received is critical, it will show up as outside the range and transmission will commence immediately. This format allows for a battery lifetime of decades, allowing for chronic monitoring of physiological conditions

 IMDs are one of the great inventions of the 20th century and are yet experiencing tremendous technological advancement during the 21st century. One particular area that is experiencing growth is the implantable glucose sensors devices. The United States obesity and health problems are contributing to the rapid growth in the diabetic population. Patients with diabetic problems usually monitor their blood sugar levels by a finger pricking process that collects samples of blood. The blood sugar levels are tested by a device to tell where the levels are in regards to where they should be. This method can quite aggravating and painful for those who must monitor their glucose levels on a daily basis. Because this intrusive method is abhorred by many, much research has been done to develop glucose sensors that are either non-intrusive or implanted [6].

 Using IMDs is an ideal solution. However, implanting the proper design can be quite the task. An implantable sensing system needs an efficient power amplifier in order to transmit commands to an implanted module. There could also be magnetic coupling that could interfere with signal transmission creating the need for a high SNR. In Figure 3 below, a downlink transceiver system is shown. One component of the system is an external transmitter module which gives command, power, and data through the skin to the implant. The other component is the internal data demodulator. Once the data is received from the external module, the internal module demodulates the data and sends signals to the MCU. Using amplitude modulation, the internal module receives data through RF telemetry which are a coupled pair of coils similar to transformers. [7]

Command Power

Data

External Module

External ASK Modulator

Internal Module

(ASIC)

Internal ASK Demodulator

Command Power

Data

Skin

Figure 3: Downlink transceiver system architecture displaying external and implantable devices. [7]

 Using a class E power amplifier for the transmitter allows for good efficiency. Other comparable amplifiers usually have power losses that are twice that of the class E. Having better efficiency helps make up for the low coupling between the transmitter and receiver. As shown in Figure 4, a carrier generator is used in conjunction with ASK modulator transmitter. The generator uses a 2 MHz oscillator circuit. The frequency choice is made in light of the attenuation of magnetic field intensity in nonmagnetic materials [8]. Also considered is the amount of power used by tissues to produce eddy currents. Enough power must be used to transmit the signal and still not so much power that tissues are heated during absorption. Since high frequencies can cause harm by overheating the tissues in the body, lower frequencies are used, slowing down transmission rates. Figure 4 shows the ASK modulator in series with eh RF choke. Since ASK modulation is easy to design and implement the proper SNR can be achieved to provide optimal quality.

M1

Co

 Cp

Lo (Antenna)

Rs

Vo

Carrier Generator

RF Choke

ASK Modulator

Figure 4: External ASK modulator (transmitter) prototype schematic [7]

 As mentioned above, once the signal is received, it must be demodulated. In the past, the component used for the receivers called for large chip area consumption. However, with the schematic show in Figure 5, a smaller area is consumed. Implementing real voltage and noise levels into programs such as MATLAB® and Hspice® the proper circuit was determined. The schematic is divided into three portions: The envelope detector, the high pass filter, and the Schmitt trigger. The envelope detector extracts the ASK signal and locks DC level using an independent biased circuit.

As medical technology continues to advance in the 21st century, newer medical devices are being created on a frequent basis. One type of device is the IMD that has recently also gained the capability of wireless transmission of data about human conditions. In 1999, the Federal Communication Commission instituted the Medical Implant Communications services standard (MICS) in the 402-405 MHz band [9]. In the past, implantable devices transmitted data using inductive coupling. However, this method was very limiting because it required the device to actually touch a base-station. However, since the creation of the MICS, frequency-shift keying and minimum-shift keying direct modulation transmitters have been invented allowing for faster data rates and rid the need for frequency synthesizers and keeping stability. The MICS band enables medical implants to communicate up to two meters away from its base.

Turned Coil Envelope Detector High Pass Filter Schmitt Trigger

D1

C1

R1

C2

R2

Figure 5: Internal ASK demodulator (receiver) prototype schematic [7]

 In constructing IMDs, one of the major hurtles to deal with is battery life. Since the device’s battery cannot be recharged, much of the technology development work goes toward creating transceivers that only use a small amount of energy while performing with proficiency and longevity. In order to accomplish this, several factors must be taken into account. One of which is the role that the body plays as a temperature regulator and a conductor. For example many wireless devices such as cell phones must have a 120°C range it which it must maintain frequency stability. However with implantable devices, the range is about 25-45°C, since the human body rarely changes temperature and when it does, it is rarely in a swift or critical manner. This fundamental difference from traditional radio transmission can be used to reduce the power consumption of implanted medical devices. However now that there are relaxed frequency stability requirements and the reduced power consumption to preserve battery life, the base station for the device is allowed to consume much more power, moving complexity of design from the implant to the base-station. [10]

 In designing implantable devices, the digitally controlled oscillator is directly modulated by frequency-key shifting which includes the driving of the loop antenna as an inductive element. In the design capacitors are used to provide tuning ranges and frequency resolution. These so called fine tuning capacitor banks divide several bits of frequency in order to achieve a large tuning range while still keeping a reasonably fine frequency resolution. A model of this frequency-key shift transmitter is shown below in Figure 6.

FPGA On-Chip Transceiver

SPI Controller

Data Generator

SP

I

7.0

PCB Antenna

Env

Det

RST Counter ENb

NT

Data Out

VCOMP

NREF<3.0>

VEP

VEM

IBIAS

Data In, m(t)

BBCLK

Figure 6: Transceiver Diagram block [10]

The device uses time division multiple access (TDMA). The transceiver uses an external loop antenna that is shared by both the receiver and the transmitter. The low radiation power allows the antenna to integrate directly into the digitally controlled oscillator. This oscillator is also used as the on-off keying super regenerative receiver and furnishes the gain that allows the envelope detector and the comparator to obtain the best power consumption.

 Most IMDs have a low bandwidth signal that can be digitized, allowing the transmitter to remain off until it is time for it to transmit data. While the data is being collected the transmitter remains off and when it does energize, it is only momentarily. Batter life is prolonged because data packets are sent in short bursts.

 As with frequency stability, the make-up of the human body plays a large role in the antenna gain of a medical implant. Inside the body, gain is much lower compared to free space because the tissues in the human body like fat and muscles are conductive, causing a large loss in transceiver gain. Also because the antenna is inside the body, it generally has to be very small of usually smaller than the signal’s wavelength. The efficiency of the antenna is measure by this equation,

 (3)

The small loop antenna’s efficiency is modeled as a resistor and an inductor in series. Since the total resistance is a combination of radiation resistance and loss, the efficiency can be show in Eqn. 1. If the antenna is inefficient, it produces a high quality factor (Q) which hinders power transfer because the inductive element of the antenna must be resonated and minute changes in the impedances can cause mismatches [11]. However, the high quality factor along with acceptable efficiency is highly desired. The conductance of body tissue creates a lossy loop antenna which lowers both the quality factor and the efficiency. This problem may be solved by using a substrate with metal patches. Therefore, even though the human body has an effect on the aforementioned properties as well the pulling frequency due to the motion of the body, technology is able to override this disadvantages to the point where transmitting through human tissue does not compromise the functionality and performance of the medical devices [10].

 As stated above, new developments in frequent shift keying (FSK) have revolutionized the usage of medical implantable devices. The FSK can be applied by modulating the oscillator’s instantaneous frequency using the following equation:

 (4)

where fc is the carrier frequency, F is the frequency deviation constant, and m(t) Є [-1, 1] is the digital modulating signal. If the frequency deviation is one-fourth the bit rate it will produce an efficient orthogonal signal that can easily be demodulated.

 The digitally controlled oscillator incorporates the small loop antenna and has an equivalent parallel resistance of

 (5)

Switched capacitors will tune and modulate the ω0 resonate frequency. As show in Figure 7 below, tunable capacitor is implemented by using four capacitor banks to provide course, medium, and fine tuning. Each of the capacitors is on a different magnitude. Although this may cause some predistortion, through careful testing a proper predistortion can be chosen that will allow the proper frequency step changes when tuning the capacitors. [10]

CC(NC)

<6 bits>

CM(NM)

<6 bits>

CSM

CF(NF)

<8 bits>

CΔF(NΔF)

<8bits>

CSΔF

CSF

Figure 7: Simplified Model Circuit of sub-ranging capacitor array [10]

**3.2 The Human Body as a Medium**

As remarkable technological advancements are made each year in various scientific fields, the amount of artificially intelligent nanotechnology manufactured increases as well. One type of application that uses such advanced technology is IMDs. With growing scientific research the need for complex functionalities of these devices are growing daily. The main issue with implantable devices is coming up with design concepts for wireless communication. A physician’s ability to readily access patient’s health status provides for much more effective treatment of medical ailments. Industrialized nations such as the United States and many countries in Europe have already set aside special guidelines for communication requirements to help in the communication and low interference for implantable devices.

 While primarily used for cardiac treatment, IMDs are also treating a wide range of neurological disorders and other ailments. Interacting directly with the nervous system, the devices have been used for deafness, epilepsy, obesity, and even mental disorders. Constant ongoing monitoring of patients with such conditions is of much more value than occasional visits to the physician. Therefore we find that some of the costs are canceling out themselves because of preventive medical care and observation.

 IMDs communicate with external monitoring devices, uploading data into a patient’s medical file. However in order to do this, the device needs a constant and sufficient source of power, one of the many design constraints. One way of providing power is through inductive coupling. While much experimentation is being done on this technique, the most common means of a power supply source is a non-rechargeable battery. These batteries generally are required to last around 5 years, meaning that battery life must be preserved during its lifetime. This is mainly accomplished by Sniff Mode technology. The circuitry in the devices normally remains de-energized except for the receiver that awakes every few moments (varies depending upon physician’s requirements, usually a few seconds) and listens to see if a signal on its frequency is being transmitted. If it is not, it returns to sleep mode. If it is, the receiver awakes and prepares for data reception/transmission. During this transmission it is important to remember that the human body is also a medium through which this signal must travel and that has complications all of its own. Since the body is made of different substances and materials with different dielectric constants, some parts of the body are more conductive than others. Therefore the body should be seen as part of the IMD’s antenna. Table 1 shows, dielectric parameters of human tissue at around 403 MHz. It gives the effective permeability εer and the conductivity σe of different human tissues. Note that the reflection must be taken into account between two different types of tissues such as muscle and fat. [12]

Table 1. Dielectric parameters human tissue at 403.5 MHz [12]

|  |  |  |
| --- | --- | --- |
| Tissue | εer | σe |
| Muscle | 57.1 | 0.797 |
| Fat | 5.6 | 0.041 |
| Lung | 23.8 | 0.375 |
| Skin (dry) | 46.7 | 0.690 |
| Skin (wet) | 49.8 | 0.670 |
| Bone Cancellous | 22.4 | 0.235 |
| Brain gray matter | 57.4 | 0.739 |
| Brain white matter | 42 | 0.445 |

 During this sleep mode cycle, only standby power is needed to operate the circuit. In dealing with transistor circuits, we have what is known as the device threshold voltage VT, the sub-threshold slope S, and the supply voltage in sleep mode VDD. Using these parameters, the standby power received can be given by this equation:  (Equation 6). As shown in Figure 8, when there is a constant current IO, it is really the construction of the device, namely the threshold voltage, which makes a difference in the amount of standby power that can be utilized. Therefore techniques have evolved as to how to lower the leakage of power in these devices by increasing VT during idle mode. [12]



Figure 8: VT influence on standby power (De Mey 334) [12]

**3.3 Medical Communication Frequencies**

The advancements in telemetry for implantable devices have been accomplished by the study of radio frequency. Manufacturers struggle with creating a module that used a minuscule amount of battery power, giving the device longevity, and lowering cost by, usually accomplished by using small external devices as well. Power and cost are two of the basic things to consider when designing implantable devices but there are several other factors to consider as well. For example, receivers need to be highly sensitive and try to find optimal transmission power to ensure a reasonable operating distance between the transmitter and the receiver. More power and more designs can ensure faster transfer rates between the receiver and transmitter so that large data may be transferred. However, this again raises the question of how much battery power to use. Most importantly the designers have to create some type of secure encryption in order to ensure that personal information remains private. One way to ensure this is through the Medical Implant Communications Service. It is an unlicensed, mobile radio service that transmits data for implanted devices. The FCC has also allocated 14 MHz to establish the Wireless Medical Telemetry Service. This allows health care providers to offer better services to their patients without fear of interference due to other signal on the electromagnetic spectrum. In Table 2 below, the U.S. frequency for medical communications is shown. The FCC has set aside these ranges for implant care and as shown, different ranges have different strengths. [13]

Table 2. U.S. Frequency Spectra for Medical Communications [13]

|  |  |
| --- | --- |
| Frequency Range (MHz) | Power or Field Strength |
| 402-405 (MICS) | -16 dBm= 25 uW effective radiated power (e.r.p.) |
| 608-614 (WMTS) | Less than 200 mV/m at 3 m |
| 1395-1400 (WMTS) | Less than 740 mV/m at 3 m |
| 1427-1429.5 (WMTS) | Less than 740 mV/m at 3 m |

 Since different implants have different abilities, it is important to realize what is called the link budget for these devices. A link budget is the accounting of all of the gains and losses from the transmitter through the medium to the receiver. The budget formula is

 (7)

where PRX is the received power (dBm), PTX is the transmitter output power, GTX is the transmitter antenna gain, LFS is the free space loss or path loss, LB is the loss within body tissues. As seen, designers must take into account several factors in designing implants, even the size of the patient since each centimeter of muscle or fat absorbs power. By estimating these power levels, the sensitivity of the wireless communications receivers and transmitters can be determined. Again there is a decision that must be made between quality and optimal battery life. One way this problem is thwarted is by not having the implants in continuous communication with the receiver. Optimal battery life can also be achieved when implants use a so-called sniff circuit to detect whether or not the external appliance is transmitting at a certain frequency. It is only at this frequency that the circuit “wakes up” and begins the transmission of data. [13]

 The wake up protocol has given rise to the increase in monitoring service for patients. Companies such as Medtronic CareLink Network are supporting several divisions of implantable devices from insulin pumps to glucose monitors. The system is an internet based monitoring system and by 2005 over 10,000 patients were using the system for follow up reports rather than returning to the doctor’s office, saving both time and money [14]. A diagram of the MICS transceiver that uses this important wakeup call is shown in Figure 9 below.

Transit Processing

If Modulator

TX

400 MHz

PA

Wake Up Receiver

Xtal

Ultra Low Power

Wake Up Circuit (250 nA)

Application Interface

Control

Receive Processing

Mode Control Registers

Base Station, Implantable, or Test Mode

Oscillator & PLL

ADC

Filter Detector RSSI

TX

2.45 GHz

Rx

400 MHz

LNA

LNA

Control

Inputs

Figure 9: MICS Transceiver Block Diagram [13]

**4. More Considerations on Modulation Schemes for IMDs Communications**

There has been a concentrated interest in the study of WBAN (Wireless Body Area Networks). This study supports data rates ranging from several kilobits per second (Kbps) up to tens of megabits per second (Mbps). These networks are typically relevant within 3 meters of its source. There are two general topics of these types of networks: in-body systems and on-body systems. In-body applications often interconnect the implanted devices inside of the human body and the apparatus sticking on the human body supports a wide range of medical applications. The on-body systems however serve various other applications between the devices on or around the human body. These applications include medical, consumer electronics, personal entertainment, and many others. WBAN is particularly significant from other existing wireless standards such as WPAN (Wireless Personal Area Network) and WLAN (Wireless Local Area Network). One primary difference is the IT-BT convergent applications implanted into the human body [15].

When dealing with high data rate implant applications such as the wireless capsule endoscope and the bionic eye, we have to take several specifications into consideration. First, the implanted system must be designed so that it can operate with low power consumption. This is due to the small size and capacity of the battery in order to fit inside of the device which must be swallowed or implanted in the body. This device must use a small amount of power in order to prolong the life of the device considering that the battery must last for a long period of time and if the battery were to fail it would be a quite difficult task to replace it. Another issue to be taken into account is high data rate transmission needed in order to ensure that the device works appropriately. Current technology allows us to transmit approximately 2-3 Mbps data rates. This is nowhere near the data rate of approximately 10 Mbps needed in order to send HD images that will more than likely be implemented in future capsule endoscopes. This also causes issues since the signals will be travelling through the body and not through the air. Propagation of signals transmitted through the body undergoes severe degradation due to the lessening affect from various tissues and organs within the human body. This adds to the issue and requires appropriate modulation scheming in order to ensure stable performance conditions in the human body [12]. Another requirement of the device is bi-directional communication. The device must not only accept communication from an outside source but it must also be able to communicate back and feed data back to the source. This makes it possible for the devices outside of the body to be able to control the behavior and processes of the implanted device. One last issue that is essentially the underlying concern with all the previous problems is the small size required of the device. For example, the capsule endoscope is designed to be as small as possible while still serving its designed purpose. This makes the capsule so that it can be easily swallowed through the mouth and can traverse through the internal organs without causing any bodily harm.

Many of the issues associated in the design of these devices were experienced and the effects of improper implementation were felt in the early designs of the wireless endoscope. The first wireless endoscope was introduced by Given Imaging and was given the name M2A. This device is used widely today; however, some of its shortcomings were discovered and have been corrected since its original conception. This device for one does not meet the requirement of producing high resolution images. It suffers from low resolution and severe distortion of images when physicians zoom in for detailed diagnosis. Another issue with this particular apparatus is that it employs unidirectional transmission meaning that it cannot both send and receive data. This has caused serious control problems in diagnosis. These control problems have caused unintentional oversight on the part of physicians. This oversight may seem minor but it could potentially lead to a non-diagnosis of important spots that may become infected from disease and lead to a major problem in the body. This is why the functions of real-time, low power, high resolution, and a bi-directional communication link are all highly demanded for medical imaging applications. Another issue in conventional implanted devices is the band of frequency allowed and the communication data rate between the devices. Typically the conventional implanted medical device uses the frequency band of 402-405 MHz MICS (Medical Implant Communication Service). This however permits implantable devices to only communicate at a low data rate. This constriction is due to the small channel bandwidth. For real-time high quality image transmission that will support a data rate of up to 200Mbps, a new and wider frequency band must be allocated instead of the MICS band[13].

Currently, in most conventional implantable wireless devices for data transmission of a few Mbps, the low power modulation techniques have been chosen. The primary reason for this decision is the characteristic of low-power techniques that allow the devices to be operated at least for several hours with small-sized batteries. For this reason, low power consumption has been one of the top priorities in deciding and implementing a modulation technique for WBAN in-body applications. However, in the high data rate transmission, it is required that a high sensitivity modulation and demodulation approach be chosen in order to overcome the serious reduction of transmitted signal strength in the human body channel. In a coherent system, binary phase shift keying (BPSK) is 3dB better than the performance of frequency shift keying (FSK) and on-off keying (OOK). This means that FSK and OOK systems should transmit 3dB more power in order to be as efficient as BPSK. However, the BPSK transmitter generally requires back-off for linearity of a power amplifier (PA). Therefore, eventually FSK or OOK will perform better than BPSK in terms of power consumption in the transmitter [15]. The OOK system is fairly easy to implement due to their simple architecture. Their transmitters also require less power than that of the FSK. This is due to the transmitter signals of OOK operating alternately between on and off modes. While the OOK and FSK systems seem to be the better of the choices, they have a weak point in terms of low spectral efficiency. The spectral efficiency of the FSK can be improved by applying a Gaussian filter, but with this being done it has to undergo the lack of link margin for the high data rate applications that can provide a speed of 20Mbps enabling high-definition image streaming. Also to improve spectral efficiency, MPSK could be used; however, in this case the transmitter would need more power to eliminate significant non-linear distortion to the transmitted signal. Symbols with a low-level envelope are more advantageous than symbols with a high-level envelope on the power efficiency of a transmitter. In this context, pulse position modulation (PPM) is more efficient than prevalent modulation such as PSK. The symbol signals of this type of modulation have a zero- or silence-envelope. One drawback with this however is that it has poor bandwidth efficiency.

A new modulation scheme has been proposed that has advantages in terms of power consumption and performance for WBAN in-body communication systems [16]. This scheme is called phase silence shift keying (PSSK). It is a type of phase shift key scheme; therefore, it is more bandwidth efficient than the orthogonal modulations such as PPM, FSK, OOK. Also great power efficiency can be achieved in that every symbol of PSSK has a zero-envelope. In the case of a symbol of M-ary PSSK, one bit determines the silence envelope position of the symbol and (log2 M-1) bits determine the phase of the symbol. The transmitter of PSSK can save the amount of power needed to transmit by 3dB. This is due to the fact that the transmitter of PSSK transmits the energy of signals during a half period of a symbol instead of a whole period. Another advantage relates to the probability of error. The minimum distance between two adjacent PSSK symbols is greater than that of PSK for M>4. This is shown in Figures 10, 11 below. The modeling of the system is also shown below through the formulas used to achieve them.

111

101

100

000

110

010

001

011

Figure 10: 8-PSK Constellation diagram [16]

001

101

000

011

111

100

010

110

(a)8-PSK (b) 8-PSSK

Figure 11: Constellation diagrams of (a)8-PSK and (b)8-PSSK [16]

The following illustrates common results on digital modulation for IMD communications. Here Re{c} means the real part of the complex number, exp[∙] is the exponential function, fc is carrier frequency, θm = 2πmod(m,0.5M)/0.5M, T is a symbol period, Bm= mod(Am,1). α (t) is the pulse shaping function having the square root raised-cosine (SRRC) spectrum where γ is the roll-off factor.

 (8)

**5. Mitigate Electromagnetic Interference in IMD Communications**

In [14] a new method is proposed to reduce the effect of electromagnetic interference (EMI) due to wireless communication devices on IMDs. The method proposed by Kawamura et al. does not require any internal modifications to the IMDs. Instead, the method makes use of a mitigating signal. The mitigation signal is a radio frequency signal that is transmitted in the idle periods of the wireless communication device. The use of the mitigation signal reduces the low frequency noise generated internally by the IMD. Related work has concluded that limiting EMI has to do with defining a minimum safe distance. Preliminary work has shown that the minimum safe distance of stationary RFID devices to be 22 cm. Minimum safe distance is interpreted as the distance at which EMI is not an issue. However, the Ministry of Internal Affairs and Communications (MIC) has reported that high power UHF RFID reader/writers may affect IMDs at distances of 75 cm. The mitigation technique proposed by Kawamura et al. is experimentally proven to improve the minimum safe distance.

Kawamura et al. discuss the internal operation of IMDs and why EMI can be dangerous to their operation. RFID reader/writers generate signals which are captured through the nonlinear characteristics of the internal IMD circuit. This is caused by inference on the operational amplifier of the IMD circuit. The typical nonlinear characteristics of an IMD sensing circuit are expressed as follows:

 (9)

where $v\_{i}$ and $v\_{o}$ are input and output voltages of the sensing circuits. The coefficients ($A\_{i}$) are the corresponding coefficients of their respective orders. External radio frequency signals (electromagnetic fields) generate an internal voltage on the circuit, $v\_{AM}$.

 (10)

In (10), B and m are the amplitude coefficient and modulation index. Also, $ω\_{c}$ and $ω\_{m}$ are the carrier signal frequency and signal frequency. Kawamura et al. show that combining (9) and (10) produces the following low frequency noise in the IMD circuit.

 (11)

 Two main cases are discussed in this paper which would lead to IMD malfunction: the signal shown in equation 3 is similar to the ECG (electrocardiograms or the human heartbeat signal) signal and cannot be removed but the internal protection functions of the IMD, or the signal shown in equation 3 is recognized as noise and the noise reversion function of the IMD is initiated [14].

 The radio frequency signals generated by electromagnetic fields can be seen in figure 12 (blue curves). The mitigation signal proposed by Kawamura et al. will be placed in the idle periods (i.e. figure 17). It was pointed out that their principle of applying a mitigation signal is only applicable to signals time-varying envelope curves (amplitude and pulse modulation, and intermittently transmitted signals). The main idea of the mitigation signal is that it suppresses the time variation in the envelope curve causing the low frequency noise signal produced internally by the IMD to be reduced. Consequently, maximum interference distance is improved.

  

Idle Period

Figure 12: Example Signal Figure 13: Example Signal + Mitigation Signal

 Three types of pacemakers were provided by the Pacemaker Committee of Japan for the experiments. In order to generate the RFID signal with the mitigation signal, they used two signal generators and output the signals through one single dipole antenna. Also, the frequency of the RFID signal and mitigation signal was controlled by a function generator. A human torso was artificially simulated and each of the pacemakers was connected to an ECG signal generator. The operation of each pacemaker was monitored by an oscilloscope and a chart recorder. The set-up can be seen in figure 14 and figure 15. Their experiments were carried out in an electromagnetically shielded anechoic chamber. The procedure Kawamura et al. followed included four steps. Step 1 included setting the sensitivity of the pacemaker to its maximum value and setting the refractory period to the minimum value [14]. The refractory period of a pacemaker is the period of time immediately following pacing or sensing. The purpose of the refractory period is to stop inappropriate signals from influencing the pacemaker following pacing or sensing. Setting the refractory period to a minimum allowed Kawamura to more accurately test the EMI influence on the pacemaker. Step 2 was to find out the maximum interference distance. In order to record the maximum distance, they increased the distance between the dipole antenna and the simulated torso. The signal used in step 2 was used without the mitigation signal. Step 3 was similar to step 2 but included the mitigation signal. Also, they varied the frequency of the mitigation signal. Lastly, step 3 was to repeat the above procedures for the different operating modes of the pacemaker.

Signal Generator # 1

RFID Signal with Mitigation

Function Generator

Signal Generator # 2

Figure 14: RFID signal set-up [14]

The experiments showed that the use of the mitigation signal can significantly reduce the effect of EMI. The method was tested on three different pacemakers and showed that the maximum interference distance could essentially be halved if the frequency of the mitigation signal was within 10 MHz of the RFID signal. They also showed that if the frequency of the mitigation signal was within 3MHz of the RFID signal then a reduction of 90% was achieved.



Figure 15: Pacemaker set-up [14]

**6. Security for IMDs**

Safety and utility goals often have conflicting requirements that create tension in device design procedure. IMDs should have appropriate data access methods readily available for authorized entities. Data access allows medical staff to gain access to valuable patient information during times of emergencies. Also, the data should be accurate. An IMD should make sure authorized entities know its presence and type. Entities should also be able to make modifications to the IMDs settings. In addition, authorized entities should be able to make software upgrades whenever necessary. In the future, multiple IMDs will need to communicate together in multi-agent systems. For example, a closed-loop insulin delivery system might automatically adjust settings based on feedback from an additional monitor. If the IMD fails, the manufacturer should be able to retrieve a system log from the IMD that details the operational history. The final utility goal discussed in this paper is resource efficiency.

**6.1 IMDs Security and Privacy: Challenges and Directions**

 Only authorized entities should be allowed to access or modify the IMD. Two different types of authorization are recognized. Personal authorization allows certain people with access to perform specific task. For example, a patient’s primary physician could be allowed access to the IMD after validating his/her personal identity. Role-based authorization is when an entity is authorized to certain task on the IMD based on its role. The IMD manufacturer might also be allowed a role-based authorization to the IMD. Also, if an entity is trying to communicate with multiple IMD’s, the entity must be able to only communicate with the intended IMD. However, authorization can become highly sensitive in certain context. For example, in emergency situations the authorization rules should be relaxed to allow for medical staff to help the patient. In contrast, the IMD should be closed to adversaries. For example, an adversary should not be able to mount a successful denial-of-service (DoS) attack on the IMD. A denial-of-service attack is when the adversary tries to overwhelm the IMD [18]. The effects of a DoS attack on an IMD could cause the device’s battery to drain, overflow its data storage media, or jam the communication channels. IMD’s should also only allow authorized entities to modify its software and settings. For example, physicians should place bounds on what the patient is allowed to modify on the IMD. Patients could change the amount of medication being injected through their body within a certain range. The existence of IMD’s should be able to be concealed from an adversary. An adversary could use the knowledge of IMD’s to harm or discriminate against a person. In the event that a device reveals its existence, the type of the device should remain hidden. The device type should only be disclosed to certain authorized entities. Consistent with medical ethics, an unauthorized entity should not be allowed to view private information about the history of the device. Finally, the IMD’s patient properties such as name, medical history, and diagnoses should not be allowed to be exploited by an outside adversary.

Adversaries can be placed into these categories: passive, active, coordinated, and insiders. Passive adversaries eavesdrop on signals of the IMD. Active adversaries can interfere with communications and initiate malicious communications with the IMD. If two or more adversaries are working together then they are said to be coordinated adversaries. Insiders could be healthcare professionals, software developers, and anyone who has a working knowledge of the IMD security architecture that would use this information to cause harm to the patient.

 There are certain tensions that exist between the security and privacy goals (mentioned above) and traditional goals of utility and safety (also mentioned above) [19]. Consider the tension between security and accessibility. Two scenarios illustrate this tension. In brief, the first scenario involves a patient in an emergency situation, possibly in a foreign country. The patient enters the emergency room where the staff identifies his/her IMD’s and extracts information, both personal and medical (if the patient was without ID). In the second scenario, the patient explicitly controls who is authorized to interact with his/her IMD’s. The IMDs use strong access control and encryption techniques to prevent unauthorized entities from accessing its IMD’s. If the patient was placed in a foreign emergency room (unfamiliar and unauthorized equipment), the patients IMD’s would not allow access. The emergency room staff would not be able to access any of the patient’s information regarding his current and past medical history/problems. Also, if the existence of the patients IMD’s was unknown (due to security techniques) certain medical procedures could be harmful to the patient. These two scenarios illustrate the tensions between security and accessibility. One solution posed would incorporate back doors for emergency-room equipment to access IMD’s. However, adversaries could take advantage of those back doors.

 Next, the tension between security and device resources is highlighted. Adding highly complex security to IMD’s can cause the device resources to be strained. While the device resources are strained the effect of DoS attacks can be amplified. The tension between added security measures for IMD’s and device resources can be easily seen from the above example. Tension also arises when discussing security versus usability. It is convenient to have long distance communication with IMD’s (in-home monitoring). However, the wider range wireless communications increases the exposure to passive and active adversaries. Also, the user interface should not be overcomplicated with added security measures.

 Future research for the security and privacy involving IMDs is proceeding in diverging directions. The first research direction is a system where a signed credential is granted from the manufacture or primary-care facility. This option is under the assumption that the emergency technicians’ external programmer is always connected to the internet. This proposed method allows the manufacturer or primary-care facility to have ultimate control of who can access the IMD. However, if the internet connection between the technicians’ programmer and the device manufacturer or primary-care facility is slow then safety concerns will be introduced or increased. Another option discussed by the author’s deals with allowing specific medical equipment access to the IMD. This would only work if the medical equipment could be validated and the lost or stolen equipment could be stopped accessing the IMD. This approach leaves the IMD exposed to adversaries in short time periods. In addition, the IMD programmers could be required to have a secondary authentication card that would further limit adversaries from accessing legitimate medical equipment. The downfall of using a secondary authentication token is decreasing usability and increasing emergency medical staff response time.

 The use of an audit log could help to deter malicious activities on the IMD. All the IMD settings and all data access could be recorded on an encrypted audit log on the IMD. At each clinical visit the IMD’s audit log could be removed to check for any malicious activities. However, the external device that downloads the IMD’s audit log would have to be tied to the IMD itself. If not, then adversaries could use external devices to download IMD audit logs and use the information maliciously. Also, a patient could be made aware of the device’s security status via alert signals. Currently, some IMDs signal battery depletion by an audible signal. The same alert system could be used to alert the patient any time the IMD establishes a wireless connection with an external programmer. After the patient receives the signal he/she could quickly visit primary-care facility.

 Environmental factors could be used as authorization. Most IMDs have accelerometers already built-in. These accelerometers could be used to sense significant environment changes such as walking out of the doctor’s office and close the communication when it senses those changes. This technique could be used when the physician opens communication with the IMD and activate the device for programming. In some cases, the activation allows the physician to program the device from long distances and at longer periods of time. The longevity could extend past the duration of the clinical check and leave the patient susceptible to adversaries.

**6.2 IMD security: Proximity-based Access Control**

 Access control as defined as a potentially malicious reader who tries to gain access to the IMD for data acquisition purposes or to send commands [20]. One scheme is based upon ultrasonic distance-bounding and allows IMDs to allow access to only devices that are in its close proximity. A protocol to support the proposed proximity scheme has begun testing. The method proposed is a form of access control based on close ranges. This type of access control has advantages but more importantly disadvantages. An attacker could use a high-gain antenna and transmitter to communicate with the IMD far outside the intended range [21]. The difference in the proposed method of proximity-based access control from conventional methods is that it guarantees that attackers cannot access the IMD from far away. This is achieved through the use of messages that are cryptographically tied to the distance bounds of the IMD.

 There are two main modes of operation for an IMD with proximity-based access control. A normal mode, in which a reader needs the shared key to access the IMD, and an emergency mode, where a reader can just be within a close range of the IMD. The emergency mode is needed for m Shared keys could either be preloaded on the IMD or stored on the external devices discussed above. The attacker is categorized in two scenarios. First, the attacker could wish to establish a connection with the IMD to steal medical data or change settings. Second, the attacker could be interested in preventing care of the patient [22].

 One proposed protocol is based upon device pairing where the reader must first run the device pairing protocol and generate a shared key. The shared key will then be used by the reader to gain access to the IMD. The protocol uses ultrasonic distance bounding to determine the operating distance of the reader. The first step in the protocol is the prover picks a secret exponent p and a nonce Np and then computes gp. Timing is very important with this protocol, so gp is computed in advance. In order to initiate the protocol the prover sends a “Hello” message to the Verifier. Once the verifier receives the “Hello” message it will choose Nv and start a rapid bit exchange. The rapid bit exchange procedure is used to record the flight time of a single bit of Nv . The reason flight time is calculated using single bit transmission is so that distance shortening attacks are avoided [23, 24]. The prover receives the first bit of Nv at time T’1. The assumption is then made that T1=T’1=T’’1. This assumption is relevant because the reply from the prover after the first bit of Nv is sent via the sound channel and the speed of sound is slow compared to the speed of radio messages. The prover XOR’s the first bit of Nv with gp and sends it back to the verifier to calculate the distance bound. The equation used to calculate this distance bound can be seen below:

 (12)

where d is the distance and vs is the speed of sound in meat (approximately 1500m/s). If the calculated distance is greater than some predefined minimum value (used for close proximity) then the protocol will terminate. The second half of the protocol is designed to ensure that the verifier is talking to the IMD within its proximity. The protocol accomplishes this by starting another rapid bit exchange between the prover and verifier and performs the same type of calculations as described in the first part of the protocol [20].

 The security that this protocol offers is designed for attackers that are far away. However, since this protocol is based upon a close proximity, in most cases the attacker would have to almost be in contact with the user. This security assurance from far away attacks is accomplished by tying a specific distance between the prover and verifier. The attackers discussed are assumed to be incapable of sending data on the sound channel faster that the speed of sound. The first possible attack is the attacker could guess Nv and generate sound messages in advance. The attacker could use Nv to pretend to be close but the attacker would have to send the messages at the appropriate times. Hence, Nv needs to be random in this protocol. The attacker who is farther away could receive the bits of Nv at roughly the same time as the prover but when the attacker sends the XOR’d message it will not arrive in time. This is how the verifier can tell if the attacker is far away and also illustrates the main principle of the proposed protocol of distance binding.

**6.3 Communication Cloakers for IMD Security**

A communication cloaker is a wearable device that is computational in nature and can communicate wirelessly [25]. A communication cloaker is different from the already used Medical Alert bracelets because the cloaker is computational and has wireless capability. The communication cloaker presented provides security while the cloaker is worn but also provides fail-open access to all external programmers if the cloaker is not being worn. The proposed communication cloaker will allow pre-specified commercial programmers to have access during normal clinical visits. The communication cloaker will also provide security during everyday wear. In case of emergency situations, doctors with unauthorized commercial programmers can remove the cloaker and be granted access.

There are four tensions associated with the design of the communication cloaker. The first is the tension between security and open access during emergency situations. Second is the tension between security and privacy under adversary conditions. IMD’s that communicate wirelessly open up vulnerabilities to adversaries because the attacks can be mounted from greater distances. Third, the added security measures of IMD’s should not hinder the battery life of the IMD. Finally, the response time of the IMD should not be hindered by added security. Any additional security should allow the IMD’s functionality to be maintained.

A security system has been proposed in which the presence of the communication cloaker (computational in nature) causes the IMD to ignore incoming communication. The absence of the device causes the IMD to fail-open. The proposed design mediates communication between the IMD and pre-authorized parties. During emergencies, medical staff can remove the cloaker and gain access.

The cloaker is assumed to first verify that the external programmer is authorized to communicate with the IMD. The cloaker is able to proxy the communication between the programmer and the IMD or the cloaker can hand off an access key to the programmer. The first approach allows the cloaker to log the communication data between the programmer and IMD for future use. The latter approach might provide a reduction in communications latency and the cloaker can be removed without disrupting the current communication session. The cloaker can be pre-loaded with access keys of external programmers. Again, when the patient is not wearing the cloaker all communication is allowed. The detection of the cloaker by the IMD is of paramount importance for without this property, adversaries could trick the IMD into thinking that the cloaker is not present when it actually is. The IMD could query the cloaker whenever it receives an external communication request. With this approach, constant keep-alive messages can be avoided in non-adversarial conditions. However, this approach can expose the IMD to denial-of-service attacks against the battery [26]. Two possible keep-alive variants are discussed. First, the IMD will initiate the keep-alive messages and the cloaker will send acknowledgements that the IMD must receive. Second, the cloaker sends keep-alive messages. To prevent the messages from revealing private information additional encryption and authentication is required. The wireless packets can also be addressed with non-persistent identifiers [27]. The time interval of the keep-alive messages creates a tradeoff between safety and battery life; shorter intervals allow for quicker fail-open in emergencies, and a longer intervals the battery is more susceptible to drain.

**6.4 Summary of IMD security**

The ideas presented discuss the security issues prevalent in IMD design and also how the design of IMD security should not hinder the performance of the IMD. Each of the security techniques takes a unique approach to solving the many security issues. Proximity-based access control would require and adversary to be within a short distance of the IMD in order to communicate with it. Communication cloakers can implement advanced encryption and transfer protocols that control access to the IMD. Solutions could range from these proactive approaches to the passive data logger which would record all data and data accesses of an IMD. Each approach has benefits and drawbacks. A sample of these may be found in Table 3 where the different solutions are presented along with their differences. As new IMDs with wireless telemetry develop, a combination of these techniques may be implemented in order to ensure the reliability and security of future IMDs and their patients.

 Table 3: Pros and Cons for several IMD security methods

|  |  |  |
| --- | --- | --- |
| Security Method | Advantages | Disadvantages |
| EMI Reduction using Mitigation Signal in [17] | -Does not require any internal modification to the IMD-Reduces the maximum interference distance | -Does not prevent attacks, only makes them very unlikely |
| Proximity-based access control in [20] | -Secure-Very dependent upon time-Pairs IMD and external programmer with distance-Guarantees an attacker cannot access the IMD from far away-Two modes of operation: Normal (uses shared keys) and Emergency (a reader can access the IMD as long as it is within certain distance) | -More complex than other methods |
| Issuing a signed credential key [19] | -Simple-Allows manufacturer or primary-care facility to have complete control over IMD | -Assumes that the emergency technicians’ external programmer is always connected to internet-Stolen external programmers-If internet connection is slow then safety issues can arise. |
| Allowing specific medical equipment access only [19] | -Simple-Only allows predetermined equipment to have access to the IMD | -Leaves patient exposed to adversaries for short time periods-Stolen equipment-Could need second authentication token which would decrease usability and increase response time for medical staff. |
| Audit log [19] | -Records all IMD settings and all data access-Encrypted-Ability to check for malicious activity | -External programmer that reads audit log would have to be tied to IMD  |
| Environmental factors [19] | -Built-in accelerometer-No internal modification of IMD | -If used alone, then the IMD could be susceptible to malicious activity |
| Communication cloakers [25] | -Computational in nature as opposed to medical alert bracelets-Wireless communication capabilities-Two modes of operation: Normal and Emergency-Can proxy communication between IMD and programmer-Can hand off an access key to the programmer | -Wearable-Possible denial-of-service attacks-Complicated |

**7. Antenna Design for IMDs**

One major aspect that goes into the design and configuration of IMDs is the design of the antenna. The design of the antenna is a very intricate and vital part of the IMD. It must have the correct design criteria to be large enough to transmit a signal outside of the body but it must also be small and discrete enough to actually fit inside the body and to be mobile without causing any harm or problems to the organs in the body. While the IMD must be designed to ensure that there is no damage done to the body, it also must be designed to prevent damage from being done to the IMD from the body. The IMD must be sturdy enough to resist the rigid terrain of the inner body yet delicate enough not to cause any harm to the muscles and ligaments.

IMD applications have many requirements for RF antennas. The antenna must have very small dimensions. This enables the antenna to fit onto the IMD and not cause any conflict inside of the body. The antenna must also be easily implemented with biocompatible materials. One particular type of antenna that has become quite prevalent is the microstrip antenna. Microstrip antennas have many attractive features that make them desirable for use with IMDs. They are of low profile, light weight, easy to fabricate, and they are conformable to mounting hosts [28]. All these characteristics make this particular category of antenna fit the description for the job of being used for IMDs. While these devices have many advantages for use with IMDs, they also have a few disadvantages as well. One significant disadvantage is the impedance bandwidth and efficiency associated with these antennas. One example where this particular antenna may not be applicable is with an IMD such as a wireless capsule endoscope system. With this system, the "smart" capsule moves through the digestive tract and takes pictures. Throughout the digestive tract the environment changes significantly. This may make it difficult for the antenna to gain the needed impedance bandwidth and efficiency to work properly [29]. This would cause the system to be out of work temporarily, if not permanently.

One way of facing this problem is to broaden the substrate thickness of the antenna. This can be done by using a substrate with a small tangent loss. Theoretical analysis shows that increasing the substrate thickness can broaden the impedance bandwidth and reduce the dielectric loss of the antenna. This helps to enhance the radiating efficiency of the antenna. It also helps to improve the overall efficiency of the antenna.

The first aspect of the design and implementation of an antenna for an IMD that is to be considered is its geometric composition. The primary issue and principle is miniaturization. The antenna is desired to be as small as possible yet include all the appropriate assets and qualities to complete its designated task. One particular approach to the miniaturization of the antenna is to use a substrate of a large permittivity. The only problem with this approach is that it has a negative effect on the impedance bandwidth. Another solution is to lengthen the excited patch surface path so as to enhance the effective electrical dimension of the antenna. This can be done by inserting slits or slots on the patch. Another way of doing this is to use a U-shaped or folded patch or to simply use irises [30, 31]. The problem with this is that the use of the last two procedures can require a complex process of fabrication. However, the gain and impedance bandwidth of a microstrip antenna are positively related to its effective volume. While this is a particularly good aspect, this still limits the number of slits and/or slots that can be put on the antenna and still give a beneficial effect. Therefore, the implementation of slits and/or slots does indeed increase the efficiency of the antenna, but it does have diminishing returns once a certain point is reached. Yet another technique taken in considering the geometry of an antenna and maximize miniaturization is to use an edge-shorted patch. This can be done by connecting the edge of a radiating patch to the ground by shorting the wall, shorting the plate, or shorting the pin. This particular approach can reduce the antenna's physical length by half because the shorting component makes the antenna act as a quarter-length structure [29].

 Another characteristic that is taken into effect when attempting to optimize an antenna for an IMD is the gain and impedance bandwidth enhancement. This is a drawback of the microstrip antenna. The microstrip antenna is capable of miniaturization; however, it usually experiences narrow impedance bandwidth and low radiating efficiency. These flaws significantly limit the application of this device. These problems have been confronted with several solutions. One solution is to increase the substrates thickness in order to compensate for the decreased thickness of the compact antenna. This allows the antenna to be made much thinner than it normally would and still receive the proper gain and impedance bandwidth. The problem with this solution is that the antenna tends to be entirely inductive. This forces the antenna to resonate less and less as the thickness of the substrate increases until it completely stops resonating. Another suggestion to correcting this problem is to induce chip-resistor loading. This will lower the quality factor of the antenna and as a result broaden the impedance bandwidth. Once again there is a flaw with the solution [29]. The flaw is that the chip-resistor greatly influences the radiating efficiency. The last solution to enhancing the gain and impedance bandwidth is to insert slits or slots on the ground plane. This will lower the quality factor of the antenna and broaden the impedance bandwidth just as with inducing a chip-resistor load. However, as with inducing the chip-resistor load, this is not very efficient for a miniature antenna that would be suitable for an IMD.

**8. Power for IMDs**

All IMDs require some form of electrical power. This electrical power is usually supplied by a battery that is embedded inside of the device. Presently there is research being done for the development of a rechargeable battery that can be used for this purpose but currently for the time being non-rechargeable batteries are being used. One problem of this configuration however is the longevity of the battery source. After the battery has reached the duration of its lifetime, either the battery or sometimes even the entire device must be surgically removed and replaced. This lifetime for IMD batteries is variable depending on the power requirements of the IMD and the amount of power that is capable of being stored in the battery. Batteries in pacemakers and defibrillators have been estimated to last approximately 5 to 10 years. However, the lifetime of a more complex and intricate device may be much shorter. For example, the approximate lifetime of implantable stimulators is only 3 to 5 years. This inconvenience leads IMD designers to a rather difficult decision. Should one choose to have a larger battery that can have more storage but makes the device undesirably larger and difficult to maneuver or should they simply apply a smaller battery? With a smaller battery however, one must consider the significantly less storage of the battery. This lack of storage will essentially lead to more surgical explants and replacement. As mentioned above, this will happen at least once every few years. This question has led to much controversy and research on this particular issue.

**8.1 Wireless Power Charge for IMDs**

A transcutaneous power supply is produced through inductive power transmission on coupling coils. This method of power production is efficient for our current technology but it is not considered the best alternative. It is used in many devices that require a rechargeable power supply, such as rechargeable implantable spinal cord stimulators. The need for this is that surgeries to replace non-rechargeable batteries in some IMDs can cause injury or death [25]. This method has been studied extensively in recent years in hopes for an improved solution. These studies have primarily been focused on the optimization of transmission with relation to the efficiency and stability of the inductive link. E. S. Hochmair showed the effects of the coupling coefficient k in an inductive link and the circuit design to acquire a better efficiency of inductive link in his studies in 1987 as shown in (13). He studied the geometric majorization for the enhancement of the coupling coefficient between two magnetically coupled coils to ameliorate the efficiency of inductive link [32]. In addition, he considered the circuit of the system. In his experiments he used a class-E amplifier to evolve the efficiency of an inductive link. He developed a variety of circuits and systems aimed at the attainment of a stable voltage or efficiency. In order to optimize the inductive link, it is necessary to consider the conversion efficiency η. In these experiments, the designed model is set up with a compensative capacitor in series for the primary coil and a compensative capacitor in parallel for the secondary coil. These are both used in order to describe the relationship between the coupling coefficient and the conversion coefficient. The equivalent load resistances in each stage, along with the conversion efficiency, are changed with the load resistance in order to study the several different stages when charging the implantable battery. These stages of charging the implantable battery include the preparatory charging stage, the constant current stage, and the constant voltage stage [33].

 (13)

The basic topology of wireless power transformer consists of three primary parts: an external power amplifier tank circuit, a wireless inductive link, and an implanted receiver. The external part creates a suitable variable frequency signal that is amplified and then added on the primary coil. This coil then generates an alternating magnetic field for the inductive link. The receive coil in the receiver can gain power from this magnetic field. However, there are leakage inductances on both coils due to mutual inductance [33]. This is represented by M in (13). These leakages were accounted for by the external power amplifier tank circuit and the receiver which were added as capacitors in series or in parallel with the coil. In order to gain a higher voltage in the primary coil, a capacitor can be put in series in the external circuit. However in this experiment, a capacitor is placed in parallel and the load receives power after the rectifier. The model of this circuit is below (Figure 16).



Figure 16: Block diagram of a wireless power transmission system [33]

**8.2 Thermoelectric Devices for IMDs**

One particular response to this issue is the use of temperature difference as a form of producing electrical power. This temperature difference can be produced from one of two sources. One source of this difference is the temperature difference between the inner surface of the skin of an individual's body and the core body temperature of the patient. The second source of temperature difference comes from the temperature difference within the IMD. This technology can be used to greatly increase the lifetime of all IMDs. This power source is indeed very efficient as well. Data shows that this specific prototype can be used to produce more than 70µW with as little difference in temperature as 0.3-1.50C [34]. As seen below from the specifications of the implantable pulse generator, this temperature difference is easily produced within a device. There is currently an experimental example of this concept being put into use. There is also more thin-film technology that allows for extremely thin-profile and lightweight devices. This technology allows for film that is 100 times thinner and 100 times more lightweight than old technology. There has also been a major improvement in the thermoelectric material figure of merit. This model has been implemented as Figure 17. This power accommodation procedure is often simply called a thermoelectric (TE) device.

Table 4: Specifications and Power Demands of an Implantable Pulse Generator [34]

|  |  |
| --- | --- |
| Power consumption | 70-100µW |
| Voltage required | 3-4V |
| Temperature differential available | 0.3-1.70C |
| Size | 6.8 cm2 and thickness < 5mm |

70-100µW

towards core of body

Tcold = 360C

towards inner surface of skin

ΔT = Thot - Tcold = 1.00C

Thot = 370C

Figure 17: Model of Temperature Difference Power Supply (TE device wired to a pacemaker) [34]

This device has been researched and put under much scrutiny. The performance of TE devices with large numbers of elements (N) has been extensively studied and modeled in many graphs and equations. One particular relationship of TE devices shows that as the number of interconnected elements increases, a larger voltage (VOC) can be generated with a smaller change in temperature (ΔT). The only disadvantage to this approach is that by doing this one must utilize a small short-circuit current; however, this technique still produces nearly an identical amount of electric power. This procedure would allow for the direct use of the power generated without the need for DC-DC power conversion. This direct use of generated power would be used to directly drive the pulse generator electronics. The equation for this mathematical manipulation and permutation is shown in (14). This equation relates the open circuit voltage (VOC) to the number of elements (N) and the change of temperature (ΔT). In this equation the values of αp and αn are given as approximately 207µV/0C and 260µV/0C respectively. These values represent the Seebeck coefficients of n- and p-type super lattice elements. Through simple manipulation and observation of this equation one can deduce that as the number of elements (N) increases, the amount of temperature change (ΔT) needed to produce an open circuit voltage (VOC) is greatly decreased.

The following is open circuit voltage in terms of the number of elements and the change in temperature,

 (14)

The power levels needed for pacemakers and other similar IMD devices are easily achievable with current TE technology. With as little as a module area of 0.16cm2 and with a temperature difference of only 2.70C one can produce nearly 1000µW of power [34]. This is and will become very useful in IMD devices as a means of producing the needed power in the near future. The only problem is the need to produce a sufficient voltage level to directly operate and maintain the electronics associated with and implemented into IMDs. Conventionally, TE devices are low-voltage, high current devices. This means that they require a substantially large level of current to produce a relatively small amount of voltage. One way to remedy this issue is to implement a larger number of TE couples connected in series. However, in order to do this one must discover a way to connect TE couples in series. One way of doing this more easily is to produce a manufacturable wafer scale thermoelectric process. This has already been done by RTI [35]. Using the wafer scale approach, modules with large numbers of elements can more easily be built. Some of this experimental data and an example schematic of a procedure to do this are shown below (Table 5 and Figure 18).

Table 5: Experimental data produced with TE modules at with temperature differentials of 1 to 30C [34]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Type of TE Module Fabrication | Number of couples (N) | ΔTi | VOC(mV) | Pmax(W) | Area(cm2) |
| Pick & Place  | 4x4=16 | 0.8 | 5.5 | 140 | 0.09 |
| Wafer-Scale | 3x10=30 | 2.7 | 41.8 | 980 | 0.16 |

****

Figure 18: Schematic of a wafer scale thermoelectric process [34]

**9. Wireless Switch Design**

One matter that is becoming an issue with IMDs is the wireless switches that have been created and designed for IMDs. These switches deliver energy to the actual device. This is performed by means of wireless energy recovery and wireless identification, and consumes no standby power. Many of the common modern-day devices complete this task by means of miniature batteries as power supplies [36]. One particular example of this is the magnetism stimulated dry reed switch. This device is often sealed inside of the IMD and can be used to power on or power off the electrical system of the IMD. It can also be used to generate other control signals.

While the dry reed switch is often used for IMDs and is currently one of the best power solutions in use today, it does have several disadvantages. These flaws are being researched and remedied by many scientists and researchers all around the world. One disadvantage is the permanent magnet or electromagnet employed by the dry reed switch. This essential apparatus makes the manufacturing, transportation, storage, and use of the IMD very difficult and complicated. The dry reed switch is made of glass and metal thus making it very fragile. If this appliance were to be jarred the wrong way, then the switch could quite easily be broken thus leaving the IMD powerless and incapable of performing it’s given function. Not only this, but the broken particles could endanger the patient. The size of the dry reed switch also serves as a barrier and a drawback. The dry reed switch's size may be too large for use in particular devices and cause a problem in the design of miniature IMDs. Yet another disadvantage of the dry reed switch is its vulnerability to electromagnetic noise and disturbance [37]. This is a major factor in that a malfunction in such a device could have serious effects on the patient. This could cause a series of problems. It could cause IMD power leakage, malfunctions, or it could even potentially be fatal. This indeed shows a very serious defect that serves as a sever risk to the patient.

One alternative to this is the use of RF signal receivers as a replacement to be employed to switch and control the IMDs. These devices are being considered but they still have drawbacks. The IMD would require the signal receiver to work at all times or at least on a periodical increment to listen for possible external commands. This would cause a problem for the RF signal receiver. The signal receiver requires a considerably excessive amount of energy to complete such a task. The IMD has a restricted power supply and the extra required power needed by the RF signal receiver would be too much for the IMD to manage, produce, and supply while still completing its primary tasks.

One concept to avoid the above complication is adopting a passive RF signal receiver in the place of the wireless switch [38]. In this particular notion, the RF receiver switches a wireless energy recovery block. This energy recovery block will collect energy from the received RF signals and deliver this energy to the switch circuit. Figure 19 also shows how the circuit is expected to operate. The switch is to be operated via an external signal source. This signal will be 915 MHz RF signal with amplitude shift keying (ASK) modulation. Each RF signal will hold and carry an ID and operation command that will be delivered to the desired destination according to the identification labeled on the diagram. The energy recovery block collects energy from the received RF signal and generates voltage. This voltage is then transferred to supply other circuit blocks. The clock and data recovery (CDR) block will recover the clock and data carried in the RF signal. The ID recognition block ensures that the ID received matches the local ID. The command recognition block checks to make that the command is valid for the particular location where it is delivered. If both of these criteria are met, then the block generates an operation signal that reflects the received signal. This operation signal level is then translated by the level shifter in order to control other circuits in the IMD. The control signal is used primarily to enable or disable the LDO in the main controller integrated circuit of the capsule endoscope. Through all this work, signal transmission, and signal reception there is no current consumed from the battery. The size of this capsule is very small. The size of this device is comparable to that of a coin.

Such a design would negate the excessive energy needed by the switch from the battery. Not only would this eliminate the need for extra power but it also uses wireless identification technology so that the switch can only be triggered by a specific RF signal sequence. This would greatly increase the efficiency of the switch make the switch immune to noise and other disturbance. As previously mentioned, disturbances and noise can be a critical weakness in an IMD. The proposed wireless switch circuit not only overcomes these obstacles but it is also capable of being fully implemented within the integrated circuit of IMDs.

other circuit

EN

LDO

level shifter

VRF

DATA

CLK

ID programming

 Switch circuit

 control core

ID and command recognition

clock and data recovery

energy recovery

ANT

endoscope controller IC

**Figure 19:** Wireless switch circuit architecture [10]

**10. Reliability Considerations for Implantable Medical IC’s**

Historically, IMDs have benefited from a wide reliability margin available in early technologies. Performance demands have increased to a point now that the reliability margin has been reduced. As the reliability margin has been reduced, the designs for IMDs need to consider internal wear out of mechanisms. Commercial off-the-shelf (COTS) components have traditionally gone unused in the IMD market because of high reliability requirements, unique applications, and long development and product life cycles [39]. Suppliers were reluctant because of the increased liability of the medical field. Ten years ago COTS components began being used in IMDs. Initially, SRAM and EEPROM memories were used for solely for non-life support functions due to their low reliability. The general operational requirements of COTS components are different from the very specific characteristics needed for IMD. Components used in IMDs need to have a higher life cycle and lower power consumption than most COTS components offered. Therefore, manufacturers were forced to redesign their products for use in IMDs. In some cases, test engineers used a “black box” strategy to characterize a test vehicle (i.e. memory for an IMD). The test engineers would develop test cases to see where the performance envelope breaks and use this method to re-screen parts for use in IMD’s. The following example illustrates how issues seen on medical COTS IC’s would not be an issue on commercial products. A medical device was flown from a factory to the medical sales representative. When the device arrived it was discovered to have a dead battery. The cause of the dead battery was linked to a commercial memory failure. The memory failure was associated with temperature changes during the course of the flight. How does this affect an IMD? The body maintains its temperature at 37 degrees Celsius. At this temperature the IC discussed in the example above would not have been affected but at a low temperature of shorter duration could have depleted the battery causing a shorter working life.

Commercial IC manufacturers are less reluctant to join the medical field and are forming partnerships with other medical device manufacturers to develop medical field specific devices. COTS manufacturers are beginning to design their products with low power consumption in mind, making their products more attractive for use in IMD’s. Intense scrutiny occurs during the design process and very detailed documentation of the entire development process is required when developing an IMD. Also, very rigorous design testing is needed to ensure the safety of the patient. Design verification testing (DVT) is more formal and complex for a commercial product. The testing procedure must be agreed upon by both parties (the manufacture and the purchaser). A final report detailing all test data and deviations and failures must be included in the report. The testing equipment used by the vendor must be certified and inspected to make sure the safety of the end user is considered.

 Scaling considerations are also presented. Scaling refers to challenges faced in decreasing the size of components and the overall device size. There are notable differences in scaling and the consequences of those scaling changes. These problems occurred during the transition from a lightly doped source/drain (LDD) scheme to a halo/extension scheme under the channel of the transistor. As this move took place, the doping concentrations increased under the gate which generated a smaller depletion region. The problems posed by this change include higher electric fields and the need to design for leakage mechanisms [39]. A reduction in the polysilicon gate length, supply voltage, gate oxide thickness, and the source/drain junction depth were also noted. The reduction in thickness seems to point to an increase in electric field. The increase in electric field could lead to gate induced drain leakage (GIDL). Also, with thinner oxides stress induced leakage current (SILC) could become an issue.

**11. IMDs Electromagnetic Compatibility**

One area of questionable reliability is when IMDs are exposed to strong external electromagnetic fields. These fields are common occurrences. One of the most common and therefore inconvenient sources of these fields is security devices at airports. The performance of electromagnetic compatibility testing (EMC) on IMDs is of utmost importance. The Food and Drug Administration (FDA) has received 109 reports since 1987 of active IMDs (AIMDs) malfunctioning in the presence of security systems [40]. Current research is focused on streamlining EMC testing. This research has led to a security system simulator. In particular, a simulator for a walk through metal detector (WTMD) has been developed. An analysis of WTMDs was conducted as part of the proposed simulator. The WTMD’s electromagnetic emissions were measured using detectors with three-axis magnetic field probes. Measurements were taken at specific locations around the WTMD. For instance, horizontal plane measurements were taken at 130 cm above the ground which is the approximate height of most IMDs. In order to simulate the effects of WTMDs, the authors had to capture the waveforms produced by the 12 different WTMDs. The field values in this paper were all peak-to-peak and defined as:

 (15)

The proposed security simulator consists of a wave generator, an amplifier and a coil system. For every amp of drive current the coil system is able to produce a magnetic field of 2.3 A/m. The waveforms produced from the simulator are designed to mimic the twelve WTMDs addressed in this paper. The coil system can produce a uniform magnetic field over a volume of 57 cm long, 42 cm wide, and 14 cm deep.

Four pacemakers were tested with the proposed simulator and are shown in Table 6. Dual channel pacemakers are set to DDD (dual pace, dual sense, and dual response to sensing) or DDDR (DDD + rate modulating). Single channel pacemakers are set to VVI (ventricular paced, ventricular sensed and response to sensing is inhibition). Two types of test were conducted on each pacemaker: a in air test, and a saline test. The saline test was monitored using a fiber optic system which limited the amount of interference of the monitoring cables. The in air test was monitored using a twisted cable with a simple resistive load. The saline test was conducted using a saline box (42 x 57 x 30 cm) with a 0.14% saline solution with a conductivity of 0.266 S/m to a height of 5 cm.

Table 6: Pacemakers used for testing [70]

|  |  |
| --- | --- |
| Pacemaker 1 | Dual channel, DDDR sensitivity setting atrial: 0.5 mV, ventricular: 1 mV |
| Pacemaker 2 | Single channel, VVI sensitivity setting: 1 mV |
| Pacemaker 3 | Dual channel, DDD sensitivity setting atrial: 0.5 mV, ventricular: 1 mV |
| Pacemaker 4 | Dual channel, DDDR sensitivity setting atrial: 0.5 mV, ventricular: 1 mV |

 The interference tests were started at the lowest possible field value, 1-2 A/m. The thresholds for interference were determined by increasing the magnetic field every 10 seconds by 2 A/m at each step. Pacemaker 1 showed interference for nine of ten pulse WTMD signals. For the “in air” testing, pacemaker 1 was characterized at two different thresholds. At the first threshold, pacemaker 1 showed partial atrial and intermittent ventricular inhibition. Partial inhibition means that the pacemaker skipped more than one consecutive pulse. Intermittent inhibition means that only once in while the pacemaker missed a pulse. At the second threshold, pacemaker 1 showed full atrial inhibition and ventricular pulse tracking at the maximum rate. While testing pacemaker 1 under continuous wave WTMDs the performance was different. Inhibitions only occurred at very high field levels, much higher than the normal operating level of the continuous wave WTMD.

 The “in air” testing of pacemaker 2 is characterized in a similar fashion. Pacemaker 2 was a single channel, as seen in Table 5. The behavior was similar for pulse and continuous wave WTMDs at the first threshold. The pacemaker showed partial atrial inhibition and intermittent ventricular inhibition at the first threshold. At the second threshold, pacemaker 2 showed full atrial inhibition and ventricular pulse tracking at the maximum rate. Interestingly, at the second threshold pacemaker 2 showed no interference when tested against continuous wave WTMDs. Pacemaker 3 showed a very different characterization for the “in air” testing. There were two windows with corresponding field levels where interference would occur and anything above or below those window field levels did not yield interference for pacemaker 3. At the first window the pacemaker showed partial inhibition only and continued this operation until the limit of the first window. At which point the pacemaker began operating normally. At the second window, the pacemaker showed both partial atrial and ventricular inhibition but once the limit of the second window was reached normal operation continued. The authors mention that during the course of their testing pacemaker 4 did not show any signs of interference for the “in air” testing or saline testing. Pacemaker 4 was not inhibited for the continuous wave or pulse waves generated by the WTMD. The saline test concluded that the performance of the pacemakers (1-3) was similar to their respective performance during the “in air” testing. However, the main difference was that the field levels of the thresholds and windows were higher during the “in saline” testing.

 A comparison of the performance of the proposed WTMD simulator against and actual WTMD was performed. The comparison was done using pacemaker 1. The testing configuration was the same as used in the simulator. In order to find the interference threshold, the authors moved the pacemaker in the WTMD until interference occurred and measured the field value at that point. Then they compared the measured value found in the actual WTMD and compared it to the value found in the simulator.

 The experimental testing shows that the simulator can mimic the interference found in actual WTMDs which makes the proposed simulator a viable option for EMC testing. One major advantage of the proposed method is the ease of switching among different types of WTMDs. As presented above the proposed simulator can simulate multiple types of WTMD field signals.

**12. Conclusions**

 In this chapter, we have surveyed new developments in the area of IMDs. We have discussed design challenges and possible solutions in several subsystems including: communication, power, and security. These challenges ranged from those found in the operating environment of the human body while others were caused by the external world in which we live. With the presentation of ideas within this chapter, the reader is now more aware of the advancing research topics within the field of implantable medical devices. IMDs are currently used to treat many chronic and life-threatening diseases. IMDs abilities allow medical professionals a way to give the patient remote, synthetic and coordinated disease control within the patient’s body. As IMD sophistication and capabilities increase, so too does the quality of service our medical professionals can provide to those who need IMDs. By improving their design, we allow patients to have lives in greater accordance with those they wish to lead.

**References:**

[1] Valdastri, Pietro. Rossi, Stefano. Menciassi, Arianna. etc. “An implantable ZigBee ready telemetric platform for in vivo monitoring of physiological parameters”, Sensors and Actuators A 142 (2008).

[2] Drew, T. and Gini, M. 2006. Implantable medical devices as agents and part of multiagent systems. In *Proceedings of the Fifth international Joint Conference on Autonomous Agents and Multiagent Systems* (Hakodate, Japan, May 08 - 12, 2006). AAMAS '06. ACM, New York, NY, 1534-1541.

[3] Wolfgang Kainz, Jon P. Casamento, Paul S. Ruggera, Dulciana D. Chan, and Donald M. Witters, “Implantable Cardiac Pacemaker Electromagnetic Compatibility Testing in a Novel Security System Simulator,” In *IEEE Transactions on Biomedical Engineering*, vol. 53, NO. 3, March 2005

[4] IEEE standard for information technology – telecommunications and information exchange

 between systems – local and metropolitan area networks specific requirements part 15.4: wireless

 medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless

 personal area networks (LR-WPANs), IEEE Std 802.15.4, 2003.

[5] C. Hofmann, C. Weigand, J. Bernhard, Evaluation of zigbee for medical sensor networks, WSEAS

 Trans. Electr. 3 (3) (2006) 121–125.

[6] Parramon JP (2001) Energy Management, Wireless and System Solutions for Highly Integrated

 Implantable Devices. Universitat Autonoma de Barcelona, Department d’Enginyeria Electronica.

[7] D.W.Y. Chung1, A.C.B. Albason, A.S.L. Lou and A.A.S. Hu. “A Low Power Wireless Downlink Transceiver for Implantable Glucose Sensing Biosystems”, ICBME 2008, Proceedings 23, pp. 418–421, 2009.

[8] Lou AS, Chen HZ (2004) A Study of RF Power Attenuation in Biotissues. Journal of Medical and

 Biological Engineering, 24(3): 141-146

[9] MICS Band Plan Federal Commun. Comm., Part 95, FCC Rules and Regulations, Jan. 2003.

[10] Bohorquez, Jose. Chandrakasan, Anantha. Dawson, Joel. “A 350 uW CMOS MSk Transmitter and

 400 uW OOK Super-Regenerative Receiver for Medial Implant Communications”, IEEE Journal of

 Solid-States Circuits, VOL. 44, NO. 4, pp 1248-1259, April 2009.

[11] D. B. Miron*, Small Antenna Design*, 1st ed. Oxford, UK: Elsevier Science and Technology, 2006.

[12] De Mey, Michel. Christensen, Craig. Blanchard, Shane. “Design Concepts for Wireless

 Communication in Implantable Medical Applications”. Analog Circuit Design, 331–343.

[13] Panescu, Dorin. “Emerging Technologies: Wireless Communication Systems for Implantable

 Medical Devices”. IEEE Engineering In Medicine and Biology Magazine. March/April 2008. p. 96-

 101.

[14] Medtronic. CareLink system. [Online]. Available:

 http://www.medtronic.com/physician/carelink/index.html. Accessed Oct. 14, 2010.

[15] Drew, T. and Gini, M. 2006. Implantable medical devices as agents and part of multiagent systems.

 In *Proceedings of the Fifth international Joint Conference on Autonomous Agents and Multiagent*

  *Systems* (Hakodate, Japan, May 08 - 12, 2006). AAMAS '06. ACM, New York, NY, 1534-1541.

[16] Oh, J.; Kin, J.; Lee, H.; Kim, J. (13 January 2010). New Modulation Scheme for High Data Rate

 Implantable Medical Devices. IEEE Trans Inf Technol Biomed. 2009 Nov 10., pg. 1464-1467.

[17] Y. Kawamura, S. Futatsumori, T. Hikage, T. Nojima, B. Koike, H. Fujimoto, T. Toyoshima, “A

 Novel Method of Mitigating EMI on Implantable Medical Devices: Experimental Validation for

 UHF RFID reader/writers,” IEEE International Symposium on [Electromagnetic Compatibility, 2009.](http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=5277433) 17-21 Aug. 2009, page(s): 197 – 202, Location: Austin, TX

[18] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend,W. Morgan, K. Fu, T.

 Kohno, andW. H. Maisel. Pacemakers and implantable cardiac defibrillators: Software radio attacks

 and zero-power defenses. In IEEE Symposium on Security and Privacy, May 2008.

[19] David Halperin, Tadayoshi Kohno, Thomas S. Heydt-Benjamin, Kevin Fu, and William H. Maisel,

 “Security and Privacy for Implantable Medical Devices,” In *IEEE Pervasive Computing*, vol. 7,

 Issue 1, pages 30-39, January 2008.

[20] T. Heydt-Benjamin, S. Capkun, C. Castelluccia, and K. B. Rasmussen, “Proximity-based Access

 Control for Implantable Medical Devices,” Conference of Computer and Communications Security

 (CCS), pages 410 -419. ACM ,November 2009.

[21] K. Fotopoulou and B. W. Flynn. Optimum antenna coil structure for inductive powering of passive

 RFID tags. In *RFID, 2007. IEEE International Conference on*, pages 71–77, 2007.

[22] Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa

 Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H. Maisel. Pacemakers and

 implantable cardiac defibrillators: Software radio attacks and zero-power defenses. *Security and*

 *Privacy, IEEE Symposium on*, 0:129–142, 2008.

[23] S. Brands and D. Chaum. Distance-bounding protocols. In *Workshop on the theory and*

 *application of cryptographic techniques on Advances in cryptology*, pages 344-359. Springer-Verlag

New York, Inc., 1994.

[24] Jolyon Chulow, Gerhard P. Hancke, Markus G. Kuhn, and Tyler Moore. So near and yet so far:

 Distance-bounding attacks in wireless networks. In *European Workshop on Security and Privacy in*

 *Ad-Hoc and Sensor Networks* (ESAS), pages 20-21, September 2006.

[25] Tamera Denning, Kevin Fu, and Tadayoshi Kohno, “Absence Makes the Heart Grow Fonder: New

 Directions for Implantable Medical Device Security,” In *Proceedings of the 3rd conference on Hot*

 *topics in security*, Article No. 5, San Jose, CA 2008.

[26] F. Stajano and R. J. Anderson. The resurrecting duckling: Security issues for ad-hoc wireless

 networks. In Proceedings of Security Protocols, 7th International Workshop, LNCS 1796, pages

 172–194, 1999.

 [27] B. Greenstein, D. McCoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall. Improving wireless

 privacy with an identifier-free link layer protocol. In MobiSys, June 2008.

[28] I.J. Bahl and P. Bhartia, *Microstrip Antenna* [M]. Dedham, MA: Artech House, 1980

[29] Yu, X.; Li, G.; Zhang, L.; Wang, Z. (13 January 2010). Design and Test of a Miniature 2.45 GHz Antenna for Implantable Medical Devices. IEEE 14th International Mixed-Signals, Sensors, and Systems TestWorkshop, 2008. Downloadable from the following website: <http://www.ime.tsinghua.edu.cn/szdw/bodao/wangzh/everyyear/papers/IMS3TW08_Yu-13.pdf>.

[30] R. Chair,K.M. Luk, and K. F. Lee, “Small Dual Patch Antenna” [J], *Electronics Letters*, Vol: 35,

 No: 10, May 13, 1999, Pages: 762–764

[31] Seo, J.-S, Woo, J.-M, “Miniaturization of microstrip antenna using irises” [J], *Electronics Letters*,

 Volume: 40 , Issue: 12 , 10 June 2004, Pages:718 – 719

[32] E. S. Hochmair, "System Optimization for Improved Accuracy in Transcutaneous Signal and

 Power Transmission," Biomedical Engineering, IEEE Transactions on Biomedical Engineering, IEEE

 Transactions on Biomedical Engineering, IEEE Transactions on, vol. BME-31, p. 177-186, 1984.

[33] Yu, Y.; Hao, H.; Wang, W.; Li, L. (13 January 2010). Simulative and Experimental Research on Wireless Power Transmission Technique in Implantable Medical Device. IEEE Xplore, pg. 923-926.

[34] Watkins, C.; Shen, Bing; Venkatasubramanian, R. (13 January 2010). Low-grade-heat energy harvesting using superlattice thermoelectrics for applications in implantable medical devices and sensors. Thermoelectrics, 2005. ICT, pg. 250-252.

[35] Wafer Scale Thin-film Thermoelectric Technology, RTI Patent Pending, September 2003.

[36] Furman, S., Hayes, D.L., and Homes, D.R. Jr.: ‘A practice of cardiac pacing’ (Futura, New York,

 USA, 1993, 3rd edn.)

[37] Buzduga, V.,Witters, D.M., Casamento, J.P., and Kainz,W.: ‘Testing the immunity of active

 implantable medical devices to CW magnetic fields up to 1 MHz by an immersion method’, IEEE

 Trans. Biomed. Eng., 2007, 54, (9), pp. 1679–1686

[38] Jiang, H; Zhang, L.; Zhang, C.; Wang, Z. (14 August 2008). Wireless switch for implantable medical devices based on passive RF receiver. ELECTRONICS LETTERS, Vol. 44 No. 17.

[39] Mark Porter, Paul Gerrish, Larry Tyler, Sharon Murray, Rob Mauriello, Frank Soto, Gaylene Phetteplace, and Scott Hareland, “Reliability Considerations for Implantable Medical IC’s,” In *46th Annual International Reliability Physics Symposium*, Phoenix, 2008.

[40] Wolfgang Kainz, Jon P. Casamento, Paul S. Ruggera, Dulciana D. Chan, and Donald M. Witters, “Implantable Cardiac Pacemaker Electromagnetic Compatibility Testing in a Novel Security System Simulator,” In *IEEE Transactions on Biomedical Engineering*, vol. 53, NO. 3, March 2005