2018

Intentional Electromagnetic Interference Attack on Sensors and Actuators

Jayaprakash Selvaraj
Iowa State University

Intentional electromagnetic interference attack on sensors and actuators

by

Jayaprakash Selvaraj

A dissertation submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Major: Electrical Engineering (Electromagnetics Microwave and Nondestructive Evaluation)

Program of Study Committee:
Mani Mina, Major Professor
Jiming Song
Arun Somani
Meng Lu
Gary Tuttle

The student author, whose presentation of the scholarship herein was approved by the program of study committee, is solely responsible for the content of this dissertation. The Graduate College will ensure this dissertation is globally accessible and will not permit alterations after a degree is conferred.

Iowa State University

Ames, Iowa

2018

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENT

I would like to thank my committee chair, Prof. Mani Mina, and my committee members, Prof. Jiming Song, Prof. Gary Tuttle, Prof. Arun Somani, and Prof. Meng Lu, for their guidance and support throughout the course of this research.

Prof. Mani Mina provided the opportunity for me to work on the electromagnetics research area, despite my little experience in this field. I am eternally thankful to him for supporting me, at my lowest points during the graduate studies.

I would like to sincerely thank my collaborators at Virginia Tech University, especially Prof. Ryan Gerdes, whose unparalleled guidance and support throughout my research, has provided me a successful platform, to prove my expertise and excel in every project, that I got an opportunity to work with him. I would also like to thank my colleagues Gökçen Yılmaz Dayanıklı, Neelam Prabhu Gaunkar and David Ware for their dedication and hard work to transform this research into a pioneering work, in hardware security field.

I would like to thank my loving wife, Priyam Rastogi, who has stood with me, through every joy and sorrow and provided me with motivation and confidence, to handle all the struggles which came towards me. I would also like to thank my in-laws who saw the potential in me and supported me throughout my graduate studies, without a hint of doubt in their mind.

In addition, I would also like to thank my parents, friends, colleagues, the department faculty and staff for making my time at Iowa State University a wonderful experience.

ABSTRACT

Embedded systems are critically relying on the integrity its input and output signals to ensure proper operation. Signal from sensors, either analog or digital, are blindly trusted by the embedded systems, to estimate the environment, in which the system is set to monitor and respond to. Similarly, actuators, that are connected to and controlled by an embedded system, are expected to behave in a reliable manner, to perform a particular physical motion. However, recent publications, from hardware security researchers, have shown that sensor signals can be manipulated by injection of false data, using intentional electromagnetic interference (IEMI). In this work, the author proves that both the input as well as the output signals of an embedded system are vulnerable to data manipulation, via physical layer of this system, which would bypass any traditional defense mechanism.

By using specially crafted IEMI attack techniques, this work has shown that the physical layer input/ output signals can be manipulated by an attacker, thereby providing the attacker, with the ability to remotely control an embedded system. Three different attack scenarios had been analyzed and the effectiveness of the attack against each scenario has been experimentally verified. First, an embedded system, gathering data through an analog sensor, was manipulated to output arbitrary sensor data, while in the second scenario, a slightly modified attack technique, has been shown to successfully inject false data into digital communication lines. Finally, commonly used digital actuators, which were controlled by embedded system, has been shown as a potential target for false data injection attack, using IEMI techniques. These attacks have been shown to be effective, at appreciable distances from the victim circuit, while using attack signals with relatively less power.

CHAPTER 1

INTRODUCTION

In a society which is increasingly concerned with privacy, securing their information from malicious hackers and prying government eyes, security for its data in the hardware and software is of utmost importance. Software data security is an ever-evolving process, in which attack and defense techniques change day-by-day. But, for most consumers, hardware security is a tough option to upgrade, every now-and-then. Hence, any hardware, especially electronic devices, needs to have foresight, in securing against potential threats in the future, to provide a trustworthy platform, for its consumers. There are several attack techniques targeted at exploiting the security vulnerabilities present in a hardware circuit, one of which is intentional electromagnetic interference attack technique.

Intentional Electro-Magnetic Interference (IEMI) attack is a rising new technique which works by intentionally inducing noise, thereby disrupting the normal operation of a system, or injecting false data into commonly used electronic systems, thus presenting the attacker with the ability to independently control the electronic system. It is of utmost importance to understand the potential risks this new attack technique possesses, before developing suitable countermeasures, to protect future generation of electronic devices, against threats posed by IEMI attacks.

Research community's interest in IEMI attack peaked when a formal definition was defined for this attack technique. In February 1999, at Zurich EMC Symposium, IEMI attack got its definition as "Intentional malicious generation of electromagnetic energy introducing

noise or signals into electric and electronic systems, thus disrupting, confusing or damaging these systems for terrorist or criminal purpose" [1].

Previous work on IEMI attacks focuses predominantly on potential threat from High Power Electro-Magnetic (HPEM) signals [2] [3]. The most interesting investigation into electronic system failures and anomalies due to HPEM sources, was performed by NASA, which shows several past occurrences of failures in automotive, aircraft and medical equipment due to EM sources [2]. This report mentions occurrence of power failure in a U.S. Navy vessel, due to HPEM signal transmission. This caused an oil pressure sensor to falsely sense a low reading and caused a power failure in the Navy vessel [2]. Although it might seem that accidental damage due to HPEM signals are minimal for civilians, the next incident would prove otherwise. Mercedes-Benz cars suffered Anti-locking Braking System (ABS) related problem on a certain stretch of German autobahn, due to HPEM signal emission from a near-by radio transmitter [2]. Even complex medical equipment are susceptible to HPEM signals, as reported by a problem in an Electroencephalogram (EEG) machine during a surgery, whose output was corrupted with HPEM signal, coupled from a local AM radio station [2]. This investigation by NASA, presents many more interesting instances of HPEM related anomalies in the past.

A more comprehensive analysis on the state of contemporary IEMI attack research has been peformed by Radasky et al., who have highlighted the potential new threat this new attack technique possesses to our modern civil society and listed the four major topics in which researchers focuses on [4]:

1) IEMI waveform generation capability and classification of the type of sources [5] [6] [7].

2) Electromagnetic (EM) coupling process with cables and systems [8] [9] [10].

3) Impact of IEMI on electronic and communication systems [11] [12] [13] [14] [15] [16].

4) Development of protection techniques, along with design of measurements and standards [17] [18] [19].

Out of these topics, the research involving the impact of IEMI on electronic and communication systems, is the most relevant area to the work described in this dissertation. In this work, Radasky et al., has summarized the work of Camp et al., who investigated the breakdown behavior of microcontrollers when they were subjected to Electromagnetic Pulse (EMP) [11]. They have determined that the susceptibility of microcontrollers to EMP depends predominantly on the signal line lengths. Also, Backstrom et al. work has been presented, which discusses in detail regarding the vulnerabilities in systems like missiles, tactical radio link, army radio, cars, computers, telecom stations and generic objects, to HPEM sources [14]. These authors have described that at frequencies below 2.8 GHz, high power (10 MW) IEMI attack is feasible at even a kilometer away from the EM source [14]. They have also explored the possibility of building a homemade IEMI transmitter which could damage electronic circuits, just like an HPEM radiation would, from a nuclear blast or high-power EMP [14].

In most of these research publications on EM attacks, shielding the exposed circuit components, cables and printed circuit board traces, has been proposed as a viable option to defend against high power EM interference attacks. But, C. Paul suggests that shielding against IEMI attack is extremely difficult, under near-field conditions [20]. Before understanding the reason for shielding ineffectiveness against near-field EM sources, it is

important to understand the difference between near-field and far-field of an antenna/EM source.

1.1 Near-field shielding

A simple definition for near-field would be, the region around the antenna/EM source where the intensity of electric and magnetic fields does not vary inversely proportional to the distance from the antenna/EM source. Another definition for near-field defines it as, the distance from the antenna/EM source, where the ratio of electric field to magnetic field components is not approximately equal to the characteristic impedance of the medium, in which radiation occurs. C. Paul claims that for the far-field assumptions to hold in an experiment, one must be far enough away from the antenna, by an order of three times the wavelength of the signal emitted from that antenna [20].

Figure 1-1 shows the wave impedance plots of a) electric dipole and b) magnetic dipole, where wave impedance was defined as the ratio of electric field intensity E_φ to the magnetic field intensity H_θ. This figure shows that the electric dipole behaves like a high-impedance source, while the magnetic dipole behaves like a low-impedance source, under near-field distances. Due to these impedance variation, the effectiveness of shielding does vary quite drastically, as suggested by the data in Figure 1-2.

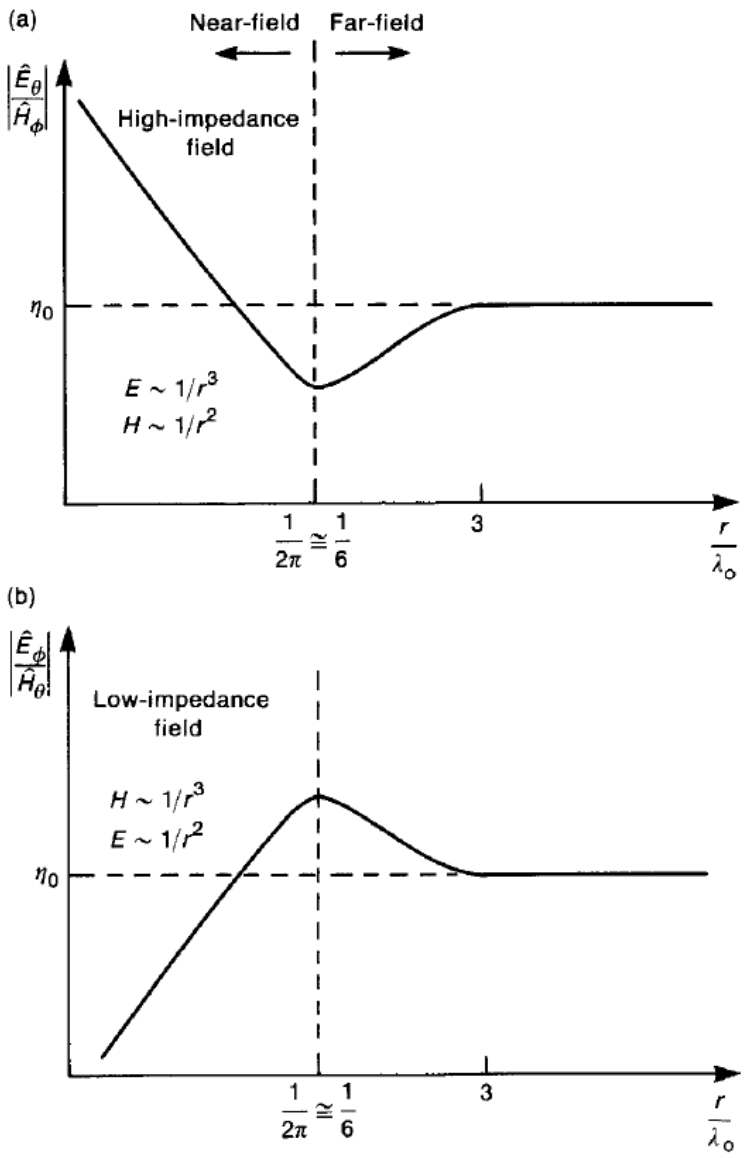


Figure 1-1 Wave impedance of a) electric dipole b) magnetic dipole *[20]*

Shielding effectiveness can be measured in terms of the electric field intensity and the magnetic field intensity absorbed as well as reflected by the shield, with respect to the field intensities that encounters this shield [20]. Although, the absorption loss provided by the shield is unaffected under near-field or far-field conditions, the reflection loss introduced by the shield varies drastically, depending on the location of shield in the near-field or far-field of the antenna/EM source.

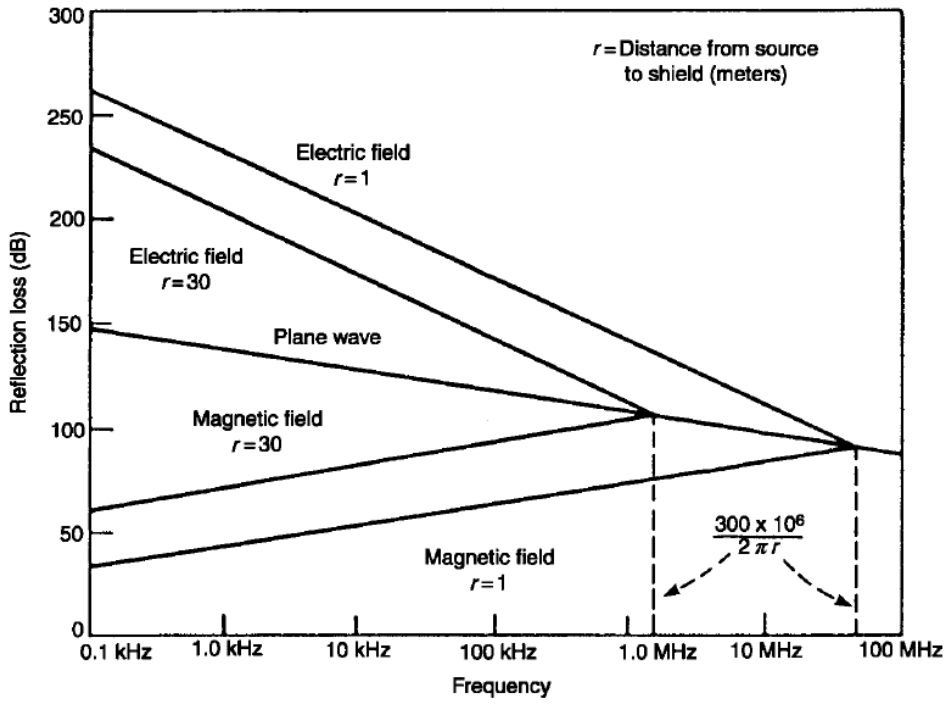


Figure 1-2 Reflection loss introduced by shields under near-field condition of electric and magnetic sources *[20]*

Figure 1-2 shows that the reflection loss provided by shields, under near-field condition, against magnetic sources, are far lower than the losses under far-field condition. Figure 1-2 also shows that, the reflection loss is relatively lower for any frequency, when the distance between the magnetic source and shield is in order of fractions of the wavelength of the signal being transmitted. This variation in the shield's reflection loss occurs due to the low impedance near-field region which exists around a magnetic source. According to the data shown in Figure 1-2, EM radiation from a simple loop antenna, which is an example of a magnetic source, can become extremely difficult to shield against, especially under low frequencies. Since, shielding techniques are relatively inefficient against near-field IEMI attacks, alternative methods must be investigated, to protect against this malicious attack technique.

1.2 Data security in embedded system

Despite the existing vulnerabilities in the current generation of electronic devices from IEMI attacks, the society is willingly accepting these devices into every aspect of their lives. Tech giants like Apple, Google and Amazon have invested hugely on creating the next generation of smart home devices, which would result in placing a computer into everything in our homes [21]. These devices consist of embedded systems built inside them, which can connect to the internet and automate day-to-day tasks like watering the plants, turning on/off air-conditioning system, locking/unlocking keyless smart doors and many more. Ultimately, these technology advancements tend to find their way into our lives, without fully securing themselves against existing security risks.

Embedded circuits are predominantly relying on sensors to gather information about a system and use that information to maintain/influence its operation. Automobiles are an excellent example of such an embedded system. The on-board embedded system in a car relies on a myriad of sensors to estimate the vehicle's speed, tire pressure, fuel level, condition of Anti-Locking Braking System (ABS), engine temperature, Vehicle Stability Control (VSC), etc. Securing these sensor's data from malicious attacks is critical to maintain the proper operation of the vehicle as well as to keep the driver and passengers safe. C. Miller and C. Valasek proved that a 2014 Jeep Cherokee could be remotely hacked and controlled by injecting malicious messages into the Controller Area Network (CAN) bus of the car through internet [22]. This attack was feasible due to the internet connected head unit (Radio) present in that car. Although Chrysler issued a recall to install a software patch to counteract the vulnerabilities exposed by C. Miller and C. Valasek [23], this attack shows the potential danger that security vulnerabilities in an embedded system poses to its users.

Traditionally, researchers have been focusing on securing the embedded systems by encryption of data, to prevent attacks from hackers [24] [25]. Embedded systems digitize the sensor data using an Analog to Digital Converter (ADC), after which the sensor data could be encrypted. Despite ensuring data security in embedded system by encryption, these systems are designed to implicitly trust the data received from sensors. Similar vulnerability exists in the actuators controlled by embedded systems, such as servo motors. In digital servo motors, the on-board microprocessor trusts the control signal received from an embedded system and uses this information to change the position of the actuator. Thus, both sensors and actuators connected to an embedded system are vulnerable to malicious data injection attacks.

Intentional Electro-Magnetic Interference (IEMI) attack has the potential to exploit this security vulnerability in sensors and actuators and inject malicious data into the embedded system. IEMI attacks has not yet been explored thoroughly enough to investigate the potential threat to embedded systems. Although it is a well-known fact that usage of enormous amount of Electro-Magnetic (EM) power, in the range of kilowatts, for an attack could essentially destroy an embedded system, attack from low power EM signal (watts) have the potential to manipulate the control signal to and from an embedded system [26] [27].

Recently low power IEMI attack techniques have gained interest among researchers [28] [29]. Shoukry et al. discussed a non-invasive attack on Antilock Braking System (ABS) in cars, using IEMI attack technique [29]. They have proved that an attack using magnetic field, which could overpower the magnetic field signal generated by the ABS sensor, resulting in a successful injection of an attack signal, without physically tampering with a circuit [29]. Since the ABS sensor tries to read the vehicle speed, injecting false magnetic

field signal would corrupt the integrity of the ABS sensor output. But, the attack technique described in this work, will only work on sensors which can measures magnetic fields.

The most relevant work in low power IEMI attack has been described by Kune et al. [30]. The authors have tried injecting EM signal into pace-maker, at the same frequency as the baseband signal. Since the attack signal lies in the same band as the baseband signal, the onboard filters cannot attenuate the attack signal [30]. Authors have claimed this method of attack to be successful at a maximum distance of 1.57m from an EM signal transmitter.

1.3 System level overview of IEMI attack

The work presented in this dissertation focuses on utilizing IEMI attacks techniques to inject false data into sensors and actuators, while using significantly less power (in the order of couple of watts), in comparison to HPEM attacks.

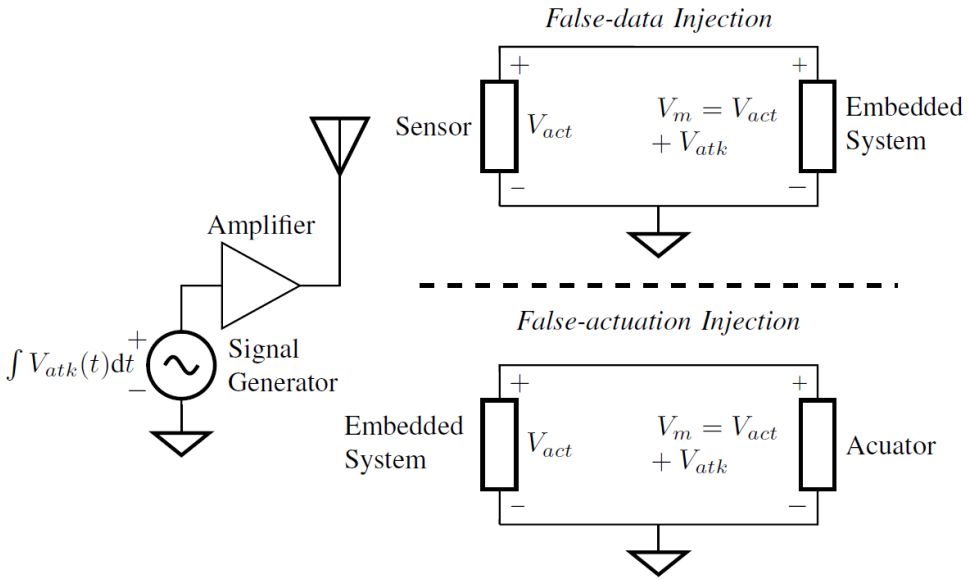


Figure 1-3 IEMI attack model showing the attacker circuit as well as circuits under attack *[31]*

Figure 1-3 shows the IEMI attack model used for injecting false data into embedded systems using sensors and actuators. In the attack model described in this figure, it was assumed that an attacker will be armed with a signal generator, amplifier and an antenna, with a goal of injecting false data into the path of sensor signal, which travel towards an embedded system, and into the path of control signal generated by the embedded system, which travel towards an actuator. The circuits on the right side of this figure, represents the embedded system connected to a sensor and an actuator. The $V_{atk(t)}$ represents the voltage induced at the embedded circuit, due to the transmission of an attack signal generated with a current amplitude of $\int V_{atk(t)}dt$, at the attacker circuit. The significance of the integral sign in the amplitude of current, will be discussed in the upcoming chapters. On the circuits under attack, V_{act} represents the voltage signal generated by the sensor, to be read by an embedded system or the voltage signal generated by the embedded system, to be read by an actuator. Finally, V_m represents the net voltage signal received by the embedded system or the actuator. In a successful IEMI false data injection attack, the induced voltage $V_{atk(t)}$ would be large enough to make significant modification to the net voltage signal , V_m.

1.4 Overview of the dissertation

This dissertation has been subdivided into chapters about IEMI attack techniques on:

1) Analog sensors
2) Digital sensors
3) Digital Actuators

Analog sensors convert a physical quantity into a current or voltage signal, which can later be converted into digital data to be processed by an embedded system. The conversion

of the electrical signal from the analog to digital domain is handled by the analog to digital converter circuit. Due to the non-linearity present in the input terminals of an embedded system, the induced time varying signal, intentionally coupled by an attacker, could get converted into Direct Current (DC) domain and corrupt the integrity of electrical signal from sensor. This chapter discusses the nature of the non-linearity present at the input terminals of embedded system, along with techniques to induce a false data, aimed to corrupt the actual signal generated from the sensor. A photo-diode based sensor circuit was chosen to serve as the circuit under an IEMI attack. Since the IEMI attack technique used to inject false data into analog sensors, rely on non-linear properties of the embedded system, to induce a tangible effect towards corrupting the sensor data, this attack technique would work on any type of analog sensor, regardless of its type (voltage/current output).

In the next chapter, digital sensors were considered as the target for false data injection attacks using IEMI technique. Mainly, the digital sensors connected to embedded system's General Purpose Input/ Output (GPIO) pins, has been considered as the system under an IEMI attack. Due to the high logic level amplitudes used by the digital circuits, they were previously considered to be immune to IEMI attacks. But, due to the non-linear properties of the embedded system's input terminal, this attack technique can induce random false data into the digital output signal path. To deterministically induce false data into these systems, special type of waveforms has been discussed and provided experimental proof, that these waveforms can induce deterministic false signal.

The last chapter on IEMI attacks investigates false data injection techniques for digital actuators. Since, digital actuators are controlled by embedded systems, using Pulse Width Modulation (PWM) signals, any attack signal aimed at deterministically inducing false

pulse width data into this system, must be in phase with the PWM signal. These digital actuators use onboard microcontrollers to determine the incoming periodic PWM signal's pulse width and use that information to make a physical motion. This chapter explores different waveform options to deterministically inject false pulse widths into the periodic PWM signal, thereby giving the attacker, the ability to make a physical motion of their liking, with the digital actuator. Also, techniques to disable the digital actuator, from responding to any new control signals, has also been investigated in this chapter. This chapter also explores, circuit design techniques used for transmitting these special waveforms, targeting digital sensors, attached with embedded system.

The final topic has been dedicated to the initial project, in which the author had gotten an opportunity to work on a magneto-optic switching circuit. This circuit helps optimize all-optical routers, which were aimed at circumventing the latency issues, introduced by the current generation of optical-to-electrical and electrical-to-optical network router infrastructure modules. This magneto-optic switching circuit was small magnetic pulse generator circuit, used to change the polarization state of magneto-optic materials, which can act as an optical ON/OFF switch, thus functioning as an optical router. The proposed circuit, in this chapter, has been proven to function better than the previous circuits, aimed at performing the same switching functionality.

The main contributions of the author from this research work are as follows:

1. Design of false data injection techniques to induce DC signal into the input/output signals of the embedded system. The attack techniques described in this work, can be used by an attacker, to inject false data into an embedded system, thereby hacking the system, to perform tasks, as dictated by the attacker. These attack techniques rely on exploiting the

non-linear properties present in the embedded systems and thus do not restrict themselves to few the type of sensor or embedded circuits, which were described in this work.

2. Pioneering research work performed on injecting false data into digital actuator control signals. At the time of writing this dissertation, to the best of the knowledge of the author, no other research team has published work on attacking digital actuators using IEMI. Author and his team had previously published this work, with experimental results proving that it is possible to arbitrarily reduce the pulse width of the PWM control signal. But in this dissertation, the author has proved, that it is also possible to arbitrarily increase the pulse width of the PWM signal. With this attack technique, any digital actuator, controlled by an embedded system, via PWM control signal, could be hacked and forced to make a motion, according to the instruction provided by the attacker.
3. A simplified enhancement solution has been proposed by the author, for magnetic pulse generator circuit, used to generate bidirectional magnetic field. The proposed circuit significantly reduces the size of the magnetic pulse generator circuit, in comparison to the previous generation of circuits.

The author hopes that by understanding the potential threats posed by IEMI attack techniques to our civil society, future researchers would show increased interest, in building next generation of embedded systems, which are secured against this malicious false data injection technique.

CHAPTER 2

FALSE-DATA INJECTION FOR ANALOG SENSORS

Embedded systems use analog sensors to convert real-world signal such as light, temperature, humidity, etc, into electrical signal (voltage or current), which can be interpreted by digital electronic systems. The part of the embedded system which reads this electrical signal from sensors is the Analog-to-Digital Converter (ADC). As mentioned earlier, the electrical signal from sensors are vulnerable to attack from IEMI attacks.

The success of an IEMI attack depends on the amount of EM signal coupled to the victim embedded circuit which is under attack. The coupled EM signal strength can be increased by determining the frequency at which the victim circuit is most susceptible to accept the incoming EM signal, which is usually its self-resonant frequency. Since any closed circuit is a loop, it can be approximated as a loop antenna. Thus, an ADC connected to analog sensor which becomes a closed circuit, can effectively receive EM signal transmitted at its resonant frequency.

In this section we illustrate false data injection into an ADC receiving data from a photo-diode based Infra-Red (IR) light sensor, using IEMI attack technique. An IR light sensor was used, since it is a commonly used sensor in solar energy harvesting system as well as automated ambient light controlling system. This sensor outputs a DC current proportional to the ambient IR light, which is typically in the order of tens of micro amperes [32], which is representative of many sensors used in embedded systems. By injecting false data into the embedded system controlling solar energy harvest or ambient light, the attacker could make

the system malfunction, by making the system overuse its energy storage, resulting in a system failure.

This IEMI attack on a IR light sensor is representative of many different sensors connected to an embedded system, since the attack primarily exploits the non-linear properties of embedded systems, to induce a tangible false data and does not depend on the type of sensor.

2.1 Mechanism of Attack

The most effective way to attack an analog sensor with IEMI attack would involve transmission of narrow-band sinusoidal signal and direct it towards the victim embedded circuit. This would induce an AC signal on the victim circuit. The author hypothesize that narrow-band signals would be most effective for an attacker, due to the reduction in complexity of the attacker circuit by designing the circuit to operate only at the resonant frequency of the victim circuit. Although it is counter-intuitive to inject AC signal into the input of ADC, which reads DC signal generated from the sensor, the induced AC signal can get rectified by the non-linear properties of the ADC input, thereby producing an DC signal injection.

Non-linearity in the input terminal of the ADC could be predominantly attributed to the Electro-Static Discharge (ESD) protection circuit [33]. Integrated Circuits (IC) are highly susceptible to permanent damage due to the high voltage introduced by ESD. To protect the ICs from this damage, manufacturers build ESD protection circuits at the Input/ Output (IO) pins of the ICs, which shunts the high voltage to positive or negative power supply terminals, with the help of diodes. Shunting the high voltages from reaching the internals of an IC,

prevents damage due to ESD. Inadvertently, these ESD protection circuits introduces signal degradation under high frequency and high amplitudes [33].

During an IEMI attack, the ESD protection diodes could be performing rectification of AC signal, which was coupled from the attacker, into DC signal. Figure 2-1 shows an example of ESD protection circuit, present between the input terminal of an ADC and its internal circuitry. In this particular ESD protection circuit, shown by Figure 2-1, which are actually being used in the TM4C123GXL microcontroller's ADC input terminals [34], there are two diodes which are present to shunt high positive as well as negative voltages to ground and positive power supply terminals, respectively. In an ideal scenario, in which both these diodes have identical current versus voltage characteristics, this ESD protection circuit will not provide rectification on AC signals. But, in a real circuit, there will always be mismatch in the current versus voltage characteristics of these two diodes, resulting in a difference in the level of AC signal shunted to the positive of negative terminals, which would indeed produce a non-zero DC component.

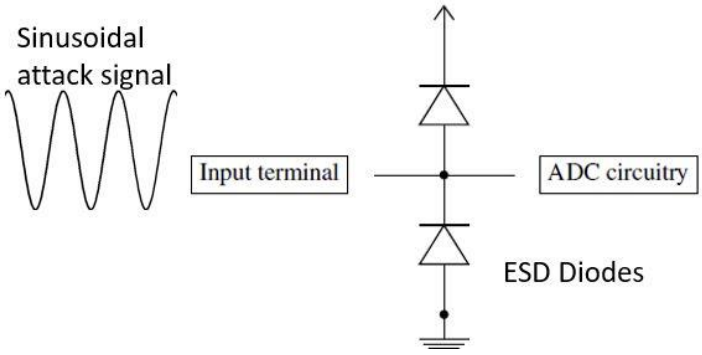


Figure 2-1 ESD protection circuits rectifying injected IEMI AC signal into DC

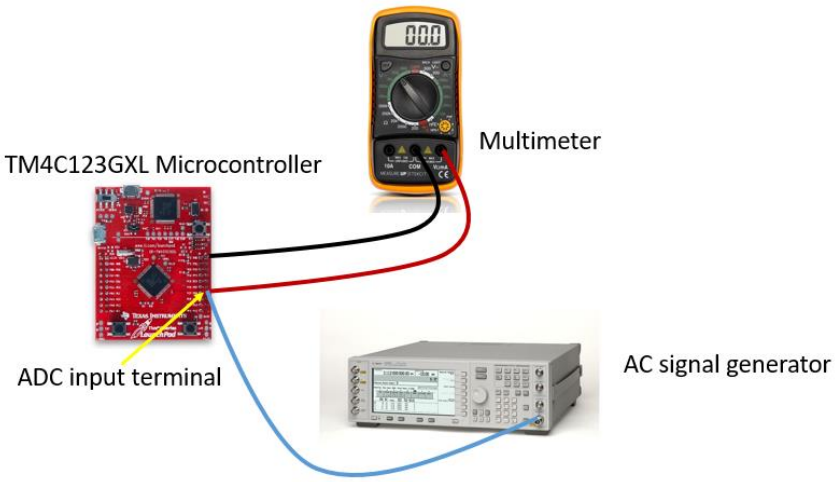


Figure 2-2 Experiment to validate rectification hypothesis due to ESD diodes

To validate this hypothesis, TM4C123GXL microcontroller from Texas Instruments, which has ADC functionality, were used. The ADC input terminal was connected to an AC signal generator, with 10 dBm (10 mW) output power level, along with a multimeter. The multimeter was set to measure DC voltages. This experimental setup is shown by Figure 2-2. While the microcontroller circuit was not connected to the multimeter and AC signal generators, the multimeter reads 0 V DC as expected, since the AC signal from the signal generator does not have any DC components. But as soon as the microcontroller was powered on and connected to the multimeter and AC signal generator, the multimeter reads a positive DC voltage. Figure 2-3 shows that the conversion of AC signal into DC is most efficient under 500 MHz frequency, beyond which there is a steep drop in the magnitude of DC voltage produces. The results from Figure 2-3 validate the hypothesis that the AC signal could get rectified into DC signal thereby having the capability to inject false data into ADC's input terminal.

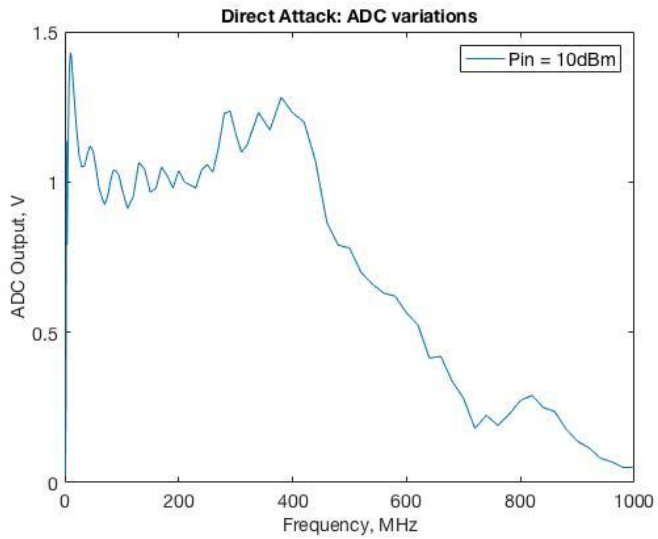


Figure 2-3 Rectified DC voltage measured at the input of ADC, while directly connecting an AC signal to the input terminal

Other type of non-linearity present in the ADC arises due to signal clipping. Signal clipping happens because of the limited voltage range which can be digitized by the ADC. In the case of ADC present in the TM4C123GXL microcontroller, voltage ranges between 0 V and 3.3 V can be digitized without any error due to signal clipping. Thus, any input voltage signal above 3.3 V, will be read as 3.3 V by the ADC and voltages below 0 V, will be rounded to 0 V in the digitization process. Figure 2-4 shows the relation between ADC input voltage and the equivalent voltage to the ADC digital output. From Figure 2-4, one can understand the case when an attack AC signal (1 V_{peak}) superimposed on a positive DC voltage (+3.3 V) would experience signal clipping, resulting in the positive cycle of the AC signal assigned digital codes equivalent to 3.3 V. The negative cycle of the AC signal would be unaffected, assuming that the ADC can sample at a faster rate than the AC signal's Nyquist frequency. Thus, the digitized signal at the output of the ADC would have a DC voltage of 2.67 V (3.3 V – 0.63 x 1 V_{peak}), which is less than the intended DC input voltage

of 3.3 V. The multiplication factor 0.63 in the above calculation, comes from sinusoidal signal averaged over half of its period.

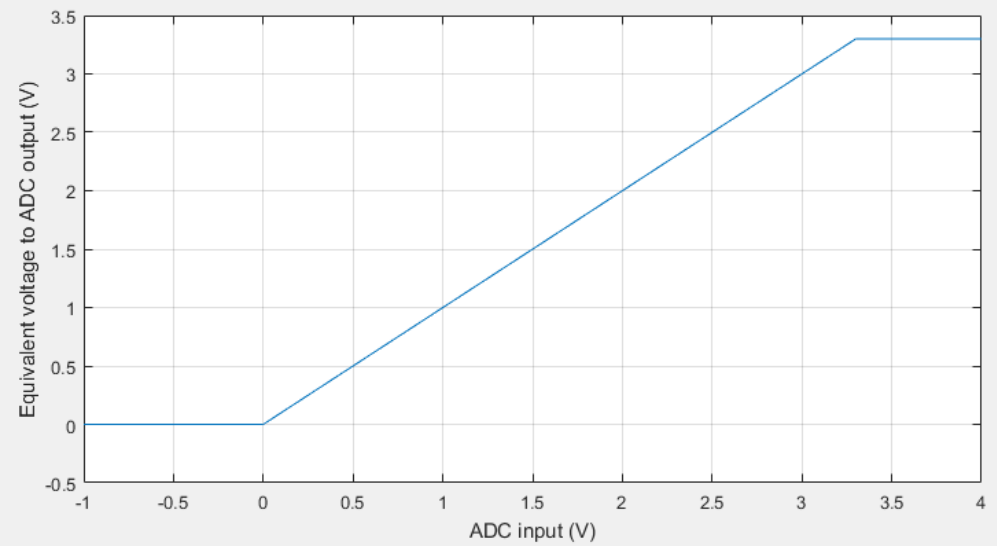


Figure 2-4 Signal clipping due to limited ADC input voltage range

2.2 Experimental Setup

Figure 2-5 shows a system level representation of the experimental setup used for injecting false data on analog sensor. The following sections describe in detail about each part of the experimental setup.

2.2.1 Victim Circuit

As mentioned earlier, the victim circuit or the circuit under IEMI attack consist of an SFH235 IR optical sensor from OSRAM Opto Semiconductors [35], connected to a Tiva C TM4C123GXL microcontroller from Texas Instruments [34], containing an ADC, with 12-bit resolution. The microcontroller communicates with a personal computer (PC) through serial communication.

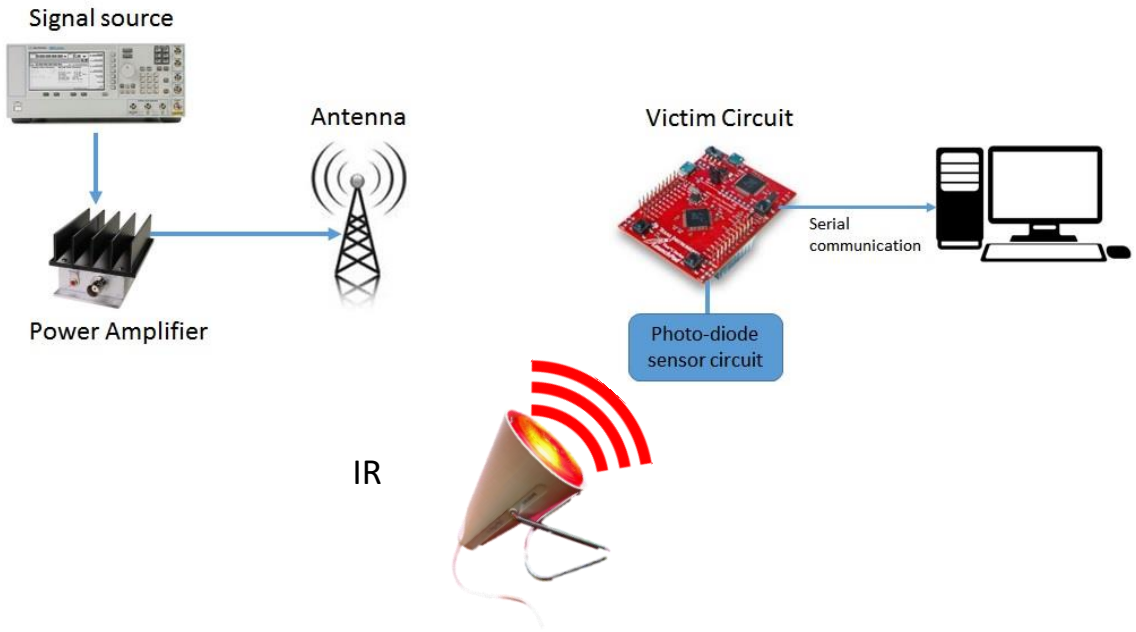


Figure 2-5 Experimental setup for false data injection on analog sensors

The IR sensor was reverse biased with a 5V DC signal from a DC power source, while the IR sensor was connected to a 330kΩ resistor, to convert the current signal generated from the IR sensor into voltage signal that can be read by an ADC. To control the output of the IR sensor, an IR lamp with an output power rating of 5 W at 850 nm wavelength was positioned towards the sensor. Figure 2-6 shows the schematic representation of the victim circuit.

The ADC present in the TM4C123GXL microcontroller was programmed to sample the input signal at a rate of 1 mega samples per second (MSPS). The sampled/digitized outputs of the ADC are averaged over 1000 samples to filter out high frequency noise and the averaged values are sent to the computer's serial terminal.

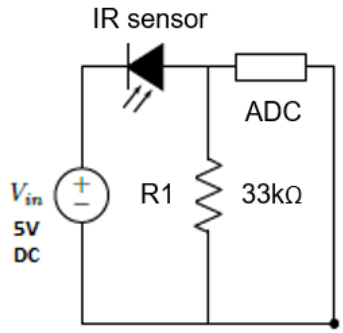


Figure 2-6 Schematic representation of victim circuit

2.2.2 Attacker Circuit

As shown by Figure 2-5, the attacker circuit consist of a signal generator, power amplifier and an antenna to transmit the attack signal. Since it is difficult to analytically determine the resonant frequency of the victim circuit, due to complex traces and lack of publicly available high frequency models for the microcontroller, the attacker circuit should be able to sweep the signal frequency across a wideband and determine the frequency at which maximum power transfer happens.

HP8350B signal generator from Hewlett Packard, which has the capability to sweep the signal frequency from 10 MHz to 20 GHz was chosen for this experiment. This signal generator produces a narrow band sinusoidal signal with a maximum output power of 20 dBm (100 mW). Since the output power from the signal generator might not be enough to perform an IEMI attack over longer distances between the attacker and victim circuits, a power amplifier was used to boost the transmitted signal's power.

ZHL-1A RF power amplifier from Mini Circuits was used to amplify the transmitted signal. This power amplifier can operate between the frequency range 2 MHz – 500 MHz, without suffering any non-linearities. The 1 dB compression point of this power amplifier is

28 dBm, which specifies the maximum output power at which the power amplifier begins to experience non-linearities and as a result produces 1 dB less output power than the expected power output due to nominal gain.

It was experimentally observed that the ZHL-1A RF power amplifier can give an output power of 32.6 dBm (1.82 W) with an input power level of 20 dBm from the signal generator. This output level was consistent between the frequencies from 2 MHz to 500 MHz, beyond which there was a sharp decrease in the output power level. Figure 2-7 shows the output power vs frequency characteristics of ZHL-1A RF power amplifier. This RF power amplifier used in the attack circuit, was biased with +24 V DC voltage from HP-E3631A DC power supply.

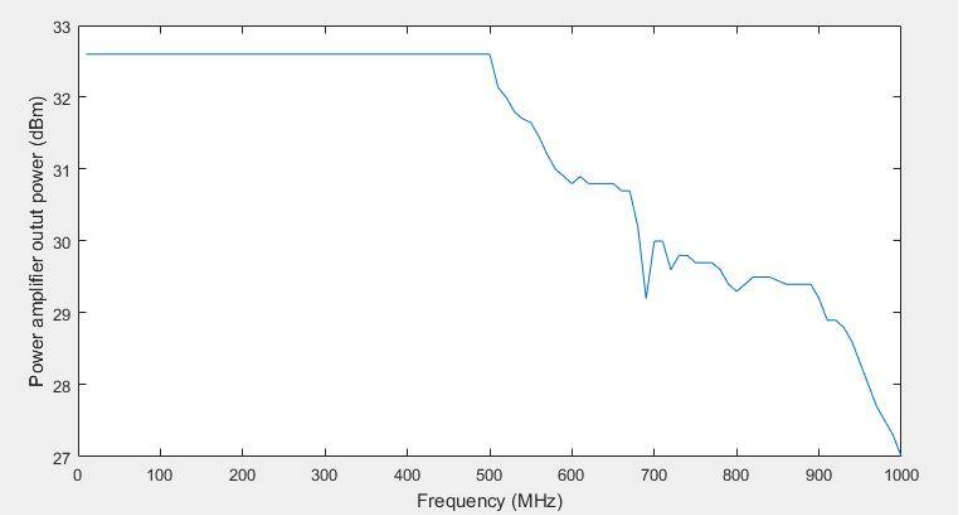


Figure 2-7 Power Amplifier output vs frequency

For the attack circuit to be efficient at coupling EM wave on the victim circuit, directional antenna is necessary. Unlike an omni-directional antenna, which emits radiation in all direction in a single plane, directional antenna tends to have narrow radiation pattern, thus less energy would be wasted in unwanted directions, compared to the energy

successfully coupled to the victim circuit. But, unlike the far-field radiation pattern of many directive antennae, under near-field it is difficult to achieve radiation in a confined direction. Although there are were attempts from P. Rastogi et. al. to create a near-field radiator with focused field [36], these solutions exists for transmitting signals in the kHz range, under which the impedance matching issues are far less prominent.

Along with focused radiation characteristics, the antenna used for IEMI attack should have wide bandwidth of operation. This is because of the difficulty in pre-determining the resonant frequency of the victim circuit, due to the complex interconnections and lack of publicly available high frequency models. Thus, having an antenna with wide band operational capability would help the attacker sweep the transmitted signal frequency across a wide range and determine the frequency at which IEMI attack takes place efficiently.

Vivaldi antenna was chosen to be used at the attack circuit as a transmitter, due to its wide band operational range. This antenna falls under the class of traveling wave antennae [37]. The chosen Vivaldi antenna has an antipodal dual exponential tapered slot antenna (DETSA), exponential lines running on both edges of the antenna. Since the antenna is antipodal, each branch of the antenna is placed on one side of the PCB, which makes input impedance match easier as compared to traditional Vivaldi antenna design [38]. This antenna was fabricated on a FR4 board with 1.5 mm substrate thickness and 35 um copper thickness. The designed antenna measured 35 cm x 30 cm in size. The antenna was designed and optimized using ANSYS HFSS software tool, which is being shown by Figure 2-8.

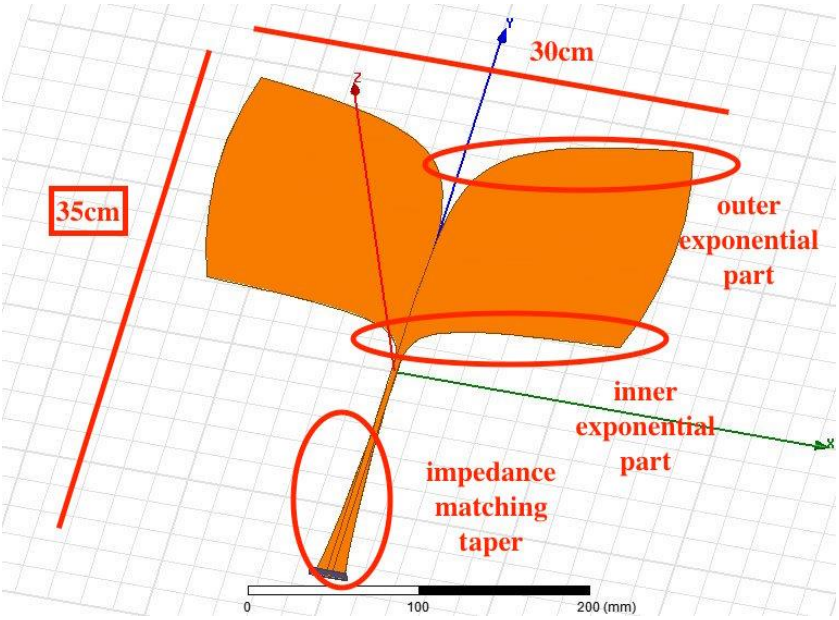


Figure 2-8 Vivaldi antenna designed in ANSYS HFSS

Return loss or S11 (scattering parameter or S-parameter) is used to quantify the amount of power successfully transferred to a load, as an antenna, from its source, compared against the amount of power reflected from the load to the source. This parameter is useful to characterize high frequency components such as an antenna. For an antenna usually S11 below -8 dB is considered acceptable, which represents the condition at which ~60% of the power generated at the source is successfully transferred to the load. Figure 2-9 compares the return loss or S11 of the Vivaldi antenna to monopole antenna. As expected, the Vivaldi antenna has an S11 less than -8 dB from 350 MHz to 2 GHz, while the monopole antenna has a narrow bandwidth of operation around 700 MHz.

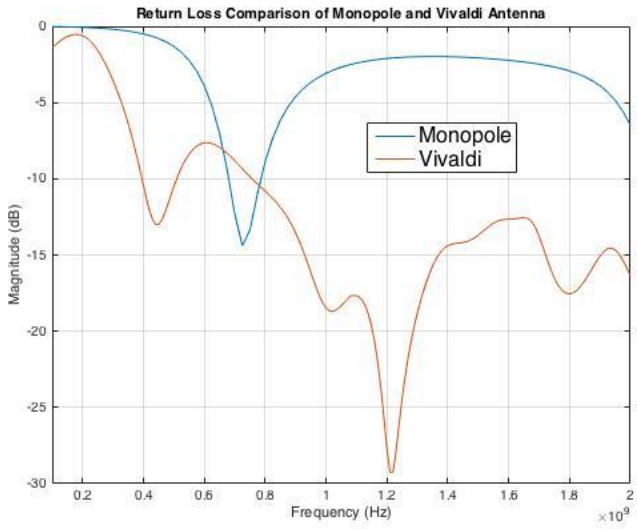


Figure 2-9 Return loss of Vivaldi antenna compared against a monopole antenna

Figure 2-10 shows the 3D plot showing the electric field radiation pattern of Vivaldi antenna, operating at 250 MHz. The color 'red' in this figure indicates the region in which maximum radiation energy is present, while light blue color indicates regions with least amount of radiation. This figure shows that the radiation pattern of a Vivaldi antenna, is not an improvement over a dipole antenna. But, the wideband frequency characteristics of this antenna, makes it a suitable candidate for IEMI attack experiments, in which the resonant frequency of the victim circuit is unknown.

Figure 2-12 shows the x, y, z components of the magnetic and electric field plots along the Y axis. The position of x, y and z, with respect to the antenna, can be seen from Figure 2-11. These plots represent the variation in the intensity of individual E-field and H-field components, as the distance increases in the end-fire direction. From this figure, it can be understood that the strongest component of E-field exists in the x direction, while the H-field's strongest component exist in the z direction. But, the magnitude of E-field is ~445 times greater than the magnitude of H-field. Hence the induced signal at the victim circuit

could have strong correlation with the electric field component existing along the x direction, while using this Vivaldi antenna to transmit the attack signal.

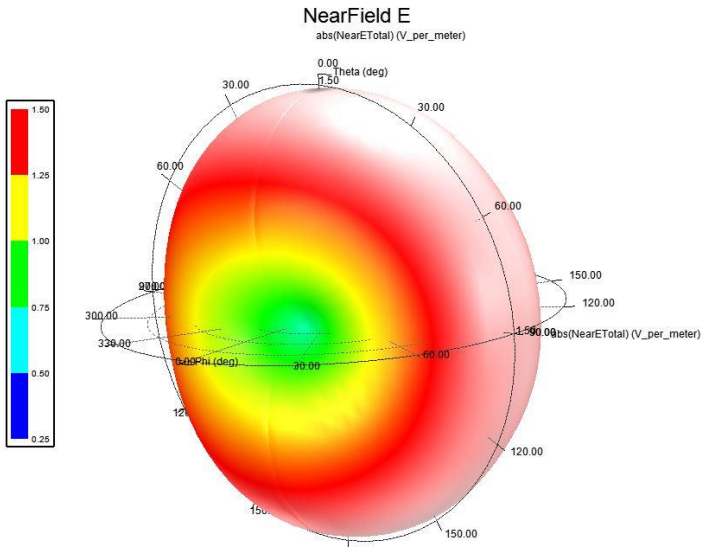


Figure 2-10 Electric field pattern of Vivaldi antenna under near-field conditions

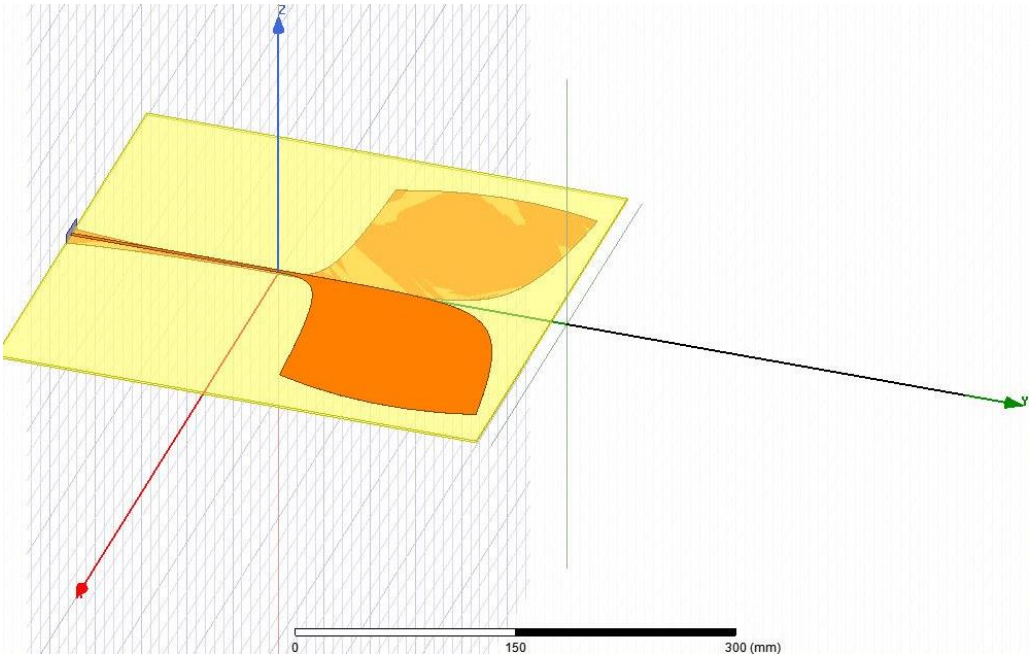
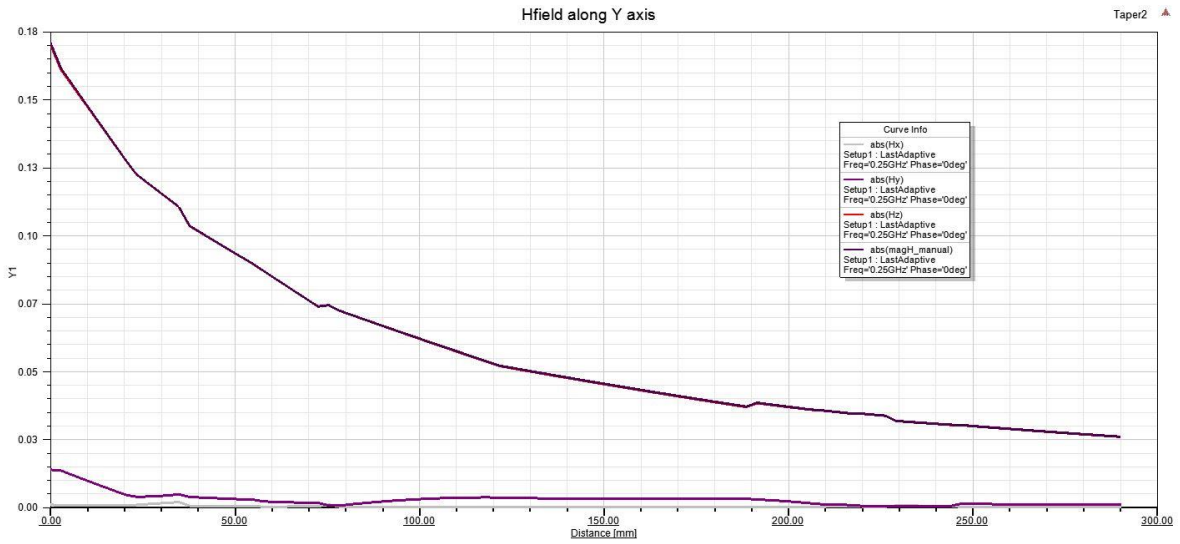
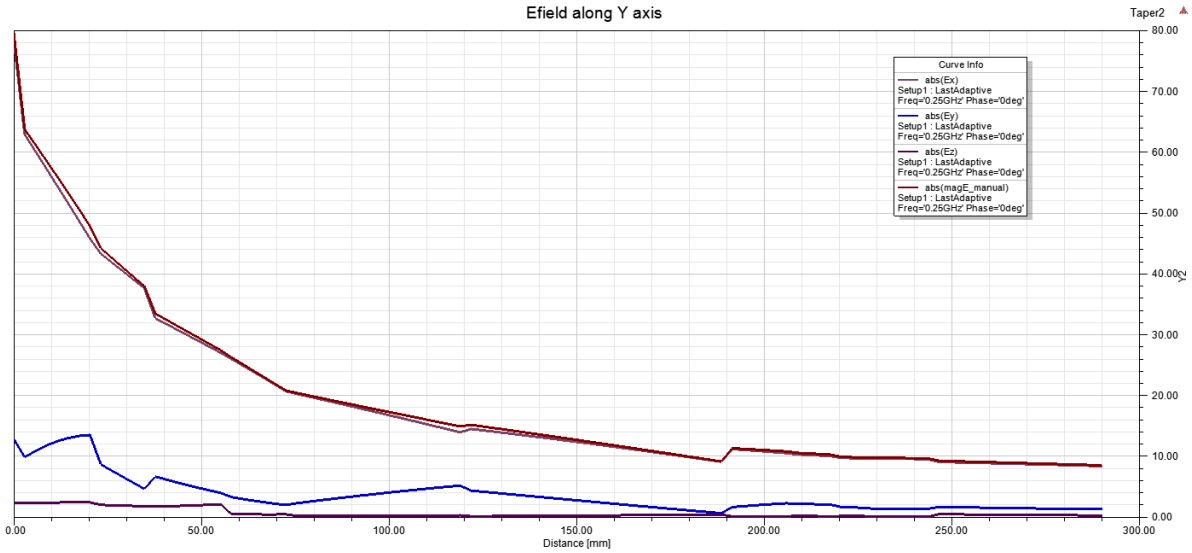


Figure 2-11 Vivaldi antenna shown with corresponding axes



(a)



(b)

Figure 2-12 a) Magnetic field and b) Electric field plots of Vivaldi antenna along the end-fire direction

2.2.3 Anechoic chamber

As mentioned earlier, IEMI attack relies on near-field power transfer. Near-field of an antenna is defined as the region in which the rate of decay of electric field and magnetic field are not inversely proportional to the distance from the antenna, but inversely related to the square or cube of the distance from the antenna, depending on the type of antenna. This effect has been shown in the field plots in Figure 2-12. For a large antenna, where the dimensions of the antenna are larger than half the wavelength of the signal being transmitted, the near field region can be described by equation (2-1) [39].

$$Near\ field\ region = \frac{2D^2}{\lambda} \tag{2-1}$$

In this equation, parameter 'D' represents the largest dimension of the antenna, while 'λ' represents the wavelength of the signal being transmitted. Any electric or magnetic conductors present within this near-field region, would interact with the antenna and would result in a change in the antenna's impedance characteristics.

For the Vivaldi antenna, the largest dimension was 35 cm and if we consider the lowest operational frequency of 350 MHz, which has a λ of ~85.6 cm, the near-field region around the antenna would be ~29 cm. Thus, any conductive elements present within 29 cm of the antenna, would result in a change in the antenna input impedance, there by changing the amount of signal power radiated from the antenna.

Along with near-field clearance around the antenna, the experimental setup could suffer from additional errors introduced by the transmitted signal bouncing from nearby objects such as wall, metallic objects, etc. This could be increasing or decreasing the amount of power coupled to the victim circuit. To avoid these interferences from the experimental

setup, the author chose to surround the experimental area with Radiation Absorbing Material (RAM), as shown by Figure 2-13.

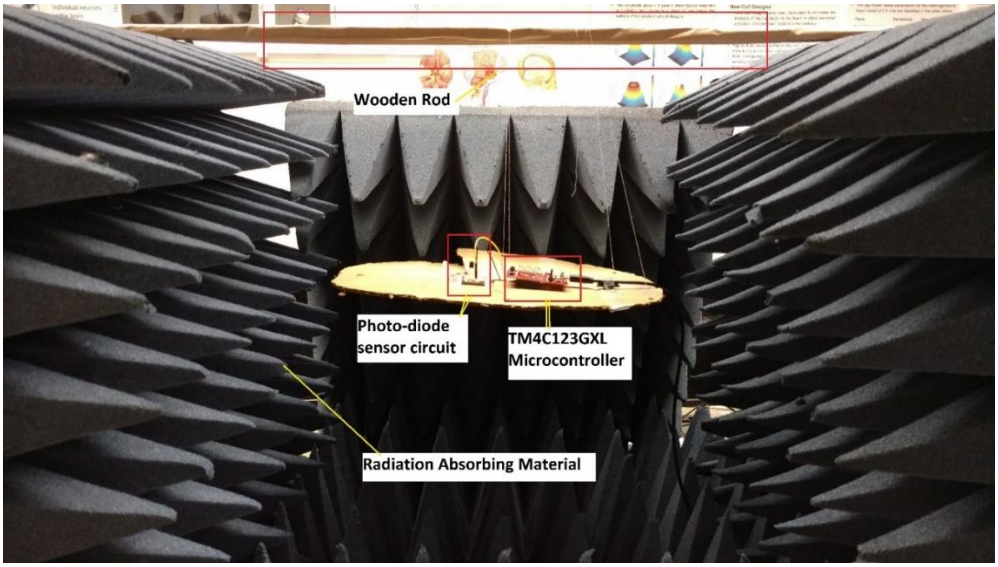


Figure 2-13 Experimental setup with Radiation Absorbing Material (RAM) shields

A chamber full of RAMs were traditionally used to absorb sound or electromagnetic wave from reflecting off the walls of the chamber. Such a chamber was called anechoic chamber. Anechoic chambers are essential in scenarios such as characterizing antenna or sound recording, where reflection of waves (electromagnetic or sound) from the walls of a chamber would introduce sources of noise.

For IEMI attack, the victim circuit was enclosed by RAMs rather than a full anechoic chamber, due to certain requirement of the victim circuit. The most important requirement of the victim circuit being the usage of short USB cables to communicate with the PC, which would avoid interference of the IEMI attack signal from disrupting the serial communication between the PC and the microcontroller. Since longer USB cables would be essential to connect the victim circuit to a PC, while placing it inside an anechoic chamber, the serial

communication could become susceptible to interference from EM signal, due to the long USB cable acting as an antenna.

Thus, the IEMI experiment was conducted by surrounding the victim circuit on four out of five sides of a cuboid. The top side of the cuboid was left open, since the antenna used for transmitting the IEMI attack signal was end-fire type, meaning the radiation emitted from the antenna travels in the direction of the Y axis (as shown in Figure 2-11). The front side of the cuboid was not covered with RAM, to have space for the large Vivaldi antenna to be positioned. This setup eliminates the need for using longer USB cables, since the experimental setup with RAM walls could be easily place close to a PC, without any issues.

This partial anechoic chamber with RAMs ensures that, the radiation emitted from the Vivaldi antenna does not get reflected from the walls of the cuboid, while the IEMI attack signal transmitter, namely Vivaldi antenna, does not experience impedance interference from sources, other than the disturbance coming from the intended victim circuit.

Figure 2-13 shows the victim circuit placed on a non-conductive cardboard surface, hung from a non-conductive wooden rod, using cotton threads. Placing the victim circuit directly on top of the RAMs might attenuate the IEMI attack signal trying to get coupled to the victim circuit. Hence, a decision was made to position the victim circuit in the middle of the partial anechoic chamber.

2.3 Experimental Results

The IEMI attack to inject false data into photo-diode sensor circuit, was performed with different ambient IR light conditions, to better understand the effects of this attack on a real-world scenario. Thus, three different IR ambient light conditions were chosen, namely, no

light, medium light and maximum light conditions. The different ambient light conditions were controlled with the help of an IR lamp capable of outputting 5W radiation at 850 nm wavelength.

Since the IR lamp used in this experiment came with metallic casing, this lamp was placed between the cones of the RAMs, which were shown in Figure 2-13. The author believes that, this setup would avoid any impedance interference or EM reflection from the IR lamp casing.

As the term ‘no light’ suggests, this lighting condition represents the experimental condition when no explicit IR radiation source was present near the experimental setup. Since the ADC present in the TM4C123GXL microcontroller can digitize voltages between 0 V and 3.3 V, the ambient IR light conditions when the ADC reads 1.5 V, which is close to the half of the maximum voltage value that the ADC can read, was assigned as medium light condition. The maximum light experimental condition uses sufficient IR radiation from the IR lamp to produce a DC voltage just below 3.3 V, by 1 mV to 20 mV. The reason for setting the DC voltage for maximum light condition to be carefully set just below 3.3 V was due to the maximum DC voltage that the ADC can read. As mentioned previously, any voltage above 3.3 V would be read as 3.3 V by the ADC. Hence, it was important to set the sensor output voltage to couple of millivolts less than 3.3 V, to fully observe the effect of the coupled attack signal, without introducing any error due to signal clipping.

The 1 mV to 20 mV variation in the maximum light condition exists due to the difficulty in precisely controlling the IR lamp output power, which was done by controlling the voltage supply to the lamp, using an external DC power supply, as well as changing the orientation of the IR lamp.

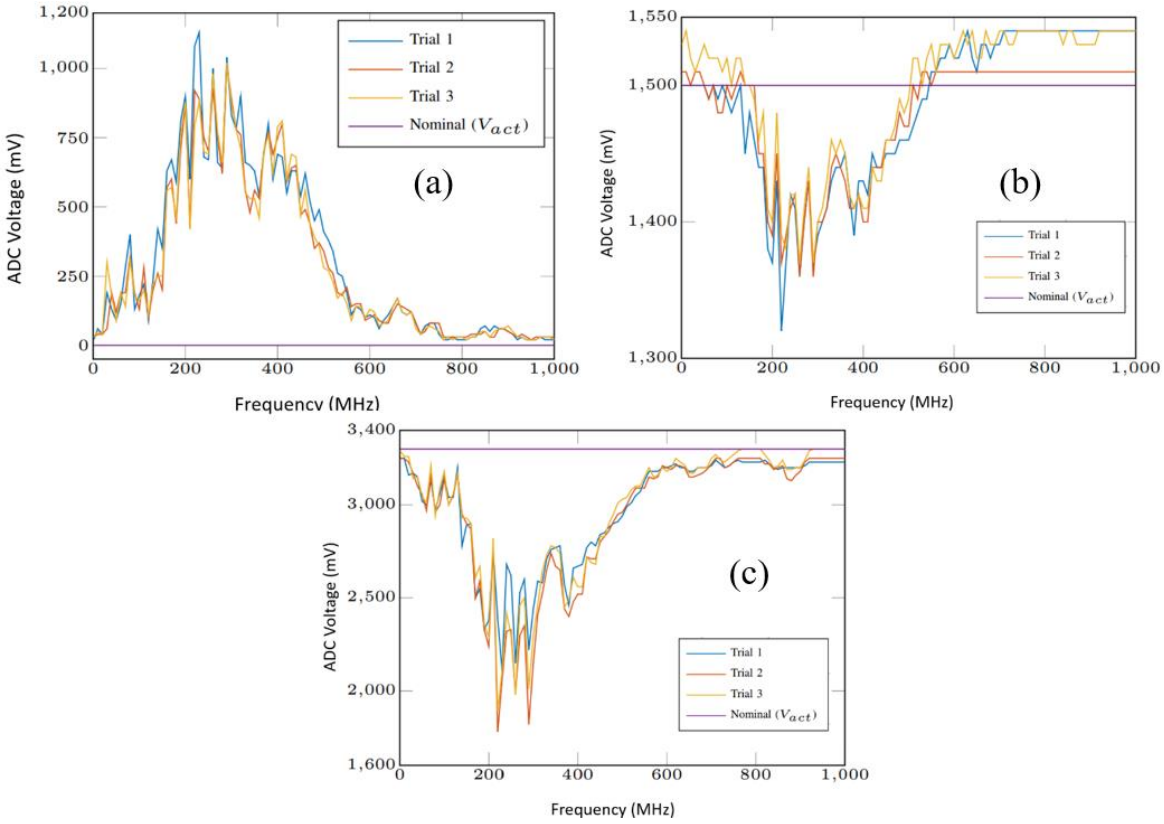


Figure 2-14 ADC output when the distance of separation between the transmitter and victim circuit was 10 cm, under (a) No IR light condition. (b) Medium IR light condition. (c) Maximum IR light condition.

Figure 2-14 (a), (b) and (c) shows the experimental results under the three different IR lighting conditions, along with results from three different trials. For all the trails presented in these plots, the distance between the IEMI attack signal transmitting Vivaldi antenna and the edge of the microcontroller/ photo-diode circuit was fixed at 10 cm. The term 'nominal

(Vact)' represents the DC voltage that the ADC would read under the condition when no IEMI attack signal was present. Thus for Figure 2-14 (a) the value of Vact is 0 V, while the values of Vact in Figure 2-14 (b) and Figure 2-14 (c) are 1.5 V and 3.3 V. The frequency dependent data for Figure 2-14 was obtained by changing the transmitted EM signal frequency by a step size of 10 MHz from 1 MHz to 1 GHz.

Figure 2-14 (a) conforms with the rectification and signal clipping hypothesis presented in the 'mechanism of attack' section. Thus, a maximum of ~1 V DC false data was introduced into the victim circuit at 290 MHz, which could be the resonant frequency of the victim circuit. Under no light condition, the effect of rectification could be dominant over signal clipping phenomenon, since the induced DC voltage were measured externally using a digital multi-meter from Fluke, which does not suffer from the signal clipping non-linearity due to the extended voltage range from -1000 V DC to + 1000 V DC [40]. Figure 2-15 shows the signal measured at the input terminal of ADC, using an oscilloscope. As seen from this figure, there is a clear DC offset of ~1.28 V, under no IR radiation condition. Like the digital multimeter, the oscilloscope has a much wider voltage measurement range and hence, proves that the DC offset induced at the victim circuit does not occur as a result of signal clipping. It is also important to note that under the no light condition, the photo-diode behaves like a capacitor, since it does not conduct current due to absence of ambient IR radiation. This capacitive behavior comes from the reverse biased P-N junction inside the photo-diode [35].

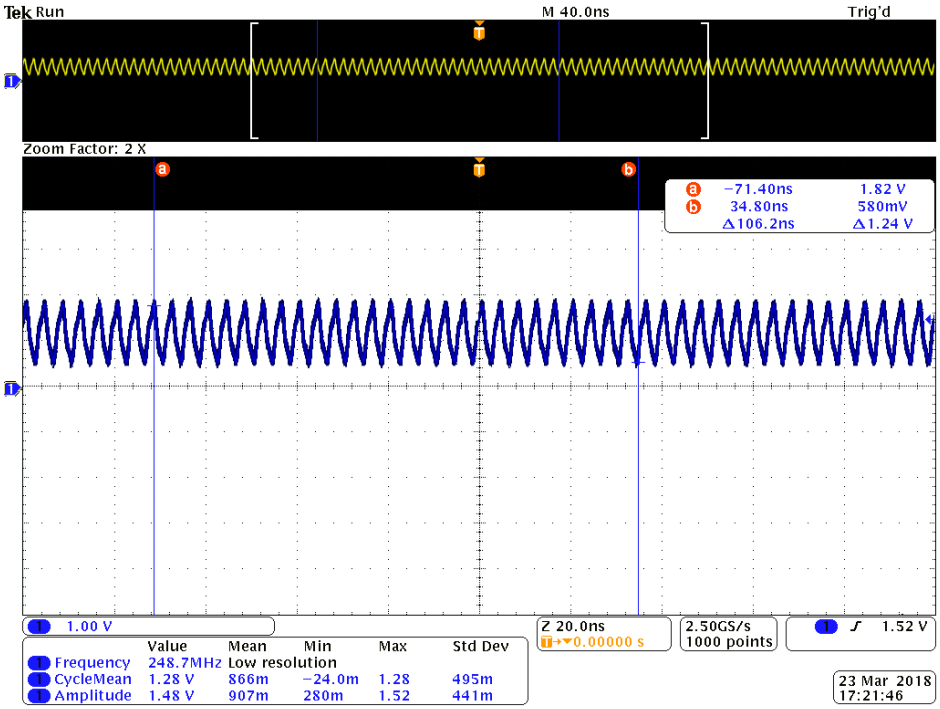


Figure 2-15 Oscilloscope screenshot showing the DC offset induced at the input terminal of ADC, under no IR light condition

Figure 2-14 (c) shows a drop in ADC voltage, rather than an increase, as with the no light condition. This is because, the DC voltage generated from the photo-diode sensor and the DC voltage generated from the rectification of coupled EM signal, acts as if the two DC voltage sources were in parallel, thereby their DC currents subtract from each other, thus resulting in a net voltage, which was the difference between the two DC voltages. This phenomenon is clear, while comparing the Figure 2-14 (a) and (c), because, Figure 2-14 (c) can be obtained by subtracting the data in Figure 2-14 (a) from 3.3 V. Also, the results shown in Figure 2-16 suggests that there was an DC offset induced at the input terminal of ADC and is not due to the signal clipping phenomenon occurring during the digitization process.

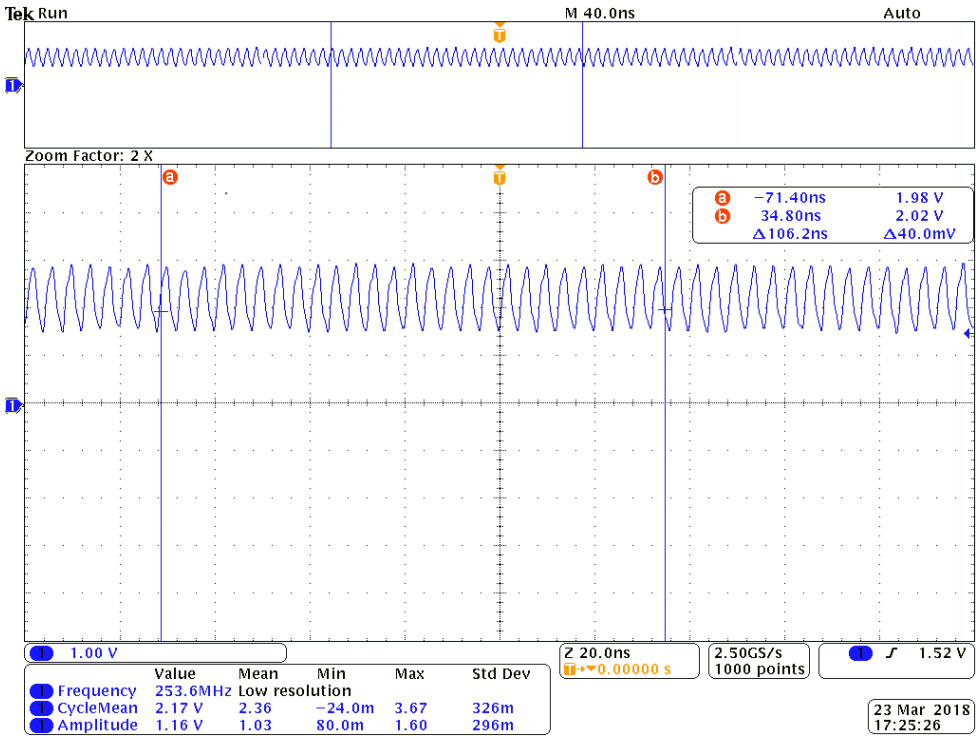


Figure 2-16 Oscilloscope image showing DC offset induced at the victim circuit, under maximum IR light condition

Under the maximum IR light condition, the photo-diode is behaving as a short circuit for AC signal, rather than a capacitor, due to the DC current flow through its P-N junction, when the photo-diode was exposed to IR light. Thus, net false data injection of ~1 V was injected at 290 MHz.

The results presented in Figure 2-14 (b) follows similar explanation as with the Figure 2-14 (c) results. Since the photo-diode was exposed to IR light, under medium IR light condition, the P-N junction inside the photo-diode was conductive and which produced a DC voltage source in parallel with the DC voltage source provided by the coupled EM signal rectification. The net results in Figure 2-14 (b) could be obtained by first scaling the data in Figure 2-14 (a) by 0.2 and then subtracting the results from 1.5 V. Thus, a maximum of -0.2

V DC was injected as false data into the ADC, under medium light condition. The reason for the decrease in the induced DC voltage at the victim circuit, could be thought of as an effect of change in impedance of the victim circuit, due to the quasi-open nature of the photo-diode, thus resulting in a reduction in the amplitude of the AC signal induced. But the oscilloscope measurement of the coupled signal amplitude, present at the input of the ADC terminal, shown by Figure 2-17, suggests otherwise. Hence, the best hypothesis for the reduction in the amplitude of induced DC signal could be attributed to the change in AC to DC conversion efficiency, caused by the ESD diodes, under different DC biasing conditions.

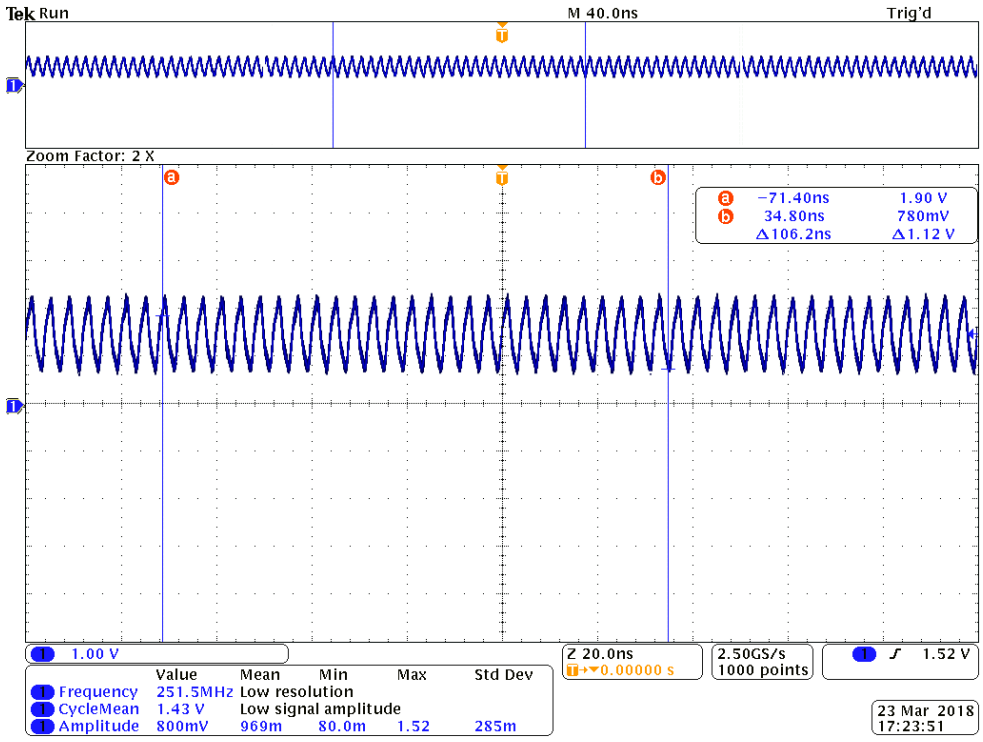


Figure 2-17 Oscilloscope image showing same amplitude of induced sinusoidal signal, under medium IR light condition

Figure 2-14 (b) shows the data slightly above 1.5 V nominal value, at frequencies below 200 MHz and above 600 MHz. This was due to the difficulty in controlling the photo-diode's

exposure with IR light. The IR light exposure was controlled by positioning the IR lamp, so that the region of maximum IR radiation was angled away from the photo-diode sensor. But due to the difficulty with the IR lamp mounting system, there were few errors introduced between different trials and thus, a maximum of 50 mV deviation occurs from the nominal value of 1.5 V.

It is important to note here that, the observations made from the experiment shows that, the rectified DC current flows in an opposing direction to the DC current generated from the photo-diode sensor, when the photo-diode is exposed to IR light. Hence, to increase the induction of negative DC voltage, the attacker must transmit more power towards the victim circuit.

Although, it may seem that an IEMI attacker could only induce a negative DC voltage into the ADC input, while the photo-diode sensor is exposed to IR radiation, while positive DC voltage induction is only possible under the conditions when no IR light presence in the environment, it is possible to induce positive DC voltage into the victim circuit using certain wideband waveforms. The details regarding these waveforms will be discussed in the chapters 3 and 4.

Figure 2-18 shows the results of induced ADC voltage with respect to frequency, while the distance between the attacker antenna and the victim circuit were varied from 10 cm to 100 cm. The data shown in Figure 2-18 were obtained under no IR light conditions, as with the Figure 2-14 (a). One can notice a slight variation between the data shown in Figure 2-14 (a) and the data corresponding to 10 cm distance between attacker and victim circuit in Figure 2-18. This variation was due to the use of 5 MHz frequency step size as opposed to the 10 MHz step size used in Figure 2-14. Also, the experimental setup was slightly modified

by opening the vertical side wall RAMs outwards away from the victim circuit, to facilitate the attack signal to better couple with the victim circuit and avoid being attenuated by the RAMs. This modification to the experimental setup was essential, since under distances beyond 50 cm between the attacker and the victim circuit, the induced DC voltages were significantly low due to EM signal attenuation by the RAM. Because of these experimental setup changes, the 10 cm data in Figure 2-18 has slight variation from Figure 2-14 (a).

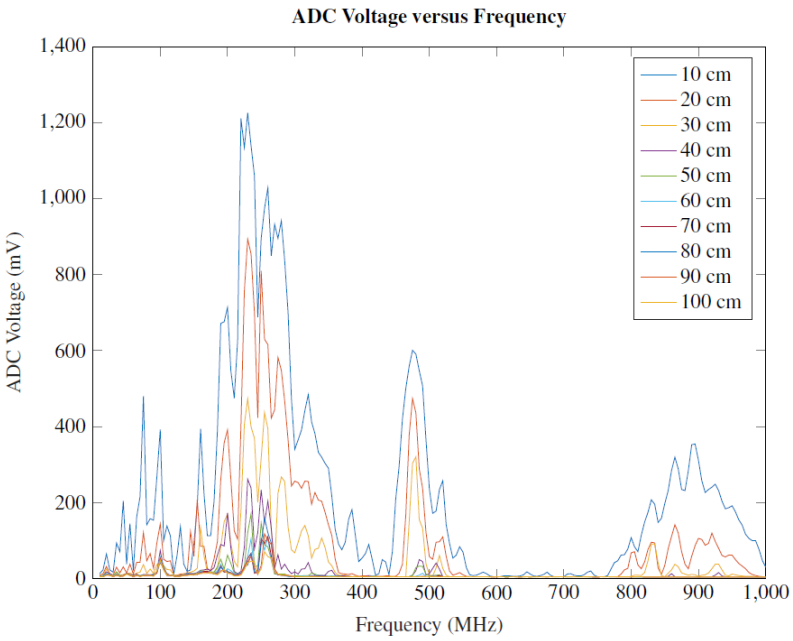


Figure 2-18 ADC voltage induced under no IR light condition, with varying distance between the EM signal transmitting antenna and the victim circuit

The following section discusses building a theoretical model for the attacker and victim circuits and using this model to get an estimate on the required amount of power from an attacker's perspective, to induce a certain amount of false DC voltage into the photo-diode sensor circuit.

2.4 Transmitted power requirement estimation

An attacker using the IEMI technique to inject false data into an analog sensor would be interested in knowing the minimum amount of power that must be transmitted to achieve a certain level of DC voltage induction at the victim circuit's ADC input, while accounting for the distance of separation between the attacker and the victim circuits. Since the IEMI attack relies on the parasitic properties of the victim circuit to couple the attack signal, it is difficult to obtain a closed form analytical solution with an accurate model of the attacker as well as the victim circuits. This problem of modelling the circuits is exacerbated by the complex interconnection and PCB traces in the victim circuit. Hence the author chose to simplify the models of attacker and victim circuits, operating under near-field conditions, to get an intuitive understanding of the EM coupling mechanism. Thus, the power requirement can be estimated by modelling both the victim and the attacker circuits as an Resistor-Inductor-Capacitor (RLC) circuit and approximating the antenna which transmits IEMI signal at the attacker side and the section of the victim circuit responsible for receiving this IEMI signal as loop antennae.

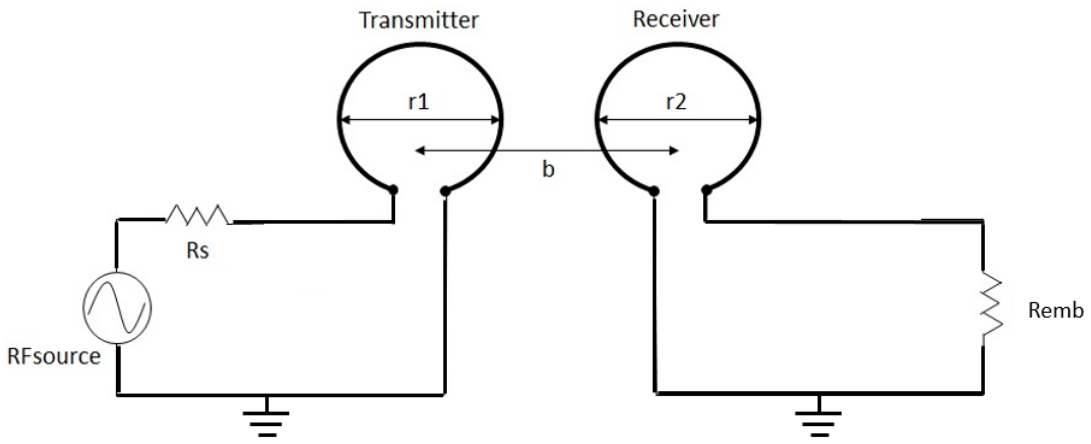


Figure 2-19 Equivalent circuit model for the IEMI attacker and the victim circuit

Figure 2-19 shows the simplified equivalent circuits of the attacker and the victim circuits. The part of the attacker circuit which is essential for getting a closed form solution, is the antenna. The transmitting antenna, which has been connected to the signal source 'RFsource', is modelled as a loop antenna with radius 'r1', while the parameter 'Rs' represents the source resistance. On the victim circuit side, the parameters 'Remb' load resistances, which the coupled EM signal experiences, while the parasitic components which were responsible for coupling the attack EM signal on to the victim circuit was modelled as a loop antenna with radius 'r2'. The two loop antennae were separated by a distance 'b', with an assumption that 'b' is within the near-field regions of the two antennae.

Figure 2-19 needs to be further simplified by reducing the loop antennae into its corresponding inductance, capacitance and resistances, before a closed form solution, for the required transmitted power, can be attempted.

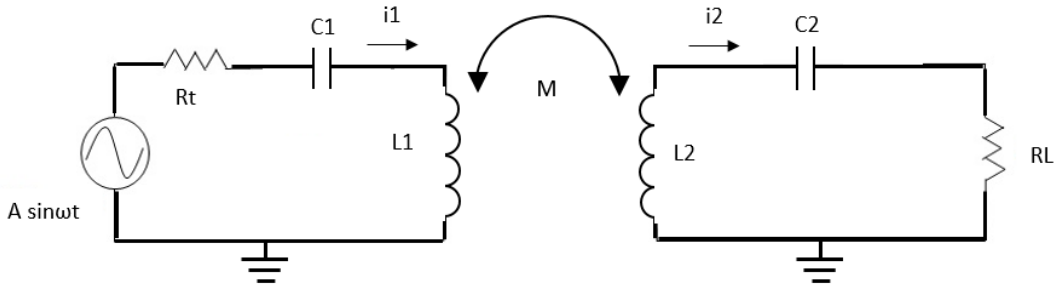


Figure 2-20 Simplified equivalent circuit models for the attacker and victim circuits

Figure 2-20 shows the simplified circuit model of the attacker and victim circuits. The RF signal source has been represented by the terms 'A sinωt', which represents the signal source outputting a sinusoidal signal with amplitude 'A' and frequency 'ω', while 't' represents time. The parameter 'Rt' represents the source resistance as well as the ohmic losses at the attacker side, while 'C1' and 'L1' represents the parasitic capacitances and

inductances of the attacker circuit, respectively. Similarly, 'RL', 'C2' and 'L2' represents the load resistance, parasitic capacitances and inductances of the victim circuit, respectively. The parameters 'i1' and 'i2' with arrows represents the AC current magnitude with direction of current flow. The parameter 'M' represents the mutual inductance between the two inductors 'L1' and 'L2', which is directly proportional to the distance between transmitting and receiving loop antennae. Using the loop antenna description provided in the Figure 2-19, one can estimate the value of 'M' using the equation (2-2) [41].

$$M = \frac{\mu_0 \pi \, r_1^2 r_2^2}{2\left(\sqrt{b^2 + r_1^2}\right)^3}, \qquad r_1 > r_2 \tag{2-2}$$

In equation (2-2), μ_0 represents the permeability of air. The assumption that the radius of the transmitting loo antenna is larger than the victim loop antenna is usually true, since the physical size of PCB traces responsible for coupling the attack EM signal, is very small, when compared to dimensions of the attacker's antenna.

If the attacking circuit is operating at the same frequency as the resonant frequency (ω_0) of the victim circuit, the impedance provided by the capacitance and inductance in each loop will get cancelled out. Hence, the only reactance in these circuits would be provided by the mutual inductances. Using Kirchhoff's voltage law for the attacker and victim circuit models, the following equations were obtained,

$$-A + i_1 R_t - j\omega_0 M \, A \, i_2 = 0 \tag{2-3}$$

$$-j\omega_0 M i_1 + i_2 R_L = 0 \tag{2-4}$$

Solving equations (2-3) and (2-4) to evaluate i2,

$$i_2 = \frac{j\omega_0 M \, A}{R_t R_L + \omega_0^2 M^2} \tag{2-5}$$

Using the value of i2, the expression for the power coupled at the victim circuit can be found as,

$$P_L = \frac{1}{2}\, i_2^2\, R_L \tag{2-6}$$

In equation (2-6) the term 'P_L' represents the power coupled at the victim circuit.

Substituting equation (2-5) in (2-6),

$$P_L = \frac{1}{2}\frac{-\omega_0^2\, M^2 A^2}{(R_t R_L + \omega_0^2 M^2)^2}\, R_L \tag{2-7}$$

Using the expression for transmitted power 'P_t', given by the following equation,

$$P_t = \frac{A^2}{8R_s} \tag{2-8}$$

the power coupled at the victim circuit can be estimated as,

$$P_L = P_t \left(\frac{2\omega_0 M}{R_t R_L + \omega_0^2 M^2}\right)^2 Rs\, R_L \tag{2-9}$$

Using the equation (2-9), one can compute the exact DC voltage induced at the input of ADC using the following equation,

$$V_{adc} = \sqrt{2P_L R_L} \tag{2-10}$$

Equation (2-10) was obtained with ideal rectifying diodes (ESD) assumption, in which the diodes don't introduce any voltage loss, during the rectification process.

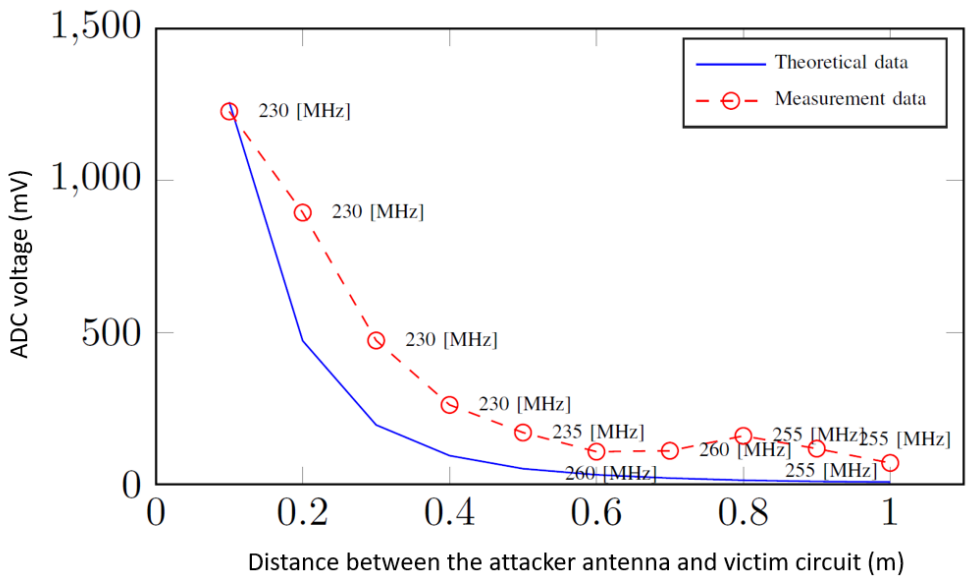


Figure 2-21 Comparison between theoretical and measured induced ADC voltage with varying distance between attacker and victim circuits

Figure 2-21 compares the induced voltage magnitude measured at the input of ADC versus the theoretical values obtained using equation (2-10). Since the circuit components shown in Figure 2-20 is an over-simplified version of the transmitter and victim circuits, the value of these components was selected using trial and error method, until a close fit between the theoretical and measured data were obtained. Thus, the values of 'r1' and 'r2' in equation (2-2) were chosen as 15 cm and 1.4 cm, while the resonant frequency 'ω_0' was chosen as 250 MHz, which was approximately close the frequencies at which maximum value of DC false data were injected at the victim circuit. The value of 'Rt' was set to 50 Ω, since the transmitting antenna was matched to 50 Ω, and the ohmic losses in the transmitter are negligible compared to this characteristic impedance. The value of 'RL' was set to 250 Ω, which was obtained using the datasheet of the TM4C123GXL microcontroller [34].

The measured data presented in Figure 2-21 were obtained by selecting the maximum induced DC voltage and neglects selecting the data from 250 MHz, as with the theoretical data. This method of data selection from the measured dataset was acceptable, since there were slight variations in the resonant frequency as the distance between the attacker and victim circuits were increased, due to the experimental setup changes involving re-positioning of the RAM side walls. This re-positioning of RAM side walls could have let the transmitting antenna impedance get affected by conductive objects present around the experimental area and might have contributed to the variation in resonant frequency. Thus, a maximum deviation of 20 MHz around the 250 MHz resonant frequency was considered acceptable to account for the change in the transmitting antenna impedance change.

Figure 2-21 shows close match between the theoretical and measured data, validating the simplified circuit model for attacker and victim circuits. Thus, as an IEMI attacker, one can use equations (2-2), (2-9) and (2-10) to compute the minimum required EM power to be transmitted to induce a particular amount of DC false data into the analog sensor circuit.

The experimental results shown in this chapter proves that besides inducing AC signal into victim circuits, as shown by Kune et. al [30], IEMI attack can induce DC signals, which tremendously expands the scope of this attack technique to all the analog sensors, which generate an DC voltage or current signal as a response to a physical change in the environment.

Since most analog sensors operate at voltage ranges in the order of hundreds of millivolts, the IEMI attack technique becomes a viable option for an attacker, even at distances in the order of meters, with transmitted power requirements in the order of few watts.

2.5 Conclusion

In this chapter, analog sensors connected to embedded systems, were considered as target for an IEMI attack technique. It has been shown that a photo-diode based analog sensor circuit, was able to be deterministically injected with false data, using IEMI attack technique. Using ~1.8 W continuous sinusoidal signal transmission, the photo-diode circuit, which was a representation of analog sensor circuits, regardless of the type, could induce ~1.2 V DC, when the analog sensor was outputting 0 V or 3.3 V DC. Under the conditions, when the analog sensor was generating 1.5 V DC signal, a maximum of ~250 mV DC false data was injected into this sensor circuit output. Theoretical analysis on the power requirement for an attacker, to deterministically induce a certain value of false data, has also been discussed. Thus, this chapter proves that IEMI attack technique poses a greater risk for a wide range of embedded systems, which rely on analog sensors, to gather information about its environment.

CHAPTER 3

FALSE DATA INJECTION FOR DIGITAL SENSORS

This section has used materials that were published in the paper "Electromagnetic Induction Attack on Embedded Systems", by J. Selvaraj et. al, with the permission of all the authors [31].

Digital sensors are a class of sensors which have data converters inbuilt, and thus outputs the data in a digital format. Compared to analog sensors, digital sensors are robust due to its tendency to resist noise in the data transmission path, which is a major problem for analog sensors. These advantages over analog counterparts have made digital sensors a predominant choice, while considering sensors in an application. Digital sensors communicate their output data serially to an embedded system.

General Purpose Input/ Output (GPIO) are a set of digital input/output pins available on an integrated circuit, which were not assigned a predefined function. In an embedded system, these GPIO pins provide the freedom for the user to define them as either digital inputs or outputs, which make them as suitable candidate to connect digital sensors, to send and receive data.

Digital sensors can communicate with embedded systems serially using pulse width modulation or serial data at a particular bit rate. There is a myriad of digital sensors available in the market currently, including, but not limited to, sensors to measure temperature, pressure, light, orientation/position, proximity, sound, speed and acceleration. These sensors are an integral part of an embedded system, allowing it to estimate a physical quantity and process the data digitally.

Navigation systems in modern smart phones, for examples, uses many sensors to determine the precise location of the user and provide them with turn-by-turn navigation. Some of the sensors used by our phone's navigation systems are Global Position System (GPS), accelerometer, gyroscope and magnetometer sensors. The gyroscope sensor is an example of fully digital sensor, with data sampling and data conversion systems built inside the chip [42].

Increased reliance on these automated navigation systems has led to several people losing their lives, the phenomenon of which has been named as death-by-GPS. In 2011, a couple lost their lives by, when they were on their way to Las Vegas. This was due to their reliance on GPS navigation system in their van, which led them into a road in the middle of nowhere, in the northeastern Nevada [43]. It was sad to notice that this was not an isolated case. Even with the advancements in navigation technologies, people's unquestioned faith on their smart phones have costed their lives. Hence, along with solving existing problems with modern navigation systems, researchers must investigate potential danger of false data injection into these digital sensors, which could pose for future consumers. Especially the non-invasive false data injection technique into digital sensors, using IEMI attack, described in this chapter, needs to be investigated thoroughly, to understand the risks it could bring to general public, who are already plagued with dangers such as death-by-GPS.

Digital sensors are generally thought to be at lower risk from IEMI attacks. The reason for digital sensor's resilience for noise was due to the high amplitude logic levels as compared to the continuously varying voltage/current signals outputted by analog sensors. Also, this makes the digital sensors a difficult target for false data injection attacks, due to the need for identification of specific bit's logic level to induce a bit flip. Along with these

challenges, an IEMI attack would require relatively large power requirement for an attacker to induce sufficient voltage shifts, to cause the bits to flip.

Despite these challenges, in this chapter, IEMI technique will be used to demonstrate false data injection into digital sensors which are connected to the GPIO pins of an embedded system and communicate serially. This attack was demonstrated by using two microcontrollers, with one being a transmitter, mimicking a digital sensor, while the other being a receiver, using the GPIO pin.

3.1 IEMI attack using continuous sinusoidal signal

Tiva C microcontroller boards from Texas Instruments was chosen for this experiment, due to the availability of GPIO pins on the circuit board [34]. Figure 3-1 shows the experimental setup used for demonstrating this attack technique. Like the setup used for attacking analog sensors, the experimental area was covered with RAMs to avoid signal reflection from the near-by objects (shown in Figure 3-2). As mentioned before, one microcontroller was assigned the task of transmitting digital bits, while the other receives this data. The receiving microcontroller was connected to a PC, through USB cables, to output the total number of 1s and 0s received.

Continuous sinusoidal signal was decided as the attack signal, due to the results from chapter 2, which showed that an DC offset could be observed while coupling AC signal on to the input pins of microcontroller. The ideal condition for an attacker would be the induced AC signal, resulting due to the transmission of continuous sinusoidal signal, would offset the DC level at the input of the GPIO terminal, such that, the received digital signals would be modified, depending on the intention of the attacker. Thus, the victim circuit's embedded system would read a logic level 0, even though the digital sensor sends out a digital bit '1',

due to the DC offset introduced by the induced AC attack signal. To verify this hypothesis, an experimental setup was shown by Figure 2-5, justifying the induction of DC offsets.

The attacker circuit was exactly same as the one used for analog sensor attack, as shown in Figure 2-5. Furthermore, Vivaldi antenna was used to transmit the attacker's signal, due to its broadband capability, which allows the attacker to sweep the frequency and identify the resonant frequency of the victim circuit, at which maximum power transfer takes place. To increase the EM signal coupling at the victim circuit, 15 cm long jumper cables were used to interconnect the transmitting and receiving microcontrollers.

In the first method, constant logic level will be transmitted to the receiving microcontroller and the total number of 1s and 0s received will be counted and sent to a PC to demonstrate that an IEMI attack can induce voltage change at the victim circuit, which is significant enough to cause bit flips. By using constant logic level transmission, the effectiveness of IEMI attack signal in causing a logic change can be estimated. Thus, if digital logic 1 was transmitted, then the data sent to the PC will indicate, the number of times logic level 1 was misread as logic level 0 by the receiving microcontroller. The receiving microcontroller was programmed to sample at a rate of 167 kbps, hence the logic level of the signal transmitted was sampled every 6 μs, with the microcontroller operating at 16 MHz clock speed.

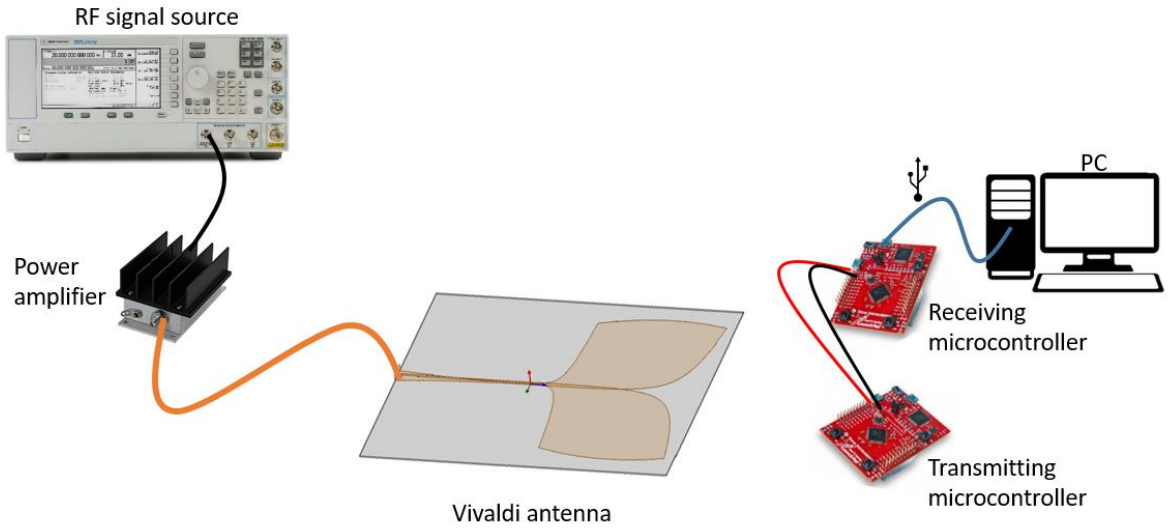


Figure 3-1 Experimental setup for demonstrating IEMI attack on digital sensors

The microcontroller was programmed to sample 10,000 data points and identify the total number of digital 1s and 0s. Thus, two different test cases were used, namely, transmitting constant 0 digital logic and transmitting constant 1 digital logic. In each of the cases, the IEMI attack signal will result in some percentage of fault injection at the receiving microcontroller, leading to 0s being misread as 1s and 1s being misread as 0s.

Figure 3-2 shows the photograph of the actual experimental setup used for this attack, with the RAMs covering the four sides of the experiment area, similar to the setup used for attacking analog sensors. Both the antenna and the victim circuits were placed on a non-conductive cardboard box, to provide elevation, away from the bottom RAM sheet, to prevent attenuation of signal directed towards the victim circuit.

The distance between the microcontrollers and the attacker's antenna was kept as close as possible, to increase the chance of bit misreads, due to the limited transmission power available at the lab facility, where this experiment was conducted. Similar to the

experimental setup used for analog sensor attack, ~1.8 W sinusoidal signal was supplied to the Vivaldi antenna's input terminal, which would be transmitted towards the victim circuit.

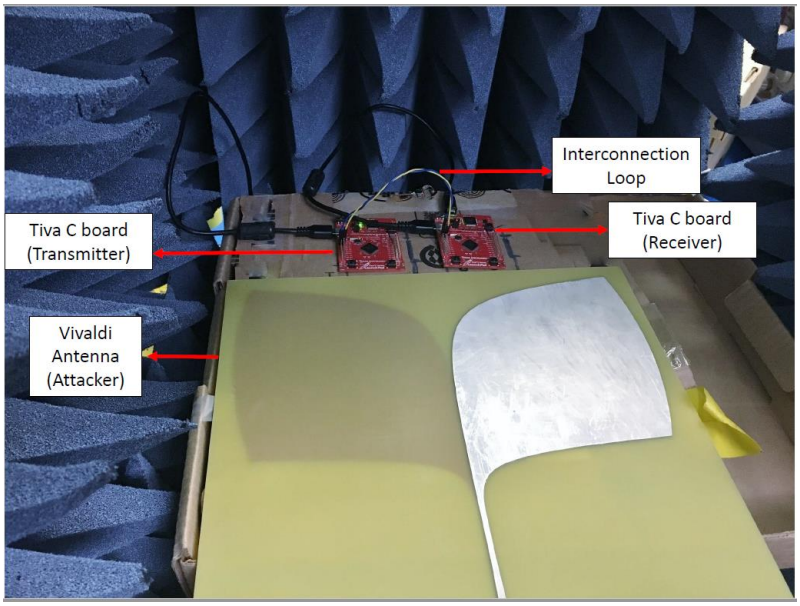


Figure 3-2 Photograph of experimental setup used to demonstrate IEMI attack on digital sensors

3.1.1 Experimental results and discussion

Figure 3-3 a and Figure 3-3 b shows the percentage of misreads at the receiving microcontroller, when the transmitting microcontroller was outputting logic level 1 and logic level 0, respectively. These figures show the aggregation of results from four different trials. The results from Figure 3-3 shows that significant misreads happened from 180 MHz to 220 MHz, for both the cases involving transmission of digital 1 and 0.

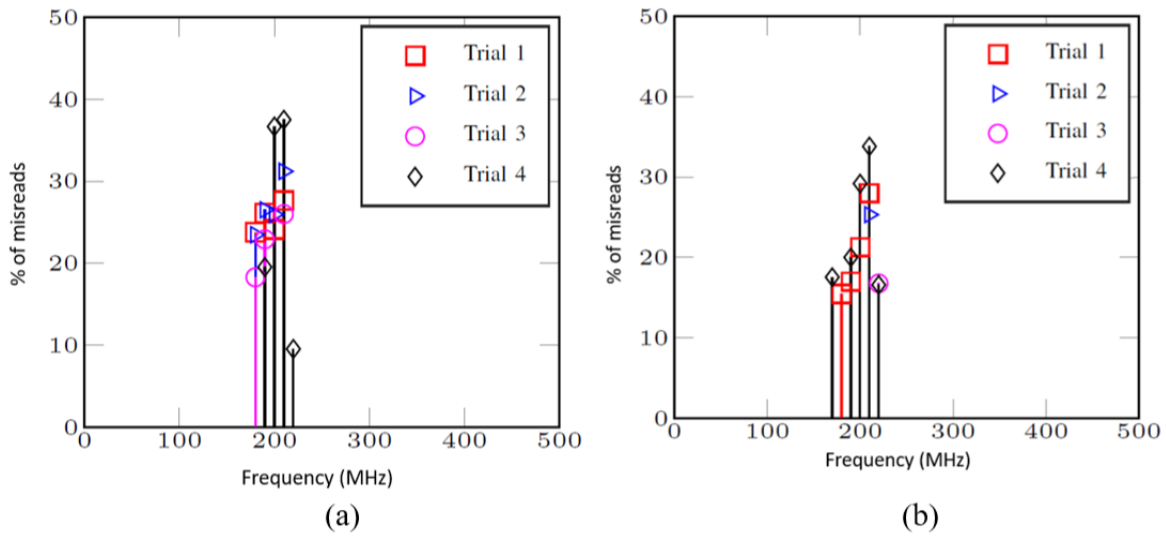


Figure 3-3 Percentage of misreads vs frequency when the transmitting microcontroller sends a) logic level 0, b) logic level 1

As shown by Figure 3-3, the maximum percentage of misreads, while transmitting logic level 0s and 1s, was ~38% and 30%, respectively. Although these misread percentage proves that the IEMI attack successfully injected false data into the victim circuit, it begs the question on why the attack was only able to result in less than 40% of misreads. This question could be answered by looking at the process of sampling a sinusoidal signal superimposed on a DC signal.

Since the attack signal and the receiving microcontroller's sampling clock signal are not synchronized, the sampling process at the receiving microcontroller can be thought of as an equivalent-time sampling [44]. Since the sinusoidal attack signal is superimposed on top of the digital logic signal, the data resulted from the sampling process would have a maximum of 50 % misreads of the logic level transmitted. This is because, a pure sinusoidal signal is symmetric and consist of equal portion of signal voltage above and below the average value

of 0 V. But this does not explain the difference between the misread percentage of logic levels 0s and 1s.

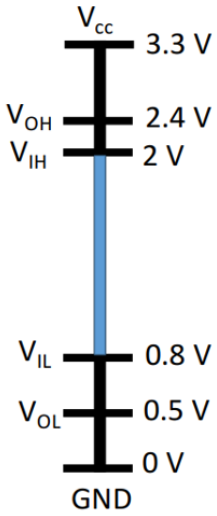


Figure 3-4 Digital logic voltage level for 3.3 V systems

The digital logic level used by the Tiva C microcontroller was 3.3 V. The logic voltage level of this microcontroller is shown in Figure 3-4, in which VIL and VIH represents the input level lower and higher voltage thresholds, respectively, while VOL and VOH represents the output level lower and higher voltage thresholds, respectively. Since the receiving microcontroller uses its input port, a total voltage shift of 2 V is needed to make the bit change from logic level 0 to 1, while a voltage drop of 2.5 V is required to achieve logic level 1 to 0-bit change. Since same amount of signal power was transmitted from the attacker circuit, the induced AC signal could achieve higher percentage of bit flips causing logic level 0 to 1-bit change, resulting in an increased misread percentage, compared to 1 to 0-bit change.

3.2 Modified experimental setup demonstrating IEMI attack using continuous sinusoidal signal

The results shown in Figure 3-3 does not align well with the theory of inducing DC offset due to the coupling of an AC signal, as inferred by the results obtained from analog sensor attacks. To understand the reasoning behind this irregularity, the author decided to modify the experimental setup as shown in Figure 3-5. This modified setup includes a longer interconnecting cable to carry the digital logic signal to the GPIO pins, along with the cable folded to form a coil with 3 turns, with an aim to increase the amplitude of the coupled signal onto the victim circuit, which would exaggerate the DC offsets induced by the coupled AC attack signal. This modification would eliminate the need for transmission of attack signal with higher power levels. The digital signal path was intercepted and connected to an oscilloscope to visualize the effect of signal coupled AC signal at the victim circuit.

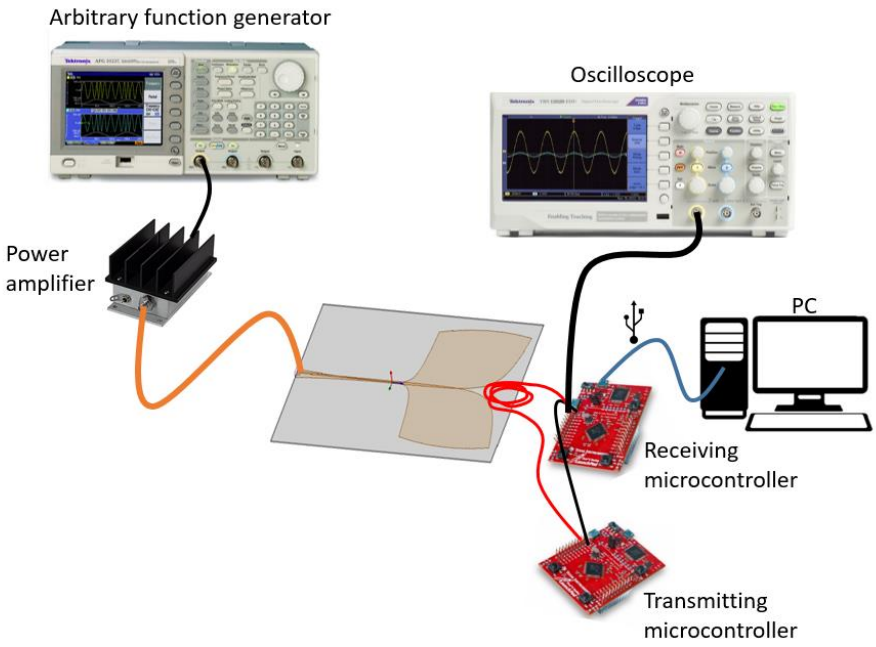


Figure 3-5 Modification to experimental setup to attack digital sensors, by using long interconnecting cable shaped as a coil

Since the interconnecting cable length was modified, it was experimentally found out that the maximum amplitude of signal coupling happened at 250 MHz. Hence, a continuous sinusoidal signal at 250 MHz frequency was transmitted from the Vivaldi antenna at maximum possible power level of 1.8W, to observe the effect on the logic levels.

3.2.1 Experimental results and discussion

Figure 3-6 shows the screenshot of the oscilloscope illustrating the DC levels present in the interconnecting cable, while the transmitting microcontroller sends logic level 1, when no attack signal was transmitted from the attacker circuit. From this figure, the DC voltage level available at the input terminal of the GPIO pin was ~ 2.1 V, which was enough to be registered as a logic level 1 at the receiving microcontroller, according to the data shown in Figure 3-4. This drop in voltage from the nominal voltage of 3.3 V, corresponding to the logic level 1, could be caused due to insufficient current supplied by the transmitting microcontroller.

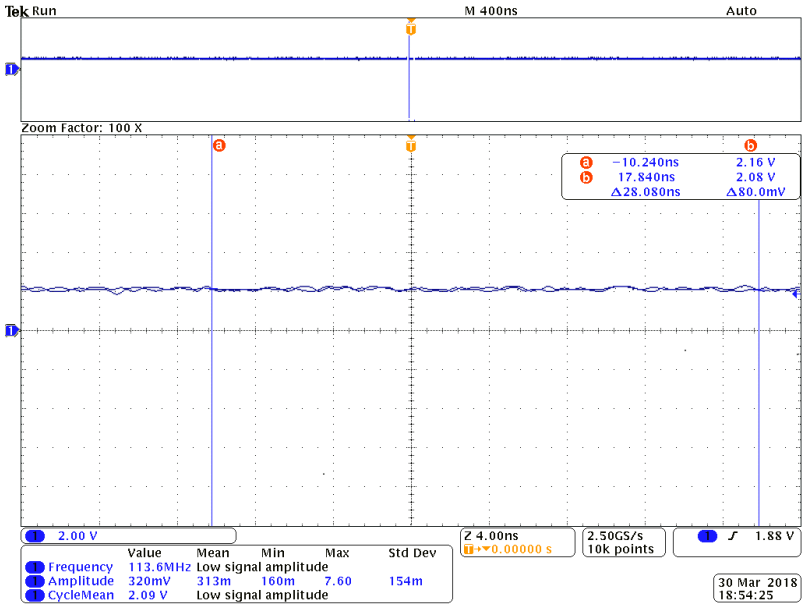


Figure 3-6 Oscilloscope image showing the DC voltage present at the interconnecting cable, while transmitting logic level 1

Figure 3-7 shows the signal present in the interconnecting cable, which was carrying the logic level 1, transmitted from a microcontroller. Since a sinusoidal signal with 4 V_{p-p} amplitude was coupled on to the victim circuit, the GPIO pin of the receiving microcontroller experiences a drop in average DC levels down to 317 mV, as shown by the measurement parameter 'CycleMean' at the bottom left corner of the oscilloscope image.

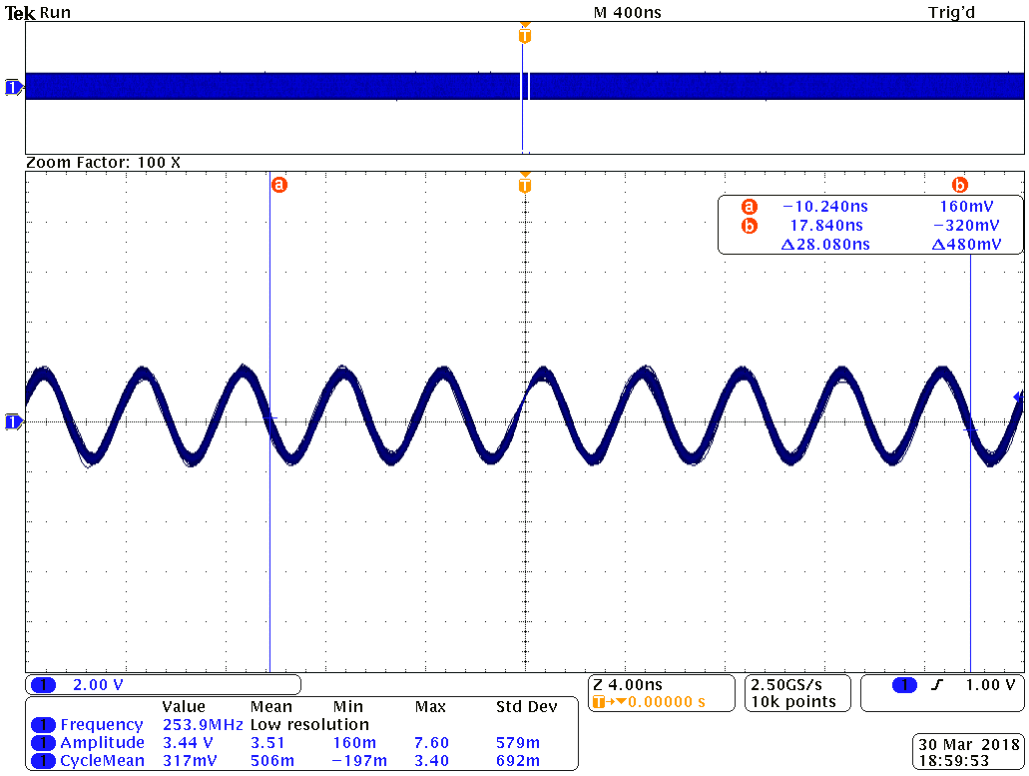


Figure 3-7 Oscilloscope image showing a drop in the DC average voltage from 2.1 V, while transmitting a sinusoidal attack signal

Due to this drop in DC levels, it was observed that a maximum of 64.7% misreads were achieved at the receiving microcontroller. This drop in the DC level agreed with the rectification effect observed during the IEMI attack on analog sensors, as described in chapter 2. The reason for not achieving 100% misread was due to the voltage peaks present in the sinusoidal signal, which were just above 2 V, that would be registered as digital logic

1, at the receiving microcontroller. The results shown by Figure 3-7 proves that, IEMI attack can induce a drop in DC levels, thus enabling a bit flip from logic level 1 to 0-bit.

For the next experiment, the author tried to use the same attack technique of transmitting continuous sinusoidal signal, to induce a positive DC level change, while the transmitting microcontroller sends a digital logic level 0.

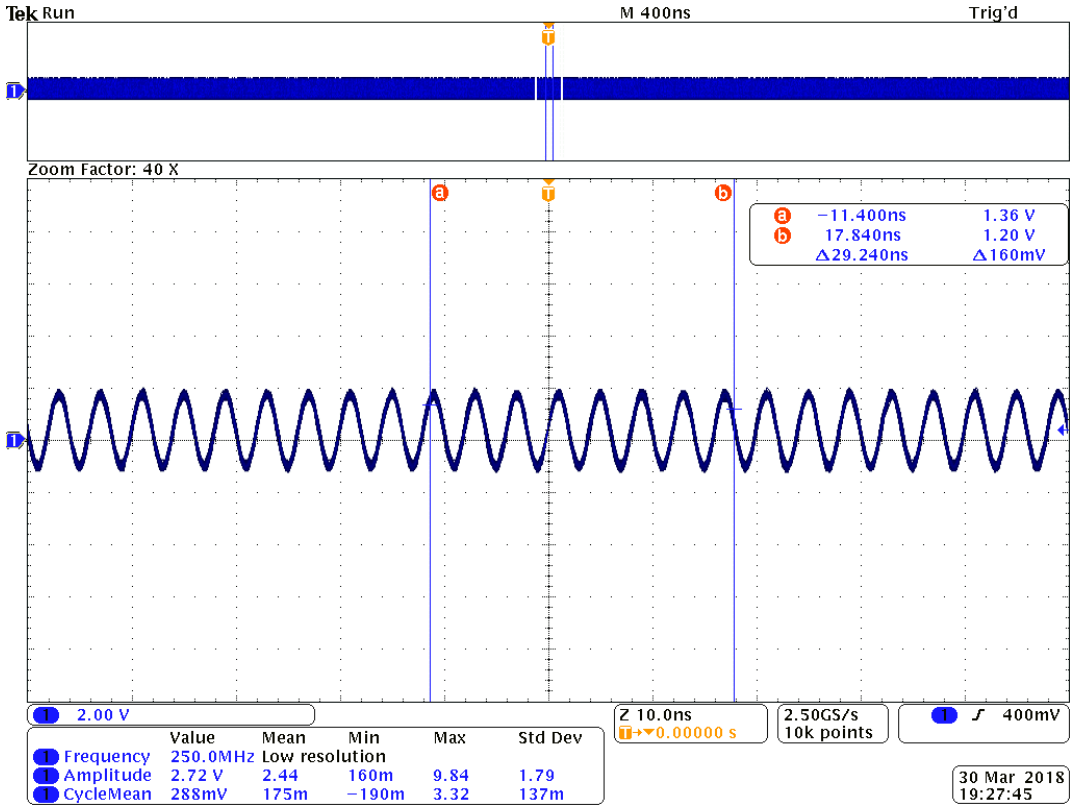


Figure 3-8 Oscilloscope image showing the signal present in the interconnecting cable, while the transmitting microcontroller sends a logic level 0

Figure 3-8 shows the signal present at the input of the GPIO pin, when the transmitting microcontroller sends a logic level 0. This figure shows that a positive DC offset of 288 mV was achieved at the input of GPIO pin, as shown by the measurement parameter 'CycleMean', at the bottom left corner of the figure. Although the sinusoidal signal

amplitude of 2.72 V was induced onto the victim circuit, only 288 mV DC offset was achieved. This DC offset resulted in a slight improvement in the misread percentage, yielding 40.3% misreads at the receiving microcontroller.

This was contradicting the results obtained from analog sensor attack, which suggested that, it was possible to achieve 1.2 V positive DC offset, when the analog sensor was not outputting any DC current, under no IR radiation condition. The reason for the reduction in the DC offset was due to the logic level 0, which was being transmitted by the microcontroller. Unlike the no IR radiation condition, described in chapter 2, which provided a capacitive load to the input terminal of microcontroller, the transmitting microcontroller provides a low resistance path to ground, while transmitting logic level 0. This low resistance path to ground would have drained most of the DC current generated from the rectification process, provided by the ESD diodes, thus resulting in a decrease in the total DC offset achieved from this attack.

These results still prove the hypothesis that, it would be possible to achieve a positive DC offset with a continuous sinusoidal attack signal, albeit with slightly higher power levels.

3.3 IEMI attack using continuous sawtooth waveform

By using continuous sinusoidal signal, the attacker attempt to inject false data into digital sensors did not prove successful in creating 100% misreads. Without achieving 100% misread, this attack method cannot be claimed as being deterministically injecting false data. But, by using continuous sawtooth waveform transmitted as an attack signal, it would be possible to induce a net positive/negative DC average, over a period of time. The theory behind the use of sawtooth waveform has been discussed in detail in the section 4.1.3 in page 77. In this section, equation (4-5) states that the voltage induced at the victim circuit will be

directly proportional to the negative derivative of the time varying current that flows through the transmitting antenna. Thus, the author hypothesizes that, by using a sawtooth waveform signal with fast changing falling edge, as the attack signal, the coupled signal at the victim circuit would have a positive DC offset. According to equation (4-5), the derivative of sawtooth signal, with fast falling edge, would be a constant positive DC, which occurs during the slow rising edge, and a negative DC offset, with larger amplitude, for a shorter duration, which occurs during the fast falling edge. Hence, the author hypothesizes that, the frequency characteristics of the victim circuit would result in an imbalance between the DC offsets induced during the slow rising edge and fast falling edge, thus resulting in a net positive or negative DC offset.

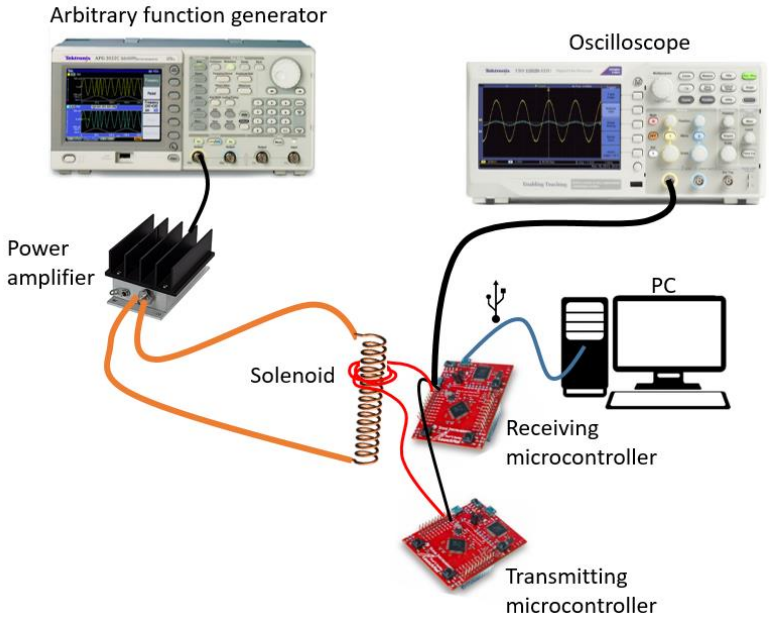


Figure 3-9 Experimental setup for injecting false data using sawtooth waveform

Figure 3-9 shows the experimental setup used for injecting false data into digital sensors using sawtooth waveform. The main difference from the setup shown by Figure 3-5 and Figure 3-9 happens to be the use of solenoid as the transmitting antenna. This may seem

counterintuitive, since sawtooth waveform is a wideband signal and usually solenoids are preferred for use with narrow band signals. But, since the arbitrary function generator AFG3021B, from Tektronix, available in the lab where the experiment was conducted, can only generate up to 12.5 MHz, the Vivaldi antenna used in the previous experiments would not be suitable to transmit, this low frequency signal. Hence, the author decided to use a solenoid instead of designing an antenna, which could transmit a sawtooth waveform with couple of MHz frequency, since the dimensions of the antenna would be very large.

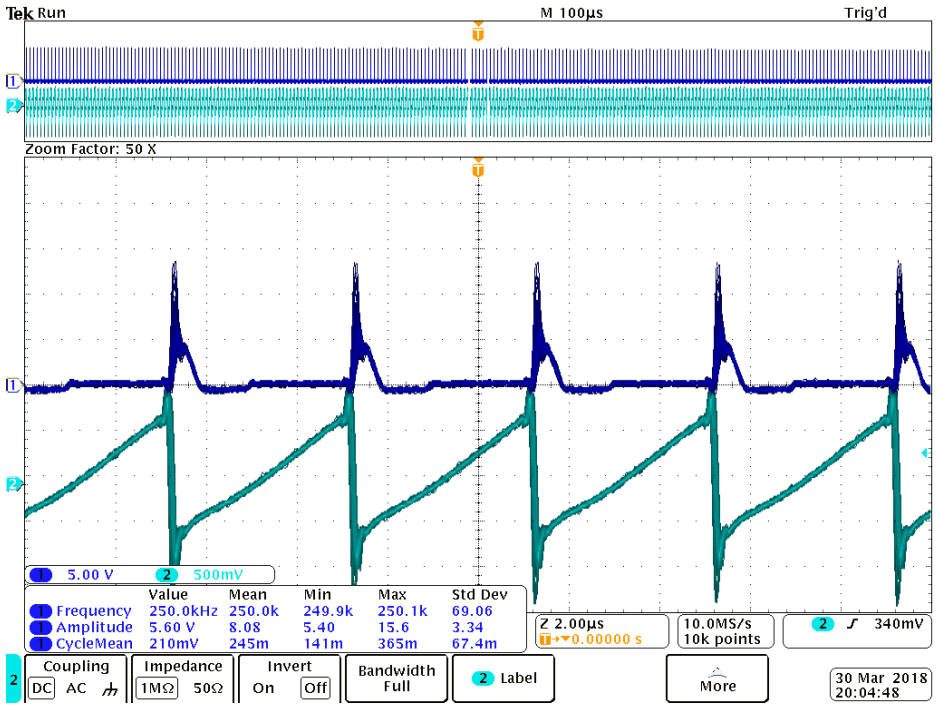


Figure 3-10 Oscilloscope image showing sawtooth attack signal and the induced signal at the victim circuit's GPIO pin

3.3.1 Experimental results and discussion

Figure 3-10 shows the 1.7 MHz sawtooth waveform, transmitted from the arbitrary function generator, while the induced signal at the victim circuit, shown by dark blue graph, demonstrates the induction of a positive DC offset at the instances when the falling edge of

sawtooth waveform occurs. As indicated by the ‘CycleMean’ parameter, the net DC offset was 210 mV, even though the induced positive DC offset had a large magnitude of 13 V.

Although, intuitively one would think about increasing the frequency of the sawtooth signal, to create more frequent positive DC offset induction, but the results from Figure 3-11, which was obtained by transmitting sawtooth waveform with 2 MHz frequency, suggests otherwise. This figure shows that the induced signal at the GPIO input pin, has oscillations along with a positive DC offset. These oscillations could have occurred due to the frequency characteristics of the solenoid, used to transmit this signal, which results in a decrease in the net positive DC offset. In Figure 3-11, value shown by the parameter ‘CycleMean’ was incorrect. This is because, at the time of performing this experiment, the oscilloscope used to capture this image could not trigger the induced signal properly, thus resulting in constant change of values shown by ‘CycleMean’ parameter.

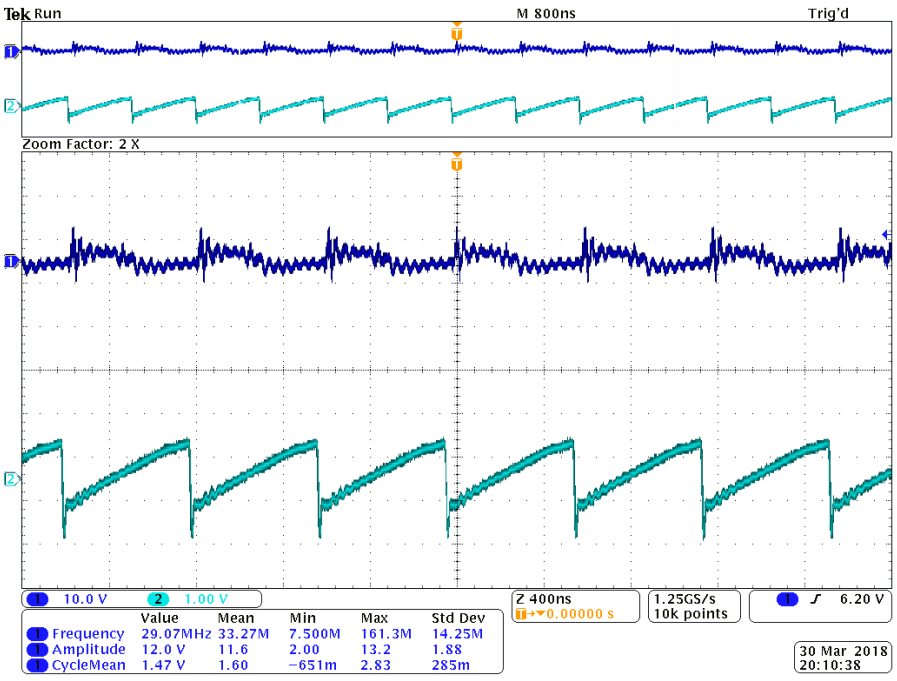


Figure 3-11 Oscilloscope image showing high frequency sawtooth attack signal and the resultant induced signal at the victim circuit

To demonstrate that this attack technique could still improve the percentage of misreads, compared to the sinusoidal signal attack, the total number of misreads where calculated at the receiving microcontroller, while the transmitting microcontroller sends a digital logic 0. It was observed that the percentage of misreads improved to 47%, which was higher than the 40.3% misread achieved using continuous sinusoidal signal attack. Thus, these results prove the author's hypothesis about the sawtooth signal inducing a net positive or negative DC offset. But, the amplitude of induced positive or negative DC offset was far too low, while considering the amplitude of the induced positive or negative signal peaks.

Figure 3-10 shows that the induced positive DC offset has an amplitude of ~4 V, for a duration of about ~800 ns. By positioning this positive DC offset precisely at the sampling window of the receiving microcontroller, an IEMI attacker could deterministically flip a digital logic '0', transmitted towards a GPIO input terminal, into a digital logic '1'. Similar technique could be used by transmitting a sawtooth waveform with fast rising edge and slow falling edge, to flip a '1' bit to '0', deterministically.

The caveat in this attack exist in the need for synchronization of a attack signal with the sampling clock of the receiving microcontroller. This is because, the induced positive DC offset can only exist for a short duration of time and to make a deterministic change in bits, the attack sawtooth signal's falling edge should occur right around the sampling window of the receiving microcontroller. Since, digital circuits are usually noisy, due to radiation of EM energy during rising and falling transitions in its signals, it is a trivial task to build a circuit which can detect these rising/falling edges and use this data to synchronize the attacker's signal.

However, this attack technique shows that the sawtooth waveform is a prime candidate for injecting false data into digital sensors, due to its ability to deterministically induce a bit flip, once the attack signal is synchronized with the sampling clock of the receiving microcontroller.

3.4 Conclusion

The attack techniques described in this chapter proves that an IEMI attack signal can induce false data into digital sensors. With continuous sinusoidal signal attack, although the expected shift in DC levels were far less prominent, in comparison to the analog sensor case, still the successful attack proves the vulnerability present in embedded systems. Also, the proposed attack using sawtooth waveform, shows its potential in deterministically inducing false data, but requires synchronization with the sampling clock of the victim circuit.

CHAPTER 4

FALSE DATA INJECTION FOR ACTUATORS

Actuators are mechanical elements which are responsible for motion in a system. Any component in a machine which causes a rotation or movement can be considered as an actuator. In automobiles, actuators are responsible for moving the dials in the instrument cluster, which shows the vehicle speed, engine rotations per minute (rpm), fuel level and engine coolant temperature. They are also responsible for automatic windows, doors, side mirrors and many more. In robotics, the actuators play a predominant role in making a robot move in different direction using wheels, rotate its head, eyes, hands and legs, for a humanoid, as well as making facial expressions, such as moving the position of the mouth or eyebrows, etc.

Just as the sensors being an integral part of an embedded system, enabling the system to evaluate its environment, the actuators play an important part in these systems, by enabling them to make a physical change in that environment. There are countless number of embedded systems with actuators, that we take for granted in our day to day lives. One such system is the automatic doors at the entrance of most businesses, airports, hospitals, etc. Automatic door systems using a sensor to sense an approaching human towards the door, using a pressure sensor located on the floor, IR sensor or ultrasonic sensor located on the top of the door. This sensor data will be sent to an embedded system, which hunts for particular level of change in the data and matches it with certain preset parameters, to determine the approach of a human. Once the embedded system determines that a human is approaching the door, it sends out electrical signals to actuators, which then perform the mechanical action of opening the door. Using similar measurements from the sensor, the embedded

system detects that movement of a human away from the door and activates the actuator mechanism to close the door.

Even though we experience these innovations in our day to day life, they are hardly given any importance. Many such actuators are responsible for critical components in many of our machines which are responsible for keeping us alive. For example, the proper operation of the power steering system in a car or the landing gear mechanism of an aircraft are extremely important to keep the occupants safe. This problem is further exacerbated by the computerization of virtually every machine in our lives. Primary example for this would be drive-by-wire or brake-by-wire systems in modern vehicles. Auto manufacturers tend to support the computerization of systems in a vehicle, since they are extremely efficient compared to a mechanical system, while offering several comfort features, such as changing the throttle response or braking intensity, as with the drive-by-wire and brake-by-wire systems, respectively.

Despite the amount of trust, we place in these electro-mechanical systems, there is hardly any research conducted to expose the possible security vulnerabilities of these actuators. In recent times, the 2010 Stuxnet attack on Iran's nuclear enrichment plant has made it clear, that the kind of damage a vulnerability in embedded system could cause [45]. Stuxnet was a malicious computer worm, which subverted the control systems responsible for the centrifuge systems in the nuclear enrichment facility. This attack let to the destruction of the centrifuge system by manipulating the control signals, so that the centrifuge spins at speeds beyond the safe operating range of the machine [45].

Since the Stuxnet attack was performed by traditional computer hacking techniques, in which hackers took advantage of the security vulnerabilities in the computers used in the

nuclear facility, the future attack using these vulnerabilities could be prevented with appropriate software patches, for the attacked computer systems. But, the vulnerabilities existing in the current generation of actuators, which could be exploited using IEMI techniques, require complete redesign of the actuators to prevent against this attack technique.

Like the IEMI attacks described in the previous chapters, this attack against the actuators aims at injecting false data into the control signals used to drive these systems. Most digital actuators, such as servo motors, uses Pulse-Width-Modulation (PWM) signals to move/ turn the actuators to a desired position. PWM signals consist of series of pulses with a specific pulse width, which dictates the actuator to reposition itself depending on the pulse width of a control signal. Digital servos are most commonly found in Unmanned Ariel Vehicles (UAV), robots and quadcopters. Since the existing security measures against malicious attacks involves encrypting the data in the embedded systems, these actuator control signals are highly susceptible to attacks from IEMI technique. Using this attack, an attacker can remotely control the servo motor's operation, without the control system's knowledge.

Before exploring the vulnerability in the actuator control signals, one must understand the mechanisms with which an actuator such as a digital servo interprets the incoming control signal and the control mechanism behind the armature positioning system.

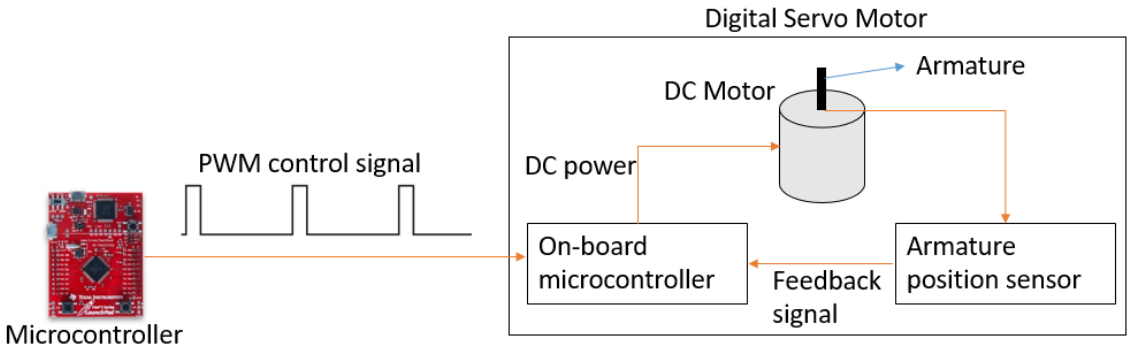


Figure 4-1 Block diagram of servo motor and control circuit

Figure 4-1 shows a block diagram of a digital servo motor and its control circuit. The PWM control signal generated by a microcontroller is received by an on-board microcontroller circuit, which determines the pulse width of the periodic pulses, by detecting the time difference between rising and falling edges. Based on the determined pulse width of the PWM signal, the microcontroller sends out DC power to rotate the armature position. The armature position is sensed by a sensor and generates a voltage signal, which would be sent back as a feedback signal to the microcontroller. This armature position sensor could be made with a simple potentiometer, which rotates in conjunction with the armature, thus providing different resistances based on the rotation angle of the armature. This varying resistance can be converted into a varying voltage signal, by sending a constant current through the potentiometer. The feedback signal from the armature position sensor would be analyzed by the microcontroller to determine whether the armature has rotated to a desired position. If the armature has reached a desired position, the microcontroller cuts the DC power, thus maintaining the desired angle of rotation, until a change in the pulse width of the PWM signal was detected. Figure 4-2 shows an example of different pulse widths and the corresponding angle of rotation of the servo motor's armature. In this figure, every 0.5 ms

change in the pulse width of the PWM signal, corresponds to 90^0 rotation of the armature angle.

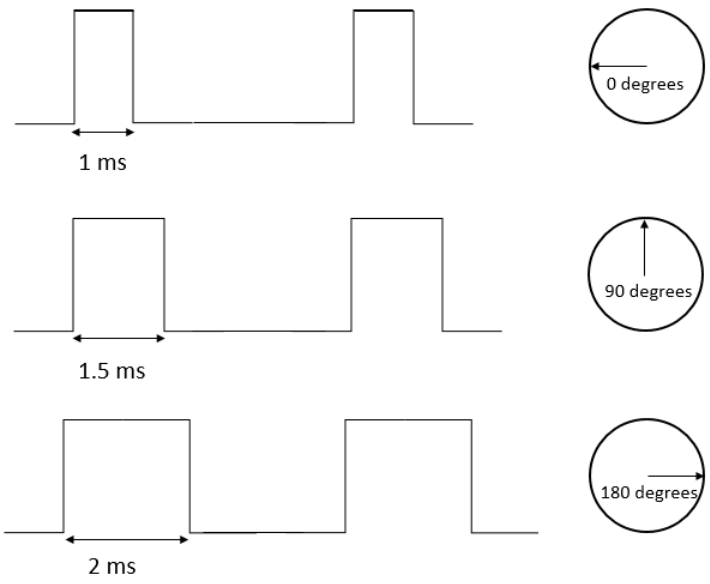


Figure 4-2 PWM control signals and the corresponding degree of rotation of the actuator's armature

4.1 Mechanism of attack for actuator

The difference in the IEMI attack for analog sensors versus the actuators, is that the actuator attacker needs to transmit EM signal in-phase with the PWM signal generated from an embedded system. This is important, if the attacker wants to rotate the actuator's armature to a desired angle. Unlike the analog sensor IEMI attack, the induction of DC signal at the victim circuit must happen around the existing pulses in the PWM signal, to change the pulse width of the periodic signal. Also, the attack to change in pulse width should be performed on the all the pulses in the periodic PWM signal, to maintain the rotation of actuator angle at a desired position.

Since the PWM control signal usually has sharp rising/falling edges in its waveform, these signals tend to contain several harmonics of the fundamental frequency. Therefore, it would be easy to detect the rising/falling edges in the PWM control signal, due to the tendency of high frequency components in the control signal to be radiated [46]. An attacker should be able to design an antenna which can pick up these high frequency components radiated from the PWM signal path and use the information to detect the rising/falling edges. Since, this task is trivial, this chapter instead will focus on the improving the effectiveness of IEMI attack on actuators, by exploring suitable waveforms and design for attacker circuit. All the IEMI attacks described in this chapter were performed under the near-field distance of the transmitting antenna.

The author chose to use a digital servo motor S3152 from Futaba, to serve as the actuator under attack [47]. This servo motor is most suitable for small toys as well as quadcopters, due to its light weight design (41 g) and compact package with dimensions of 40 x 20 x 38mm.

This digital servo motor responds to PWM signals with pulse widths ranging from 0.8 ms to 2.1 ms, with a maximum of 50 ms time period, which corresponds to 0^0 to 180^0 angle of armature rotation. Experimentally it was found that, while operating the servo motor with 5 V DC supply, the lowest amplitude of PWM signal which successfully controls the armature's rotation was 1 V. Since it would be easier to inject false data into the PWM signal having lower amplitude, using a low power IEMI attack, the author has used PWM signals with 1 V amplitude to demonstrate all the attacks on the servo motor.

4.2 Continuous sinusoidal attack

Since the servo motor has an on-board microcontroller, the first attempt to induce required amount of DC voltage was attempted by using continuous sinusoidal signal. The author hypothesizes that, the on-board microcontroller would have non-linearity, with AC to DC conversion efficiency high enough to produce significant DC offset, and to change the logic levels of the PWM signal. Figure 4-3 shows the experimental setup for the IEMI attack on actuators with continuous sinusoidal signal. This experiment hopes to determine the effects of continuous AC signal coupling to the victim circuit. The transmitting Vivaldi antenna was replaced by a solenoid, since the Vivaldi antenna does not perform well under low frequencies (< 200 MHz), which can be seen from the Figure 2-9.

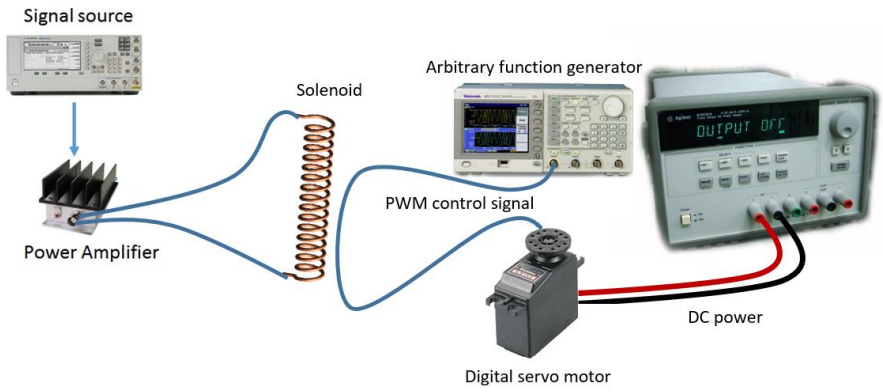


Figure 4-3 Experimental setup for continuous sinusoidal signal attack

The PWM control signal was generated using an Arbitrary Function Generator AFG3021B from Tektronix. Although the PWM control signal for the servo motor could be generated using a microcontroller, using an arbitrary function generator provides the freedom to change the pulse amplitude as well as the pulse width, without having to change the program inside the microcontroller. The PWM signal path was intercepted and connected to an oscilloscope, to identify the effect of coupling an AC signal to the actuator.

4.2.1 Experimental results and discussion

The frequency of the sinusoidal signal transmitted from the attacker was swept to find the frequencies at which maximum power transfer takes place, which would be close to the resonant frequency of the attacker circuit as well as the victim circuit. The results from this experiment showed that, there was no DC voltage generated because of the coupled AC signal. This could be due to the use of different kind of ESD diodes inside the onboard microcontroller, which resulted in negligible amount of rectification of the coupled AC signal. But, while transmitting sinusoidal signals from 7 MHz to 13 MHz, the servo motor stopped responding to PWM control signal and behaved as it was powered off.

The reason for this unresponsive was due to the superposition of the PWM signal and the sinusoidal attack signal, which resulted in a waveform shown in Figure 4-3. This figure was taken from an oscilloscope, which seems to show three different waveforms. However, the oscilloscope image is showing data from two channels, connected to the PWM signal path and the continuous sinusoidal attack signal path (dark blue waveform). Since the oscilloscope tries to continuously sample the incoming signal and display the results, the PWM signal with ON (1 V) and OFF (0 V) regions are merged together and displayed on the same region of screen.

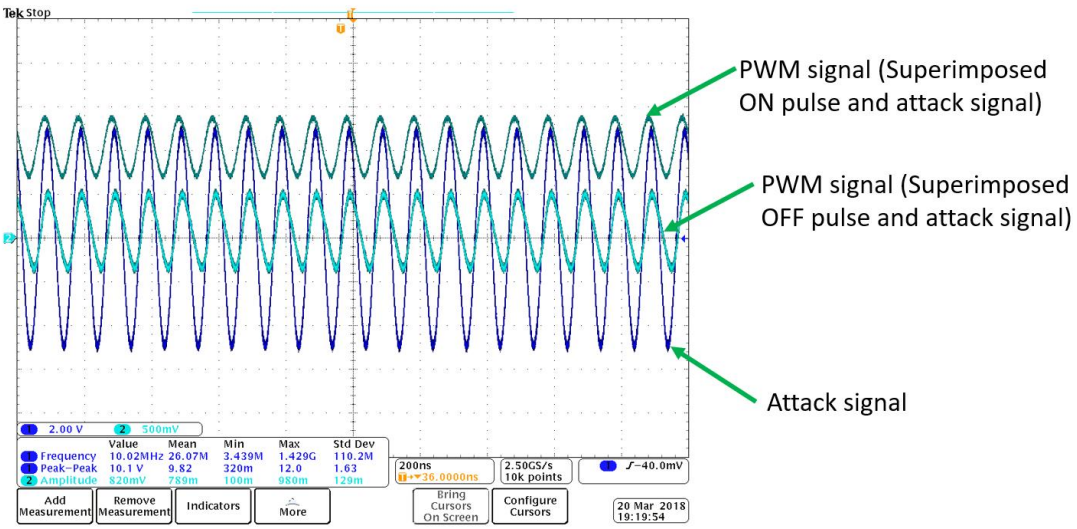


Figure 4-4 Oscilloscope screenshot showing continuous sinusoidal attack signal and PWM signal

Figure 4-4 shows the PWM signal superimposed with the coupled attack signal, which results in the ON pulse of the PWM signal consisting of regions with highest voltage of 1.25 V and lowest voltage of 750 mV. These 750 mV regions in the ON pulse of the PWM signal, was read as digital zeros, while the signal regions above 750 mV would be considered as digital ones, by the onboard microcontroller. But, when the microcontroller looks for rising edges in the PWM signal, which represents the presence of periodic pulses in the signal, received PWM signal would appear to be devoid of any rising edges, which results in the digital servo motor assuming that the PWM control signal consist of all zeros. This unresponsive state of the servo motor vanished, when the amplitude of the PWM control signal was increased by 10 mV above the minimum required 1 V PWM amplitude, upon which the servo motor responds to PWM control signal, as expected.

The attack signal frequencies from 7 MHz to 13 MHz, in which the digital servo motor switches to unresponsive state, must be related to the frequencies at which the

amplitude of the coupled sinusoidal signal is larger than 500 mVp-p. These frequencies must be close to the resonant frequency of the solenoid or the victim circuit.

Although this attack was successful and could push a digital servo motor into an unresponsive state by injecting false data into the PWM control signal, this result was not enough to satisfy the initial goals set to arbitrarily control an actuator. Also, these results disprove the hypothesis of the author, because of the insignificant amount of the DC offset induced by the non-linearities resent at the input terminal of on-board microcontroller.

4.3 Pulsed sinusoidal attack

Equipped with the knowledge gained from previous experiment, the author hypothesizes that, transmitting a pulsed sinusoidal signal positioned before the falling edge of the PWM pulses, would result in a net increase in the pulse width of the PWM pulses. This is because, after receiving the rising edge of the ON pulse, the on-board microcontroller would be unable to detect an OFF region of the PWM signal, due to the presence of coupled sinusoidal signal.

The experimental setup for the attack attempting to increase the PWM pulse width is shown in Figure 4-5. Attacker circuit shown in Figure 4-5 is similar to the circuit in chapter 2, but with certain differences. One important change in the attacker circuit for the actuator case comes from the use of RF switch. This RF switch component named as ZASWA-2-50DR+, was a high isolation Single-Pole-Double-Throw (SPDT) switch from Minicircuits, which can switch its output from fully ON to fully OFF stages, while maintaining 50Ω output impedance. The arbitrary function generator (AFG3021B from Tektronix) shown in Figure 4-5, generates pulses, which acts as the control signal for the RF switch. Although not shown explicitly in Figure 4-5, there was a clock synchronization connection between the two arbitrary function generators, which generates the control signal for the RF switch on the

attacker side and the PWM signal at the victim side. The pulse width of the signal generated from the attacker's arbitrary function generator was set to 400 μs, with a pulse period of 50 ms, which was the same as the PWM signal's period, generated from the victim's arbitrary function generator. The pulse width of the PWM signal generated at the victim circuit was set to 1 ms. The pulsed sinusoidal signal was fed to the Vivaldi antenna, to radiate the attack signal towards the victim actuator circuit.

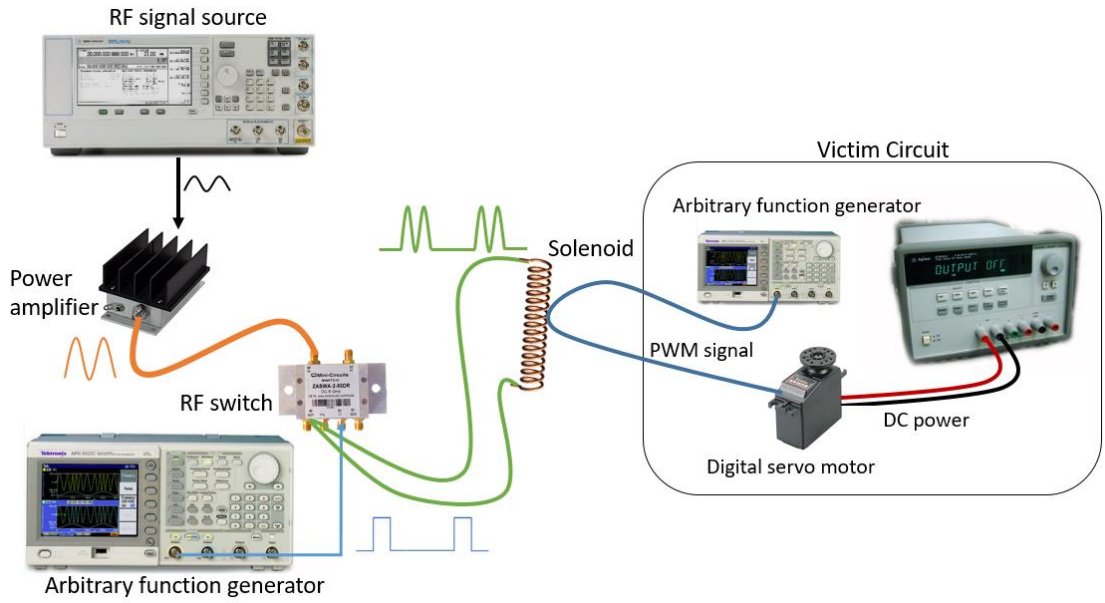


Figure 4-5 Pulsed sinusoidal attack on actuator

The frequency of the transmitted sinusoidal signal set to 10 MHz, since it was found from the previous experiment that signals transmitted from 7 MHz to 13 MHz were having maximum power transfer between the attacker and the victim circuits.

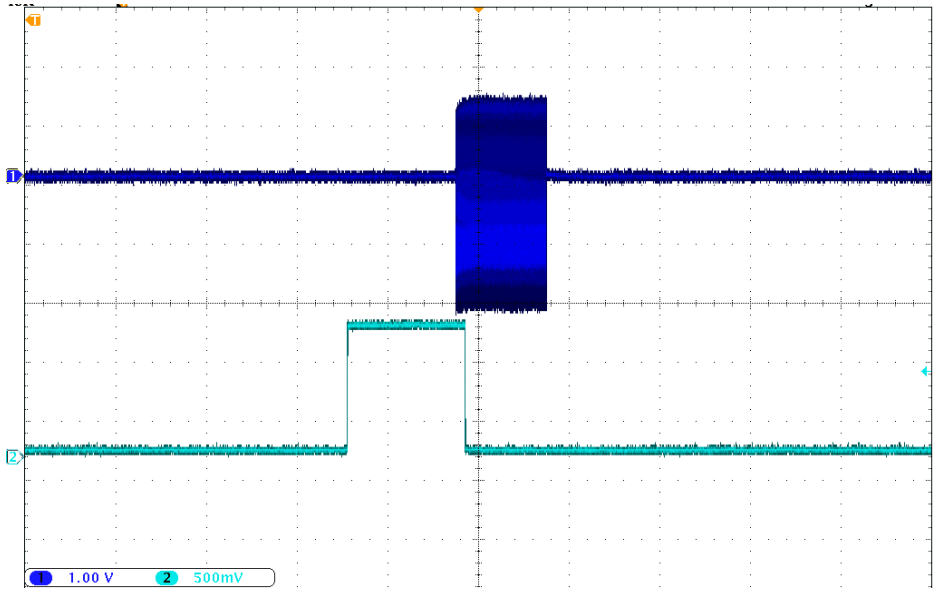


Figure 4-6 Oscilloscope measurement of the pulsed sinusoidal signal from the attacker and the coupled signal at the victim's PWM signal path

4.3.1 Experimental results and discussion

Figure 4-6 shows the pulsed sinusoidal signal generated using a 10 MHz sinusoidal signal that is synchronized with the PWM signal, so that when this attack signal couples onto the victim circuit, the induced signal would disrupt the pulse width of the PWM control signal.

Figure 4-7 shows the coupled pulsed sinusoidal signal getting superimposed with the PWM control signal, precisely at the end of the ON pulses. The figure does not show clearly the presence of pulsed sinusoidal signal, since it is difficult for the oscilloscope's trigger to lock on to the phase of the pulses as well as the sinusoidal signal. Hence the regions of the PWM signal which has the coupled sinusoidal signal, appears as a distortion in the DC voltage levels, although it is far from the truth.

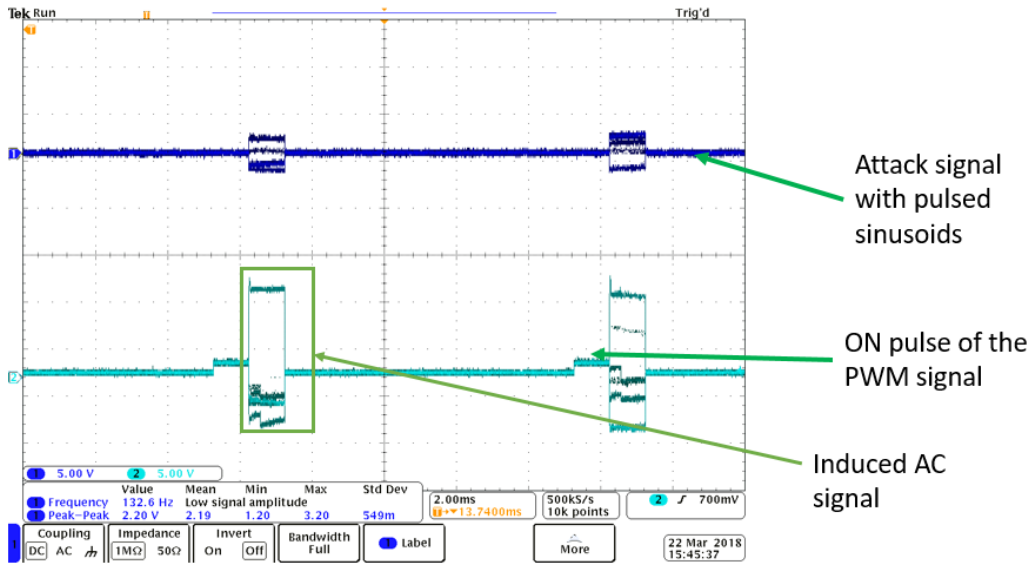


Figure 4-7 Oscilloscope screenshot showing the pulsed sinusoidal attack signal superimposed on the PWM control signal

Figure 4-7 shows the PWM signal with pulse width of ~1 ms, while the attack signal consisting of sinusoidal pulses exists for ~1 ms. It was observed during the experiment that the servo motor's armature precisely rotates to an angle corresponding to ~2 ms, despite the original PWM signal having pulse width of 1 ms. The rotation angle of the servo motor's armature, returns to the position corresponding to 1 ms, when the attack signal was switched off.

This result seemingly proves the author's hypothesis, by suggesting that, the onboard microcontroller tries to look for a falling edge after the original PWM signal's ON pulse, but fails to find this, due to the presence of sinusoidal signal. The OFF region of the PWM pulse would be detected when the pulsed sinusoidal signal disappears. But, if this hypothesis was completely accurate, then by positioning the sinusoidal pulses before the rising edge of the PWM ON pulses, the net pulse width should decrease. However, such an experiment resulted

in the servo motor's armature rotating to a new angle, corresponding to the increase in pulse width, resulted due to the superposition of PWM ON pulses and pulsed sinusoidal attack signal. This suggests that the author's hypothesis that the on-board microcontroller not being able to detect the rising or falling edge of the PWM signal might not be accurate. Despite the disproval of this hypothesis, the experimental results suggest that pulsed sinusoidal signal could be used to increase the pulse width of PWM signal.

4.4 Saw tooth waveform attack

As mentioned earlier, the best approach to arbitrarily control an actuator is by injecting false data around the ON pulses of the PWM signal, in a synchronized way, thereby changing its pulse width. In the previous experiment, this change in the pulse width was caused by inducing pulsed sinusoidal signal. This effect could also be caused at the victim circuit by transmitting waveforms that would induce a sharp change in the voltage at the victim's circuit.

It was experimentally determined that the Futaba S3152 digital servo detects any rising/falling edge every 800 us, which corresponds to the minimum acceptable pulse width of the PWM signal. Hence, any sudden drop in the DC level, during an ON pulse, would result in the onboard microcontroller assuming that the pulse width of the PWM signal has decreased.

The author hypothesizes that, transmitting saw tooth waveform with fast rising edge, it could induce a drop in DC level, for a short duration in the PWM signal, thereby reducing the pulse width. Like the previous experiment, this attack technique also requires synchronization of the PWM signal and the attack signal. Before the details of the attacking circuit can be discussed, it is important to understand the mechanism behind the sawtooth

waveform's ability to induce DC level shift for a short duration of time at the victim's PWM signal.

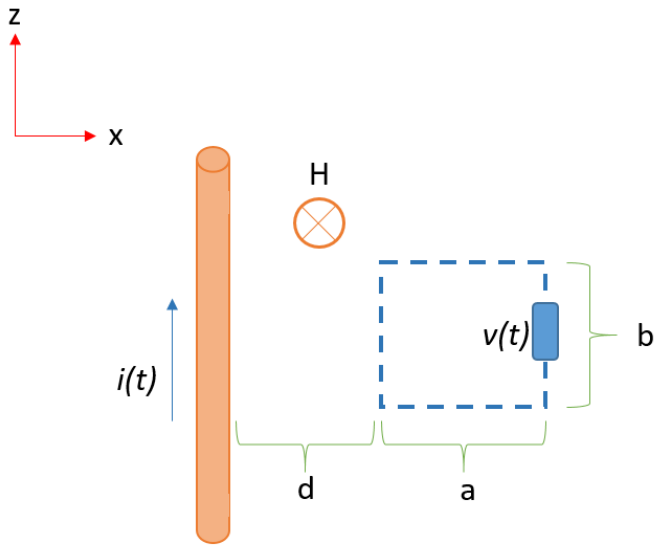


Figure 4-8 EM coupling model demonstrating Faraday's law

Figure 4-8 shows the EM coupling model in which a time varying current *i(t)* flows through an infinitely long conductor, represented by the cylinder, in +z direction. The H-field generated due to this current flow exists in a perpendicular direction to the x-z plane, which is represented by the letter 'H' above a circle with a cross. At a distance 'd', which is under the near-field conditions, there exists a conducting loop with dimensions a x b. This EM coupling model would be used to estimate the time varying voltage *'v(t)'* induced at the conducting loop, which represents the victim circuit, due to the current *'i(t)'*, which represents the current flow in the attacker circuit.

The magnitude of the H-field generated from the conductor carrying *'i(t)'* can be found using the following equation:

$$H = \hat{y}\frac{i(t)}{2\pi x} \tag{4-1}$$

Using Faraday's law, the voltage induced at the conducting loop, due to the time varying H-field can be calculated as,

$$v(t) = \oint E.dl = -\frac{d}{dt}\iint B.ds = -\frac{d}{dt}\iint \mu H.ds \tag{4-2}$$

where,

$$dS = \hat{y}\, dx\, dz \tag{4-3}$$

The variable μ in equation (4-2) represents permeability.

Thus, the induced voltage v(t) can be estimated as,

$$v(t) = -\frac{di(t)}{dt}\int_{d}^{d+a}\frac{\mu}{2\pi x}dx\int_{0}^{b}dz \tag{4-4}$$

$$v(t) = -\frac{di(t)}{dt}\left[\frac{\mu}{2\pi}b\, ln\left(\frac{d+a}{d}\right)\right] \tag{4-5}$$

Equation (4-5) shows that the relationship between the current flow in the attacker's transmitter and the voltage induced at the victim circuit has a time derivative relation. Figure 4-9 shows the relation between the current at the transmitting cylinder and the voltage induced at the conducting loop, which is present at a distance of 1 cm, using the equation (4-5). For the purpose of this calculation it was assumed that the cylinder and the conducting loop are present in vacuum and the conducting loop has a dimension of 1 cm x 1 cm.

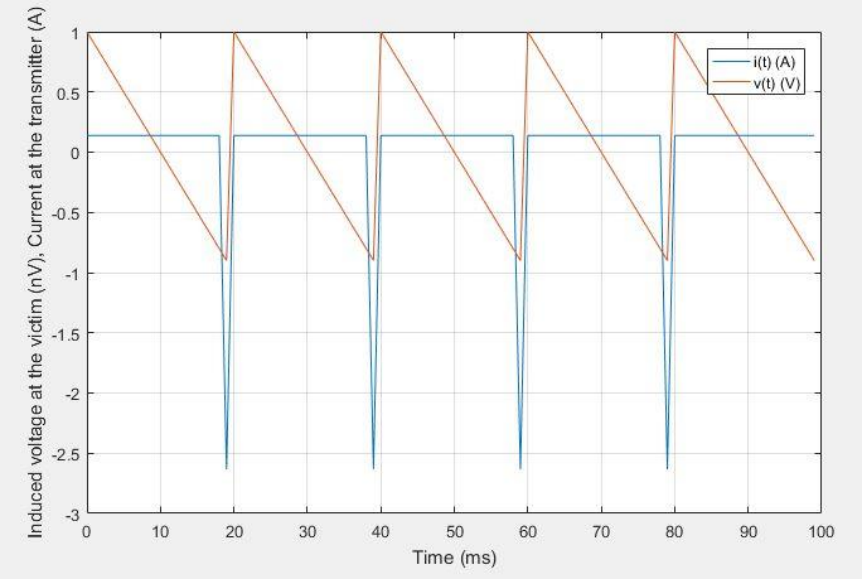


Figure 4-9 MATLAB plot comparing the current at the transmitter with the voltage induced at the victim circuit

Figure 4-9 shows that for a duration less than ~1 ms, the time varying current in the cylinder induces a voltage drop at the conducting loop. The magnitude of the induced voltage at the conducting loop is in the order of nV, since the H-field emitted from the transmitting cylinder is only partially coupled with the conducting loop and also, the loop's dimension is directly proportional to the magnitude of the voltage induced.

As seen by Figure 4-9, if the voltage drop was induced in-between the ON pulses of the PWM control signal at the victim circuit, then the onboard microcontroller inside the servo would consider these voltage drops as falling edge and assumes that the pulse width of the PWM signal has been reduced. Thus, the sawtooth waveform transmitted by the attacker needs to have a frequency and phase same as that of the PWM signal.

4.4.1 Transmitter circuit design

This section has used materials that were published in the paper "Transcranial Magnetic Stimulation: Design of a stimulator and a focused coil for the application of small animals", by J. Selvaraj et. al, with the permission of all the authors [48].

Unlike transmitting a narrow band sinusoidal signal, the sawtooth waveform occupies a wider bandwidth, due to the sharp changes in its waveform. Vivaldi antenna is an excellent candidate to transmit a wideband waveform, as discussed in the page 21, but the required frequency of sawtooth waveform would be too low ($20\ Hz = \frac{1}{50\ ms}$). This is because, the dimension of the antenna is related to the longest wavelength of the signal which needs to be transmitted and the wavelength of the 20 Hz signal would be 15000 km, which would be unreasonably huge for an antenna. Hence, the author decided to use solenoids to couple the wideband attack signal to the victim circuit.

Even though the solenoid does not have a wideband bandwidth characteristic, the frequency components of a 20 Hz sawtooth signal should not be high enough to cause any impedance mismatch, due to its long wavelengths.

The next challenge in using this attack technique involves transmitting a large amount of power from the attacker. This large power requirement can be understood from equation (4-5), which states that the amplitude of the voltage induced at the victim circuit would be directly proportional to the victim circuit's dimension and the current through the transmitter. With the assumptions made for making the MATLAB plot shown in Figure 4-9, the amplitude of the current needs to be ~166 MA to achieve a 500 mV drop in voltage at the victim circuit. This unreasonably large current requirement can be reduced by using a

solenoid which generates a much stronger H-field for a given current as compared against an infinitely long conductor.

$$B = \mu \frac{N}{L} I \tag{4-6}$$

Equation (4-6) states the magnetic field intensity generate by a solenoid, which has its length 'L' much larger than the diameter of the coils. In this equation, 'N' represents the number of turns in the solenoid, while 'I' represents the time varying current flowing through the it. Thus, by increasing the permeability μ, number of turns 'N' or by decreasing the length 'L', the magnitude of current required to induce the necessary voltage drop can be reduced.

Thus, by using a material with its relative permeability value as 1000 and by using a solenoid with $\frac{N}{L}$ value in the order of 1000, the magnitude of current required to induce a ~500 mV DC offset at the victim circuit can be reduced by an order of 10^6. Along with all these techniques to reduce the required transmitted power, the distance between the transmitting solenoid and the victim circuit can be reduced to help with the reduction in required current magnitude. However, it is important not to increase the inductance of the solenoid to the order of several milli Henry, which would significantly reduce the bandwidth of the solenoid, thereby increasing the rise or fall times of a sawtooth waveform, even though the frequency of the waveform is 20 Hz.

The author decided to design a circuit which can generate a sawtooth waveform current with 1000 A magnitude and drive it into a solenoid with a high permeability core material.

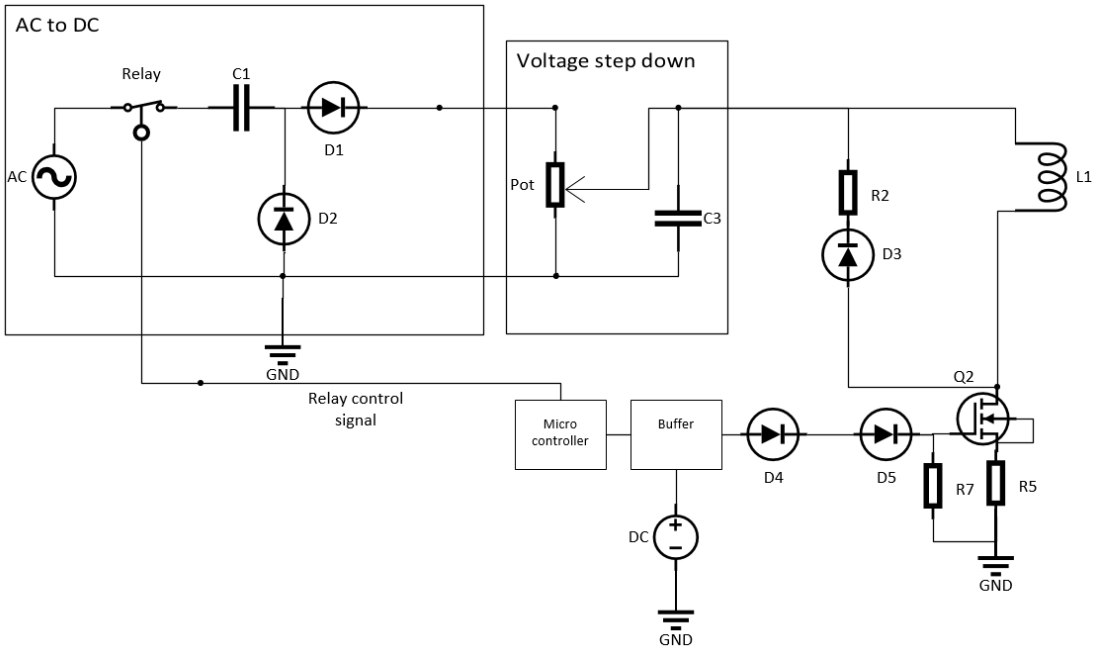


Figure 4-10 Schematic of the attacker circuit

Figure 4-10 shows the schematic of the attacker's circuit, which has been divided into three main sections: AC to DC converter/rectifier, voltage step down and load with high current switch.

In the rectifier section, 115 VAC signal from the US power outlet was converted to DC voltage with the help of two diodes and a capacitor (C1, D1 and D2). These diodes and capacitors form the voltage doubler circuit. The relay connected at the input of the voltage doubler circuit was controlled by the microcontroller, which reads the output voltage from the rectifier and shuts down the rectifier circuit, when the circuit is not in use, so that overheating issues could be prevented.

The converted DC voltage is applied across the Potentiometer (Pot), which is a variable resistor, using which the voltage can be stepped down to required value. Ability to control the DC voltage connected to the switching transistor will allow the user to change the bias condition of the transistor, there by changing the magnitude of current flowing through

it. The output DC current from the rectifier and the voltage step down stages was used to charge the capacitor C3, which would filter out the noise from the rectification process.

In the final stage, C3 is connected to the inductive load (L1), which has the feedback path connected to the resistors for the dissipation of the return power. Diodes (D3-D5) are used to make sure that the current travels only in one direction, during the discharge cycle. Transistor (Q2) acts as a high current switch, while the microcontroller feeds the control signal to the switching system. Insulated Gate Bipolar Transistor (IGBT) was used to function as the switching transistor, due to its ability to support high current, with minimal switching resistance. Current sense resistor (R5) is used to measure the current across the transistor, while the resistor R7 was used to discharge any residual charge stored in the gate of the transistor, which might prevent the switching transistor from fully shutting down.

Design considerations for AC to DC converter/rectifier:

Capacitor C1 would be charged and discharged every half cycle of the 60 Hz sinusoidal signal, coming from the 115V AC power outlet. Assuming 10 A of peak current flow through the AC to DC converter circuit, the capacitor C1 can be calculated and chosen using the equation (4-7).

$$C_1 = \frac{I\,t}{V} \tag{4-7}$$

In equation (4-7), 'I' represents the average current flowing through the capacitor in one half cycle of the sinusoidal signal, which is 6.37 A (= 10 A × 0.637), while 't' represents the half cycle of a sinusoidal period, which is 8.34 ms (= $\frac{1}{2\times 60\ Hz}$). 'V' represents the average voltage experienced by the capacitor C1, which can be calculated as 73.255 V (=115 V × 0.637). Thus, the minimum value of C1 can be calculated as ~725 µF. The authors have

chosen to use a 1200 µF capacitor, with a voltage rating of 250 V, which is beyond the required 115 V rating, to provide a more stable operation, under high current loads.

Ignoring any voltage loss across the diodes D1 and D2, the potentiometer which had a total resistance of 1 kΩ would experience a total voltage of about 230 V, across them, due to the voltage doubler outputting an DC voltage with magnitude twice that of the peak voltage of AC input signal. Hence these resistors need to handle a minimum of 52.9 W ($= \frac{V^2}{R} = \frac{230^2}{1000}$). Thus, the 1 kΩ potentiometer was chosen with 100 W power rating to have extra headroom in terms of power dissipation.

The relay connected between the AC power outlet and capacitor C1 was used to shut down the charging circuit, whenever the switching transistor is not operating. This would prevent the potentiometer from getting heated up, since the potentiometer would constantly drain 230 mA ($\frac{230\ V}{1000\ \Omega}$), which would constantly heat the potentiometer and might result in failure of this component. The control signal for this relay was sent by the microcontroller, which determines the instances when the switching transistor is not under operation.

Power Rating Design Consideration for Voltage Step Down Stage:

Capacitor C3 serves as the charge storage bank, which would supply the required amount of charge during the transmission of sawtooth waveform, while maintaining a stable collector to emitter voltage across the IGBT transistor. The discharge cycle represents the duration of time, in which current flows through the solenoid. Equation (4-8) describes the calculation of minimum capacitance for C3.

$$C_3 = \frac{I\,t}{V_{initial} - V_{final}} \tag{4-8}$$

In equation (4-8), 'I' and 't' represents the average current and time, like equation (4-7), while Vinitial and Vfinal represents the initial capacitor voltage before the discharge cycle and final capacitor voltage after the discharge cycle, respectively. Ignoring any additional drop in voltage across the diodes D1 and D2, the maximum value of Vinitial can be 230 V, from the voltage doubler, while the value of Vfinal was assumed to be 30 V. The 200 V difference between the initial and final voltage values should not cause any issues for the transmitted power, since IGBTs are very resilient to minor changes in the collector to emitter voltage [49].

The required current flow through the coil was 1000 A (= I). Assuming that an attacker would like to interfere with the digital servo motor for a duration of 1 s (= t), the minimum required capacitance value of C3 was calculated as 5 F. This shorter duration of time to inject false data and thus control the servo motor was chosen to keep the capacitance value low, thereby bringing the cost of the overall circuit low. Despite this shorter duration, 5 F was a large amount of capacitance. The author decided on using 10 mF capacitor, to design a cost-effective circuit, which would serve as a proof of concept for this attack. Although, this circuit would only support a single cycle of sawtooth waveform transmission, its capability can be improved by adding additional capacitors in parallel.

Switching Transistor Power Rating Design Consideration

The resistors (R2) was built using 20 resistors in parallel, which were used to dissipate the energy after the transistor shuts off completely, to avoid any return power to the transistor or control circuits, which were connected to the gate of transistor. These 20

resistors connected in parallel reduces the cost compared to having a single resistor, as the resistors cost increases with the rated wattage. If 1000 A flows through the 20 resistors, each with 0.2 Ω resistance, during the discharge cycle, then 500 watts ($= I^2R = \left(\frac{1000}{20}\right)^2 \times 0.2$) rating per resistor is required. But, this would be the requirement for resistor power rating, if 1000 A of current continuously flows through the resistors. The authors have chosen resistors rated at 100 watts, since it should be enough to handle 500 watts of current during 100 us (assuming 100 us to the discharge time), which would be significantly less in terms of dissipated energy (= power x discharge time).

The voltage developed across the IGBT transistor (Q2) was due to supply voltage and from the voltage developed across the load coil, when current flows through it. During the fall time of the pulse, the voltage polarity across the inductor is reversed, resulting in a net voltage appearing across the collector-emitter nodes of the transistor, as the summation of inductor voltage and supply voltage. But, due to the long falling time of the sawtooth waveform used for this attack, which is ~50 ms, the inductor voltage developed during the rising edge is much more critical to manage than the voltage developed during the falling edge. Assuming that the rising edge of the sawtooth waveform to be 100 ns, the voltage developed across the inductor can be calculated by the following equation.

$$V_{ind} = L\,\frac{dI}{dt} \tag{4-9}$$

Using equation (4-9), the inductor voltage can be estimated as 200 V, if the inductance of the solenoid was assumed as 200 V. The author decided to use a IGBT transistor with voltage rating of 1200 V and current rating of 800 A (pulsed current over 1 ms) for the safe and stable operation range of the transistor.

The last component which needs to have its power rating estimated was the current sense resistor. This component would allow the attacker to verify the rise/fall times of the the sawtooth waveform using an oscilloscope connected across this resistor. The current sense resistor was chosen with a resistance of 0.5 mΩ and 100 W power rating. Despite the need to handle 500 watts ($= 1000^2 \times 0.5m\Omega$), since, the current sense resistor will only be operated for a shorter duration of time, due to the limited size of capacitor C3, the author decided to use this particular current sense resistor.

Buffer circuit:

The buffer circuit used to control the switching transistor was built as a simple digital inverter, which boosts the incoming signal to a specified voltage.

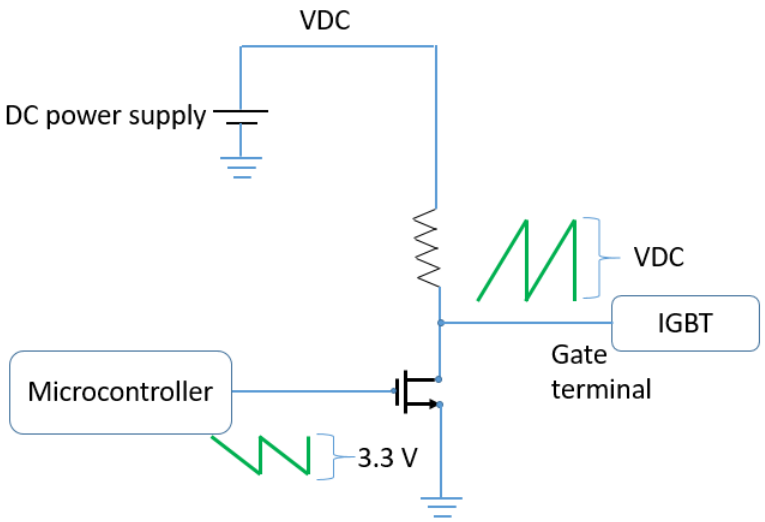


Figure 4-11 Buffer circuit used to boost the signal from microcontroller to gate terminal of IGBT

Figure 4-11 shows the buffer circuit used to boost the sawtooth waveform the has its voltage ranging from 0 V to 3.3 V. The output waveform from this buffer circuit was an

inverted version of the signal from the microcontroller, with boosted voltage levels ranging from 0 V to VDC. Because of the buffer circuit, it was relatively easy to control the output current from the attacker circuit, since the output current from the switching IGBT transistor has a strong dependence on the voltage levels at its gate terminal [49].

Table 4-1. Summary of the components used in the attacker circuit.

Name	**Labels in Figure 4-10**	**Values and power ratings**
Capacitor	C1	1200 µF, 250 V
Diodes	D1 and D2	15ETH03PBF-ND, 300V, 15A
Potentiometer/Variable resistor	Pot	1kohm, 100watts
Resistor	R6	1kohm, 100watts
Discharge capacitor	C3	10000 µF, 200 V
Feedback resistors	R2	0.2ohm, 100 watts
Feedback diode	D3	VS-1N1186GI, 200V, 35V
Inductor	L1	22 µH
Insulated-Gate Bipolar Transistor (IGBT)	Q2	FZ400R12KE4, 1200 V, 800 A
Diodes	D4 and D5	1N4004DICT-ND, 400V, 1A
Current sense resistor	R5	0.0005ohm,100 watts

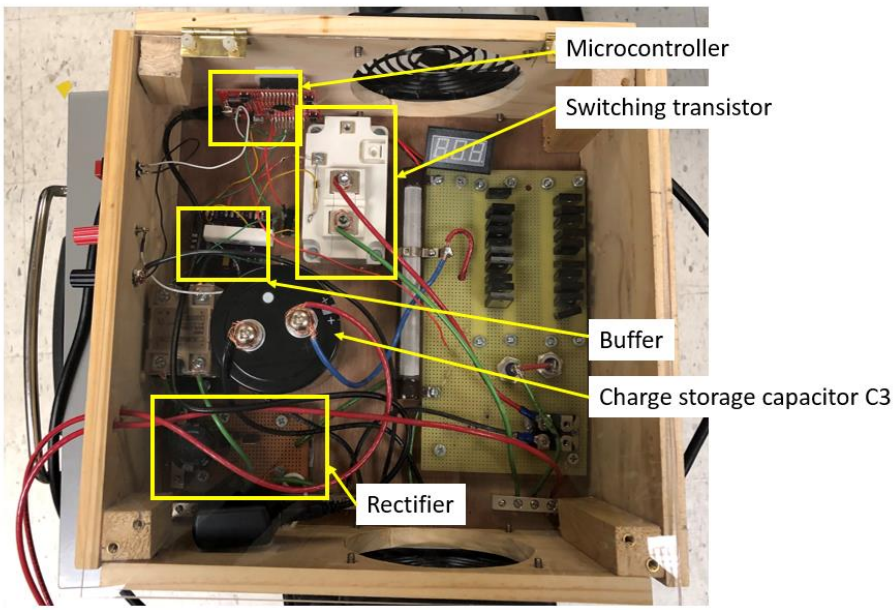


Figure 4-12 Attacker circuit

Figure 4-12 shows the designed attacker circuit with highlights on key components, such as, microcontroller, switching transistor, buffer and rectifier. The yellow perforated PCB board on the ride side of Figure 4-12 has the potentiometer and 20 resistors (R2), along with the current sense resistors (R5). The sawtooth signal was applied to the circuit using a microcontroller circuit board, which was mounted on the side walls of this circuit. The power rating for each component used, was calculated above the required power rating for better durability. Several ground bars are used for stable connections to ground, positive supply and for the connection between the solenoid and the capacitors.

4.4.2 Experimental results and discussion

Due to cost consideration, the attacker circuit was built to support sawtooth waveform transmission with 1000 A of current for 1 ms, due to the limited size of storage capacitor. Since 1 ms was less than the required period of sawtooth waveform, which was 50 ms, the attacker circuit would not be able to demonstrate a successful IEMI attack on digital servo motor. Hence, the author decided on reducing the output current level from the designed circuit to 200 mA, which would enable the attacker to sustain the attack for 5 seconds. However, the reduced output current from the attacker circuit would result in a decreased voltage induction at the victim circuit at 1 cm distance from the transmitter. To compensate for the reduced transmitted power, the victim circuit's PWM signal cable was wrapped around the solenoid to enable better coupling, thus enabling improved coupling between the transmitter and victim circuits.

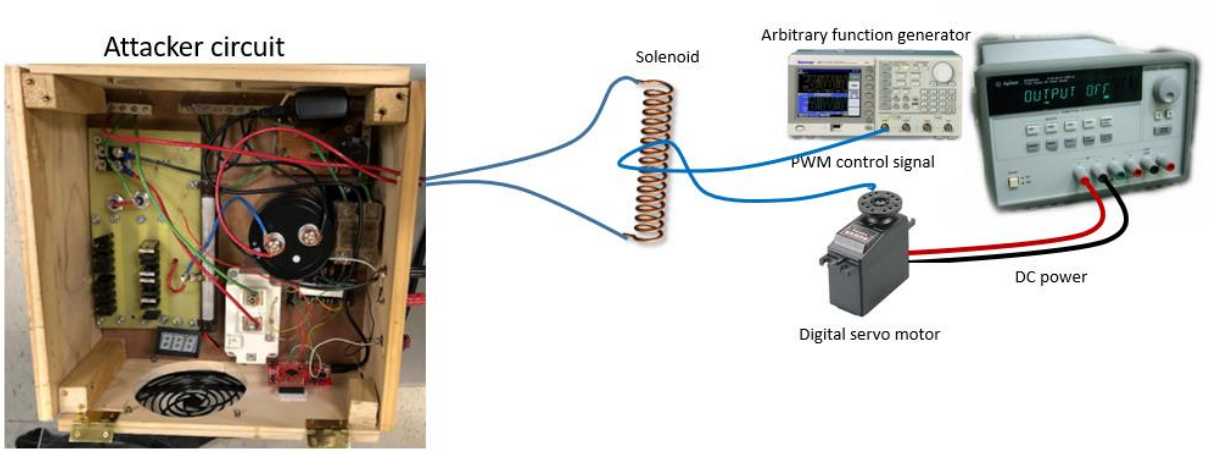
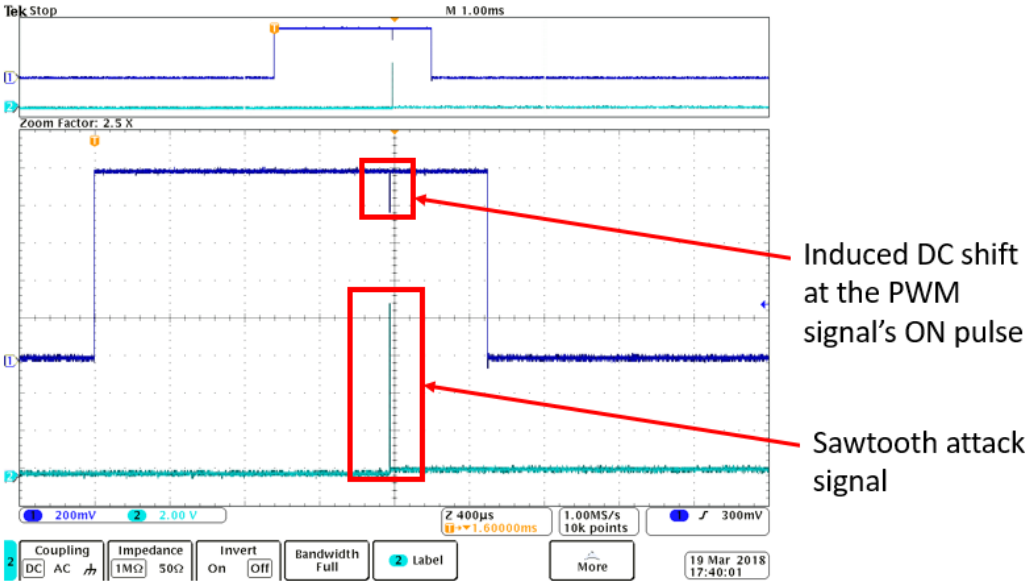
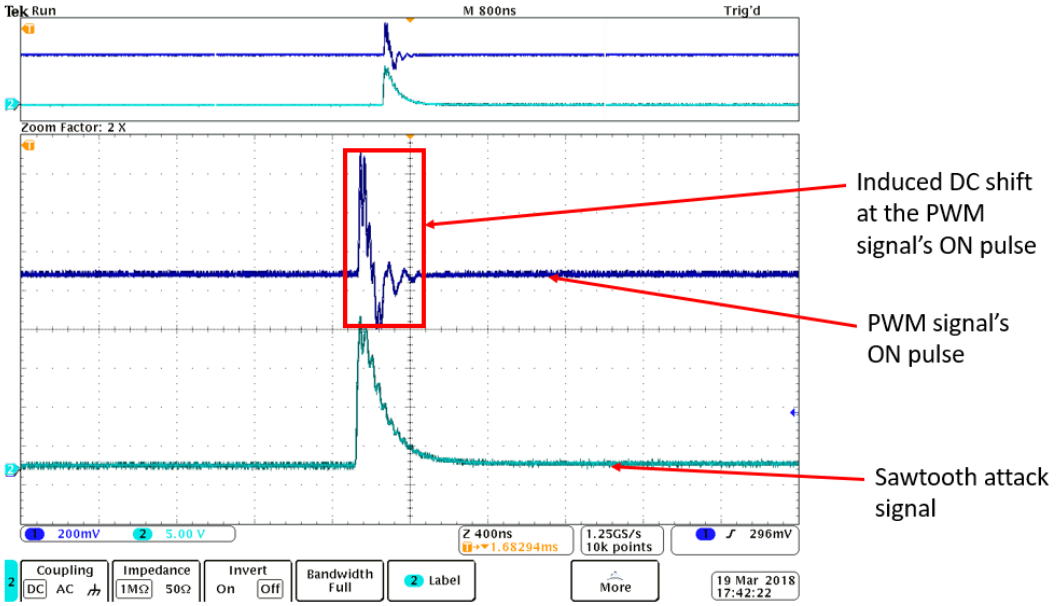


Figure 4-13 Experimental setup showing sawtooth waveform attack on digital servo motor

Figure 4-13 shows the experimental setup used to demonstrate the IEMI attack on servo motor using sawtooth waveform. The cable carrying the PWM signal was wrapped around the solenoid, to form a secondary coil, with one turn, to increase the coupling between the transmitting solenoid and the victim circuit. The microcontroller's clock was synchronized with the arbitrary function generator, which generates the PWM signal. The phase of the PWM signal was adjusted so that the rising edge of the sawtooth waveform aligns at the center of the PWM signal's ON pulses. Using the buffer circuit, the amplitude of signal applied to the gate terminal of the IGBT transistor was adjusted in such a way that, the output current flowing through the solenoid was 200 mA.



(a)



(b)

Figure 4-14 Oscilloscope image showing the sawtooth attack signal as well as the DC offset induced in the PWM signal

Figure 4-14 shows the sawtooth attack signal and the induced DC offset at the PWM signal's ON pulse. Figure 4-14 (b) shows the zoomed-in version of Figure 4-14 (a) around

the rising edge of the sawtooth waveform. This figure shows a 200 mV drop in the DC level for about ~50 ns. It was observed that the servo motor's armature rotated successfully to a new angle, which was in accordance with the reduction in pulse width, due to the induced DC offset from the IEMI attack. This result proves the author's hypothesis on sawtooth waveform's ability to induce drop in the DC level for a shorter duration, resulting in a net reduction of the pulse width of PWM signal.

4.5 Conclusion

In this chapter, three different IEMI attack techniques were demonstrated for injecting false data into the digital servo motor's PWM control signal. The technique involving continuous sinusoidal signal transmission resulted in the digital servo motor entering an unresponsive state, while the pulsed sinusoidal signal could increase the pulse width of the PWM signal resulting in anti-clockwise rotation of the digital servo motor's armature. The final attack technique demonstrated using a sawtooth waveform needed the design of a high current driver, which was successfully able to induce DC offset for a short duration, between the ON pulses of the PWM signal, resulting in clockwise rotation of the digital servo motor's armature, in accordance to the net reduction in pulse width of the PWM control signal.

CHAPTER 5

OTHER CONTRIBUTIONS

This chapter has used materials that were published in the paper "Enhancement for High-Speed Switching of Magneto-Optic Fiber-Based Routing Using Single Magnetizing Coil", by J. Selvaraj et. al, with the permission of all the authors [50].

Being an active member or the High Speed Systems Engineering (HSSE) lab, I have been involved in related research. One of the leading projects of the lab focus on improving the existing small magnetic pulse generator circuit, used to control magneto-optic switch.

5.1 Introduction

All-optical networking systems are being actively investigated to improve the speed of fiber-based communication systems [51] [52] [53] [54] [55]. The major bottleneck for switching speeds in current fiber-based systems comes from the optical-to-electrical/electrical-to-optical conversion process handled by the routers in a network, since the maximum bandwidth of electrical systems are lower than that of the optical fibers. Magneto-Optic (MO) material with an interferometer setup are being explored to replace contemporary routers and remove this bottleneck, thereby enabling an all-optical network [56].

MO materials alter the state-of-polarization (SoP) of the optical signals passing through an interferometer setup, which would result in constructive or destructive interference at the output ports. Also, MO materials has the capability to introduce varying levels of SoP for an optical signal, depending on the strength and direction of magnetic field applied to them. The phenomenon which causes an optical signal to experience a change in

the SoP is called Faraday rotation [56]. Thus, an MO material present in an optical interferometer setup could produce different levels of interference, with varying magnetic field strength, thereby achieving the capability to function as an all-optical router. Recently there has been several investigations on the techniques to improve the switching speed of such all-optical routers.

Wu et al. has proposed a magnetic field generator circuit which can generate current pulses with 6-20 ns pulse width and 2-5 ns rise time [52]. Despite the shorter rise time, they showed that the fall time of the optical signal is in the order of 200 ns. Pritchard et al. has shown that the residual magnetic field present in the coil after the demagnetization process results in a slower fall time of optical signal [57]. They have proposed a two-coil system with two separate driver circuits, used to generate forward and reverse magnetic fields. With the help of the reverse magnetic field, Pritchard et al. showed that the fall time of optical output can be reduced to ~130 ns. But, the system suffered from a 10% reduction in the optical amplitude, due to interaction between the two coils, along with minor perturbation in the optical output under no-output conditions. In this paper, a new magnetic pulse generator system is proposed with a single coil and a single driver circuit. The newly proposed system generates magnetic field in forward and reverse direction, while achieving similar performance in terms of switching speed compared to previous works and reduced circuit complexity.

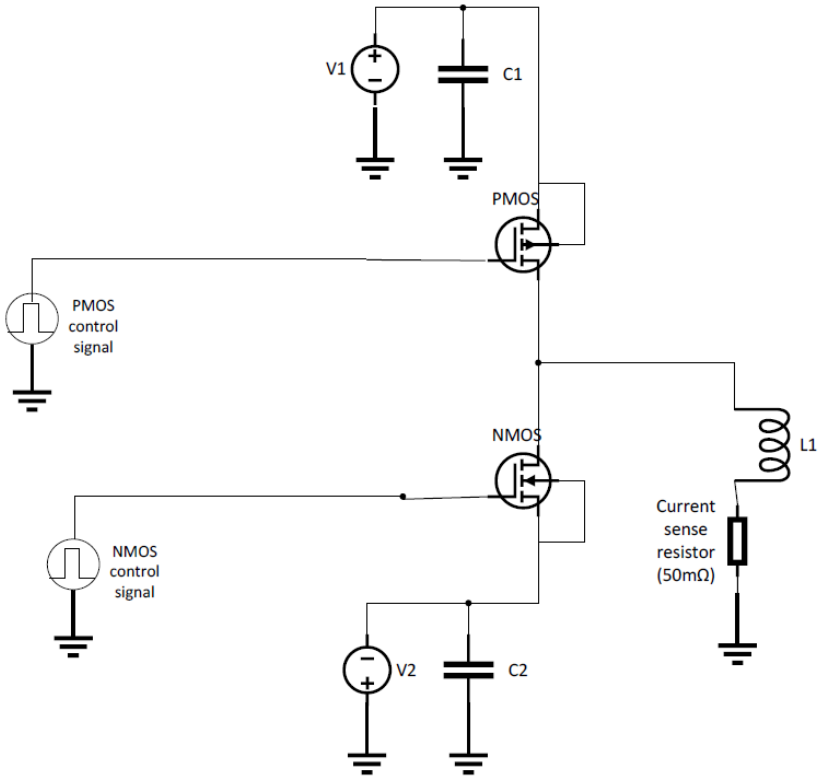


Figure 5-1 Proposed magnetic field generator circuit

5.2 Magnetic Field Generator Circuit

The proposed magnetic field generator circuit is shown in Figure 5-1. This circuit has an NMOS and PMOS transistor combination. PMOS circuit has been used to supply positive voltage from the DC source 'V1' to the coil 'L1', thus sending a forward current to the coil, while the NMOS circuit has been used to supply negative voltage from the DC source 'V2', thus sending a reverse current to the coil. Consequently, the coil will be able to produce magnetic field in forward or reverse direction, based on the direction of current flow. The supply voltages used in this circuit were +3.5V and -3.5V. The capacitors C1 and C2 help to store positive and negative charges from the DC supply, which would be used during the fast

charging and discharging phases of the coil. The minimum size of the capacitors C1 and C2 can be determined from the below equation.

$$c = \frac{I\,t}{V_{initial} - V_{final}} \tag{5-1}$$

In equation (5-1), 'I' represents the peak current amplitude (amperes), while 't' represents the amount of time (seconds), during which there would be current flow through the coil. 'Vinitial' represents the initial voltage (volts) of the capacitor, which would be equal to the supply voltage, while the 'Vfinal' represents the capacitor voltage after the duration 't'. In this study, the authors used 'Vinitial' and 'Vfinal' as 3.5 V and 3.4 V, respectively, while the required 'I' was ~10A and 't' was 5 us. From equation (5-1), the minimum capacitance size for the proposed circuit would be 500 uF. Authors chose to use 3300 uF capacitors to have freedom in terms of the current amplitude and duration of current flow to the coil.

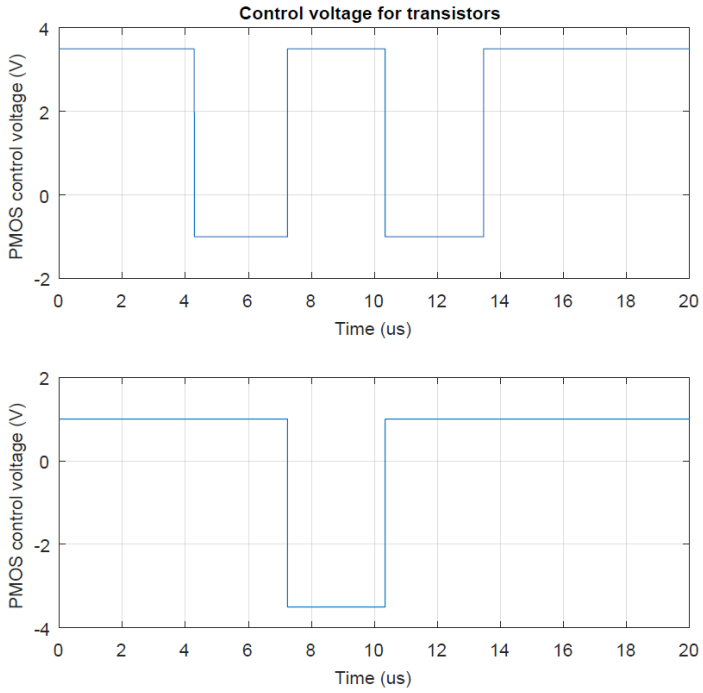


Figure 5-2 Control signals for PMOS and NMOS transistors

To ensure that the current flow exists only between the DC sources and avoid direct connection between positive and negative DC sources, the NMOS and PMOS transistors are never made to operate in ON condition together. This was achieved by providing separate control signals to the gate of PMOS and NMOS transistors. The current flow in the coil can be monitored by measuring the voltage generated across the 'current sense resistor' (50 mΩ) that is in series with the coil.

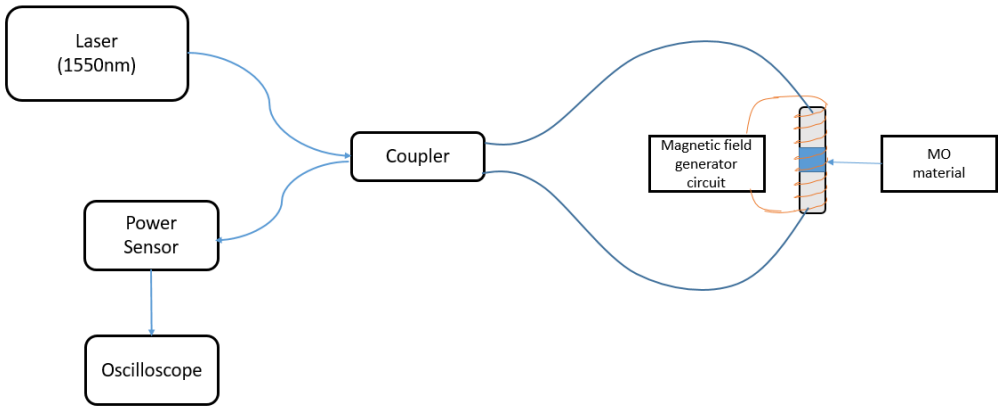


Figure 5-3 Optical interferometer setup

Figure 5-2 shows the control signals supplied to the two transistors. The control signal for PMOS varies from +3.5V to -1V, while the NMOS control signal varies from -3.5V to +1V. When the PMOS transistor receives a control voltage of

+3.5V at its gate, the gate to source voltage (Vgs) of the PMOS becomes 0V, thus the PMOS transistor turns OFF. But, application of -1V to the PMOS transistor's gate terminal turns the transistor ON, with a 'Vgs' of -4.5V. Under 'ON' condition, the transistor provides least amount of resistance to the current flow. The control voltages at which the NMOS transistor turns ON and OFF is exactly opposite to that of the PMOS transistor. Changing the magnitude of the control voltages will result in a change in the amplitude of the current

flowing to the coil. The control signals for the two transistors were synchronized to avoid simultaneous turning ON of PMOS and NMOS transistors. With the help of these synchronized control signals, the proposed circuit can generate magnetic fields in forward and reverse directions during distinct phases in time.

In the control signal of PMOS transistor, Figure 5-2 shows three distinct phases. During the first phase, which is from 4.2 us to 7.2 us, the PMOS transistor was turned ON, thus charging the coil with a positive current, while the NMOS transistor was turned OFF. Magnetic field was generated in forward direction during this phase. During the second phase (from 7.2 us to 10.2 us), the PMOS transistor was turned OFF, while the NMOS transistor was turned ON, which results in the discharge of the magnetic energy stored in the coil, thus resulting in a magnetic field generated in the reverse direction. Finally, in the third phase (from 10.2 us to 13.8 us), the PMOS transistor was turned back ON, while the NMOS was turned OFF, thus generating a second magnetic field in the forward direction.

The presence of forward (first phase) and reverse (second phase) magnetic field ensures that the MO material is magnetized and demagnetized faster, while the third phase generates an additional forward magnetic field to bring the MO material to its initial unmagnetized state. Thus, the proposed circuit can generate magnetic field in forward and reverse direction, with the freedom to change the strength as well as the duration of each of the magnetic fields.

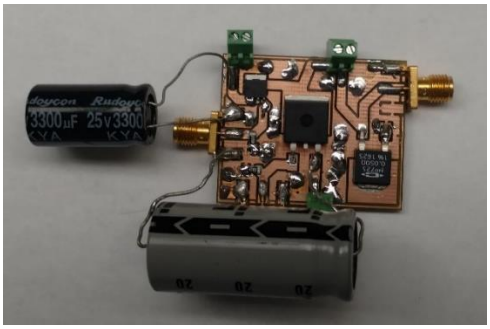


Figure 5-4 Magnetic field generator circuit fabricated on a PCB

5.3 Optical Interferometer Setup

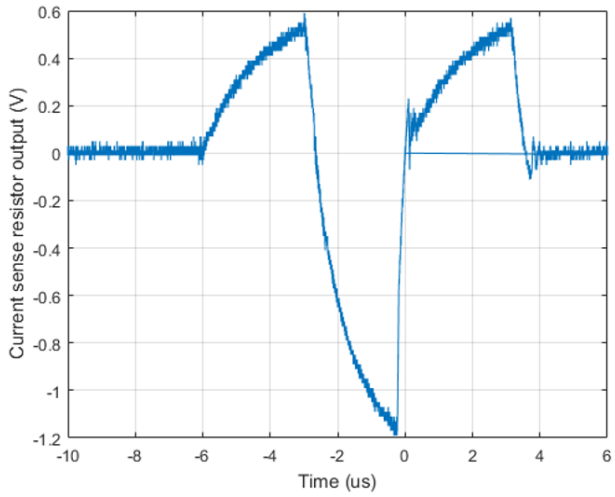
Sagnac interferometer setup utilizing MO material and magnetic field generator circuit is shown in Fig. 3. Sagnac interferometer was chosen due to its stability over different temperature ranges [56]. The MO material was placed inside a zirconia sleeve, with optical cables placed against its sides. MO material was placed at the center of the Sagnac loop to produce Faraday rotation to the optical signal, resulting in a change of SoP. This optical signal creates a constructive or destructive interference at the output port of the 3dB coupler, depending on the state of the MO material's magnetization. The MO material used in this setup was a "Bismuth-doped rare-earth iron garnet thick film", which had a thickness of 470□m and provides a maximum of 45° Faraday rotation. This MO material was magnetized/demagnetized using a coil connected to the proposed circuit.

The coil wrapped around the MO material has 5 turns with 4mm length and 1.6mm wire thickness. The strength of magnetic field (B) produced by this coil can be calculated by the following equation [58]:

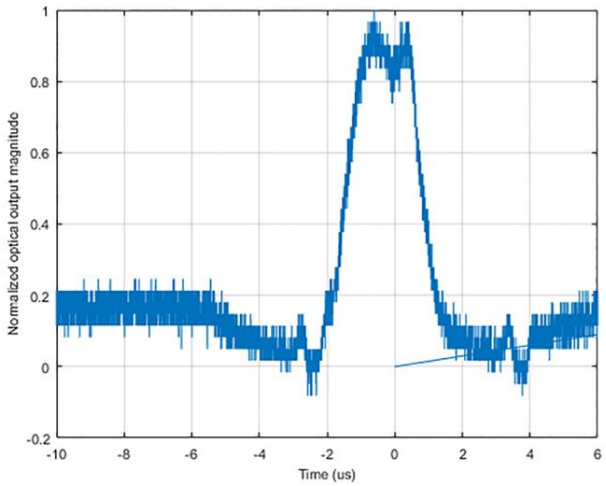
$$B = \frac{\mu_o NI}{\sqrt{l^2 + 4R^2}} \tag{5-2}$$

Here, ‘N’ represents the number of turns in the coil, while ‘l’ and ‘R’ represents the length and radius of the coil, respectively. The magnitude of peak current flowing through the coil is represented by ‘I’.

The optical interferometer setup receives power from a laser source with 1550nm wavelength. The output port of the coupler was connected to a power sensor, which converts optical signal into electrical signal to be monitored using oscilloscope.



(a)



(b)

Figure 5-5 a) Current sense resistor’s voltage output. b) Normalized optical output.

5.4 Results and Discussion

Figure 5-4 shows the proposed magnetic driver circuit fabricated on a PCB. Two SMA connectors were used to supply the control signal to the transistors, while another SMA connector was used to read the 'current sense resistor' voltage output. The current sense resistor output obtained from the fabricated circuit is shown in Figure 5-5a. The corresponding optical output measured from the power sensor of the interferometer setup is shown in Figure 5-5b. The rise/fall time of the optical output was ~500ns. The reason for the longer switching speed was due to the PMOS transistor (Infineon SPB80P06PG) used in this circuit had a very large gate capacitance of ~5nF. This resulted in a slowdown of the input control signal applied to the PMOS transistor. Also, the NMOS transistor (PSMN4R0-30YLD) used in this circuit also had a large capacitance of ~1.2nF. For a desired 100ns rise time of control signal, with a source resistance of 50Ω, the input capacitance should be in the order of ~500pF. This requirement comes from the time constant equation for a (Resistor-Capacitor) RC circuit:

$$\tau = RC \tag{5-3}$$

Rise/fall time of a RC circuit can be approximated to be ~5τ. Thus, the control signals applied to the gate of the transistors would have had a rise/fall time of about ~1550 ns, due to the large total input capacitance of 6.2nF (=5nF+1.2nF). The slow rising/falling control signals ultimately resulted in current pulses with longer rise/fall times.

Figure 5-5a shows that the positive peak amplitude of the current sense resistor output was 0.55V, while the negative peak amplitude was -1.2V. We can calculate the corresponding peak current amplitude as 11A and -24A. The reason for the difference in the peak current levels arises from the difference in the PMOS and NMOS transistor

characteristics. As mentioned earlier, the peak positive or negative current amplitudes can be varied by changing the amplitude of the control voltages supplied to the corresponding transistors.

Despite the shortcomings in the maximum switching speed of the control signals, the proposed circuit could achieve switching speeds in the order of ~500ns. Figure 5-5b shows that the optical output has a rise and fall time ~500ns and a pulse width of ~2 us. Also, the optical output shows no perturbation in the signal when no magnetic field was applied to the MO material. The switching speed of the optical output can be improved significantly by using transistors with low input capacitances.

It is important to note that the proposed circuit provides the freedom to control the magnitude as well as time period of each one of the three phases of the magnetic pulses to fine tune the optical output. Also, the third phase of the magnetic pulse is provided to aid the MO material reach a fixed state, at the end of each switching cycle, which would help fast magnetization in the next switching cycle. This way both the rise and the fall time of the optical signal can be improved. The proposed circuit will show a significant improvement in the fall time of latching MO materials, which needs a strong reverse magnetic field in order to be able to demagnetize quickly [57]. In future, the authors are planning to use transistors with low input capacitance to further improve the switching speed.

5.5 Conclusion

This work reports on a newly proposed circuit that can generate magnetic field in forward as well as reverse direction. The circuit provides the user with the freedom of fine tuning the magnitude and period of each magnetic pulses. This circuit has been used as the field generator in a Sagnac interferometer setup utilizing an MO material and the

experimental results prove that the switching speed of optical output can be improved with the help of magnetic fields generated from the proposed circuit.

CHAPTER 6

CONCLUSION AND FUTURE WORK

In this dissertation, the feasibility of low power IEMI attack techniques to inject false-data into input and output signals of an embedded system, has been explored. It has been experimentally proved that the chosen analog sensor circuit, gets influenced by the induced time varying signal, due to AC to DC conversion phenomenon, which happens due to the non-linear properties of embedded systems. The experimental results prove that, it would be possible to arbitrarily increase or decrease the DC voltage seen by the ADC circuit, thereby corrupting the analog sensor's output data.

Also, the same non-linear properties of the embedded system's input terminal, make them vulnerable to IEMI attacks, even if the sensors used by this system are fully digital. It had been previously assumed that digital signals are resilient to false data injection attack from IEMI attack techniques. But, the results shown in this dissertation proves otherwise and demand alternative options to detect and eliminate the false data injected because of this attack.

Finally, the IEMI attack on digital actuators were also proven to be affected by false data injection into the control signal's path. Experimental data presented in this dissertation shows that it is possible to disable the digital actuator from responding to any new control signal input, while also showing the feasibility of independently controlling the digital actuator, regardless of the control signal generated by an embedded system, using this attack technique.

6.1 Suggestions for future researchers

Although the work discussed in this dissertation, highlights the potential threat posed by IEMI attack technique, there are lot more questions which needs to be answered, before considering this technique as a viable option for successful false data injection. The most important of which is, design of EM signal detection circuit, that can detect the digital signal transitions. This circuit would have to be integrated with the IEMI attacker circuits, to be able to inject false data in-phase with the digital signals present in the victim circuit. With successful integration of this circuit with the IEMI attacker's system, the injected false data would be completely indistinguishable from the actual digital data, from the point of view of an embedded system.

The second main concern which holds back IEMI attack technique from becoming main stream, is the portability of the attacker's circuit. Currently the proposed circuits which were used to perform IEMI attacks on embedded systems were bulky and requires constant AC power supply from wall outlets, to sustain this attack. Ideally, an attacker's circuit should be portable, at the least, it should be small enough to be carried inside a shoulder bag, with the entire circuit powered by portable battery power. To realize this portable circuit, the power transfer efficiency between attacker and the victim circuit must be improved, thereby reducing the power consumption of the attacker circuit.

One of the key components to ensure maximum power transfer efficiency between the attacker and victim circuits would be the transmission of attack signal at the resonant frequency of the victim circuit. Currently, there are no direct method to determine the resonant frequency of the victim circuit, without experimentally sweeping the attack signal's frequency over a range of frequencies and then use the output data of the embedded system,

in a controlled environment, to estimate the resonant frequency. Although, there are circuit's like grid-dip-meter, which have been traditionally used to detect the resonant frequency of a receiver, the complexity of embedded circuits requires design of special techniques, to accurately determine the resonant frequency, thereby improving the efficiency of the IEMI attack technique.

REFERENCES

[1] Workshop on "Electromagnetic Terrorism and Adverse Effects of High Power Electromagnetic (HPE) Environments," *Proceedings of the 13th International Zurich Symposium and Technical Exhibition on Electromagnetic Compatibility*, February, 1999.

[2] R. D. Leach and M. B. Alexander, "Electronic Systems Failures and Anomalies Attributed to Electromagnetic Interference," NASA, Washington DC, July 1995.

[3] House of Commons Defence Committee, UK, "Developing Threats: Electro-Magnetic Pulses (EMP)," The Stationery Office by Order of the House, London, February 2012.

[4] 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.

[5] D. V. Giri and F. M. Tesche, "Classifications of Intentional Electromagnetic Environments (IEMI)," *IEEE Transactions on Electromagnetic Compatability*, vol. 46, no. 3, pp. 322-328, 2004.

[6] F. Sabath, M. Bäckström, B. Nordström, D. Sérafin, A. Kaiser, B. A. K. Kerr and D. Nitsch, "Overview of Four European High-Power Microwave Narrow-Band Test Facilities," *IEEE Transactions on Electromagnetic Compatability*, vol. 46, no. 3, pp. 329-334, 2004.

[7] W. D. Prather, C. E. Baum, R. J. Torres, F. Sabath and D. Nitsch, "Survey of Worldwide High-Power Wideband Capabilities," *IEEE Transactions on Electromagnetic Compatability*, vol. 46, no. 3, pp. 355-344, 2004.

[8] H. Haase, T. Steinmetz and J. Nitsch, "New Propagation Models for Electromagnetic Waves Along Uniform and Nonuniform Cables," *IEEE Transactions on Electromagnetic Compatability*, vol. 46, no. 3, pp. 345-352, 2004.

[9] J. Carlsson, T. Karlsson and G. Undén, "EMEC—An EM Simulator Based on Topology," *IEEE Transactions on Electromagnetic Compatability*, vol. 46, no. 3, pp. 359-367, 2004.

[10] J. Parmantier, "Numerical Coupling Models for Complex Systems and Results," *IEEE Transactions on Electromagnetic Compatability*, vol. 46, no. 3, pp. 359-367, 2004.

[11] M. Camp, H. Gerth, H. Garbe and H. Haase, "“Predicting the Breakdown Behavior of Microcontrollers under EMP/UWB Impact Using a Statistical Analysis," *IEEE Transaction on Electromagnetic Compatability,* vol. 46, no. 3, pp. 368-379, 2004.

[12] D. Nitsch, M. Camp, F. Sabath, J. L. Haseborg and H. Garbe, "Susceptibility of Some Electronic Equipment to HPEM Threats," *IEEE Transaction on Electromagnetic Compatability,* vol. 46, no. 3, pp. 380-389, 2004.

[13] R. Hoad, N. J. Carter, D. Herke and S. P. Watkins, "Trends in EM Susceptibility of IT Equipment," *IEEE Transaction on Electromagnetic Compatability,* vol. 46, no. 3, pp. 390-395, 2004.

[14] M. G. Bäckström and K. G. Lövstrand, "Susceptibility of Electronic Systems to High Power Microwaves: Summary of Test Experience," *IEEE Transactions on Electromagnetic Compatability,* vol. 46, no. 3, pp. 396-403, 2004.

[15] Y. V. Parfenov, L. N. Zdoukhov, W. A. Radasky and M. Ianoz, "Conducted IEMI Threats for Commercial Buildings," *IEEE Transactions on Electromagnetic Compatability,* vol. 46, no. 3, pp. 404-411, 2004.

[16] I. Jeffrey, C. Gilmore, G. Siemens and J. LoVetri, "Hardware Invariant Protocol Disruptive Interference for 100BaseTX Ethernet Communications," *IEEE Transactions on Electromagnetic Compatability,* vol. 46, no. 3, pp. 412-422, 2004.

[17] T. Weber, R. Krzikalla and J. L. Haseborg, "Linear and Nonlinear Filters Suppressing UWB Pulses," *IEEE Transactions on Electromagnetic Compatability,* vol. 46, no. 3, pp. 423-430, 2004.

[18] T. Weber and J. L. Haseborg, "Measurement Techniques for Conducted HPEM Signals," *IEEE Transactions on Electromagnetic Compatability,* vol. 46, no. 3, pp. 431-438, 2004.

[19] M. W. Wik and W. A. Radasky, "“Development of High-Power Electromagnetic (HPEM) Standards," *IEEE Transactions on Electromagnetic Compatability,* vol. 46, no. 3, pp. 439-445, 2004.

[20] C. Paul, Introduction to Electromagnetic Compatibility, ser. Wiley Series in Microwave and Optical Engineering, Wiley, 2006.

[21] R. T. Paley, "Bloomberg Pursuits," Bloomberg, 16 2 2018. [Online]. Available: https://www.bloomberg.com/news/articles/2018-03-30/boom-volcanic-wines-are-heating-up-around-the-globe. [Accessed 2 4 2018].

[22] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," *Black Hat USA 2015*, 2015.

[23] A. Greenberg, "Wried," 24 07 2015. [Online]. Available: https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/. [Accessed 09 02 2018].

[24] P. Rouget, B. Badrignans, P. Benoit and L. Torres, "SecBoot — lightweight secure boot mechanism for Linuxbased embedded systems on FPGAs," *12th International Symposium on Reconfigurable Communicationcentric Systems-on-Chip (ReCoSoC)*, pp. 1-5, 2017.

[25] A. Stanciu, F. D. Moldoveanu and M. Cirstea, "A novel PUF-based encryption protocol for embedded System," *2016 International Conference on Development and Application Systems (DAS), Suceava,* pp. 158-165, 2016.

[26] W. Radasky, C. Baum and M. Wik, "Introduction to the special issue on high-power electromagnetics," *IEEE Transactions on Electromagnetic Compatibility 46(3),* pp. 314-321, 2004.

[27] N. PARRA, "Contribution to the study of the vulnerability of critical systems to Intentional Electromagnetic Interference (IEMI). PhD. thesis," ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE, 2016.

[28] K. Fu and W. Xu, "Risks of Trusting the Physics of Sensors," *Communications of the ACM*, pp. 20-23, February 2018.

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

[30] 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," *IEEE Symposium on Scurity and Privacy (SP)*, pp. 145-159, 2013.

[31] J. Selvaraj, G. Y. Dayanikli, N. P. Gaunkar, D. Ware, R. M. Gerdes and M. Mina, "Electromagnetic Induction Attacks Against Embedded Systems," in *ACM Asia Conference on Computer, Communication & Security*, Incheon, Korea, 2018.

[32] OSRAM Opto Semiconductors, "SFH 235FA PhotoDiode," 23 Dec 2015. [Online]. Available: https://dammedia.osram.info/media/resource/hires/osram-dam-2495944/SFH%20235%20FA.pdf. [Accessed 16 Feb 2018].

[33] J. H. Chun and B. Murmann, "Analysis and measuremetn of signal distortion due to esd protection circuits," *IEEE Journal of solid-state circuits*, vol. 41, no. 10, pp. 2354-2358, 2006.

[34] Texas Instruments- Production Data, "Tiva C TM4C123GH6PM Microcontroller Datasheet," 12 June 2014. [Online]. Available: http://www.ti.com/lit/ds/symlink/tm4c123gh6pm.pdf. [Accessed 02 March 2018].

[35] OSRAM Opto Semiconductors, "Radial Sidelooker, SFH 235 FA," 23 December 2015. [Online]. Available: https://dammedia.osram.info/media/resource/hires/osram-dam-2495944/SFH%20235%20FA.pdf. [Accessed 03 March 2018].

[36] P. Rastogi, Y. Tang, B. Zhang, E. G. Lee, R. Hadimani and D. Jiles, "Quadruple butterfly coil with passive magnetic shielding for focused Transcranial Magnetic Stimulation," in *IEEE International Magnetics Conference (INTERMAG)*, Dublin, 2017.

[37] Y. So, W. Kim, J. Kim, Y. J. Yoon and J. Park, "Double-slot antipodal vivaldi antenna for improved directivity and radiation patterns.," in *Internaltional Symposium on Antennas and Propagation (ISAP)*, Okinawa, October, 2016.

[38] K. Ebnabbasi, D. Busuioc, R. Birken and M. Wang, "Taper Design of Vivaldi and Co-Planar Tapered Slot Antenna (TSA) by Chebyshev Transformer," *IEEE Transactions on Antennas and Propagation*, vol. 60, no. 5, pp. 2252-2259, May 2012.

[39] C. A. Balanis, Antenna Theory: Analysis and Design, Volume 1, John Wiley & Sons, 2005.

[40] "Fluke 87 Multimeter manual," [Online]. Available: https://assets.fluke.com/manuals/87_____umeng0800.pdf. [Accessed 12 03 2018].

[41] U. Azad and Y. E. Wang, "Analysis and Experimental Results for an Inductively Coupled Near-Field Power," in *2012 IEEE International Workshop on Antenna Technology (iWAT)*, Tucson, Az, 2012.

[42] Maxim Integrated, "MAX21000 Ultra-Accurate, Low Power, 3- Axis digital output gyroscope," 2013. [Online]. Available: https://datasheets.maximintegrated.com/en/ds/MAX21000.pdf. [Accessed 29 03 2018].

[43] G. MILNER, "Death by GPS," Arstechnica, 03 05 2016. [Online]. Available: https://arstechnica.com/cars/2016/05/death-by-gps/. [Accessed 29 03 2018].

[44] Y. Zhao, J. Liu and X. Zhuang, "A sparse signal reconstruction approach for sequential equivalent time sampling," in *2016 IEEE International Instrumentation and Measurement Technology Conference Proceedings*, Taipei, 2016.

[45] D. Kushner, "The real story of stuxnet," *IEEE Spectrum*, vol. 50, no. 3, pp. 48-53, March 2013..

[46] C. Melear, "Control of electromagnetic radiation in digital circuits," in *WESCON 97*, Santa Clara, CA, 1997.

[47] Futaba, "Futaba S3152 Digital Standard High-Torque Servo," [Online]. Available: https://www.gpdealera.com/cgi-bin/wgainf100p.pgm?I=FUTM0311. [Accessed 18 March 2018].

[48] J. Selvaraj, P. Rastogi, N. P. Gaunkar, R. L. Hadimani and M. Mina, "Transcranial Magnetic Stimulation: Design of a stimulator and a focused coil for the application of small animals," *IEEE Transactions on Magnetics (Under review)*, 2018.

[49] Infineon, "Technical information IGBT modules FZ400R12KE4," 04 11 2013. [Online]. Available: https://www.infineon.com/dgdl/Infineon-FZ400R12KE4-DS-v02_02-en_de.pdf?fileId=db3a30431f848401011fb7c1e8565958. [Accessed 26 03 2018].

[50] J. Selvaraj, W. S. Theh, N. P. Gaunkar, J. Hong, L. H. Bauer and M. Mina, "Enhancement for High-Speed Switching of Magneto-Optic Fiber-Based Routing Using Single Magnetizing Coil," *EEE Transactions on Magnetics*, vol. 53, no. 11, pp. 1-4, 2017.

[51] G. Zhang, M. D. Leenheer, A. Morea and B. Mukherjee, "A Survey on OFDM-Based Elastic Core Optical Networking," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 65-87, 2013.

[52] Q. Wu, J. Ruan, Z. Weng and S. Lin, "A novel magneto-optic switch based on nanosecond pulse," in *Asia Communications and Photonics conference and Exhibition (ACP)*, Shanghai, 2009.

[53] Z. Zheng and J. Wang, "A Study of Network Throughput Gain in Optical-Wireless (FiWi) Networks Subject to Peer-to-Peer Communications," in *IEEE International Conference on Communications*, Dresden, 2009.

[54] Q. Xu, H. Rastegarfar, Y. B. M'Sallem, A. Leon-Garcia, S. LaRochelle and L. A. Rusch, "Analysis of large-scale multi-stage all-optical packet switching routers," *IEEE/OSA Journal of Optical Communications and Networking*, vol. 4, no. 5, pp. 412-425, 20112.

[55] M. Ryohei, T. Goto, J. Pritchard, H. Takagi, Y. Nakamura, P. B. Lim, H. Uchida, M. Mina, T. Taira and M. Inoue, "Magnetic domains driving a Q-switched laser," *Scientific Reports,* vol. 6, 2016.

[56] M. M. a. P. D. J. W. Pritchard, "Demonstration of Magnetooptic Latching Router for All-Optical Networking Applications," *IEEE Transactions on Magnetics,* vol. 50, no. 11, pp. 1-4, 2014.

[57] J. W. Pritchard and M. Mina, "Magneto-Optic Interferometric Switch with Resonator Configuration," *IEEE Magnetics Letters,* vol. 4, pp. 6000104-6000104, 2013.

[58] J. A. Stratton, Electromagnetic Theory, New York: McGraw-Hill, 1941.

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

[60] N. Parra, "Contribution to the study of the vulnerability of critical systems to intentional electromagnetic interference (IEMI)," ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE, 2016.