EFFECTS OF INTENTIONAL ELECTROMAGNETIC INTERFERENCE ON ANALOG TO DIGITAL CONVERTER MEASUREMENTS OF SENSOR OUTPUTS AND GENERAL PURPOSE INPUT OUTPUT PINS

by

David A. Ware

A thesis submitted in partial fulfillment
of the requirements for the degree

of

MASTER OF SCIENCE

in

Computer Engineering

Approved:

Ryan Gerdes, Ph.D. Major Professor	Reyhan Baktur, Ph.D. Committee Member
Rose Qingyang Hu, Ph.D. Committee Member	Mark R. McLellan, Ph.D. Vice President for Research and Dean of the School of Graduate Studies

UTAH STATE UNIVERSITY
Logan, Utah

2017

ABSTRACT

Effects of Intentional Electromagnetic Interference on
Analog to Digital Converter Measurements of Sensor
Outputs and General Purpose Input Output Pins

by

David A. Ware, Master of Science

Utah State University, 2017

Major Professor: Ryan Gerdes, Ph.D.
Department: Electrical and Computer Engineering

The use of sensors in embedded systems has grown dramatically in recent years. These sensors are used to increase the safety and efficiency of many electrical systems. With the increased use of automation and plans for the development of the internet of things, smart cities and other similar undertakings, the use of these sensors will continue to grow. This growth will ideally lead to greater connectivity, accessibility of information, efficiency, and security.

However, the use of these sensors creates a potential vulnerability to attacks that use intentional electromagnetic interference (IEMI). While high power IEMI attacks, on the order of kilowatts, have been studied extensively, low power IEMI attacks, on the order of watts, haven't received much attention. Recent research on low power IEMI attacks has shown that systems using sensors operating in the range of a few millivolts are vulnerable to these attacks. This work examines low power IEMI attacks against systems using sensors that operate in the range of volts and digital logic. This work also attempts to identify circuit attributes that make systems more vulnerable to low power IEMI attacks.

The experimental results of this research indicate that IEMI attacks against embedded systems using sensors operating on the order of volts and digital logic are possible, but will require more power and, potentially, better antennas to be successful. These experiments also identified several circuit elements that can significantly affect the performance of low power IEMI attacks.

(64 pages)

PUBLIC ABSTRACT

Effects of Intentional Electromagnetic Interference on
Analog to Digital Converter Measurements of Sensor
Outputs and General Purpose Input Output Pins
David A. Ware

As technology becomes more prevalent, its application to safety and security in critical systems continues to increase. This leads to an increased dependence on sensors to provide an accurate view of the environment surrounding an application. These sensors can also be exploited by a malicious individual to attack a system and compromise its safety or security. These attacks change the reported value of a sensor so that it doesn't reflect the real situation. The systems in a car can be used as an example of this. Cars can have numerous sensors that measure a variety of things, including the car's distance from an object, if the tires are locking up, or if the gas is low. The use of these sensors makes cars safer and more convenient to use. Using IEMI, an attacker could compromise some of these systems by changing the reported value so that an object appears further away than it actually is or that the tires aren't locking up when they are, possibly causing the car to crash. By doing this, a malicious individual could compromise the safety or security of a car.

This work attempts to understand what would be required for a malicious individual to conduct such an attack, thereby allowing for the identification of systems that are vulnerable to such attacks. This understanding would also provide the basis for designing defenses against these attacks, thereby increasing the safety of society at large.

I would like to dedicate this to my wife and parents whose support has never gone unappreciated...

ACKNOWLEDGMENTS

I would like to thank and acknowledge the many people that have helped me with this project, many of whom will be continuing the research after I leave.

Dr. Gerdes, I have appreciated the opportunity to work with you on this research. I have learned a lot from you and have always appreciated your time whether in classes or on this project. You have probably been the most influential teacher that I have had in my college career.

I would also like to thank Dr. Mina for all your questions. They always helped us refocus on our goals and prevented us from becoming lost in the details of our experiments.

Finally, my thanks to my fellow students Jayaprakash Selvaraj and Neelam Prabhu Gaunkar for helping me to better understand electromagnetic principles and antennas. Your help and insights have been invaluable.

David A. Ware

CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACRONYMS

EMC	Electromagnetic Compatibility
EME	Electromagnetic Emissions
EMI	Electromagnetic Interference
HPM	High-Power Microwave
IEMI	Intentional Electromagnetic Interference
HPIEMI	High Power Intentional Electromagnetic Interference

CHAPTER 1

INTRODUCTION

1.1 Background

Sensors are critical components in embedded systems that allow the system to acquire information about the analog world. A few examples of systems that use sensors include cars, digital cameras, phones, and medical equipment. In cars, these sensors make anti-lock braking systems, vehicle detection, automated cruise control, and other features possible. These features increase the safety and usability of cars. The use of sensors to improve the safety and security of systems is only going to increase and has a positive effect on society, e.g., pacemakers help prevent cardiac arrest, anti-lock brakes help cars stop quickly, and fire alarms allow for the timely evacuation of burning buildings. They can also increase the efficiency of a system - for example, dryers turn off when clothes are dry, lights turn on and off automatically and stoplights change colors when they sense that cars are waiting in only one direction. However, all of these benefits come with a price. They allow for the possibility that a malicious individual could attack the system by altering sensor readings. If these attacks are not prevented or guarded against, they could easily result in property damage or loss of life [1]. These attacks, among others, are often referred to as cyber attacks, and protecting against them is part of cyber security.

The importance of cyber security is widely recognized and many books and articles have been written to help designers identify security flaws and protect against cyber attacks [2–4]. Several cyber attacks that have been identified and researched include buffer overflows, hardware trojans, side channel analysis, and man-in-the-middle attacks. When these attacks are used against embedded systems, most of them attempt to change sensor data after the measurements have been taken, if they target sensor data at all. Incidentally, most embedded systems implicitly trust their sensor readings and secure them after they

are taken. This makes them vulnerable to attacks that target the sensor output directly. One way that the sensor output can be directly corrupted is through the presence of electromagnetic interference (EMI) which induces a voltage and current in the affected system. Attacks that use EMI to alter a measurement or damage a system are called intentional electromagnetic interference (IEMI) attacks. IEMI attacks bypass common security methods, potentially giving an attacker the ability to control the sensor readings [5].

1.2 Thesis Goals

Microcontrollers often use analog to digital converters (ADCs) or general purpose input/output pins (GPIOs) to interface with sensors. This work focuses on understanding the susceptibility of these microcontroller inputs to IEMI attacks. Applications that use microcontrollers or similar hardware to interface with sensors are extremely common and only continue to increase in number. Unfortunately, while the robustness of sensor output from a system's perspective has been researched extensively; research on the vulnerability of sensor measurements to IEMI attacks is scarce [6]. This work focuses on IEMI attacks against microcontrollers measuring sensors and expands existing work by:

- Examining a first-order circuit model of IEMI attacks.
- Evaluating the effects of various circuit elements on IEMI attacks.
- Testing the possibility of low power IEMI attacks against analog sensors operating in the range of volts.
- Testing the possibility of low power IEMI attacks against digital logic.

By examining a first-order circuit model of an IEMI attack, this work hopes to identify potentially important circuit elements. Identifying these elements will help increase the understanding of what makes a system vulnerable to IEMI attacks. The effects of these elements will then be evaluated by conducting IEMI attacks against a system and systematically varying these elements. This will allow for a better understanding of which circuit elements have the greatest effect on the performance of IEMI attacks. Experiments will

then be done using the worst-case scenario for an attacker, to evaluate the vulnerability of microcontrollers or other hardware, using analog sensors operating in the range of volts or digital logic, to IEMI attacks. To the knowledge of the authors, IEMI attacks targeting these applications have not been examined.

CHAPTER 2

BACKGROUND

This chapter presents previous research that has been done on this topic directly or is related to it. Sources are grouped by the type and intent of the attack that they researched.

2.1 High Power IEMI Attacks

Currently, a substantial body of work exists on the effects of high power EMI or high power IEMI (HPIEMI), as it will be called here [7–9]. However, most of this work is not directly comparable to this research since kilowatts of power were used and the intended effect of the IEMI was different. Much of the research on the use of HPIEMI focuses on the destruction or disruption of electric systems instead of influencing a measurement. The most applicable work we found was written by Mats G. Backstrom and Karl Gunnar Lovstrand, who summarize work that was done by various military groups using HPIEMI to disrupt or destroy electronic systems [8]. This research focused on attacks that were high power and high frequency and described front- and back-door coupling. Front-door coupling has two orders. The first order is when the frequency of the EM radiation coincides with the operating frequency of the electronic system under attack [8]. The second order of front-door coupling is when the frequency of the EM radiation doesn't coincide with the operating frequency of the equipment [8]. Back-door coupling happens when the coupling takes place through shielding, intentional or unintentional, or through things that could easily be shielded, such as connecting wires [8]. Using high power antennas and generators, multiple electrical systems were successfully destroyed or disrupted. Backstrom and Lovstrand observed that each attack was dependent on frequency and angle. They concluded that this method could be used up to a kilometer away but requires careful pre-analysis of the system. In summary, the research done on HPIEMI attacks focuses on the destruction or disruption of electric systems.

2.2 Modifying Sensor Readings

Despite extensive searching, only a few papers were found that examined the use of IEMI to attack sensor outputs or readings directly [5, 10–14]. The oldest paper that was found on the subject was written by J. Delsing et al. in 2006 and examined the effects of IEMI on sensor networks by looking at a particular sensor network node named MULLE [14]. A number of methods for mitigating the effects of IEMI on sensor networks were observed including shielding, redundancy, and different forms of communication. J. Delsing et al. observed that because of the size of the MULLE it shouldn't be susceptible to IEMI at low frequencies but rather at high frequencies in the gigahertz range. The lack of susceptibility at low frequencies was verified by using standard electromagnetic compatibility (EMC) testing signals with amplification and a BiLog antenna from 80 MHz - 1000 MHz with field strengths of 10 - 20 V/m [14]. No IEMI effects were observed for these tests. The effects of frequencies in the gigahertz range were then tested using the same methodology. These tests revealed that the sensor node was susceptible to frequencies around 2 GHz with an electrical field around .2 kV/m. J. Delsing et al. conclude that sensor networks need improved immunity to IEMI and that "current research in sensor networks does not consider IEMI to be a serious threat [14]."

Yasser Shoukry et al. conducted an IEMI attack against the anti-lock braking system (ABS) in a car [13]. They did this by attacking the magnetic speed sensors used on individual wheels to provide input to ABS control algorithms. Magnetic speed sensors work by measuring the changes in the magnetic flux density caused by the movement of a ferromagnetic toothed gear or tone gear that is placed in front of it. To affect the measurements, Yasser Shoukry et al. designed custom hardware with a PCB coil that was placed between the tone gear and the sensor. Using this hardware, they were able to cancel the legitimate signal from the tone gear and effectively control the value read by the magnetic speed sensor. They then simulated the effect their most successful attack would have on a car driving on an icy road. This simulation showed that their attack caused the driver to lose control of the car and careen off the road. As defined by Mats G. Backstrom and Karl Gunnar

Lovstrand, this attack was a front-door attack since the sensor could not be shielded and operated at the same frequency as the sensor.

Denis Foo Kune et al. researched baseband and modulated IEMI attacks [5]. Both of these attacks were back-door coupling attacks since they targeted circuitry that could potentially be shielded. Both attacks assumed that a filter was placed in between the sensor and the microcontroller and that they were attacking analog sensors operating on the order of millivolts. Baseband attacks took place in the same frequency range as the signals being generated and were nearly impossible to filter out because doing so would filter out legitimate signals. Modulated attacks took place at a higher frequency and used some part of the circuit to down-modulate their attack into the baseband. The authors attempted both attacks in their paper with varying success [5].

For the baseband attack, Kune et al. used a simple whip pole antenna, audio amplifier, and an arbitrary function generator (AFG) to attack cardiac implanted electrical devices (CIEDs) [5]. Since the baseband frequency for a CIED is between 0.1 Hz and 1 kHz this frequency range was used for the attack. With this setup, they were able to stop pacing from 0.68 - 1.57 m away when the device was exposed to free air, however, when they covered the ECG with a saline fluid they were unable to stop pacing even from 2 - 3 cm away.

One of the weaknesses of this experimental setup was the use of a simple whip pole antenna. For a whip pole antenna to have an effective transmission, it should be half or a quarter of the wavelength of the transmission frequency [15]. Using equation 2.1, where c is the speed of light $(3 * 10^8)$ in meters per second, f is the frequency in hertz, and λ is the wavelength in meters, it can be seen that a quarter wavelength antenna with a transmission frequency of 1 kHz would need to be 75,000 m.

$$\lambda = \frac{c}{f} \tag{2.1}$$

For the modulated attack, a signal generator was used to modulate and transmit using monopole and dipole antennas to attack various microphones. Different frequencies were

used depending on the microphone that was attacked. These ranged from around 800 MHz to 1.2 GHz. All the attacks that were tested relied on nonlinear elements of the amplifier to demodulate the attack signal that was transmitted to the microphone. The attack was tested in three different cases: automated dialing, session hijacking, and denial of services (DoS). The attack was successfully demonstrated in all three cases. For automated dialing, the attackers successfully entered credit card information over a phone using the antenna. Session hijacking was a partial success; while the original user could not be completely overwhelmed, they were pushed to the background. The DoS attack, however, was able to completely overwhelm the user's voice, rendering the phone call useless.

2.3 Changing GPIO Readings

To the knowledge of the author, no work has attempted to influence GPIO pins using an IEMI attack. The most similar work that was found was done by A. Boyer et al. and created a model of the harmonic susceptibility of integrated circuits (ICs) to direct power injection attacks [16]. They started by conducting a direct power injection attack against a 16-bit microcontroller created with 0.25 μm technology. The authors found that the amount of power required to change the value of the digital logic increased nearly exponentially as the frequency of the injected signal increased. They noted that if the voltage of the injected signal was high enough it could induce rectification using the ESD protection that was built into the pin. They also found that the susceptibility of the pin depended on its supply network. Their model showed that a major factor in the susceptibility of a pin to power injection attacks was the input capacitance. It also showed that the power necessary to change the pin state at higher frequencies increased because of the changes in the impedance of the pin. As the frequency increased, so did the impedance of the pin.

CHAPTER 3

THEORY AND MODELS

3.1 Threat Model

A single attacker against a victim circuit with a single sensor is assumed for this research. The attacker is able to gain physical proximity to the victim circuit but can only interact with it through IEMI. A system diagram of this is shown in Figure 3.1. The ideal range for these types of attacks is dependent on the frequency and power of the attack but is generally under 5 m. Because of limitations in power and antenna design, this research limits its examination of the attack to 5 cm.

The goal of the attacker is to control the output that the victim perceives. For an analog-to-digital converter (ADC) the attacker wants to be able to increase or decrease the output value of the sensor at the input to the microcontroller. For a GPIO pin, the attacker wants to be able to flip the bit that is being sent from one microcontroller to another. The attacker is assumed to have access to any hardware required to mount the attack (ie. power supplies, RF amplifier, signal generator, etc.). This work does not consider transmission power directly, though most attacks could be improved by increasing the transmission power.

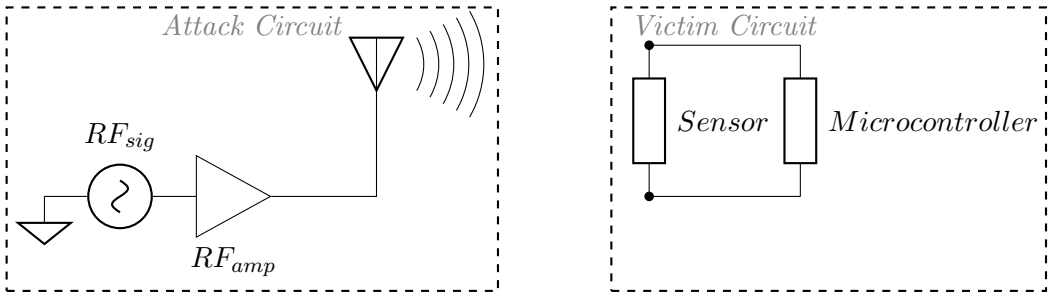

Fig. 3.1: System model for IEMI attacks.

3.2 Theoretical Model of IEMI Attacks

IEMI attacks depend on Faraday's law of induction, which states that a time-varying EM field through a loop will induce a time-varying voltage and current in that loop. The mathematical description of Faraday's law is shown in Equation 3.1.

$$V_{emf} = -N\frac{d}{dt}\int_S Bds \tag{3.1}$$

Where V_{emf} is the induced voltage or electromotive force, N is the number of turns in a coil, B is the magnetic flux density, and the integral is taken over the surface area of the loop [17]. B is in reference to a point in space and can be converted to the magnetic field intensity H using a magnetization factor or permeability μ as shown in Equation 3.2.

$$B = \mu H \tag{3.2}$$

Therefore, the amount of induced voltage depends on the H field in a loop. For an IEMI attack, the victim circuit forms the loop that is being influenced. Therefore, maximizing the amount of H field will increase the effectiveness of the attack. There are two parts to maximizing the H field: first, the region of the field where the attack is conducted, and second, the antenna that is used. Different antennas have different amounts of directivity. The directivity of an antenna is defined to be "the ratio of the radiation intensity in a given direction from the antenna to the radiation intensity averaged over all directions [15]." This means that the more directed an antenna is, the more intense the radiated field is in a particular direction.

For an RF antenna, the region around the antenna can be separated out into two regions: the near field and the far field. In the near field region, the relationship between E and H is complicated and depends on the antenna that is being used [18]. In the far field region, E and H are proportional and locally orthogonal [18]. Determining the exact boundary between the near field and far field is difficult since multiple definitions exist. Introduction to Electromagnetic Compatibility by Clayton R. Paul defines the boundary to

be "the larger of $3\lambda_0$ or $2D^2/\lambda$, where D is the largest dimension of the antenna [18]" and λ_0 is the wavelength. Antenna Theory and Analysis by Constantine A. Balanis generally defines the boundary to be $2D^2/\lambda$ [15]. Most other definitions define the boundary to be $N\lambda$ from the antenna where N can be 2, 4, 5, or 10. For the purposes of this research, the near field is considered to be closer than 5λ of the transmission frequency. Therefore, most of the experiments that are done in this work take place in the near field.

The voltage induced in a loop depends on the amount and direction of change in the H field. An increase in the intensity of the H field induces a higher voltage potential in the loop, while a decrease in the intensity of the H field creates a lower potential voltage in the loop. Equation 3.1 describes this behavior mathematically. This provides a potential method for controlling the voltage induced in the circuit. This control will increase the effectiveness of IEMI attacks by allowing the attacker to control how they affect the circuit. This also increases the efficacy of the attack since it allows the attacker to increase and decrease the voltage in the victim circuit and affect a variety of sensors.

Another vital section of the attack takes place in the victim circuit. Because the induced waveform is an AC signal, it must be converted to DC in order to effectively change the value of a sensor or GPIO pin. This can be accomplished using the inherent rectification in the GPIO pin which is caused by the presence of diodes in the electro-static discharge (ESD) protection for the pin as shown in Figure 3.2 [16]. How this is accomplished can be understood by examining the equation for the forward current through a single diode, shown in Equation 3.3.

$$I_d = I_s \left(\exp\left(\frac{qV}{kT}\right) - 1 \right) \tag{3.3}$$

Where I_d is the forward current of the diode, I_s is the reverse saturation current, q is the electron charge, V is the forward voltage across the diode, T is the absolute temperature of the diode in Kelvin, and k is Boltzmann's constant. Using Taylor series, the exponential

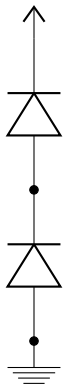

Fig. 3.2: Model of the ESD protection of an I/O pin.

term in Equation 3.3 can be expanded to Equation 3.4.

$$I_d = I_s \left(\frac{qV}{kT} + \frac{\left(\frac{qV}{kT}\right)^2}{2!} + \frac{\left(\frac{qV}{kT}\right)^3}{3!} + \frac{\left(\frac{qV}{kT}\right)^4}{4!} + ... \right) \tag{3.4}$$

If an AC voltage as shown in Equation 3.5 is inserted into Equation 3.4, then Equation 3.6 can be obtained. As can be seen, the terms that are raised to an even power have a DC component.

$$V = A.sin(2\pi ft) \tag{3.5}$$

$$I_d = I_s(\frac{q \times A.sin(2\pi ft)}{kT} + \frac{(qA)^2}{4\ (kT)^2} - \frac{(qA)^2 cos(4\pi ft)}{4\ (kT)^2} + \frac{(\frac{q \times A.sin(2\pi ft)}{kT})^3}{3!} + ...) \tag{3.6}$$

The main disadvantage to using the ESD diodes to do the DC rectification is that higher frequencies require more power input to have an effect. This was observed by A. Boyer et al. [16] and confirmed in this research as shown in Figure 3.3, which shows the amount of power seen by the microcontroller, from a directly injected signal with a constant amplitude. Supporting the previous observation, the amount of power received by the microcontroller decreases as the frequency increases.

Another source of rectification can be the way that the measurements are taken. Many applications use the ADC on a microcontroller to directly acquire values from sensors. These applications usually do not rely on a single value from the ADC, instead, they rely

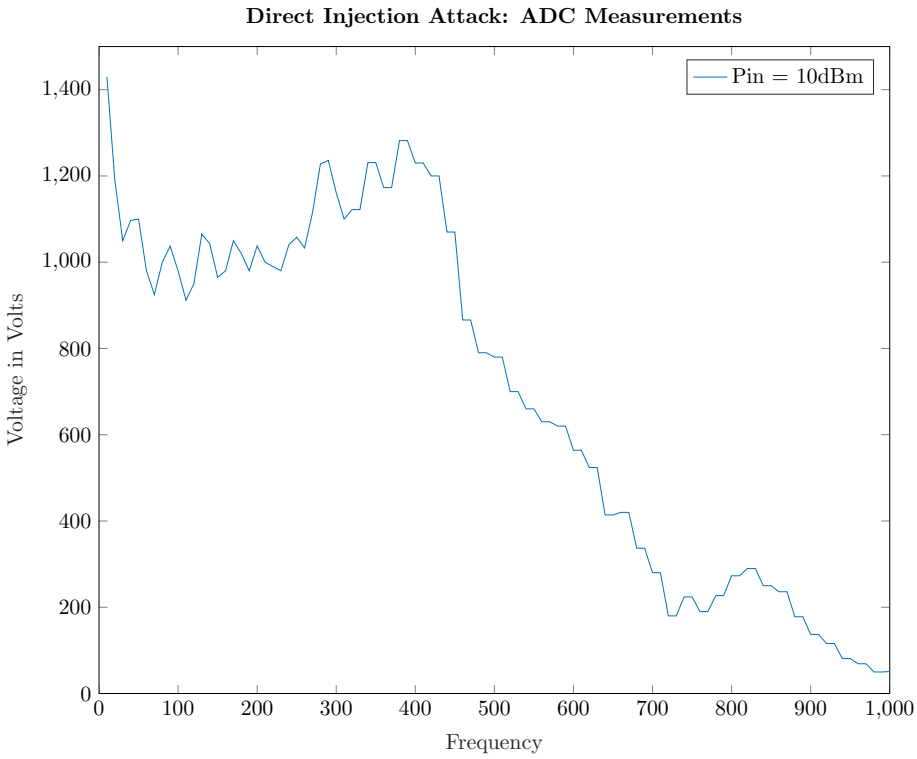

Fig. 3.3: ADC measurements from a microcontroller's GPIO pin when an AC signal was injected directly onto the pin.

on a averaged value of several measurements. Since ADCs on microcontrollers are typically clamped between 0 and 3.3 or 5 V, they won't usually report a negative voltage. Therefore, an IEMI attack against a microcontroller using an ADC will cause a non-zero increase in the measured value even if the received signal has a mean of zero.

3.3 First-Order Model of the Victim Circuit

To gain an idea of the potential effect of IEMI attacks at various frequencies, a first-order circuit model of the victim circuit (shown in Figure 3.4) was examined before any experiments were done. In this model, V_{DD} represents the power supply of a sensor. L_2 is the parasitic inductance that exists between the sensor and the power supply. *Sensor* represents the location of the sensor in the circuit, although its circuit effects are considered to be mostly inductive and can, therefore, be lumped in with the value of L_2. R_1 is the resistance between the power supply and ground. L_1 is the parasitic inductance that exists

after the sensor. C is the capacitance introduced by the I/O pin from the microcontroller and other parasitic capacitances between the sensor and ground. This model had limited accuracy and only provided a rudimentary understanding of how the victim circuit behaved. IEMI attacks on this circuit using inductive coupling could be modeled by treating the attack as a weak transformer between L_2 and the attack circuit. This transformer is assumed to have a very poor coupling coefficient and a small number of turns; since only some of the transmitted EM radiation will reach the victim circuit and the victim circuit was never designed to act as a transformer.

Using the described model, two types of IEMI attacks can be observed: nonresonant and resonant. The resonant frequency is also called the natural response of a circuit and refers to how a circuit dissipates stored energy [19]. Nonresonant attacks can occur at any frequency that effectively transfers power to the victim circuit that is not resonating in the victim circuit. The victim circuit will be inefficient at receiving this transferred power and because of this, nonresonant attacks may not be effective. The effectiveness of transferring power at nonresonant frequencies depends heavily on the physical parameters of the circuit and, therefore, cannot be predicted from this model. Resonant frequency attacks occur at a frequency that resonates in the victim circuit. This will allow the attacker to build up energy in the victim circuit, potentially increasing the efficiency of the power transfer [20]. This increased efficiency could allow the attacker to use less power while making the attack. This model can identify if a resonant frequency below 1 GHz can exist in a victim circuit

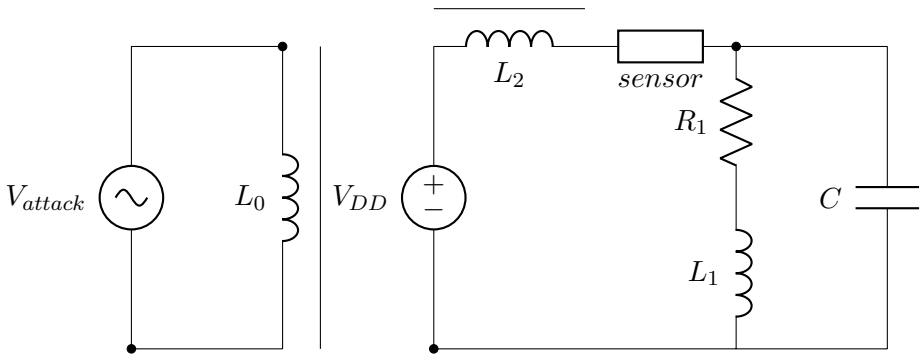

Fig. 3.4: Schematic of the first-order model of the victim circuit.

and give some insight about resonant IEMI attacks.

Using the circuit shown in Figure 3.4, a mathematical model for the expected resonant frequency was derived. The circuit element labeled *sensor* was assumed to be mostly inductive and was therefore lumped in with L_2. The mathematical model that was obtained from doing this can be seen in Equation 3.7 where $\omega = 2\pi f$ and the other terms are the circuit elements.

$$0 = \omega^4 c^2 L_1^2 L_2 - \omega^2 C L_1 (L_1 + 2L_2) + \omega^2 R^2 C^2 L_2 - R^2 C + L_1 + L_2 \tag{3.7}$$

From this equation, the resonant frequency is solved for using several sets of values. Using reasonable values from data sheets, such as $R_1 = 100k$, $L_1 = 100nH$, $L_2 = 170nH$, and $C = 10pF$ the resonant frequency of the circuit was 122 MHz, a value within the defined attack range. Further experimentation with different values showed that the value of the resistance had only a small effect on the resonant frequency, while the values of L_2 and C played the most important roles. Note that the resonant frequency got lower for larger values of L_2 and C.

CHAPTER 4

ATTACKING ANALOG TO DIGITAL CONVERTERS (ADC'S)

This section details the setups and results for both the attacker and victim circuits when the victim used the analog to digital converter (ADC) on the Tiva C microcontroller to take the measurements of a sensor. This circuit was used as the starting point since the level of influence of the attacker was directly measurable. This chapter is broken up into two sections. The first section details the materials and setup of each circuit. The second section details the experimental results. Before these experiments were attempted, there was extensive experimentation with the attacker and victim setups without the presence of the microcontroller. These experiments helped determine the values of resistors and the layout of the circuit. They also showed that the output of the RF amplifiers used in the attacker circuit varied with the frequency of the input waveform. This variation was caused by the lack of impedance matching in the attack circuit. Therefore, it was necessary to be aware of variations in the output of the RF amplifier.

4.1 Setup

This section described the materials and setup of the individual circuits that were used. First, the physical materials and setup will be described. Second, any intangible elements will be described.

4.1.1 Victim Setup

The victim circuit has three parts: the physical circuit, the system level victim setup, and the code running on the microcontroller. For this work, the Tiva C microcontroller was used [21]. This was used for several reasons: its availability, extensive documentation, familiarity, and low cost. A circuit diagram of the victim circuit is shown in Figure 4.2 and a picture is shown in Figure 4.1. For D_1 shown in Figure 4.2 an SFH 235 FA photodiode was

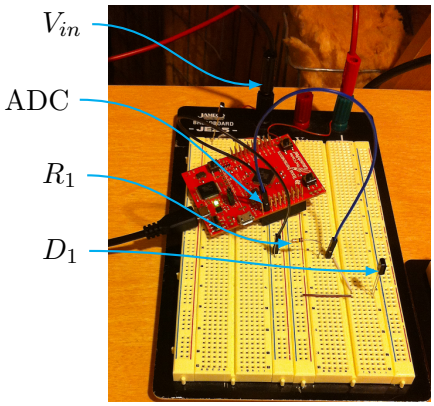

Fig. 4.1: Picture of the victim circuit.

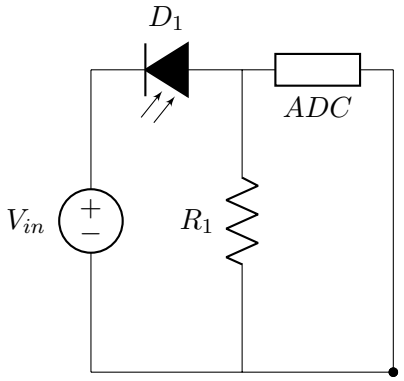

Fig. 4.2: Schematic of the first victim circuit setup.

used, an infrared photodiode with a sunlight filter. Several diodes were examined, however, this one was selected because of its availability and the simple setup that was required. The values for R_1 and V_{in} were 10 kΩ and 10V respectively, both of which are in the operating region of D_1. The physical layout of the board went through two iterations. The first iteration was set up on a bread board and can be seen in Figure 4.1. This was done for speed, simplicity, and flexibility. The results of experiments done with this setup showed that the material setup could significantly influence the results. To reduce the number of variables in the material setup and minimize cable lengths, the same board was put on a printed circuit board (PCB), shown in Figure 4.3. During this change, the value of R_1 was changed to 22 kΩ.

The setup of the system containing the victim circuit, Tiva C microcontroller, CPS250 triple output power supply, and a laptop can be seen in Figure 4.4. The Tiva C microcontroller's ADC measured the output of D_1 in the victim circuit, as the schematic in Figure 4.2 shows. The Tiva C microcontroller was also connected to a laptop for power and to provide the user a method for interfacing with the microcontroller. The CPS250 triple output power supply provided V_{in} for the victim circuit.

The code that was on the microcontroller served two purposes: to take measurements like a victim circuit and to provide an interface for data output. When simulating a potential victim circuit, the code initialized the microcontroller so that it took regular measurements

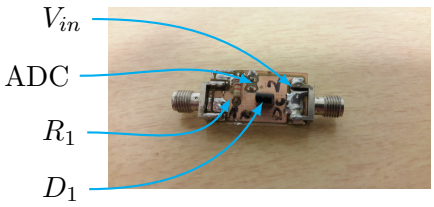

Fig. 4.3: Picture of the victim circuit on a PCB.

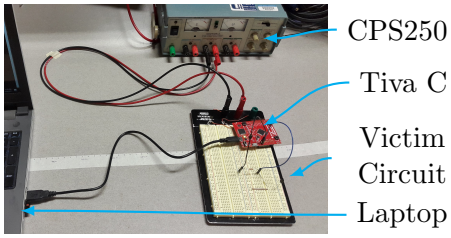

Fig. 4.4: Picture of the setup of the victim system.

with the ADC. For comparison, these measurements were then stored so that they could be averaged and the behavior of the circuit analyzed. This was accomplished using a timer and the ADC. The timer was initialized to be periodic with a 4-microsecond interval that triggered the ADC when it expired. The ADC was initialized to take and store a measurement when the timer interrupt was thrown. This sequence of events made it so that measurements were taken periodically with the timer and stored to be read out later. The timer value of 4 μs was determined empirically as the shortest period that allowed the program to execute normally. To output data, a serial connection was created between the microcontroller and the laptop.

4.1.2 Light Circuit Setup

The light circuit was used in some experiments to stimulate the photodiode used in the design of the victim circuit. A picture of the circuit that was used is shown in Figure 4.5 and a schematic of the circuit that was used is shown in Figure 4.6. An HIR323C Infrared LED was used for D_{light} and was selected as the diode because the wavelength of light it emitted correlated well with the wavelength that D_1 in the victim circuit (Figure 4.2) was sensitive to. In this circuit, the value of R_{light} was set to 51 Ω to reduce the amount of voltage required to turn D_{light} on. The value of $V_{LightSupply}$ was determined manually by comparing the output of the ADC to the desired value.

4.1.3 Attacker Setup

The attacker circuit was composed of the physical circuit and the equipment connected

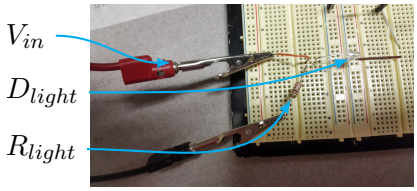

Fig. 4.5: Picture of the light circuit.

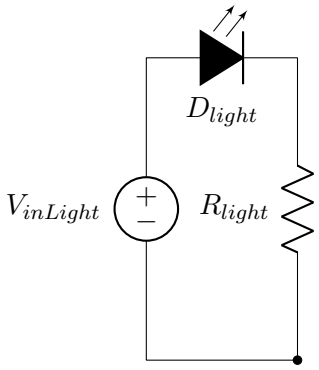

Fig. 4.6: Schematic of the light circuit.

to it, which controlled the input to the circuit. All inputs into the attacker circuit were selected by hand because of the complexity that automation would present. A picture of the attacker circuit is shown in Figure 4.7 and a circuit diagram is shown in Figure 4.8. The attack circuit was set up on a breadboard. This was largely done because of the choice of antenna, which was modeled as L_1 in the circuit diagram and was made by creating a coil of wire from approximately 25 ft (7.6 m) of 22 gauge mag-wire and a plastic spool. The gauge of wire was selected for its ability to handle the current. The antenna was created this

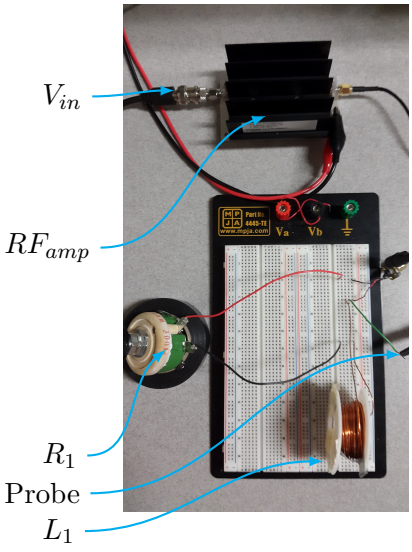

Fig. 4.7: Picture of the attacker circuit.

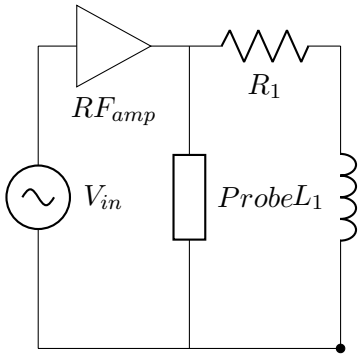

Fig. 4.8: Schematic of the attacker circuit setup.

way to maximize inductance and therefore maximize the inductive coupling that occurred between the attacker and victim circuits. As noted earlier, this was believed to be the most efficient method of conducting this type of attack. A high power potentiometer was used for R_1. This was done to make it easy to experiment with different values for R_1. The RF_{amp} was broadband to allow for experiments over a range of frequencies and provided enough power to make the experiments possible. Over the course of this research, two different RF amplifiers (ZHL-6A+ and ZHL-1A) were used. The ZHL-6A+ provided 22 dBm power output and the ZHL-1A provided 28 dBm power output according to the data sheets [22, 23]. The ZHL-1A amplifier was acquired later and was used exclusively in latter experiments because it had a higher power output. Two different input sources were used as an input source to the RF amplifiers: first, a Tektronix AFG 3252 dual channel arbitrary function generator and second, a Hewlett Packard ESG-3000a signal generator. The AFG 3252 was used for most low-frequency experiments because it was readily available and capable of providing a sine wave input from 0 - 240 MHz [24]. The ESG-3000a was used for all high-frequency experiments, since it could provide a sine wave output from 250 kHz - 3 GHz, and was used to verify the results of many of the low-frequency experiments [25].

4.2 Experimental Results

The experiments were sensitive to the environment and often measured small effects. Therefore, to ensure accurate measurements and correct understanding, the first step was to understand how the setup and environment affected the measurements. This process is detailed in Section 4.2.1. The remaining sections deal with how different variables affected the attack. First, the effects from a different physical layout of the victim circuit are discussed. Second, the effects of using different sampling times in the victim circuit are discussed. Third, the effects that different orientations of the transmitting coil had are covered. Finally, the effectiveness of the attack at different frequencies is discussed.

4.2.1 Accuracy of Experimental Results

For the initial sets of experiments, the victim circuit (Figure 4.2) was placed approximately 5 cm in front of the attack circuit (Figure 4.8) with the photodiode positioned at approximately the center of L_1. The victim circuit was placed 5 cm away to maximize the power provided by the RF amplifier since it only provided about half a watt. It was concluded from previous works and EM theory that the amount of power used was critical to an experiment's success. The validity of doing this attack in a lower power environment at close range was also seen from the model of the attack presented in Section 3.2. Power decays with distance at a rate of r^4 where r is the distance from the antenna. A Tektronix MDO4000 oscilloscope was used to measure the output of the RF amplifier in the attacker circuit. The initial results using the ZHL-6A+ are shown in Figure 4.9. These measurements were intended to help identify the resonant frequency of the circuit because it was impossible to measure the parasitic elements of the circuit adequately in order to calculate the resonant frequency. The idea was that the largest peak in the measurements would likely correspond with the resonant frequency. These initial results raised concerns about the accuracy of the electrical circuit model that was presented Section 3.2. From this model, a single resonant frequency and, therefore, a single large peak was predicted. However, these results showed four peaks, two of which were similar in strength and obviously not harmonics of each other. What caused the four peaks and why did they appear to be unrelated?

Since these were the first experimental tests, the validity of the model was investigated first. It was assumed that the two largest peaks occurred because of resonant frequencies inside the circuit. For this to be the case, there needed to exist multiple resonant cavities inside the circuit. To examine this possibility, several models that accounted for additional parasitic elements in the circuit and a more extensive model of the microcontroller pin were examined. However, these models ultimately couldn't account for the second peak when realistic values were used. The second possibility investigated was that these peaks were caused by interference from another source or from some aspect of the setup. In the process

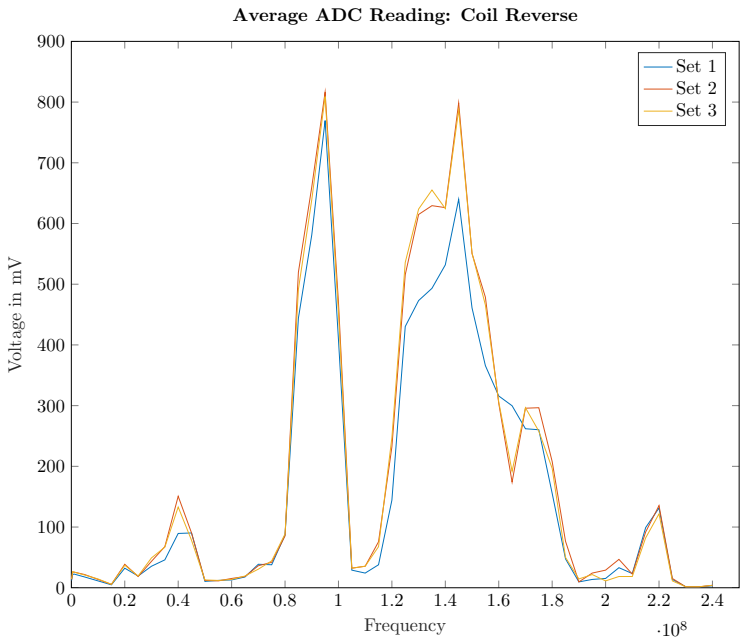

Fig. 4.9: ADC measurements using the ZHL-6A+ amplifier as an input to the attacker and a sensor output of 0.

of investigating the setup, it was discovered that the position of the wire connecting the oscilloscope to its probe affected the measurements, specifically the second peak around 135 MHz. Further experimentation showed that when the oscilloscope wire came close to the power cables supplying power to the victim circuit or other parts of the circuit, greater effects were measured and the second peak around 135 MHz appeared. The most likely reason for this is that the oscilloscope wire itself was acting as an antenna and coupling power to the victim circuit instead of L_1 because of its proximity to parts of the victim circuit. This led to an investigation of other cables in the setup to determine if any other unintended coupling was occurring. This experimentation showed that if any cables connected to the opposite setups were close to each other, the measurements were affected. To prevent any unintended coupling from occurring, the wires for the attacker and victim circuit were separated from each other as much as possible. After the separation of wires was completed, experiments to be sure the oscilloscope probe wasn't acting as an unintended antenna were conducted with and without the oscilloscope probe connected to the output of the amplifier. Some of

the first sets of measurements that were done this way can be seen in Figure 4.10.

As can be seen clearly from Figure 4.10, when the oscilloscope probe was present in the attack circuit, the attack was able to transfer an additional 100 mV at 100 MHz and approximately 300 mV at 210 MHz, making the attack much more effective. Was the oscilloscope probe acting like an antenna again or was it changing something fundamentally in the circuit? To determine if the oscilloscope was acting like an antenna, the position of the probe relative to cables connected to the victim circuit was experimented with. This was done by fixing the input frequency to the amplifier and moving the cable to several positions and seeing if the average value of ADC readings changed meaningfully. Several frequencies were tried but no meaningful changes in the average value of the ADC readings were observed. From this experiment, it was concluded that the oscilloscope probe was improving the transmission of the attack circuit. To attempt to replicate these effects, capacitors were added in parallel with the output of the amplifier. Since the estimated capacitance present in the probe was 3.5 pF, the values of capacitors tested were 3, 4, and 5 pFs. The results of this test are shown in Figure 4.11. For these experiments, values equal

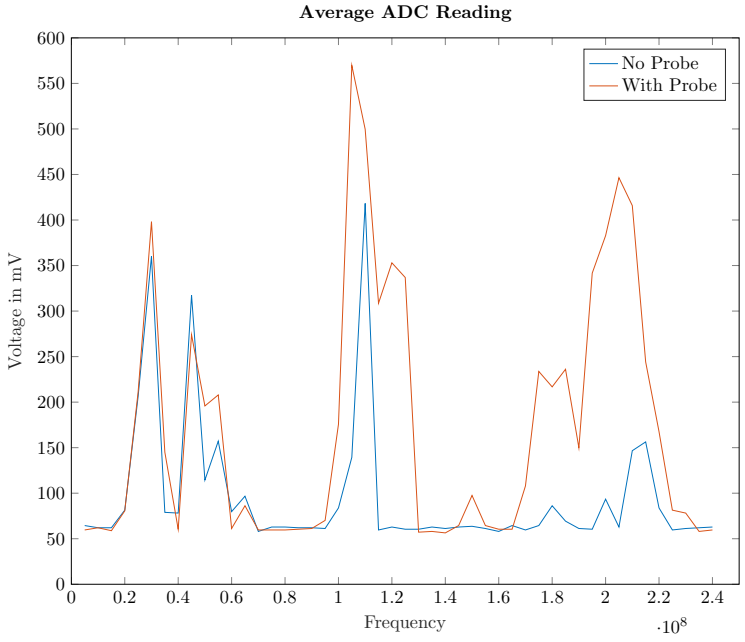

Fig. 4.10: ADC measurements with and without the oscilloscope probe.

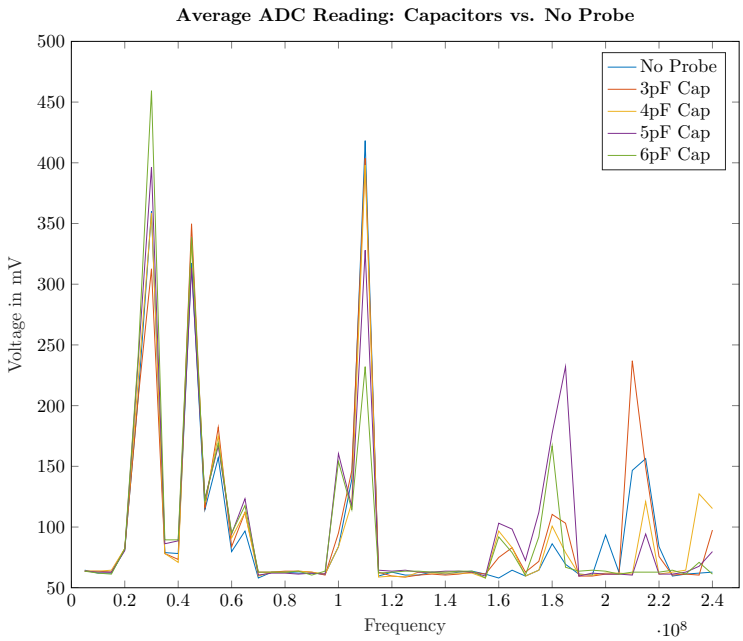

Fig. 4.11: Effects of adding capacitors instead of the oscilloscope probe.

to or less than 425 mV were read, which was similar to the results of experiments done without a probe. Experiments done with the probe consistently measured around 550 mV which is about 125 mV more than experiments without a probe. To definitively prove if the circuit characteristics of the attacker changed, a network analyzer was used to measure the S function of the attacker circuit without power from 0 - 1 GHz. These results are shown in Figures 4.12 and 4.13. These figures show that the S11 response of the circuit improved when the oscilloscope probe was present, confirming the theory that the presence of the probe improved the transmission of the attacker circuit.

4.2.2 Physical Layout

This section focuses on the effects that the physical setup of the victim circuit had on the effectiveness of the IEMI attack. The results of these experiments combined with the results of Section 4.2.1 lead to the creation of the PCB setup of the victim circuit. For these experiments, the victim circuit was placed approximately 5 cm away from the attack circuit. The photodiode was positioned to be in the center of L_1 with the microcontroller 2

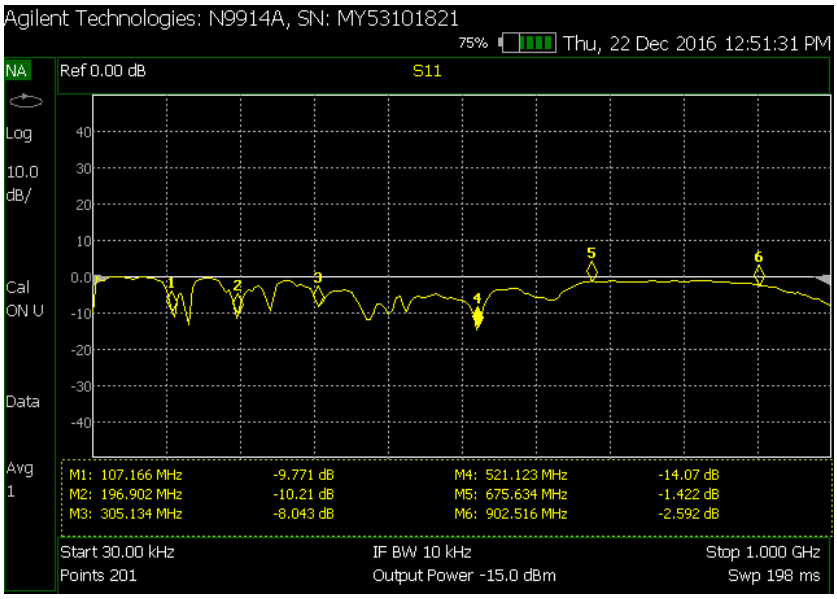

Fig. 4.12: Frequency response without the oscilloscope probe.

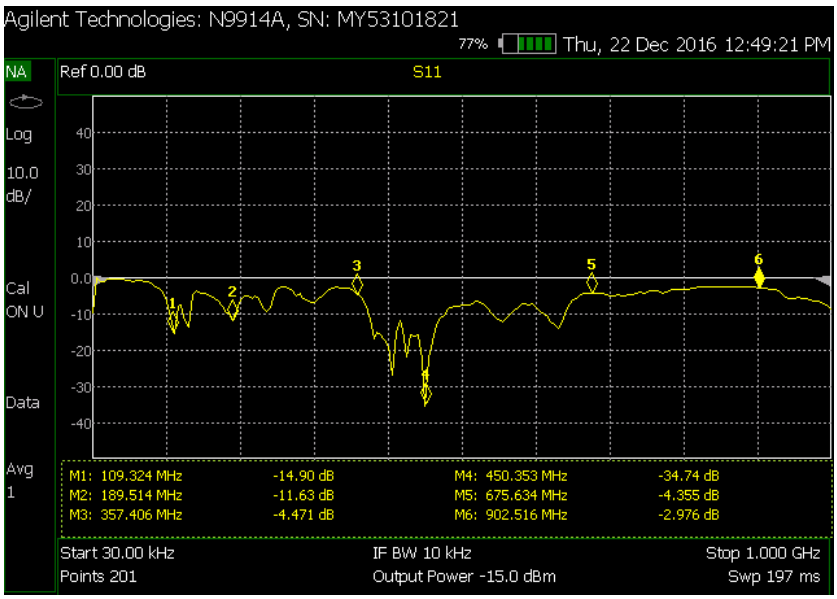

Fig. 4.13: Frequency response with the oscilloscope probe.

- 3 cm further back and offset to the side of D_1. With this physical setup, frequency sweeps were done with a fixed power input of approximately 9 dBm or 600 mV. These experiments were done after the separation of cables described in Section 4.2.1 took place.

Two circuit factors were investigated: first, pin usage for the ADC and second, the lead lengths of different connections. The first question - does the pin that is used make a difference to the effectiveness of IEMI attacks - had several implications. If using different pins to take measurements affected the effectiveness of IEMI attacks, the danger of these attacks could be easily minimized. The researchers identified the pins' proximity to ground as a potential cause of these differences. The theory was that proximity to a ground plane could reduce the effectiveness of the attack for two reasons. First, it could absorb more of the EMI and second, it could reduce the size of any fluctuations in the ground plane relative to the pin. Both of these factors could potentially reduce the effectiveness of the attack. To see if this was the case, two different pins were used to take ADC measurements: PE3 and PB5. Pin PB5 was selected because of its proximity to a ground pin, while pin PE3 was selected because it was far away from a ground pin. The results of these experiments can be seen in Figure 4.14 and show that little, if any, effect from using a different pin was observed.

The second question - do the lead lengths make a difference to the effectiveness of IEMI attacks - also had clear implications. If lead lengths affected the effectiveness of IEMI attacks, protecting a circuit could be as simple as shortening lead lengths. Changing the lead lengths had multiple effects on the circuit. First, increasing or decreasing the lead lengths changed the value of parasitic inductance or capacitance that existed in the circuit, potentially affecting the resonant frequency. Second, the lead lengths affected the ability of the wire to act as an antenna for different frequencies. Third, it changed the sizes of loops in the circuit potentially changing the amount of the H field passing through the loop and thus affecting the amount of energy that was transferred. To determine the impact of these effects, the lead lengths of several connections were examined on the breadboard setup. These experiments were done using PB5 to take the ADC measurement with the

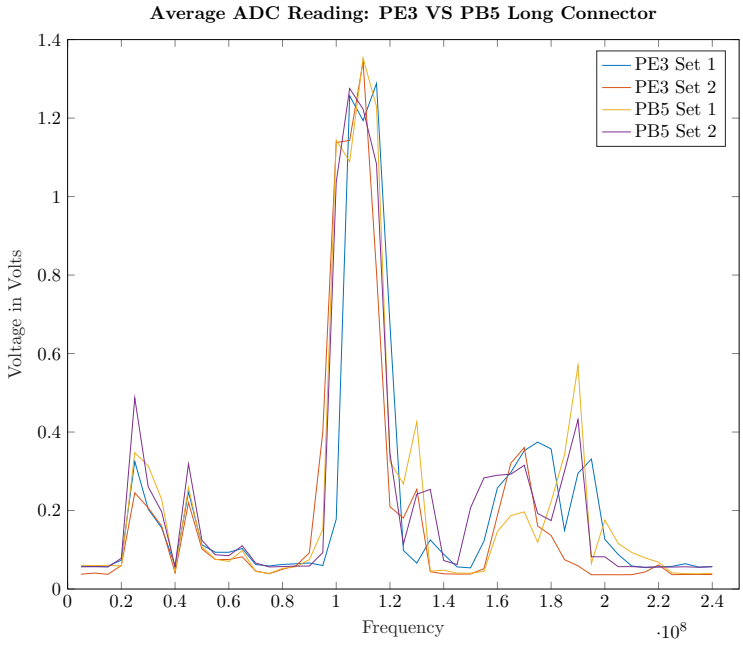

Fig. 4.14: Comparison of the effects of using PE3 vs. PB5 as the input to the ADC.

attacker and victim circuit as previously described. First, the length of connections between the breadboard and the microcontroller were examined. These leads connected the ADC pin to the output of the photodiode and provided a common ground. The two lead lengths that were used were 20 cm and 5 cm. The microcontroller had previously been positioned so that its position relative to the rest of the circuit did not change when new leads were connected. The prediction was that the peaks that were seen might increase in frequency as it was believed that the resonant frequency played a significant role. The results of this experiment are shown in Figure 4.15.

The most noticeable change was the absence of the peak around 100 MHz, which was unexpected. If this peak was caused by resonant coupling, as was first hypothesized, the peak should have shifted, not disappeared. The absence of the peak suggested that another factor was primarily or totally responsible for it. Another supporting factor for this was that the other peaks in the circuit's response remained unchanged. This suggested that the resonant frequency may not be the dominant factor at low frequencies.

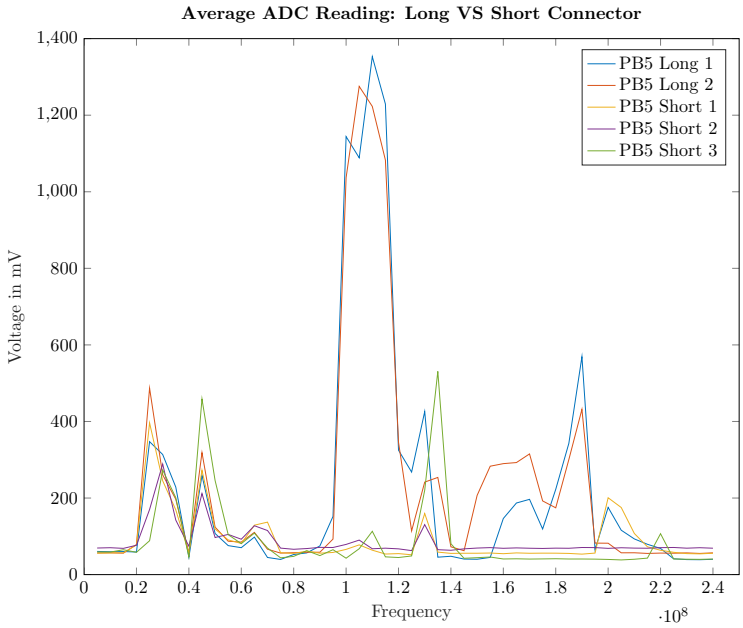

Fig. 4.15: Comparison of the effects of using different lengths of header pin cables.

To further test how lead lengths affected the response of the circuit, the power leads were examined. The power leads of the circuit were nearly 1 m or 100 cm long, much larger than the 15-cm difference between the different connectors. For this experiment, an additional set of power leads was connected to the victim circuit. This made the total length of the power leads 2 m or 200 cm. The additional lengths of power cables were positioned so that the position of the power cables relative to the victim circuit was similar to previous experiments. The position of the rest of the victim circuit didn't change at all. After the additional power cables were connected, the experiment as described above was conducted again. Those results are shown in Figures 4.16 and 4.17. When there was only one set of power leads there was a clear peak around 40 MHz. This peak shifted to 15 MHz with the addition of the second set of leads, validating the hypothesis that the peak would shift to a lower frequency with the addition of more power cables.

The results presented in this section show that the length of connections in the victim circuit played an important role in the circuit's susceptibility to IEMI attacks. Long lead

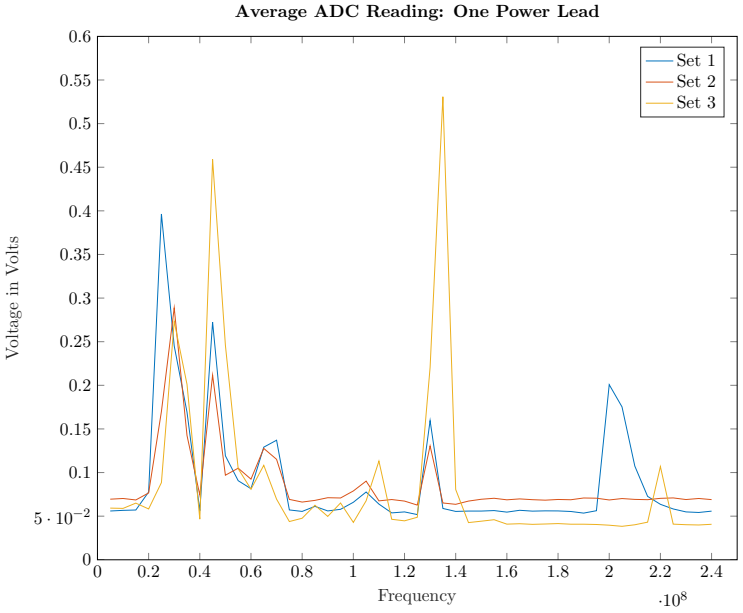

Fig. 4.16: ADC measurements with one power lead.

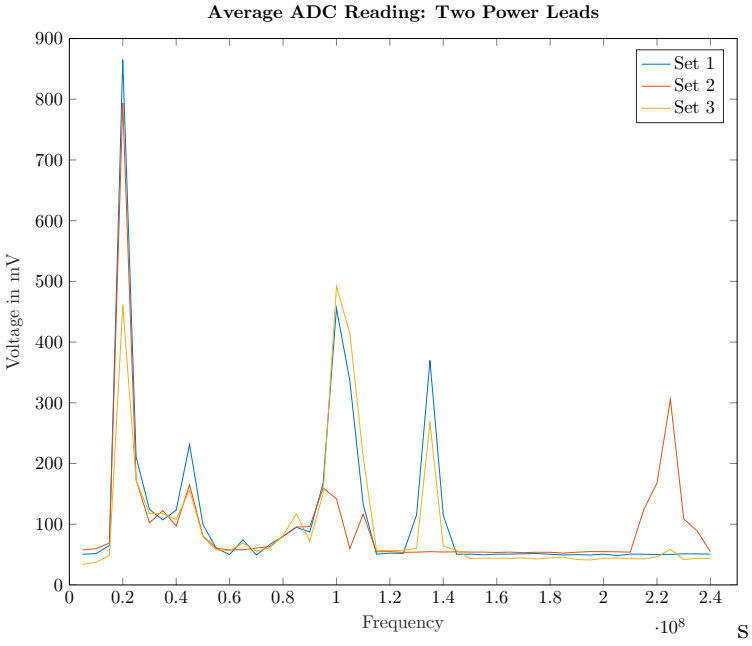

Fig. 4.17: ADC measurements with two power leads.

lengths consistently showed higher effects from IEMI attacks. To minimize these effects and to provide a consistent setup, a PCB board was created using the schematic and circuit values described in Section 4.1.1. The PCB board was connected directly to the header on the back of the Tiva C and was approximately 1 cm by 3 cm in total size. This size estimate excludes the SMA connectors that were attached to the circuit board. This entire setup was then placed 5 cm from the attack circuit and frequency sweeps from 5 - 240 MHz were done. The input power to the amplifier was 1.2 Vpp which is .424 V_{rms} or approximately 6 dBm. These experiments were expected to show two things: a dramatic decrease in the amount of coupled voltage and changes in the effective frequencies for coupling energy to the circuit. The results of these experiments are shown in Figure 4.18. As can be seen, the effect was greatly reduced. When the experiment was done using the breadboard, values 500 - 800 mV were consistently found. However, when the PCB was used, at most 60 mV were detected. This is approximately an order of magnitude decrease in the coupled energy for the same transmission power. The experimental results of increasing the transmission power

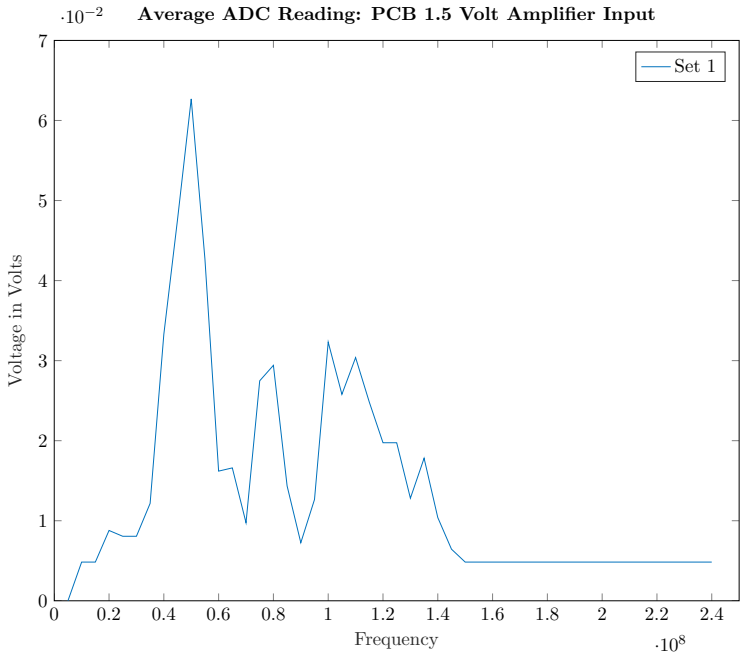

Fig. 4.18: ADC measurements from the PCB setup with an attacker input power of 6 dBm or 1.2 Vpp.

to 5.6 Vpp or 2 V_{rms}, which is approximately 19 dBm, and redoing the experiment showed a maximum influence around 140 mV as shown in Figure 4.19. These results were still significantly less than the results from when the breadboard was used, despite increasing the power by a factor of 4.1. Another note is that the peaks of highest influence were seen in different locations on the PCB than the breadboard setup. The major peaks in the breadboard were around 30 MHz and 45 MHz where on the PCB they were around 45 MHz and 65 MHz. This shift in the peaks was probably partially due to decreased stray inductances caused by decreased area and wire size. These results support the previous experiments and show that IEMI attacks require more power when lead lengths are shorter.

4.2.3 Sampling Time Effects

Denis Foo Kune et al. discussed the use of ADCs for demodulating AC signals. They observed that by matching the sampling frequency of the ADC with the attack signal the ADC would demodulate the signal. Clearly, this would be an ideal way to attack an ADC

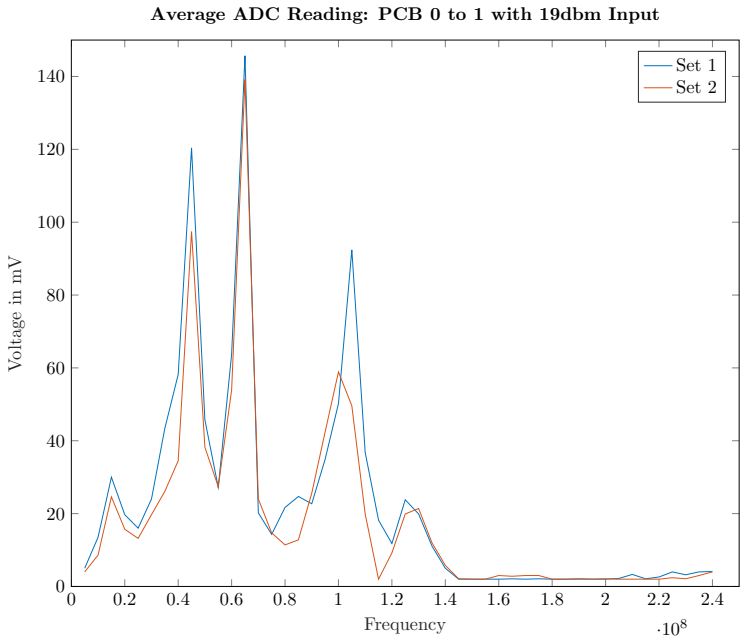

Fig. 4.19: ADC measurements from PCB setup with an attacker input power of 19 dBm or 5.6 Vpp

since it would allow the attacker complete control of the signal measured by the ADC. A question related to this theory is how different ADC sampling frequencies affect the results of an IEMI attack, especially when the sampling frequencies of the ADC don't correspond well with the attack frequency. To test this, the PCB victim circuit was placed 5 cm from the attacking circuit using a power input of 19 dBm. Sweeps of possible attack frequencies from 0 - 240 MHz were done with changes in the sampling frequency of the ADC. If this effect made a significant difference, then the effective frequencies for an IEMI attack on a circuit should have changed with changes in sampling time. To see if this was the case, experiments were run with sampling times of 4, 8, and 25 μs which translate into sampling frequencies of 250, 125, and 40 kHz. The results of these experiments can be seen in Figure 4.20. The most interesting result of these tests was that the average value seen by the ADC didn't really change when the sample time was changed. This suggests that while the sample time may affect the measurements that are done, it does not affect the most efficient attack frequency. The Nyquist theory may provide a partial explanation for this. More detailed experiments would need to be done to be sure. Since the sampling frequency

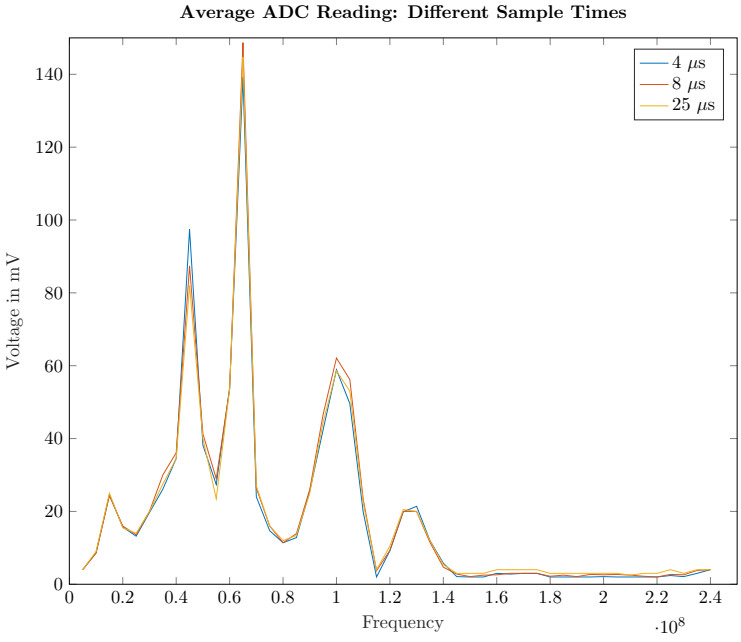

Fig. 4.20: ADC measurements comparing different sample times.

was significantly less than twice the attack frequency, the bandwidth of the ADC may have been too small to detect changes in the attack frequency. Small variations in the attack signal would contribute to this problem. The effects that Nyquist theory describes, combined with the effects of averaging of the measurements, which reduces measurement noise, may explain why IEMI attacks significantly above the Nyquist frequency seemed unaffected by the sampling time. Some support for this can be seen in Figure 4.21, which shows 10,000 consecutive values read by the ADC before they are averaged together. This shows that the value read by the ADC varies widely over time and may provide a potential way of detecting IEMI attacks. It also shows that while different sampling frequencies may increase or decrease the effectiveness of the attack, the attack will always be able to be conducted. These effects may be specific to sine wave input attacks since these attacks are inefficient because the mean value of a sine wave is zero, and a sine wave spends equal amounts of time with an increasing and decreasing slope.

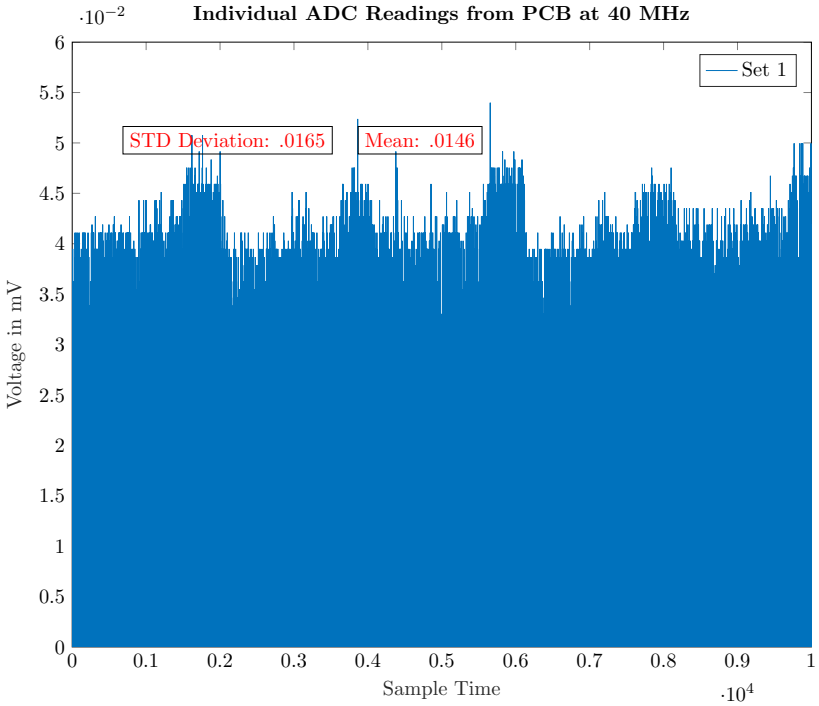

Fig. 4.21: 10,000 consecutive ADC measurements at 40 MHz.

4.2.4 Increasing or Decreasing ADC Measurements

One of the goals of this research was to show that it is possible to both increase and decrease the average value seen by the microcontroller using its ADC. Theoretically, this could be accomplished by inverting the EM field. With a coil, the inverse EM field can be obtained by reversing the direction of the winding on a coil or reversing the direction the coil faces. To determine if this would provide a way for the attacker to control if they were increasing or decreasing the victim circuit's readings, two experiments were conducted with opposite orientations. These experiments were done using the bread board setup positioned approximately 5 cm from the coil. The results of these experiments are shown in Figures 4.22 and 4.23. They show that changing the orientation of the coil didn't affect the results that were seen when the output of the light sensor was zero. In both cases, the attack was conducted using the same voltage at the same frequencies.

This calls into question if IEMI attacks using a sine wave input will be able to decrease the average value read by an ADC on a microcontroller. To determine if this was the case, a variety of tests were conducted using the light circuit described in Section 4.1.2. This

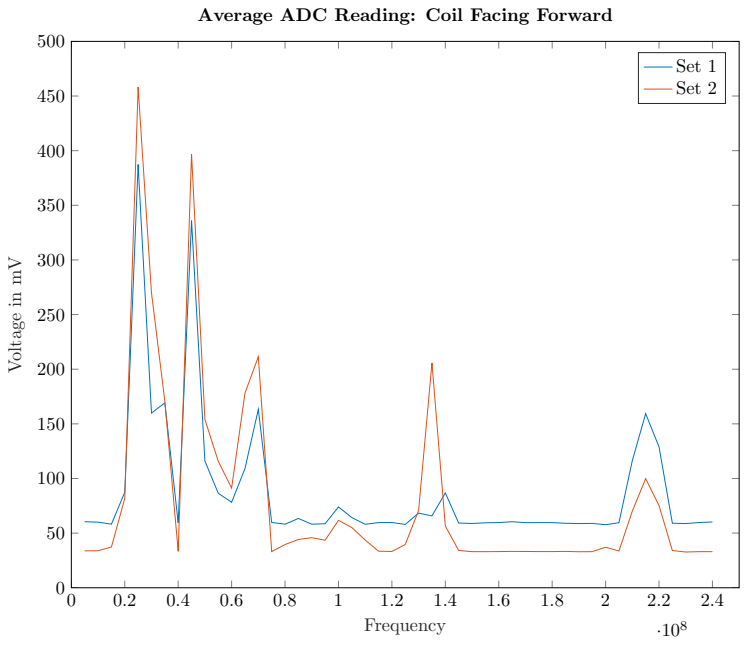

Fig. 4.22: ADC measurements with coil facing forward.

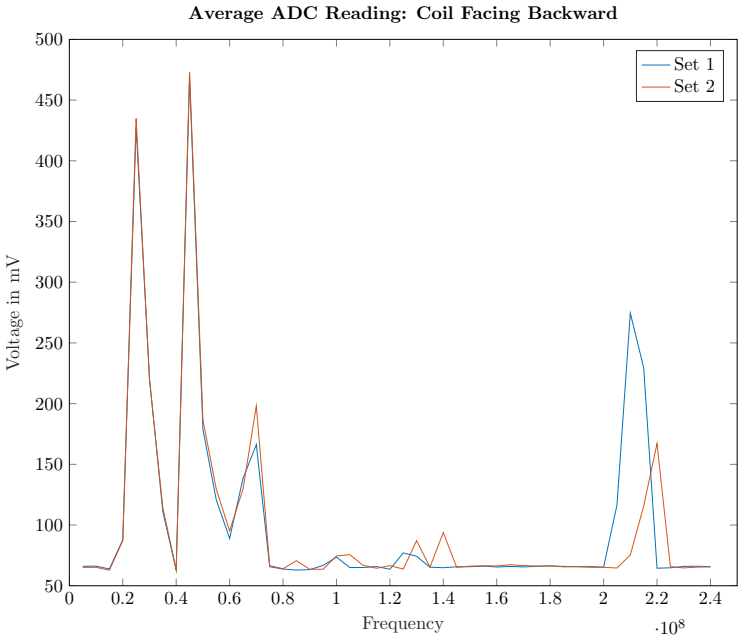

Fig. 4.23: ADC measurements with coil facing backward.

circuit was added to the setup to provide stimulation for the light sensor. This circuit was positioned 3 - 5 cm away from the D_1 in the victim circuit on the same breadboard and was powered from a separate output of the same dual channel power supply that was powering the victim circuit. Using the light circuit, the average output of the ADC on the Tiva C was increased to just over 3 V and 3.2 V for two separate sets of tests. The results of these experiments can be seen in Figure 4.24. These results show that the IEMI attack was able to decrease the average value of the ADC, regardless of the orientation of the coil or sensor output. In addition to this, Figure 4.24 displays other interesting qualities. First, the frequency that had the largest effect was around 25 MHz, which is one of the frequencies that was very effective at increasing the average value of the ADC. Second, the peak at 45 MHz was reduced to almost nothing and was only noticeable when the output of D_1 was around 3.2 V. Also, there was an additional small peak around 100 MHz that did not show up in the previous experiment. The final interesting note is that even though all four experiments used the same setup, with the exception of the intensity of light, all of the measurements taken with an attack signal of 25 MHz and 100 MHz were almost identical.

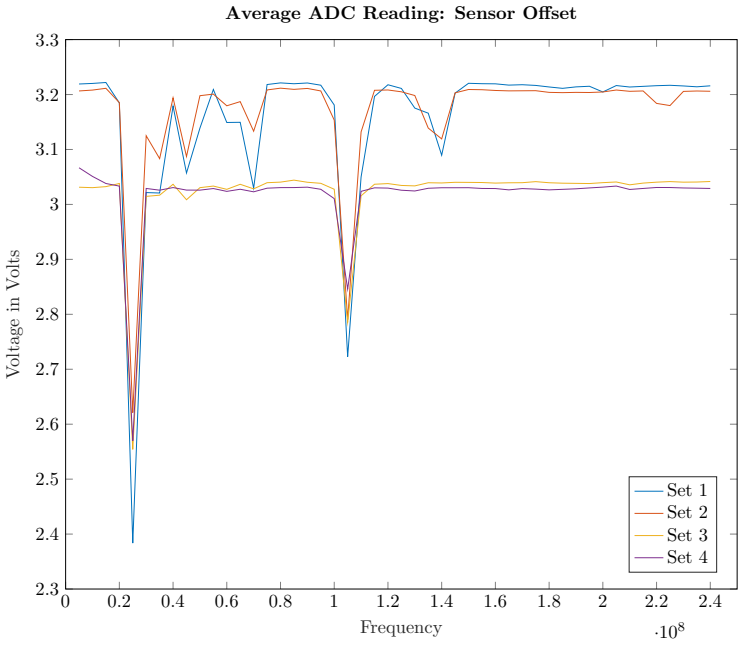

Fig. 4.24: Results of testing with a high output from the light sensor.

This suggests that the effective frequency of IEMI attacks that attempt to increase or decrease the average value measured by the ADC are related since 25 MHz was one of the most effective frequencies for changing the average value of the ADC in both cases. However, the exact nature of the relationship between attacks that increase or decrease a sensor's average output is unclear because of the reaction of the circuit at 45 MHz and 100 MHz. The behavior of the circuit at these frequencies presents two concerns. The first concern is that the 100 MHz peak was only present in these experiments when the attacker was trying to decrease the value read by the ADC, though it was seen on occasion in other experiments, suggesting that it may have been caused by environmental factors. Unfortunately, this was never definitively determined. The second concern is the fact that all of the experiments that attempted to decrease the average value output by the ADC had nearly the same value at 25 MHz and 100 MHz, despite having two different voltage offsets, which suggests that there may be a limit on how far a sine wave can decrease the average value of the ADC.

4.2.5 Resonant Coupling

This section details the experiments that were done to determine the resonant frequency of the victim circuit and what the effectiveness of a resonant IEMI attack was for this research. The results presented in this section were obtained by placing the PCB victim circuit approximately 5 cm in front of the attacker circuit. Other experiments were done but will not be presented since the PCB setup most accurately represents a real victim. The first difficulty in testing the effectiveness of a resonant attack is identifying if an attack is at the resonant frequency. This can't be done mathematically because the existence of a resonant attack relies on the effects of parasitic elements in the circuit which are difficult to measure accurately. Several methods of identifying the resonant frequency of the circuit were attempted. First, frequency sweeps were done to look for the peak response. This method assumed there would be a single peak and that this peak would correspond to the resonant frequency, which could then be verified. However, the existence of multiple peaks and the difficulty of identifying environmental factors made this method ineffective. To remove environmental and setup variables, a network analyzer was used to measure the S11 response of the entire circuit. An AT-N9914A FIELDFOX was used to take these measurements of the victim circuit from 0 - 1 GHz and the results can be seen in Figure 4.25. This shows that three peaks existed for the received power of the setup, around 600, 745, and 839 MHz respectively. Additional measurements on multiple circuits led to the conclusion that the resonant frequency was around 745 MHz, which was on the high end of the intended frequency range of the attack. To test the effectiveness of a resonant attack, several frequency sweeps were done from 0 - 800 MHz. These experiments didn't show any power being coupled to the victim circuit at frequencies above 400 MHz. The results of one of these sweeps are shown in Figure 4.26. This lack of success could be due to any number of factors that are beyond the scope of this research. One possibility is the equipment that was used. The antenna, a coil of mag-wire, was not impedance matched nor did it function well at high frequencies. Furthermore, the ZHL-1A amplifier is only rated to 500 MHz and the frequency of the attack is well above that. Another plausible reason, or at least a

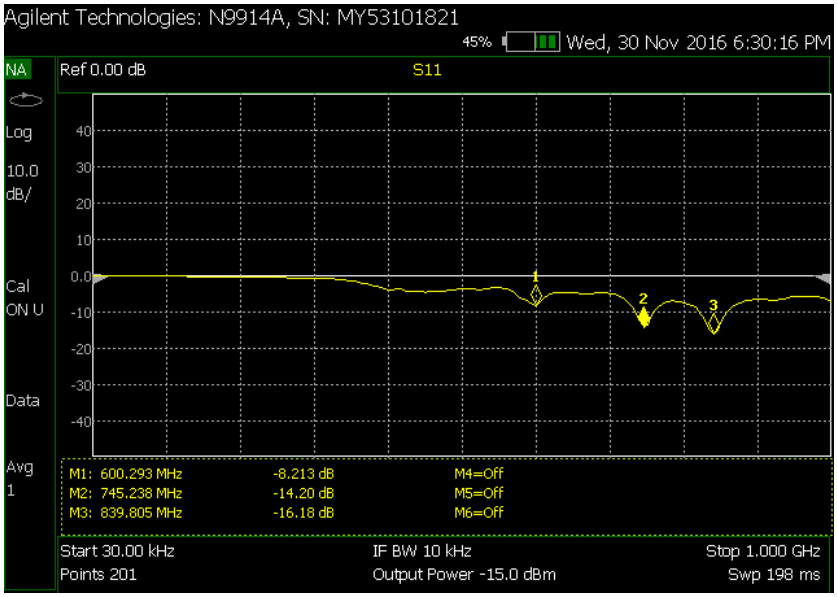

Fig. 4.25: S11 measurements from the network analyzer from 0 - 1 GHz.

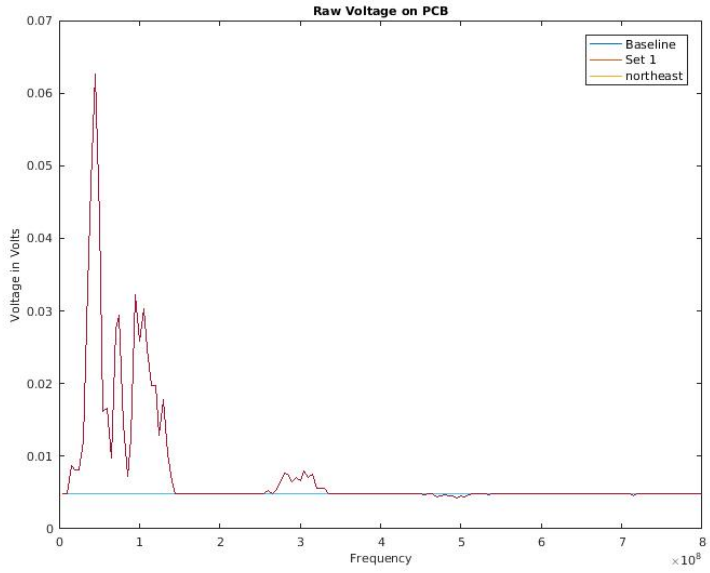

Fig. 4.26: Voltage read by the ADC of the microcontroller over an 800 MHz attack sweep.

contributing factor, is explained by A. Boyer et al. Their study modeled and tested a direct power injection attack on a 16-bit microcontroller, and found that the amount of power

required to flip a bit increased with attack frequency [16].

4.3 Summary of Experiments

No new information is presented in this section. Tables 4.1 and 4.2 summarize the experiments that were done to obtain the graphs that are presented in this chapter and the reference for the graph.

Table 4.1: Table of Graphs in ATTACKING ANALOG TO DIGITAL CONVERTERS (ADC'S) including a brief description and figure number.

Description	Figure Number
This shows initial experiments on the breadboard setup. The ZHL-6A amplifier was used with an input of 600 mV_{pp}. The photodiode was setup to output a low voltage.	4.9
This shows experiments on the breadboard setup with and without the oscilloscope probe. The ZHL-1A amplifier was used with an input of 1.2 V_{pp}. The photodiode was setup to output a low voltage.	4.10
This compares experiments on the breadboard setup without the oscilloscope probe against experiments using various capacitors. The ZHL-1A amplifier was used with an input of 1.2 V_{pp}. The photodiode was setup to output a low voltage.	4.11
This shows experiments on the breadboard setup comparing measurements taken on pins PE3 and PB5. The ZHL-1A amplifier was used with an input of 1.2 V_{pp}. The photodiode was setup to output a low voltage.	4.14
This shows experiments on the breadboard setup comparing measurements taken with long and short connectors. The ZHL-1A amplifier was used with an input of 1.2 V_{pp}. The photodiode was setup to output a low voltage.	4.15
This shows experiments on the breadboard setup comparing measurements taken with one set of power leads. The ZHL-1A amplifier was used with an input of 1.2 V_{pp}. The photodiode was setup to output a low voltage.	4.16
This shows experiments on the breadboard setup comparing measurements taken with two sets of power leads. The ZHL-1A amplifier was used with an input of 1.2 V_{pp}. The photodiode was setup to output a low voltage.	4.17

Table 4.2: Continuation of the Graphs in ATTACKING ANALOG TO DIGITAL CONVERTERS (ADC'S) including a brief description and figure number.

Description	Figure Number
This shows the initial experiments on the PCB setup. The ZHL-1A amplifier was used with an input of 1.2 V_{pp}. The photodiode was setup to output a low voltage.	4.18
This shows the experiments on the PCB setup. The ZHL-1A amplifier was used with an input of 5.6 V_{pp}. The photodiode was setup to output a low voltage.	4.19
This compares experiments on the PCB setup using different sample times. The ZHL-1A amplifier was used with an input of 5.6 V_{pp}. The photodiode was setup to output a low voltage.	4.20
This shows the individual values read on the PCB setup at an attack frequency of 40 MHz. The ZHL-1A amplifier was used with an input of 5.6 V_{pp}. The photodiode was setup to output a low voltage.	4.21
This shows experiments on the breadboard setup comparing measurements taken with the antenna coil pointing forward. The ZHL-1A amplifier was used with an input of 1.2 V_{pp}. The photodiode was setup to output a low voltage.	4.22
This shows experiments on the breadboard setup comparing measurements taken with the antenna coil pointing backward. The ZHL-1A amplifier was used with an input of 1.2 V_{pp}. The photodiode was setup to output a low voltage.	4.23
This shows experiments on the breadboard setup. Both orientations of the antenna coil were used. The ZHL-1A amplifier was used with an input of 1.2 V_{pp}. The photodiode was setup to output a high voltage.	4.24
This shows the results of frequency experiments on the PCB setup. This frequency sweep attempted to test the resonant frequency of the PCB setup. The ZHL-1A amplifier was used with an input of 1.2 V_{pp}. The photodiode was setup to output a low voltage.	4.26

CHAPTER 5

ATTACKING GPIO PINS AND DIGITAL LOGIC

This section details the setups and results for both the attacker and victim circuits when the victim used GPIO pins to communicate digital logic between two Tiva C microcontrollers. To test the success of these attacks, the percentage of times that a GPIO pin reported the wrong value was measured. Changing the logic level of a GPIO pin is much harder than changing the average value reported by the ADC, since much larger voltages must be induced. In previous experiments, voltages large enough to force an unsteady logical level were only measured on the breadboard setup. Therefore, any lack of success with these experiments may be attributed to insufficient power. In this case, additional testing with better antennas and higher power will be necessary to determine any potential threat of IEMI attacks against digital logic which would be beyond the scope of this research. To the knowledge of the author, this is the first attempt at using low power IEMI to change digital logic.

5.1 Initial Setup

This section describes the individual setups that were used in the system. The setup of the victim and then the setup of the attacker will be described.

5.1.1 Victim Setup

The victim circuit had two parts to it: first, the physical circuit and second, the code running on the microcontrollers. For this work, two Tiva C microcontrollers were used [21]. A picture of the setup is shown in Figure 5.1. For the circuit, two GPIO pins were connected directly using male to female header cables. The GPIO pin that was configured as an input was also configured to have a weak pull-up resistor. This setup was tested with and without a common ground.

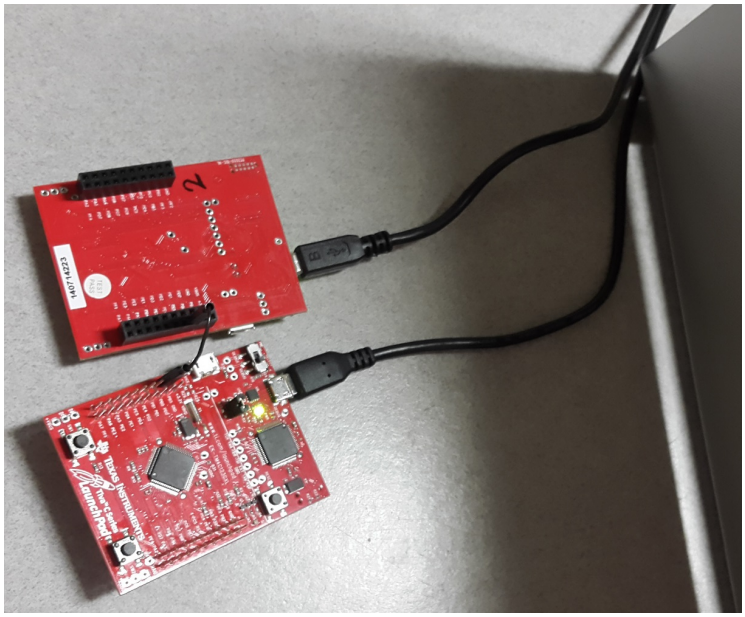

Fig. 5.1: Picture of the victim circuit for testing GPIO attacks.

The code that was on the microcontroller served two purposes: to take regular measurements of a digital output and to provide an interface for data output. To take regular measurements of a digital output the microcontroller was initialized to use a GPIO pin and timer to take readings. The timer was periodic and threw an interrupt when it expired which triggered a read of the GPIO pin. The interface for data output was created using a serial connection between a laptop and the microcontroller. Through this connection, the user had a text interface that allowed the user to enter information about the surrounding environment and then start a set of measurements. After a set of measurements was taken, the total number of logical 1's and 0's measured were output over the serial connection.

5.1.2 Attacker Setup

The attacker circuit primarily consisted of the physical circuit and the equipment connected to it that controlled the input to the circuit. All inputs into the attacker circuit were selected by hand because of the complexity of automation. A picture of the attacker circuit is shown in Figure 5.2 and a circuit diagram of the attacker circuit is shown in Figure 5.3. The attack circuit was set up on a breadboard. This was largely done because

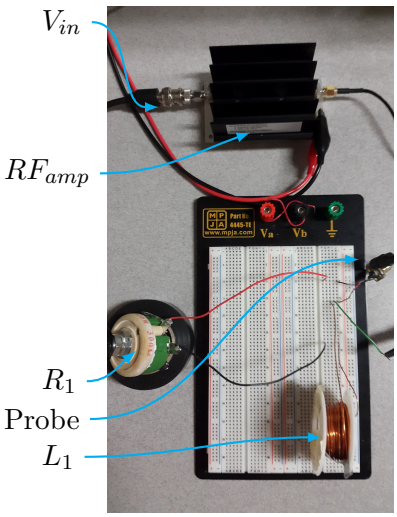

Fig. 5.2: Picture of the attacker circuit.

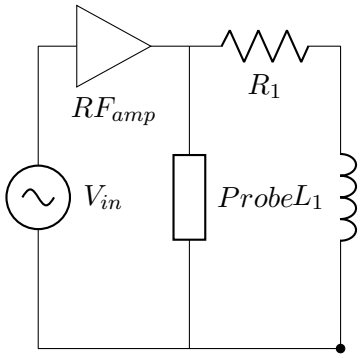

Fig. 5.3: Schematic of the attacker circuit setup.

of the choice of antenna. The antenna was modeled as L_1 in the circuit diagram and was made by creating a coil of wire from approximately 25 ft (7.6 m) of 22 gauge mag-wire and a plastic spool. The gauge of wire was selected for its ability to handle the current. The antenna was created in this way to maximize inductance and therefore maximize the inductive coupling that was occurring between the attacker and victim circuits. As noted earlier, this was believed to be the most efficient method of conducting this type of attack. A high power potentiometer was used for R_1 so that it was easy to experiment with different values. The RF_{amp} was broadband to allow for experiments over a range of frequencies and provided enough power to make the experiment possible. Over the course of this research, two different RF amplifiers (ZHL-6A+ and ZHL-1A) were used. The ZHL-6A+ provided 22 dBm power output and the ZHL-1A provided 28 dBm power output according to the data sheets [22, 23]. The ZHL-1A amplifier was acquired later and was used exclusively in latter experiments because of the increased power. Two different input sources were used as an input source to the RF amplifiers: first, an AFG Tektronix 3252 dual channel arbitrary function generator and second, a Hewlett Packard ESG-3000a signal generator. The AFG 3252 was used for most low-frequency experiments because it was readily available and capable of providing a sine wave input from 0 - 240 MHz [24]. The ESG-3000a was used for all

high-frequency experiments and to verify the results of many low-frequency experiments. It was able to provide a sine wave output from 250 kHz - 3 GHz [25].

5.2 Experimental Results

The first set of experiments that were done used the victim circuit without the common ground. The victim was placed 5 cm in front of the attack circuit and frequency sweeps were done with a 19 dBm input to the RF amplifier. These experiments were repeated with high and low outputs from the second microcontroller. The results are shown in Figures 5.4 and 5.5. The highest percentage of misreads in these experiments was about 35%, which occurred when the logical output being measured was zero. This likely had something to do with logic levels. For similar experiments attacking the ADC, no voltage over 1 V was ever observed. Assuming that a similar amount of voltage was being coupled to the GPIO circuit, a true bit flip could not be accomplished; however, this amount of voltage would likely put the logic level into an undetermined state. This is a possible explanation for why no more than 35% of the bits ever flipped.

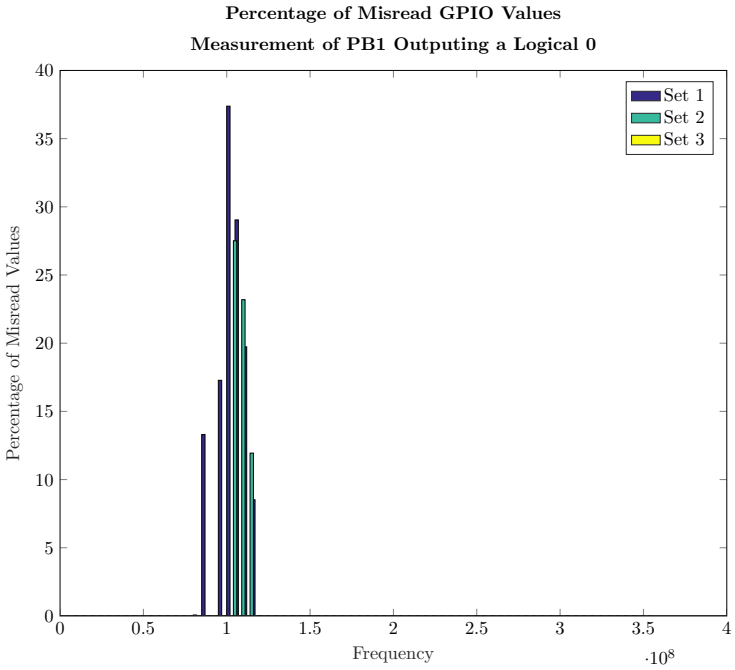

Fig. 5.4: GPIO misreads of PB5 measuring PB1 outputting a logical 0.

As can also be seen in Figures 5.4 and 5.5, the frequency at which each configuration responded is different despite the only differences in the setup being the logical output. This indicates that the circuit seen by the attacker changes as the logic level changes. Also of note, is that no bits were ever flipped above 200MHz. There are likely many contributing factors to this phenomenon; one may be poor transmission power by the antenna at these frequencies. Another contributing factor is explained by A. Boyer et al. [16], who showed that the power required to change the logical value of an I/O pin using a direct power injection attack increases with the frequency of the attacking sine wave. This was verified for the Tiva C microcontroller during this research, see Section 3.2 for details.

As can be seen in Figure 5.4, although separate frequency sweeps were done, only two affected the digital output of the microcontroller. Additional experimentation into what happened with this third measurement revealed that the setup was sensitive to its environment, particularly, the position of the USB cables connecting the microcontroller to the computer. Sometimes, the presence of a person or sheet of metal next to the setup could increase the number of misread values. Additionally, placing shielding between the

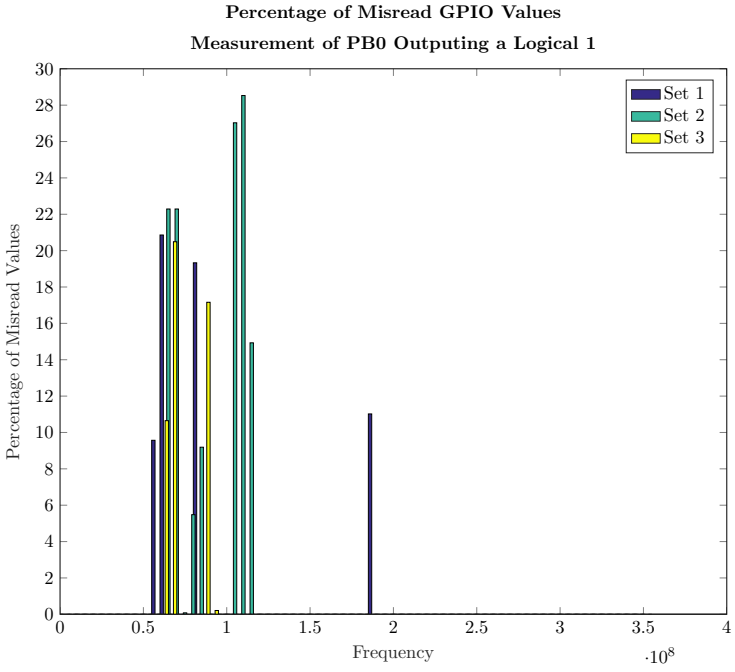

Fig. 5.5: GPIO misread of PB5 measuring PB1 outputting a logical 1.

microcontroller and the computer it was connected to decreased the number of misread values, strongly indicating that the cables had something to do with the effects that were observed. Several different cable configurations were experimented with, including twisting the cables around each other and putting as much distance between them as possible. Neither of these experiments produced meaningfully different results. It was also observed that taking quickly repeated measurements seemed to affect the results, indicating that there was a capacitive effect involved. These experiments were later repeated using the second setup, which had a common ground. This caused all the effects previously observed to go away, indicating that it was likely that the IEMI attack was influencing the ground potentials on both microcontrollers and thereby influencing the digital logic.

5.3 Summary of Experiments

No new information is presented in this section. Table 5.1 summarizes the experiments that were done to obtain the graphs that are presented in this chapter and the reference for the graph.

Table 5.1: Table of figures in ATTACKING GPIO PINS AND DIGITAL LOGIC including a brief description and figure number.

Description	Figure Number
GPIO misreads reading a logic 0 no common ground	5.4
GPIO misreads reading a logic 1 no common ground	5.5
GPIO misreads reading digital logic with common ground	No Figures Provided

CHAPTER 6

CONCLUSION

Understanding the capabilities and important factors of IEMI attacks is an important step to increase the security of modern electrical systems. The prevalence of sensors in electrical systems continues to grow because of the benefits they provide. This trend creates more potential victims to IEMI attacks. The consequences of these attacks are varied, but potentially life-threatening. For the safety and security of society, understanding the potential effects of IEMI attacks and their boundaries is important. Although some research has been done in this area, much more needs to be done to provide an adequate understanding and develop robust defenses against potential threats.

This research attempts to increase the understanding of IEMI attacks by determining how, why, and if a relatively low power, low-frequency IEMI attack could be used to attack higher power sensors and digital logic. To the knowledge of the author, while low power IEMI attacks have successfully been used to attack low power sensors [5], EM sensors [13], and a sensor network node [14], no research has attempted to attack digital logic or extensively explored the use of low-frequency IEMI attacks. To identify how an IEMI attack could be used, a simplistic circuit model was examined and several relevant topics of electromagnetics were discussed. To accomplish the rest of these goals, low-frequency IEMI attacks were conducted on higher power sensors and digital logic as part of victim setups. As part of determining why a victim circuit may be susceptible to an IEMI attack, this research identified key elements about the circuit under attack that may make it more susceptible. This understanding could be used by an attacker to identify vulnerable circuits or by a defender to minimize their vulnerability to an IEMI attack. The question of whether IEMI attacks can effectively be used follows directly out of the results of the experiments that were done after the effects of power and antennas were accounted for.

To begin this research, the theory of conducting IEMI attacks was investigated. This

led to the formulation of a simple circuit model for the victim circuit and basic ideas for its operation. This formulation revealed the existence of two types of basic attacks: non-resonant coupling and resonant coupling. Non-resonant attacks took place at any frequency where energy was effectively transmitted to the victim circuit without resonating inside that circuit. Resonant attacks happened at the frequency that the transmitted wave resonated within the victim circuit, thus increasing the efficiency of the attack. This model also revealed the possibility that the resonant frequency of a circuit could be below 1 GHz. This depended heavily on the amount of parasitic capacitance and inductance in a circuit. Unfortunately, because of the difficulty of measuring parasitic elements, this made determining the resonant frequency directly through circuit analysis nearly impossible. Another factor that made determining the resonant frequency difficult was that the desired field range for the attack was in the near field. This made the resonant frequency of the victim circuit dependent at least partially on the attack circuit, since the electromagnetic coupling would change each circuit's impedance. Further research needs to be done on these effects.

The design of the victim circuit and code was done using the data sheets for the SFH 235 FA photodiode and the Tiva C microcontrollers. The code and circuit were then tested for basic functionality without the presence of IEMI attacks. The attack circuit was designed around the chosen antenna. In order to maximize the inductance in the attack circuit and the size of the H field that the antenna produced, a coil antenna was used. The amount of current through the antenna was maximized using an RF amplifier to allow for a broad spectrum of attack. These two circuits were then placed 5 cm away from each other and frequency sweeps of the IEMI attack frequency were done, measuring the average output of the ADC amplifier in the victim circuit over a serial connection. An accurate understanding of the environmental factors was obtained by comparing the results of experiments examining a single environmental element at a time. Then the effects of various elements in the victim circuit were determined using the same method.

From the results of these experiments, some answers to the original questions can be answered. A summary of the results that were obtained using the PCB setup can be seen

in Table 6.1, which summarizes attacks against a victim using an ADC, and Table 6.2, which summarizes attacks against the GPIO pins on a victim circuit. Only these results are summarized since they most closely resemble what an actual victim circuit would be. These results show that the environment and setup of the victim circuit plays a vital role in the effectiveness of IEMI attacks. Considering the worst-case scenario, an IEMI attack against a system on a PCB using a sensor with similar power to the ones used in this research, more power is required for the attack to be effective. However, the amount of power required to make the attack effective would still likely be reasonable and significantly less than other similar IEMI attacks [5, 7–9]. The other concern for the effectiveness of these attacks is the minimum effective distance of the attack. This research does little to answer this particular question, since all of the experiments were 5 cm or less. However, from the theory of IEMI attacks, it is clear that increasing the distance will probably increase the required power at an exponential rate.

The requirements for an IEMI attack on a victim circuit that is not a worst-case scenario would still likely require more power than these experiments used to be effective. Though the power increase required for these could be as much as 50% less than what would be required for the worst-case scenario. To be this susceptible, a victim would only need to use connectors or wires that were 20 cm long to connect to the sensor. Wires this length can be seen in some electrical systems and very few systems don't use any wires at all, as considered in the worst-case scenario. Therefore, it can safely be concluded that low power IEMI attacks are a potential security flaw in a number of security or safety critical applications, though further research needs to be done to better understand these potential

Table 6.1: Summary of experimental results attacking an ADC using the PCB setup.

Direction	Frequency	Success
L->H	65 MHz	145.7 mV
L->H	65 MHz	139.2 mV
L->H	70 MHz	145.1 mV
H->L	65 MHz	-97.6 mV
H->L	75 MHz	-227 mV
H->L	30 MHz	-111 mV

Table 6.2: Summary of experimental results attacking digital logic.

Direction	Frequency	Success
1->0	65 MHz	21%
1->0	110 MHz	28%
1->0	65 MHz	20%
0->1	105 MHz	37%
0->1	105 MHz	27%
0->1	0 MHz	0%

flaws.

To gain a better understanding of this issue, several things need to be investigated in further detail. This experiment should be verified on commodity hardware. Will the IEMI attack influence every part of the circuit simultaneously, or will different parts of a circuit be susceptible to different frequencies? Another question that needs to be answered is: what are the current EMC standards that most commodity hardware must meet, and will these standards affect the system's susceptibility to IEMI attacks? Yet another topic of IEMI attacks that requires investigation is the relationship between power, distance, and the antenna used for the attack. How much will different antennas affect the power requirements for an IEMI attack and the distance that power is effective at, and will more directed antennas increase the distance by better focusing the energy used for the attack?

REFERENCES

[1] V. M. Igure, S. A. Laughter, and R. D. Williams, "Security issues in scada networks," *Computers & Security*, vol. 25, no. 7, pp. 498–506, 2006.

[2] E. D. Knapp and J. T. Langill, *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Syngress, 2014.

[3] S. Amin, X. Litrico, S. Sastry, and A. M. Bayen, "Cyber security of water scada systemspart i: Analysis and experimentation of stealthy deception attacks," *IEEE Transactions on Control Systems Technology*, vol. 21, no. 5, pp. 1963–1970, 2013.

[4] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Computer Networks*, vol. 57, no. 5, pp. 1344–1371, 2013.

[5] D. F. Kune, J. Backes, S. S. Clark, D. Kramer, M. Reynolds, K. Fu, Y. Kim, and W. Xu, "Ghost talk: Mitigating emi signal injection attacks against analog sensors," in *Security and Privacy (SP), 2013 IEEE Symposium on*. IEEE, 2013, pp. 145–159.

[6] Y. Shoukry, P. Martin, Y. Yona, S. Diggavi, and M. Srivastava, "Pycra: Physical challenge-response authentication for active sensors under spoofing attacks," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2015, pp. 1004–1015.

[7] W. A. Radasky, C. E. Baum, and M. W. Wik, "Introduction to the special issue on high-power electromagnetics (hpem) and intentional electromagnetic interference (iemi)," *IEEE Transactions on Electromagnetic Compatibility*, vol. 46, no. 3, pp. 314–321, 2004.

[8] M. G. Backstrom and K. G. Lovstrand, "Susceptibility of electronic systems to high-power microwaves: Summary of test experience," *IEEE Transactions on Electromagnetic Compatibility*, vol. 46, no. 3, pp. 396–403, 2004.

[9] N. M. PARRA, "Contribution to the study of the vulnerability of critical systems to intentional electromagnetic interference (iemi)," Ph.D. dissertation, ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE, 2016.

[10] C. Yan, X. Wenyuan, and J. Liu, "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle," *DEF CON*, 2016.

[11] M. Harris, "Researcher hacks self-driving car sensors," *IEEE Spectrum*, 2015.

[12] R. Chauhan, "A platform for false data injection in frequency modulated continuous wave radar," Ph.D. dissertation, UTAH STATE UNIVERSITY, 2014.

[13] Y. Shoukry, P. Martin, P. Tabuada, and M. Srivastava, "Non-invasive spoofing attacks for anti-lock braking systems," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2013, pp. 55–72.

[14] J. Delsing, J. Ekman, J. Johansson, S. Sundberg, M. Backstrom, and T. Nilsson, "Susceptibility of sensor networks to intentional electromagnetic interference," in *2006 17th International Zurich Symposium on Electromagnetic Compatibility*. IEEE, 2006, pp. 172–175.

[15] C. A. Balanis, *Antenna theory: analysis and design*. John Wiley & Sons, 2016.

[16] A. Boyer, S. Bendhia, and E. Sicard, "Modelling of a direct power injection aggression on a 16 bit microcontroller input buffer," *EMC Compo*, vol. 7, pp. 35–39, 2007.

[17] F. T. Ulaby, E. Michielssen, and U. Ravaioli, "Fundamentals of applied electromagnetics 6e," *Boston, Massachussetts: Prentice Hall*, 2010.

[18] C. R. Paul, *Introduction to electromagnetic compatibility*. John Wiley & Sons, 2006, vol. 184.

[19] J. W. Nilsson and S. A. Riedel, *Electric Circuits*. Prentice Hall/Pearson, 2011.

[20] B. L. Cannon, J. F. Hoburg, D. D. Stancil, and S. C. Goldstein, "Magnetic resonant coupling as a potential means for wireless power transfer to multiple small receivers," *IEEE Transactions on Power Electronics*, vol. 24, no. 7, pp. 1819–1825, 2009.

[21] T. I. Incorporated, "Tiva tm4c123gh6pm microcontroller," 2017.

[22] Mini-Circuits, "Coaxial amplifier zhl-1a zhl-1a+."

[23] ——, "Coaxial amplifier zhl-6a zhl-6a+."

[24] Tektronix, "Arbitrary/function generators afg 3011 / 3021b / 3022b / 3101 / 3102 / 3251 / 3252 datasheet."

[25] A. Technologies, "E4421a analog rf signal generator, 250 khz to 3000 mhz (discontinued - support information only)."