Wireless Power Charge Security Via Chaos-base Frequency Adjustment

Securing Wireless Power Charging

(Lab Reading Materials)

Department of Electrical and Computer Engineering

The University of Alabama

Credits to:

Austin Burnett; Nathan Howdon; Allison O’Shea; D’Arrys Smith; Philip Zicarelli

Faculty Advisor: Dr. Fei Hu

December 12, 2014

**ABSTRACT**

Wireless power charge for implanted devices (IMDs) is becoming more prominent in today’s society. It allows for surgery-based battery replacement to be avoided; these surgeries are accompanied by risks which could lead to patient complications and high medical costs. Wireless power charging for IMDs is implemented by using two coupled coils with the same resonant frequency to exchange energy wirelessly. This exchange of wireless energy is assumed to occur in a safe environment. As one must realize, every environment is not always safe for wireless energy transfer. An attacker who is aware of the implanted device’s coupling frequency could easily obtain power charge from the patient’s device by using a customized self-resonant coil circuit. This type of attack could cause organ damage due to the overheating of the implanted device, an inverse charge effect from intentional de-coupling, as well as dysfunctionality of the implanted device due to voltage instability. In efforts to perform safe wireless power transfer, the proposal of wireless power transfer via chaos-based frequency adjustment was set into place. A frequency tuner that is driven by a chaotic source would keep potential attackers at bay. The attacker would not be capable of manipulating a static resonant frequency, thus, resulting in added security to a wireless power transfer scheme.

**TABLE OF CONTENTS**

Introduction…………………………………………………………………………………….....4

Project Motivation………………………………………………………………………………...4

Project Goals………………………………………………………………………………………5

Components……………………………………………………………………………………….5

Chaotic Code……………………………………………………………………………………...7

Circuitry/Integration………………………………………………………………………………8

Conclusion………………………………………………………………………………………...9

APPENDIX………………………………………………………………………………………10

***Introduction***

A cyber-physical system is a system of computational elements interacting physical entities. In today’s society, there are several different implementations of cyber physical systems. For this particular project, an Implanted Medical Device was the example used to portray the concept of the secure wireless power charging transfer. To approach the implementation of the wireless power charging security, the source of the insecure charging had to be identified. It was found that it was due to the use of a preset, fixed resonance frequency. To tackle this problem, it was proposed that the coupling coefficients should be updated into the hardware to achieve a time-varying resonance frequency switch. To make the switching sequence unpredictable, a Chaotic Map based capacity control was used. After the implementation of the wireless power transfer circuit, MOSFET switches were added into the circuit in place of the switches to integrate with a microcontroller. This report will discuss in thorough detail the project goal, components used, circuitry and chaotic code used to implement a solution to this proposition.

***Project Motivation***

The motivation behind this project to increase the security of wireless charging is to open up the door to many implementations of devices with this characteristic. Many different areas of electronic devices can be impacted through the development of secure wireless charging. One major area would be the medical field. With secure charging, implanted medical devices could be safely charged without surgery. This opens doors to the reduced risks of surgeries required to replace or recharge batteries for implanted medical devices. While the medical field could greatly benefit from this development, most areas of electronic devices could benefit as well. Any device that requires some sort of periodic charging could be vulnerable to cyber attacks if they are charged by an unsecure connection. With the security, charging can be monitored and ensured to be safe for the user and the device.

***Project Goals***

The major goals for this project to achieve the proof of concept for the secure wireless charging circuit are as follows: Static wireless power transfer, switching capacitance, chaos code implemented through microcontroller circuit, microcontroller circuit integrated with power transfer circuit.

The overall goal for this project was to prove the concept of securing wireless charge by frequency variation so our focus was geared toward creating the circuits and testing all possibilities. To begin, creating a simple wireless power transfer circuit was necessary. Once the simple circuit was completed, testing for the capacitance change through mechanical switches was started. Minor goals that occurred during the process include the component selection and purchasing process. While testing was ongoing on the wireless power transfer circuit, chaos code and microcontroller testing was being completed. Developing and debugging the code for the microcontroller was a task that had to be completed in order to allow us to begin the initial integration attempts.

***Components***

We needed a microcontroller in the circuit to program and run the chaotic code, and we selected the Arduino Uno microcontroller for our project. The Arduino Uno served us well and was very cost effective. It came with a starter kit and many additional parts. The clock speed of the Arduino Uno was 16 Mhz, and it had 14 digital input/output pins. The Arduino was user-friendly and was a pivotal part of putting the entire project together. It was the key piece of integrated between our cyber and physical counterparts. The Arduino was necessary to not only implement the chaotic code, but also to serve as the link between the major parts of the project.

Switches are a key component in the wireless power transfer circuit. Two types of switches were used over the course of this project, mechanical and MOSFET. For the initial simple circuit, mechanical slide switches were chosen. Slide switches are a simple device that allowed data to be directly obtained during testing. Since multiple switches are used in the circuit, a switch that could stay on or off without constant contact was vital. The slide switches chosen were small enough to easily fit on the breadboard and met the necessary parameters for the current and voltage ratings needed. The current and voltage ratings for the chosen slide switch are 300 mA and 6 V, respectively. These parameters were determined suitable for our use since low voltage and current values within the circuit were expected to be low. With only human delay, the slide switch allowed us to achieve almost instantaneous switching capabilities. Once we were able to move into using the microcontroller, MOSFET switches were introduced into our system. The main purpose of changing the type of switch used in our circuit was to remove the need for a person to manually turn the switches on or off. Once the MOSFET switches were implemented, we were able to control each switch through the code being applied to the Arduino microcontroller. The chosen n-channel MOSFET has a drain source breakdown voltage of 60 V, a gate source breakdown of 16 V and a continuous drain current of 55 A. With these parameters being safely inside the expected values obtained in our circuit, the MOSFET was determined to be sufficient. The MOSFET used in the circuit has a delay of approximately 40 ns. The delay is acceptable since complete control through the microcontroller is achieved.

Capacitors are another significant component in our circuit. The purpose of the three capacitors is to achieve frequency variation. By using switch control, different capacitance values were applied to the circuit to change the resonance frequency. The values of the capacitors for the wireless power transfer circuit are 1 nF, 4.7 nF, and 0.1 nF. Small capacitance values were chosen to achieve the desired frequency ranges. Individual capacitors were chosen so that each capacitor could be connected in parallel with a switch to allow control of the total capacitance value. The capacitors chosen have low capacitance as well as low tolerance.

Inductors were vital components as well for the circuit. The inductors were needed to properly transfer the power from the transmitter circuit to the receiver circuit. By using five turns of insulated wire, the current transferring from one circuit to the other was strengthened. The insulated wire was chosen opposed to the copper wire for security and consistency reasons. By using the insulated wires for the inductor, protection from power frequency in security systems would be provided. Although every aspect is conceptual, this would be a huge benefit in the progression of securing wireless power charge.

***Chaotic Code***

The chaotic code that we implemented on the microcontroller was essential to represent the key concept of our project, security. To incorporate the concept of security we needed to use a random sequence to control the capacitance switching. We chose to use the logistic map equation to achieve our randomness. The equation is:

Xn+1 = A Xn(1 − Xn) ≡ fA(X) (1)

A logistic map is a simple, straightforward way of obtaining chaotic behavior. Chaotic systems are extremely sensitive to initial conditions; with a logistic map, the constant A is literally controls the chaos. Constant A in the above equation is a reference to the constant r on the bifurcation diagram shown in Figure-1 in the Appendix. When A > 3.5, chaotic behavior begins. Truly unpredictable behavior is obtained when the constant is set to the highest value of four. In Figure-1, you will also notice the x value on the y-axis of the graph; it corresponds to the Xn  in equation (1). This value is called an attractor. It is essentially the starting point value. If constant r is low, then the output would approximate be near the starting value. However, if r constant is high, then the logistic map equation opens the output to many possibilities.

The quality of unpredictability and apparent randomness has led the logistic map to be widely used as a pseudo random number generator. Those same qualities are also what made the logistic map an ideal tool for us to use in achieving the randomness that we needed in our project. The microcontroller was programmed with the logistic map equation and that code and be found in the Appendix. The code was then fed into the MOSFET switches of the circuit, providing a random digital high/low voltage, to operate the switches and control the capacitance.

***Circuitry/Integration***

After much research, the decision was made to implement a simple RLC circuit to achieve the wireless power transfer. The figure shown in the Appendix shows the schematic for this simple RLC circuit. The transmitter circuit consisted of a 9 V input, a 100 kiloohm resistor, 100 nF, 1nF and 4.7 nF capacitors, switches, 2N3904 transistor and an inductor. The 2N3904 transistor was needed to amplify the current so that it was large enough to recognize and would be able to be coupled. The base for this transistor was connected to the capacitors and resistor while the emitter was connected to ground. The receiver circuit consisted of two 1N4148 diodes connected in series with an LED and inductor.

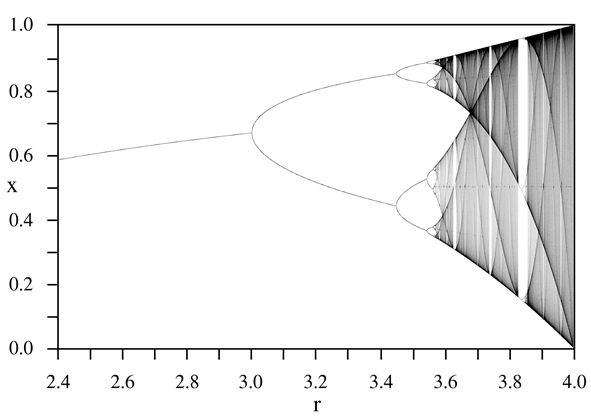
The most vital component of both the transmitter and receiver circuits was the inductors. These inductors were essential in creating the wireless power transfer from one circuit to the other. When a current flows through it, energy is stored temporarily in the magnetic field in the inductor. When the current through an inductor changes, the time-varying magnetic field induces a voltage in the conductor which creates the change in current. To test the functionality of the each circuit, one turn inductors at 6 ½ cm diameter were created. The resonance frequency testing results can be seen in Table 1 in the Appendix. Although the transfer of power deemed successful with the inductors created, it was imperative to have them in a close proximity to complete the power transfer. Ideally, an inductor with 5 turns at 6 ½ cm diameter was essential to create a stronger wireless power transfer. Figure 2 in the Appendix shows the actual transmitter and receiver circuits.

After the completion of the circuit, modifications were made to implement MOSFET switches and integration of the microcontroller and wireless power transfer circuit. Figure 4 in the Appendix shows the schematic of the circuit including the MOSFET switches and microcontroller. After creating the schematic, the implementation of the primary circuit after integration was completed shown in Figure 5 in the Appendix.

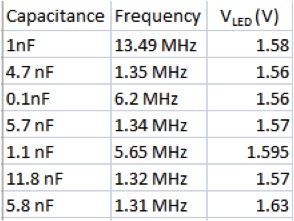
***Conclusion***

In conclusion, with the wireless power charge for implanted devices (IMDs) becoming more prominent, this particular project could potentially be a breakthrough in the cyber-physical world. A whole new realm of research could lead to the successful implementation of security of a wireless power charge for an implanted device. The overall goal of this project was to show the proof of concept of wireless power charge security by implementing a wireless power transfer circuit integrated with chaos sequence. The goal of this project was achieved through thorough research about wireless power charge security via Chaos-base frequency adjustment, implementation of the wireless power circuit and the chaotic sequence code.

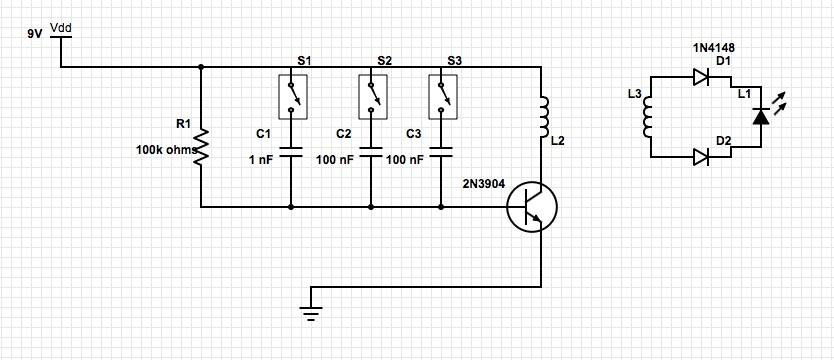
APPENDIX



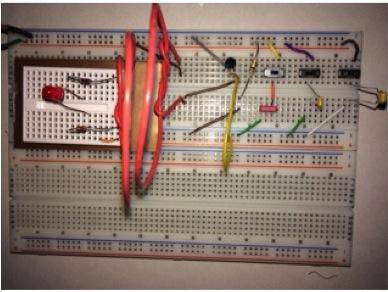
*Figure-1 - Bifurcation Diagram for Logistic Map*



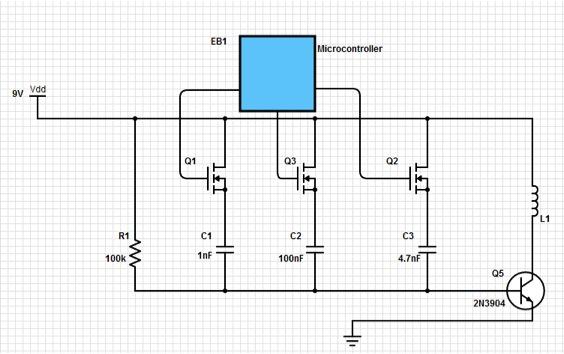
*Table 1: Frequency Values*



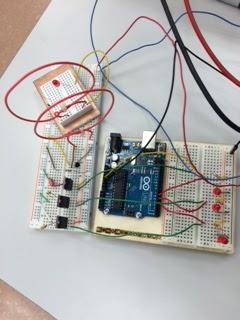
*Figure 2: Wireless Power Transfer Circuit Schematic*



*Figure 3: Wireless Power Transfer Circuit*



*Figure 4: Complete Circuit with Integration*



*Figure 5: Actual Wireless power transfer circuit integrated with microcontroller*

Code for Microcontroller

// Blinking Logistic Map

// choose the pin for each LED

const int NbrLEDs = 3;

const int LEDpin[] = {4,5,6};

const int wait = 250; // wait for 500 milliseconds

// Logistic Map Parameters

const double A = 4.0; // Logistic map constant

double X0 = 0.1; // Initial position (0 < X0 < 0.8)

double X = X0; // Use X0 as your first calculated point

// setup() initializes the LED pins

void setup() {

for (int i = 0; i < NbrLEDs; i++) {

pinMode(LEDpin[i], OUTPUT);

}

}

// loop() iterates the Logistic Map and turn on/off LEDs

void loop()

{

if (X < 0.1)

{ digitalWrite(LEDpin[0],LOW);

digitalWrite(LEDpin[1],LOW);

digitalWrite(LEDpin[2],LOW);

delay(wait);}

else if ((X >= 0.1) && (X < 0.2))

blinkLED (LEDpin[2]);

else if ((X >= 0.2) && (X < 0.3))

blinkLED (LEDpin[1]);

else if ((X >= 0.3) && (X < 0.4)) //Truth Table Case 3

{digitalWrite(LEDpin[1],HIGH);

digitalWrite(LEDpin[2],HIGH);

delay(wait);

digitalWrite(LEDpin[1],LOW);

digitalWrite(LEDpin[2],LOW);}

else if ((X >= 0.4) && (X < 0.5)) //Truth Table Case 4

blinkLED (LEDpin[0]);

else if ((X >= 0.5) && (X < 0.6)) //Truth Table Case 5

{digitalWrite(LEDpin[0],HIGH);

digitalWrite(LEDpin[2],HIGH);

delay(wait);

digitalWrite(LEDpin[0],LOW);

digitalWrite(LEDpin[2],LOW); }

else if ((X >= 0.6) && (X < 0.7)) //Truth Table Case 6

{digitalWrite(LEDpin[0],HIGH);

digitalWrite(LEDpin[1],HIGH);

delay(wait);

digitalWrite(LEDpin[0],LOW);

digitalWrite(LEDpin[1],LOW); }

else //Truth Table Case 7

{digitalWrite(LEDpin[0],HIGH);

digitalWrite(LEDpin[1],HIGH);

digitalWrite(LEDpin[2],HIGH);

delay(wait);

digitalWrite(LEDpin[0],LOW);

digitalWrite(LEDpin[1],LOW);

digitalWrite(LEDpin[2],LOW);}

// iterates the Logistic Map function

X0 = X;

X = A \* X0 \* (1.0 - X0);

}

// blinkLED function

// turn on/off LEDs

void blinkLED (const int pin) {

digitalWrite(pin, HIGH); // turn LED on

delay(wait); // wait 500 milliseconds

digitalWrite(pin, LOW); // turn LED off

}

References

1. CPS Security*. 492 Design Statement SP14*. Tuscaloosa, AL. Feb. 24 2014. Aug. 26 2014.
2. CPS Security*. CPS Critical Design Review*. Tuscaloosa, AL. Apr. 7 2014. Aug. 26 2014.
3. *Cyber-Physical System Security*. PowerPoint presentation. Department of Electrical Engineering, University of Alabama, Tuscaloosa, AL. 17 Feb. 2014. 26 Apr. 2014
4. Hu, Fei. *Introduction to CPS Security*. PowerPoint presentation. Department of Electrical Engineering, University of Alabama, Tuscaloosa, AL. 26 Apr. 2014
5. Hu, Fei. *Secure Wireless Powering of Implanted Devices via Secret Resonance Frequency.* Department of Electrical and Computer Engineering, University of Alabama, Tuscaloosa, AL. 17 Feb. 2014. 26 Apr. 2014.