Electromagnetic Interference Attacks on Cyber–Physical Systems: Theory, Demonstration, and Defense

Gökçen Yılmaz Dayanıklı

Dissertation submitted to the Faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy
in
Electrical Engineering

Ryan M. Gerdes, Chair
Patrick R. Schaumont
Cameron D. Patterson
Leyla Nazhand-Ali
Mazen Farhood
Majid Manteghi

August, 2021
Arlington, Virginia

Keywords: Cyber-Physical System Security, Intentional Electromagnetic Interference (IEMI), Electromagnetic Attacks, Signal Integrity

Electromagnetic Interference Attacks on Cyber–Physical Systems: Theory, Demonstration, and Defense

Gökçen Yılmaz Dayanıklı

(ABSTRACT)

A cyber-physical system (CPS) is a complex integration of hardware and software components to perform well-defined tasks. Up to this point, many software-based attacks targeting the network and computation layers have been reported by the researchers. However, the physical layer attacks that utilize natural phenomena (e.g., electromagnetic waves) to manipulate safety-critic signals such as analog sensor outputs, digital data, and actuation signals have recently taken the attention. The purpose of this dissertation is to detect the weaknesses of cyber-physical systems against low-power Intentional Electromagnetic Interference (IEMI) attacks and provide hardware-level countermeasures.

Actuators are irreplaceable components of electronic systems that control the physically moving sections, e.g., servo motors that control robot arms. In Chapter 2, the potential effects of IEMI attacks on actuation control are presented. Pulse Width Modulation (PWM) signal, which is the industry–standard for actuation control, is observed to be vulnerable to IEMI with specific frequency and modulated–waveforms. Additionally, an advanced attacker with limited information about the victim can prevent the actuation, e.g., stop the rotation of a DC or servo motor. For some specific actuator models, the attacker can even take the control of the actuators and consequently the motion of the CPS, e.g., the flight trajectory of a UAV. The attacks are demonstrated on a fixed-wing unmanned aerial vehicle (UAV) during varying flight scenarios, and it is observed that the attacker can block or take control

of the flight surfaces (e.g., aileron) which results in a crash of the UAV or a controllable change in its trajectory, respectively.

Serial communication protocols such as UART or SPI are widely employed in electronic systems to establish communication between peripherals (e.g., sensors) and controllers. It is observed that an adversary with the reported three-phase attack mechanism can replace the original victim data with the 'desired' false data. In the *detection* phase, the attacker listens to the EM leakage of the victim system. In the *signal processing* phase, the exact timing of the victim data is determined from the victim EM leakage, and in the *transmission* phase, the radiated attack waveform replaces the original data with the 'desired' false data. The attack waveform is a narrowband signal at the victim baud rate, and in a proof–of–concept demonstration, the attacks are observed to be over 98% effective at inducing a desired bit sequence into pseudo–random UART frames. Countermeasures such as twisted cables are discussed and experimentally validated in high-IEMI scenarios.

In Chapter 4, a state-of-art electrical vehicle (EV) charger is assessed in IEMI attack scenarios, and it is observed that an attacker can use low–cost RF components to inject false current or voltage sensor readings into the system. The manipulated sensor data results in a drastic increase in the current supplied to the EV which can easily result in physical damage due to thermal runaway of the batteries. The current switches, which control the output current of the EV charger, can be controlled (i.e., turned on) by relatively high–power IEMI, which gives the attacker direct control of the current supplied to the EV.

The attacks on UAVs, communication systems, and EV chargers show that additional hardware countermeasures should be added to the state-of-art system design to alleviate the effect of IEMI attacks. The fiber-optic transmission and low-frequency magnetic field shielding can be used to transmit 'significant signals' or PCB-level countermeasures can be utilized which are reported in Chapter 5.

Electromagnetic Interference Attacks on Cyber–Physical Systems: Theory, Demonstration, and Defense

Gökçen Yılmaz Dayanıklı

(GENERAL AUDIENCE ABSTRACT)

The secure operation of an electronic system depends on the integrity of the signals transmitted from/to components like sensors, actuators, and controllers. Adversaries frequently aim to block or manipulate the information carried in sensor and actuation signals to disrupt the operation of the victim system with physical phenomena, e.g., infrared light or acoustic waves. In this dissertation, it is shown that low-power electromagnetic (EM) waves, with specific frequency and form devised for the victim system, can be utilized as an attack tool to disrupt, and, in some scenarios, control the operation of the system; moreover, it is shown that these attacks can be mitigated with hardware-level countermeasures. In Chapter 2, the attacks are applied to electric motors on an unmanned aerial vehicle (UAV), and it is observed that an attacker can block (i.e., crash of the UAV) or control the UAV motion with EM waves. In Chapter 3, it is shown that digital communication systems are not resilient against intentional electromagnetic interference (IEMI), either. Low–power EM waves can be utilized by attackers to replace the data in serial communication systems with a success rate %98 or more. In Chapter 4, the attacks are applied to the sensors and actuators of electric vehicle chargers with low–cost over–the–shelf amplifiers and antennas, and it is shown that EM interference attacks can manipulate the sensor data and boosts the current supplied to the EV, which can result in overheating and fire. To ensure secure electronic system operation, hardware–level defense mechanisms are discussed and validated with analytical solutions, simulations, and experiments.

In memory of my father.

Acknowledgments

I would like to thank my supervisor Dr. Ryan Gerdes for his guidance throughout my doctoral research. I want to express my gratitude to Dr. Leyla Nazhand-Ali, Dr. Patrick Schaumont, and Dr. Mazen Farhood for their encouragement, and Dr. Cameron Patterson and Dr. Majid Manteghi for serving on my committee. Also, I want to thank Dr. Mani Mina for the deep discussions about life and research, and Roxanne Narsesian Paul for making this process a smooth one.

Lastly, I want to thank my mother, Sibel, and my sister, Gökçe, for being strong in the hard times and being content but not arrogant in the good times, your support is valuable.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Electromagnetic Interference (EMI) is a disturbance of a system from external electromagnetic radiation; EMI is a well-known phenomenon that disrupts the operation of electronic systems, which is already a point of interest for disciplines like electromagnetic compatibility (EMC) and signal integrity (SI). However, in EMC and SI domains, it is assumed that the undesired radiation is from a source (e.g., a transmission line carrying a clock signal) with a known position and radiation frequency. On the other side, electromagnetic waves can be used 'intentionally' to manipulate a system's operation, which is classified as Intentional Electromagnetic Interference (IEMI) in security literature. The attacker's freedom to choose the position and frequency of the radiation makes IEMI attacks a serious threat to signal integrity and secure system operation. The goal of this dissertation is to analyze the resilience of cyber-physical systems, e.g., unmanned aerial vehicles, in scenarios the attacker uses EM waves as an attack tool. The theoretical explanation of the attack scenarios is reported with experimental validations, and hardware-level countermeasures are investigated.

With decreasing transistor sizes, more calculation power can be achieved from a unit volume, which enables the system designers to move from traditional analog signal control to the advanced digital embedded system control [27]. Such changes have already been observed in physical infrastructures, e.g., power grids. On the other side, this maximized processing capability opens new horizons for system designers. For instance, an Unmanned Aerial Vehicle (UAV), equipped with many peripheral devices such as Global Positioning

System (GPS), accelerometer, and actuators, can be controlled autonomously by small-size controllers. Modern processors in CPSs process a vast amount of data from sensors and control the physical response of the system through the actuators. Although the improved processing power opens the way for high-end CPSs with many peripheral devices from sensors to actuators, the vast integration of these devices in a system poses many attack points for IEMI attacks.

1.1 Cyber-Physical Systems

A cyber-physical system (CPS) is an integration of computation, communication, and control elements. From smart grids to autonomous systems (e.g., drones), with the introduction of communication technologies like 5G that enables the integration of many devices, CPSs become more prominent in our lives. However, CPSs, which combine many subsystems and consequently weak points, become a target for adversaries as well. In 2015, a smart grid attack left a quarter-million people in Ukraine without electricity for hours [37]; In 2008, the Stuxnet targeting the Natanz nuclear plant in Iran halt the operation temporarily leaving physical damage on enrichment centrifuges [63]. These attacks have something in common, they exploit the weaknesses of a system to cause damage in the physical domain, and their effects are catastrophic.

A generic CPS, which is illustrated in Figure 1.1, employs sensors, actuators, and controllers. The sensors convert a physical property (e.g., speed) to an electric signal that is processed by the controller. The controller decides for the next state with a robust state algorithm and sends actuation signals to actuators (e.g. servo motor) which controls the physical sections of the CPS (e.g., aileron of a UAV). The operation of the system relies on the integrity and availability of the sensor and actuation data.

1.2 Physical Layer Attacks on Cyber-Physical Systems

Although software-layer attacks, which exploits the software domain weaknesses of CPSs, traditionally take more attention of researchers [27], physical-layer attacks, which utilizes a physical phenomenon (e.g., electromagnetic waves) to manipulate sensor or actuation data, are an important threat for secure CPS operation as well [43]. Researchers show that attackers can use electromagnetic waves [32, 57, 61, 93, 95], acoustic waves [73, 100, 109, 110], and Infrared (IR) signals [78, 94, 120] to attack electronic systems. The variety of attack modalities (e.g., electromagnetic), attack mechanisms (e.g., Analog to digital converter-ADC nonlinearity) and target devices (e.g., GPS) motivate researchers to provide systematic ways to describe physical layer attacks on CPSs [45, 121].

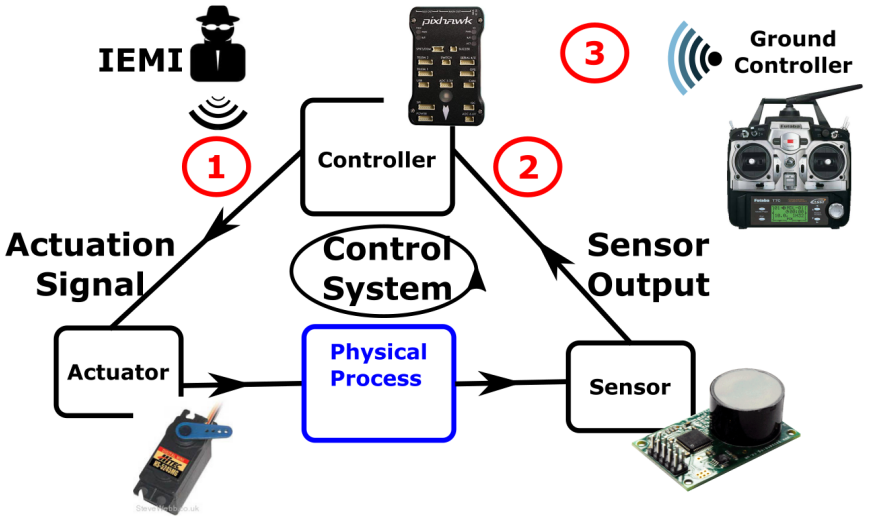


Figure 1.1: IEMI attacks target a variety of points in a cyber-physical system: Actuation Signal (1), sensor output (2), and radio control signal (3) can be manipulated or blocked (i.e., jammed) by an electromagnetic signal.

Attack Modality: Acoustic Waves

Acoustics waves are widely used by attackers to induce mechanical effects on devices like gyroscopic sensors, hard disk drivers, and accelerometers. Trippel et al. inject acoustics signals to capacitive MEMS-based accelerometers and conclude that the attacks are successful due to the flaws in filter and amplifier circuitry. They successfully inject 'fake steps' into a FitBit device through acoustic waves [109]. Son et al. report that 7 of 15 gyroscopic sensors tested in their study are vulnerable to intentional acoustic injection attacks, and drones equipped with vulnerable gyroscopes can be crashed with the reported attacks [100]. Tu et al. provides a systematic approach to control the output of inertia sensors by showing the effect of sensor manipulation on the performance of the control system [110]. Bolton et al. show that the head stack assembly of hard disk drivers can be vibrated out of operational bounds by acoustic waves which result in false positives in shock sensors and a loss of data throughput [21].

Attack Modality: Infrared (IR) and Visible Light

Although IR and visible light are technically electromagnetic waves, for convenience, they will be discussed separately from IEMI which utilizes waves at RF band (from a few Hz to 300 GHz). Park et al. show that an infrared source, which exploits the structural design of IR sensors in medical infusion pumps, can be used by an attacker to spoof and saturate the IR sensor and adjust the drug infusion rate to the patient [78]. Lidars, which are environment perception sensors and widely used in autonomous cars (e.g., Waymo), can be spoofed by Lasers [80]. Researchers show that relay attacks, which capture the victim's pulse and play it back to the system, can inject fake dots; also, by illuminating the lidar with a high-intensity source, the sensing ability of the lidar to that direction can be paralyzed [94].

1.3 Electromagnetic Waves as an Attack Modality

An electromagnetic (EM) wave is a general term that defines waves in all frequency spectrum that includes radio frequency, infrared, visible light, ultraviolet, and so on. In this work, the EM wave term is used for the lower end of the spectrum (from a few Hz to 300 GHz), which is also called the radio frequency spectrum in the communications discipline of electrical engineering. The Radio Frequency (RF) term is avoided to eliminate any confusion between the largely accepted name of the attacks (i.e., Intentional Electromagnetic Interference Attacks) that uses RF waves in the security community. The focus of this study is IEMI attacks that utilize EM waves in the RF spectrum, and attacks that employ waves in other parts (i.e., IR) of the spectrum are not the interest of this research.

Faradays's law of induction states that a time-varying magnetic field normal to the surface of a conductor loop induces a voltage in the terminals of the conductor [16]. Considering Ampere's law which states that any time-varying current generates a time-varying magnetic field [16], there are two ways for an adversary to utilize EM waves to attack a system. Firstly, the adversary can adopt a 'passive' approach and electromagnetically listen to the EM leakage of a victim system (with an antenna or a field probe) to extract secret information (e.g., a cryptographic key), which is called 'eavesdropping'. Secondly, the attacker can choose an 'active' approach, radiate an EM field on the victim circuitry, and induce a voltage to manipulate or physically damage the victim system. The former approach is called 'Intentional Electromagnetic Interference'.

1.3.1 Eavesdropping Attacks

From the early days of World War II, it is known that electronic devices emanate acoustic, optical, thermal, and electromagnetic waves largely correlated to their operation [26]. The

time-varying currents in an electronic system (e.g., cryptographic hardware) generates a magnetic field which can be eavesdropped on by an attacker with a field probe or an antenna; and the captured field can be processed to extract secret information, e.g., cryptographic key [60, 88, 112]. This attack vector, which is historically named as 'TEMPEST', is identified by bodies like NATO, and official guidelines are publicly shared to protect systems [7]. Sayakkara et al. review a variety of EM eavesdropping attacks on Internet of Things (IoT) devices [88]. The EM leakage of the computer screens (or TV screens with cathode ray tubes) lets attackers detect the image or text displayed on the screen [38, 51, 112]. In Section 3, an eavesdropping attack will be used combined with an intentional electromagnetic interference attack (IEMI) to demonstrate an IEMI attack on a digital communication system.

1.3.2 Intentional Electromagnetic Interference (IEMI) Attacks

IEMI attacks are classified as high-power or low-power IEMI [48]. In high power attacks, the attacker aims to physically damage the victim device through excessive EM power and thermal runaway of circuit components like resistors or transistors [49]. Backstrom et al. show that L and S-band EM waves, which are at the lower end of microwave spectrum and a field magnitude of $15\,\mathrm{kV\,m^{-1}}$ or more, damage the in input transistors of electronic systems [14]. Shurenkov and Pershenkov report that depending on the power level of the EM pulse, a hard-kill (e.g., permanent damage due to overheating) or soft-kill (i.e., disruption in the operation but not physical damage) occurs in semiconductor devices [96].

Unlike the IEMI attacks reported in this research, 'Communication jamming' attacks target the communication link between the ground/radio controller and the system with EM waves (Point 3 in Figure 1.1) [26]. For instance, in a jamming attack scenario on a UAV system, a ground controller sends the position control data (e.g., flight trajectory) through an RF

communication link, and an adversary transmits a wideband EM signal into the channel to obstruct the communication. Hooper et al. reported that Denial of Service Attacks can be applied to commercial UAVs utilizing Wi-Fi as the control system [52]. Samy Kamkar, with SkyJack attack, takes control of drones with malicious Wi-Fi signals [56]. Although 'communication jamming' blocks or alters the transferred data between the ground controller and main system (e.g., drone), its efficacy is limited when the victim device is in autonomous mode and the supervisor is not in control. Adding to that, controllers (e.g., PixHawk) can be deployed with robust state estimation and control algorithms [77] that mitigate communication jamming attacks.

IEMI attacks have been reported on light sensors, temperature sensors, speed sensors, implantable cardiac devices, and microphones [61, 93, 95, 111]. Although each attack starts with EM wave radiation at the resonance frequency of the targeted device, device-specific non-linearities, due to amplifiers [61, 111] and ADCs [93], can be exploited by attackers to manipulate the sensor data. The reader is referred to [45, 121] for a systematic description of mechanisms that results in sensor data manipulation due to EMI. Although sensor data manipulation is explained in these works, the false actuation injection attacks are not addressed, which is one of the contributions of this work.

Kune et al., with the first study that describes the low-power EMI as an attack tool on sensors, examine two types of cardiac devices: external electrocardiogram machines (ECG) and cardiac implementable electric devices (CIED)[61]. With an attack power of 10 W and a monopole antenna, it is reported that the attacker can induce an artificial pacing inhibition on CIEDs through the air from a distance of '1 m to 2 m'. However, when the cardiac devices are in a saline solution that simulates the human tissue, the attack distance decreases to 5 cm. This is an expected result because the attacker employs a monopole antenna with a dominant electric field that capacitively couples to the victim system; and as the saline solution is a

conductor, the E fields are not able to penetrate well which decreases the attack distance significantly. In the research subject to this dissertation, magnetic fields (i.e., inductive coupling) are utilized in attack scenarios, because of their capability to penetrate shielding.

Kune et al. also concluded that coupled RF signals to the victim PCB traces (or cables) between the microphones and amplifier are modulated due to the nonlinearities of amplifiers, passive components (e.g., capacitor diode couples), and ADCs, which results in an inband signal that is perceived as the legitimate audio signal sent from the microphone[61]. The amplifier nonlinearity is also exploited by Tu et al. in long-distance IEMI attacks on the temperature sensors of newborn incubators [111]; with an attack power of 4 W and attack distance of 1 m, the skin temperature can be artificially increased by 8.5°or reduced by 4.3°by adjusting attack frequency to 515 MHz and 910 MHz, respectively. Considering a directional log-periodic antenna is employed [111], and attack distances down to 0.2 m are tested, the coupling mechanism of the attack can be capacitive (antenna near field) or radiation (antenna far-field) and depends on the attack distance.

The headphone cables that connect the microphone and the mobile phone can act as receiver antennas which can be exploited to inject false audio commands into a mobile phone. Kasmi and Esteves demonstrate that an amplitude-modulated waveform, envelope of which is the voice command to be injected, with an attack power of 20 W injects false voice commands like "OK Google" and "Hey Siri" to a mobile phone [57]. They comment that these attacks have serious consequences; an attacker can "force the target to visit a malicious web page which exploits a vulnerability to compromise the target operating system." or "forces them to send a text message or place a call to a paid service."[57].

Shoukry et al. report IEMI attacks on the magnetic speed sensors of anti-lock braking systems (ABSs) [95]. The first attack, which is called 'disruptive', disrupts the speed data in an uncontrollable manner through radiated magnetic field radiated from a loop antenna; the

second attack, which is called 'spoofing', senses and erases (i.e., active shielding) the original magnetic field that carries the wheel speed information, and inject false speed information with a specially crafted magnetic field. The spoofing attack is demonstrated on a Mazda ABS, and by simulation results, it is concluded that the attacker can cause the victim to lose traction. The ABS attack has some important characteristics: first, the 'spoofing' attack 'eavesdrops' the victim's magnetic field, and then injects the false data into the sensors, unlike other examples that only radiate EMI without eavesdropping on the victim. This has similarities with false data injection attacks which is reported in Chapter 3. Second, the attacker uses time-varying magnetic fields to manipulate the victim system (i.e., inductive coupling), unlike other IEMI attacks [61, 111] in which capacitive coupling or radiation coupling is utilized.

In some scenarios, attackers can use static or very low-frequency magnetic fields as well. Hall sensors, operating principles of which are based on Lorentz force law, measure current with a reference external static magnetic field. An additional static magnetic field can be applied by an attacker to change the reference field to manipulate the current readings [19]. In this dissertation, the static magnetic fields are not a point of interest because the victim systems (actuators, sensors, and digital channels) require time-varying induced voltages that can only be induced by time-varying magnetic fields (Faraday's law of induction).

1.4 Outline and Research Focus

An IEMI attack targets sensor outputs (Point 1), actuation signals (Point 2), and communication signals (Point 2) in a cyber-physical system (Figure 1.1). There is a large body of literature on analog sensor attacks with IEMI [61, 93, 111]; however, to the best of the author's knowledge, the False Actuation Injection (FAI) attacks demonstrated in [32, 93] are

the first examples of an FAI attack with IEMI. This research aims to detect the weaknesses of actuation control applications in IEMI scenarios, demonstrate attacks on actual systems (e.g., UAVs), and provide countermeasures.

The focus of Chapter 2 is the IEMI attacks on Pulse Width Modulation (PWM) based actuation control. In the first section of the chapter, the weaknesses of PWM-based actuation control are analyzed, and a short-distance attack with a low-frequency sawtooth waveform is demonstrated. In the second part, the focus is to increase the attack distance with high-frequency attack waveforms with resonant inductive coupling. The attacks are demonstrated indoor and outdoor on an Unmanned Aerial System, and it is observed that the attacker can block or take control of the victim actuators.

In Chapter 3, the focus is the physical layer security of wired serial communication systems like UART or SPI, and in a proof-of-concept, it is shown that an attacker can flip-bits in a controllable manner (i.e., inject the desired data) with a success rate of 98% or more with the reported attack phases and waveforms. Countermeasures like twisted cables are suggested for digital transmission, which are validated with experimental results. Chapter 4 focuses on the IEMI attacks on sensors and actuators widely employed in power converters, which are utilized in extremely fast power converters for EV chargers. Three attacks, on current and voltage sensors and current switches, are demonstrated to show that both the sensor and actuation signals of power converters can be altered by intentional EMI which can result in extremely high current supply to the EV with catastrophic results. In Chapter 5, the focus is to provide physical layer methods (e.g., with shielding or PCB design) to mitigate IEMI, and an analytical model that relates the attacker field and induced voltage on the victim circuitry is reported to lay the basis of suggested countermeasures like shorter transmission lines for 'significant' signals and thinner PCBs which are validated with analytical and 3D electromagnetic simulations. In Chapter 6, two side-projects are discussed. The first one

is a design of a Rogowski coil to improve the side-channel attacks on cryptosystems with Correlational Power Analysis, the design procedure and the transfer function of the Rogowski coil is reported with simulation results. In the second part, the advantages and disadvantages of magnetic field radiators like solenoids or loops are discussed for inductively coupled IEMI, and a magnetic field array, with ferrite rods as an array element, is designed to improve the field focus by 31%.

Chapter 2

Electromagnetic Interference Attacks on Pulse Width Modulation–Controlled Actuators

A cyber-physical system (CPS) consists of integrated computational and physical components. The dynamics of physical sections (e.g., robotic arm) are controlled by actuators (e.g., servo motor) through actuation signals. The actuation signal carries the actuation data such as rotation angle or speed which controls the actuators like servo motors and DC motors, and the integrity of the actuation signal has utmost significance, as any distortion in the actuation data results in physical consequences and damage. In this chapter, the potential of intentional electromagnetic interference (IEMI) as an attack tool to manipulate the widely used Pulse Width Modulation (PWM)–controlled actuators (e.g., servo motors) is analyzed; a theory of actuator attacks is developed, and experimentally validated, to explain how these actuators can be manipulated with IEMI at certain frequencies and forms.

The discussion will start with the explanation of the actuation control with Pulse Width Modulation (PWM) signal and possible mechanisms an attacker can exploit to manipulate the actuation data through IEMI. In the following section, a short–distance attack, which utilizes a low–frequency sawtooth waveform to change the actuation data and control a servo motor, is reported and demonstrated [93]. In the next phase, the focus is on increasing the

attack distance with reasonable attack power and distance: It is experimentally shown that the control of widely used actuators (e.g., servos) can be manipulated by attack waveforms at certain frequencies and forms from appreciable distances. For some servo models, it is also possible for the attacker to take control of the victim actuator with the reported attack waveforms. Three attack waveforms, namely *Block*, *Block & Rotate* and *Full Control* are reported that can be utilized by an attacker to block and/or manipulate the actuation data encoded in the PWM and the efficacy of waveforms is tested on widely used servo models. An electromagnetic coupling model between the attacker antenna and victim PWM circuitry (e.g., cables) is presented to show that the attacker can utilize magnetic resonant coupling (similar to Wireless Power Transfer (WPT) Applications) for longer–distance or less–power attacks. Indoor and in–flight attacks are demonstrated on the actuators of an unmanned aerial vehicle (UAV), the effects of which are shown to seriously impact the safe operation of the victim UAV e.g., change in the flight trajectory. The attacks are demonstrated on DC motors during which the speed data encoded to PWM is distorted, and it is observed the EMI at relatively low frequencies (e.g., lower than 35 MHz) can halt the rotation of a DC motor.

2.1 Importance of False Actuation Injection

A generic CPS includes actuators, sensors, and a controller as illustrated in Figure 1.1. The controller processes the information streamed from the sensors and makes a decision for the next state and sends an actuation signal to actuators (e.g. servo motor) to move the physical section of the CPS. Pulse Width Modulation (PWM) is a widely used actuation signal, which carries the actuation information (e.g., rotation angle of a servo motor). The integrity of PWM is very important because any distortion in actuation data can result in loss of control of physical parts of the CPS. For instance, if the control of a motion surface (e.g., aileron) in a fixed-wing Unmanned Aerial Vehicle (UAV) is compromised, the UAV can deviate from

its original trajectory, and even crash.

Faraday's law of induction states that a time-varying magnetic field normal to a conductor loop results in an induced voltage at the terminals of the conductor [16]. An attacker can exploit this phenomenon with specific waveform and frequency fields to affect certain cables (e.g., PWM cables) to manipulate the operation of the victim system. In certain conditions (e.g., when the attacker resonate the victim cables.), the induced voltage can be large enough to block or change the actuation and sensor data lissutrated as Point 1 and 2 in Figure 1.1, respectively.

While a few-100 mVs induced voltage [93] is sufficient to manipulate analog sensor readings through ADC-clipping effect [47] and component-nonlinearities [61, 111], False Actuation Injection (FAI) requires an induced voltage comparable to the logic level (e.g., 5 V for TTL), which requires the attacker to utilize a high-power with an efficient coupling mechanism such as magnetic resonant coupling. Although analog sensor manipulation is possible with less power, its effect is also limited, to some extent, through the use of robust state estimators to detect and correct the false senor reading [77]. FAI attacks, on the other hand, are more difficult to counter because there is no control and decision mechanism (i.e., controller) between the attack point and the actuator Figure 1.1. That is, even should a controller detect the existence of an attack and send a 'recovery' actuation signal, the attacker still overrides or blocks this signal.

2.1.1 Related Work

EMI is a significant threat for the integrity of analog sensor outputs (Attack point 2 in Figure 1.1). Kune *et al.* reported baseband and modulated waveform attacks to inject false data to microphones and implantable cardiac devices [61]. An IEMI attack on magnetic speed

sensors of anti-lock braking system (ABS) is reported in [95]. Kasmi and Esteves show false voice commands to mobile phones can be injected through headphone cables with IEMI[57]. Analog sensor attacks generally relied on the nonlinearities of amplifiers or Analog to Digital Converters (ADCs) [32, 93] of the sensor systems.

Despite the large body of literature about analog sensor attacks with IEMI [57, 61, 95, 110], FAI attacks are not very common. A sawtooth waveform and a pulsed sinusoidal are suggested to inject false rotation angle to a PWM channel to control servo rotation [92, 93]. However, these methods have only been shown to work at relatively short distances and require synchronization with the targeted PWM signal. It was reported that the output current switches of a power charger can be turned on with a strong magnetic field, which can be classified as FAI[32]. Although jamming attacks (Point 3 in Figure 1.1) can be considered as a subclass of IEMI, they are fundamentally different from FAI because they target the communication channel with high power and large bandwidth waveforms [26, 59].

As the attacks will be demonstrated on a UAV, it is helpful to discuss the literature of UAV–attacks which are classified as wireless, hardware, and sensor spoofing attacks [59]. The wireless attacks take advantage of natural phenomena like acoustics, laser, and electromagnetic waves. Denial of Service attacks on Wi-Fi based commercial UAVs is demonstrated [52]. Samy Kamkar showed that multi–copter drones can be taken control of with WiFi signals through SkyJack attack [56]. Additionally, sensor spoofing attacks UAV GPSs and optical sensors are reported [30, 58].

2.1.2 Contributions

Although the short and long–distance attacks both target the PWM-controlled actuators, the attack mechanisms are different, e.g., long-distance attacks rely on magnetic resonant

coupling (MRC). The contributions in Section 2.3 that discusses short–distance FAI are [1]:

- Actuation control with PWM is analyzed from the perspective of an attacker, and a method, i.e., inducing a voltage drop to the PWM, to manipulate the actuation data is reported.
- A coupling model between the attacker and victim circuitry is derived to determine attack waveforms, e.g., as sawtooth, to manipulate actuation data.
- The attacks are demonstrated on a victim actuation operation that employs a microcontroller to generate a PWM and a servo motor. The attacker is successful in rotating the victim servo to one-direction; however, the attack range is limited to the proximity of the victim, i.e., the attacker field radiator should be placed around victim PWM cables. Additionally, the attacker waveform should be synchronized to the victim PWM which requires additional hardware, i.e., a receiver.
- The efficacy of defenses such as low–frequency magnetic field shielding is addressed.

In Section 2.4, the limitations of attacks in Section 2.3 (e.g., short attack distance, synchronization) are addressed with high frequency attack waveforms and magnetic resonant coupling. The contributions are as follows:

- Three attack waveforms are devised, namely *Block*, *Block & Rotate*, and *Full Control*, which consist of amplitude modulated signals matched to the resonant frequency of the victim PWM circuitry. While *Block* prevents actuator control, *Block & Rotate* and *Full Control* are shown to be capable of controlling the actuator rotation for certain servo models.

[1] The false actuation injection attack with sawtooth waveform is the contribution of the author to [93], which is acknowledged by the co-authors.

- An electromagnetic (EM) analysis is presented to determine the optimal attack parameters that maximize attack efficacy with distance. The analysis allows an attacker to determine the coupling ratio between an attacker antenna and victim PWM circuitry. From this the (resonant) frequency at which power from the attack setup can be delivered with the greatest efficiency can be found, thereby lowering the cost of attack.

- An attacker system that consists of an optical transmitter, RF module, attacker antenna, and carbon fiber frame is designed and mounted on a fixed-wing UAV for in-flight proof-of-concept validation of the attack waveforms. The *Block* and *Full Control* attacks are demonstrated and the flight data (e.g., aileron rotation, roll angle, and trajectory) during the attacks are reported.

- The effectiveness of countermeasures (e.g., optical signaling and shielding) to mitigate IEMI attacks on actuators are discussed.

In the interest of spurring research on IEMI attacks, an analytical and experimental method to detect the resonant frequency of victim circuitry is reported. A Zero Phase Shift Line (ZPSL) resonant antenna is designed and produced for attack demonstrations, which is believed to be useful to other researchers investigating IEMI attacks.

2.2 Actuator Control with Pulse Width Modulation

A PWM is a rectangular signal with a fixed period, t_{PWM}, of 20 ms as illustrated in Figure 2.1a. The time duration (i.e., pulse width), t_{high}, gets values between 1 ms and 2 ms and carries the actuation information such as rotation angle or speed (i.e., rpm) depending on the type of the actuator, e.g., speed for a DC motor. For clarity, the PWM operation

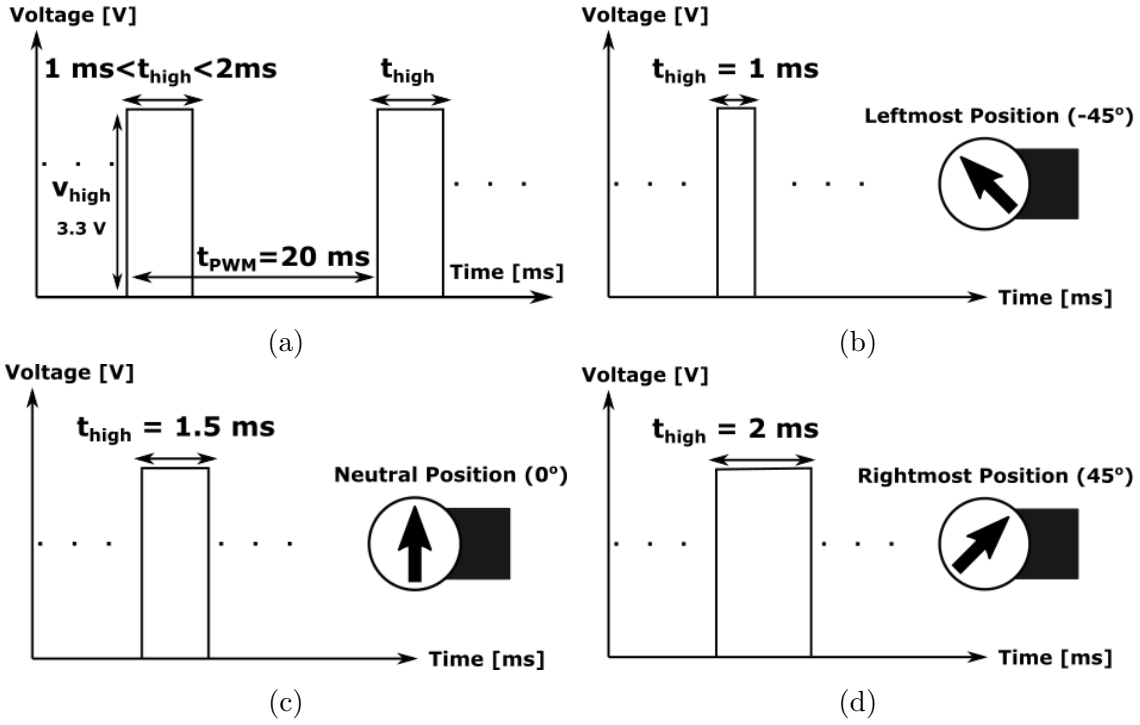


Figure 2.1: Actuators such as servo and DC motors are controlled with PWM. (a) PWM signal has a rectangular form. (b) $t_{high} = 1\,\text{ms}$, servo motor rotates to leftmost position. (c) $t_{high} = 1.5\,\text{ms}$, servo motor rotates to center position. (d) $t_{high} = 2\,\text{ms}$, servo motor rotates to rightmost position.

is explained for a servo motor application in which the PWM carries the rotation angle data; however, the same mechanism (i.e., data encoded to t_{high}) is utilized for DC motor applications in which the rotational speed (rpm) is transferred. A generic servo spans an overall rotation angle of 90°and rotates in the clockwise direction with increasing t_{high}. For instance, $t_{high} = 1\,\text{ms}$, $1.5\,\text{ms}$, and $2\,\text{ms}$ corresponds to the rotation angles $-45°$, $0°$, and $45°$ respectively, as illustrated in Figure 2.1b, 2.1c and 2.1d. The servo motors can be analog or digital depending on how the incoming PWM is processed. Due to their fast response, accurate positioning, reliability and larger torque, digital servos are preferred to analog ones in CPS applications (e.g., fixed-wing UAVs, surgical robots). The digital servos in Figure 2.2 are tested in varying attack scenarios which are reported in Section 2.4

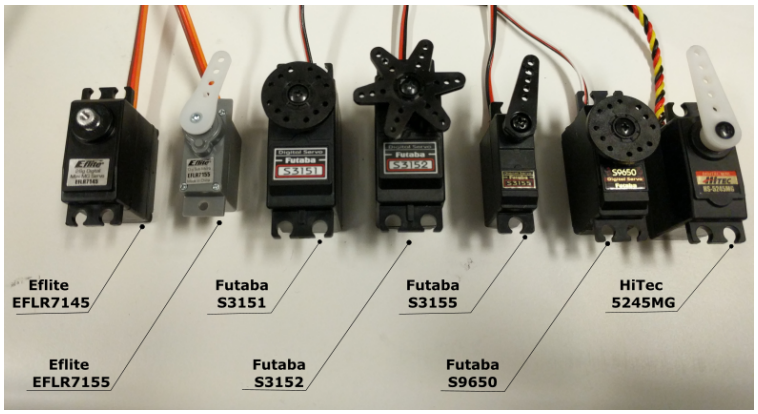


Figure 2.2: Digital servos, widely used in CPS applications, are tested in varying attack scenarios.

2.3 Short-Distance False Actuation Injection

The actuation data is encoded to the pulse duration, t_{high}, of the PWM so, if an attacker aims to prevent or manipulate the actuation data, s/he should focus to distort or change the PWM pulse.

2.3.1 Threat Model for Short-Distance False Actuation Injection

For short-distance FAI, an attacker, that radiates EMI to change the actuation data and control the victim actuator, is assumed. The attacker and the victim circuitry are not physically connected and all the interaction between the attacker and the victim circuitry takes place through electromagnetic waves. The attacker can acquire COTS hardware such as an oscillator, an audio amplifier, a power resistor, and a ferrite toroid. The attacker can approach the victim circuitry (e.g., PWM cables) to locate the field radiator which can be a magnetic field generator, e.g., a toroid or a solenoid. Additionally, the attacker has the timing information of the victim PWM signal to synchronize the attack waveform to the victim PWM pulse. The victim is a fully operational actuation system with a DC supply, a

PWM generator, and an electric motor (servo or DC).

2.3.2 Mechanism for Short-Distance False Actuation Injection

In Section 2.2, it is concluded that the victim t_{high}, which carries the actuation data, should be modified by the attacker to control the actuator (e.g., servo motor). However, it is not clear how the digital servo process PWM and determines the data, i.e., t_{high}. Different techniques to detect t_{high} can be in use: For instance, the DC average of the PWM (e.g., LPF) or the time duration between the rising and falling edges of the PWM pulse can be used to detect t_{high}. To determine the specific mechanism utilized by the victim servo (Futaba S3152), a DC voltage smaller than the supply voltage is applied to the PWM input of the servo motor, and it is observed that servo motor is unresponsive. This observation proves that the DC average is not used for t_{high} detection. It can be hypothesized that the digital servo is looking for the rising and falling edges of the PWM signal and detect t_{high} with a timer. To check this hypothesis, a voltage drop of varying amplitude and duration is added to a legitimate PWM with an OPAMP adder as depicted in Figure 2.1. The victim servo, Futaba S3152, is observed to use the time difference between the rising and falling edges of the signal to calculate the rotation angle. The blue waveform in Figure 2.3 shows a PWM signal with an added voltage drop, which causes the servo to detect a 1.5 ms duration signal as opposed to the original duration, 2 ms. Thus, when the frequency of the induced voltage drop and victim PWM is the same (i.e., the attacker and victim are synchronized), the phase of the attack waveform can be adjusted to the desired false actuation data or t_{high}.

To determine the minimum amplitude and duration of the induced voltage for a successful attack, the amplitude and duration of the voltage drop is varied and the servo response is observed. A voltage drop of 2.2 V with a duration of 5 µs is observed to be the minimum

voltage for rotating the servo. In other words, an attacker able to induce a waveform at the victim circuitry that creates at least a 2.2 V voltage drop for 5 µs, will cause the perceived t_{high} to be decreased and hence cause the servo to rotate in one direction (clockwise as shown in Figure 2.3 (Futaba S3152 has a different gearbox configuration and rotates counter-clockwise with increasing t_{high} as opposed to the illustration in Figure 2.1).

In the threat model, it is assumed the period of the PWM signal, which is generally a fixed value in CPS applications (e.g., $t_{PWM} = 20\,\text{ms}$ for UAV applications Figure 2.1a), is known by the attacker. It is also assumed that the attacker knows the exact timing of the original PWM, which is possible by eavesdropping victim PWM signal (An attack demonstration with eavesdropping is reported in Chapter 3 which has a similar mechanism and can be implemented with this attack as well.). However, even though t_{PWM} and phase of the victim UAV are not known, an attacker can move the servo in one direction in an uncontrolled manner, as the attacker signal would sweep the original PWM signal and randomly reduce t_{high} in the case of the non-synchronized attacker and victim frequencies.

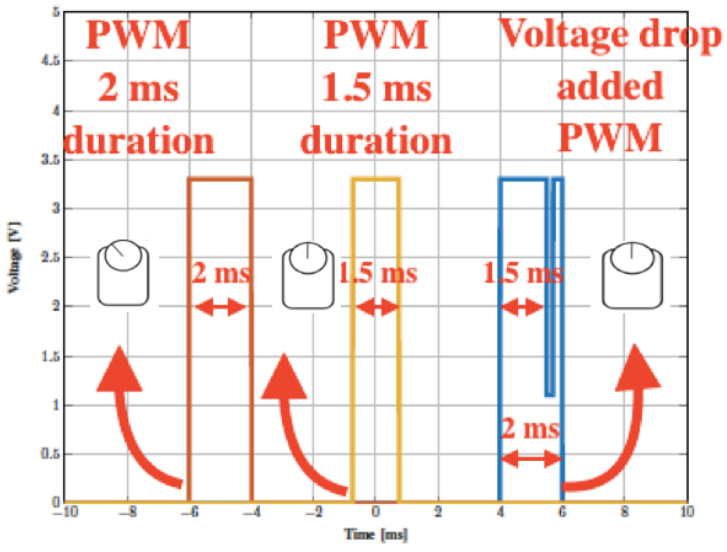


Figure 2.3: Adding a voltage drop to a PWM with $t_{high} = 2\,\text{ms}$ (blue) spoofs and rotates the servo to an angle determined by the position of voltage drop [93]. An attacker can use voltage drops to determine the actuation data, e.g., rotation angle.

A voltage drop on the victim PWM manipulates the actuation data; nevertheless, the relationship between the attack waveform, v_A, and induced waveform, v_{ind}, is still needed to determine an effective attack waveform to induce a voltage drop. It is assumed that the attacker employs a ferrite toroid to generate magnetic fields and the lumped circuit model (Figure 2.5c) with a magnetoquasistatic solution is employed to determine the voltage relationship [64, 113]. is used to determine the relationship between the attack waveform, v_A, (the waveform on the attacker radiator) and induced voltage in the victim circuitry, v_{ind}. The coupling model assumes that the victim PWM coil is around the attacker toroid and captures all the magnetic flux generated by the toroid. This relationship will be validated with measurement results in the setup given in Figure 2.4. The ferrite toroid with coils

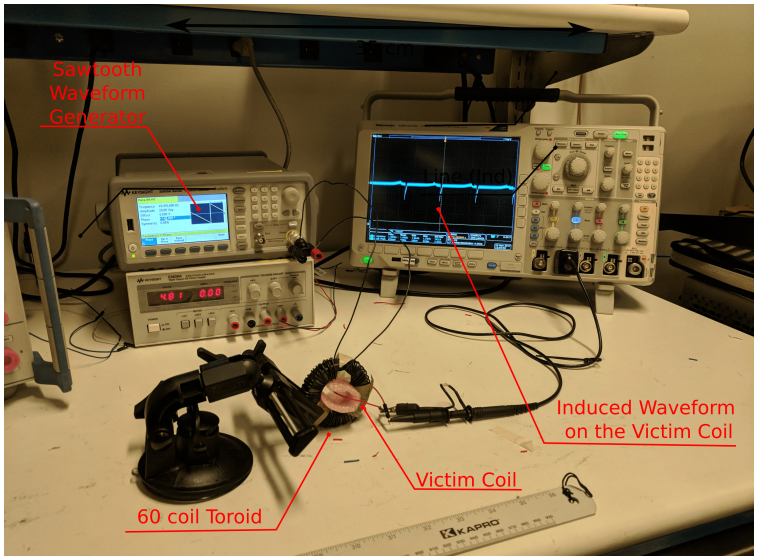


Figure 2.4: The attacker voltage, v_a, and induced voltage, v_{ind}, relationship (2.6) is validated with experiments.

has a dominantly inductive characteristic at low–frequencies where the parasitic capacitance (generally due to the closely spaced coils) is negligible. The relationship of the time–varying attacker current, i_a, and induced voltage, v_{ind}, is [123]:

$$v_{ind}(t) = \kappa \frac{d}{dt} i_a(t) \tag{2.1}$$

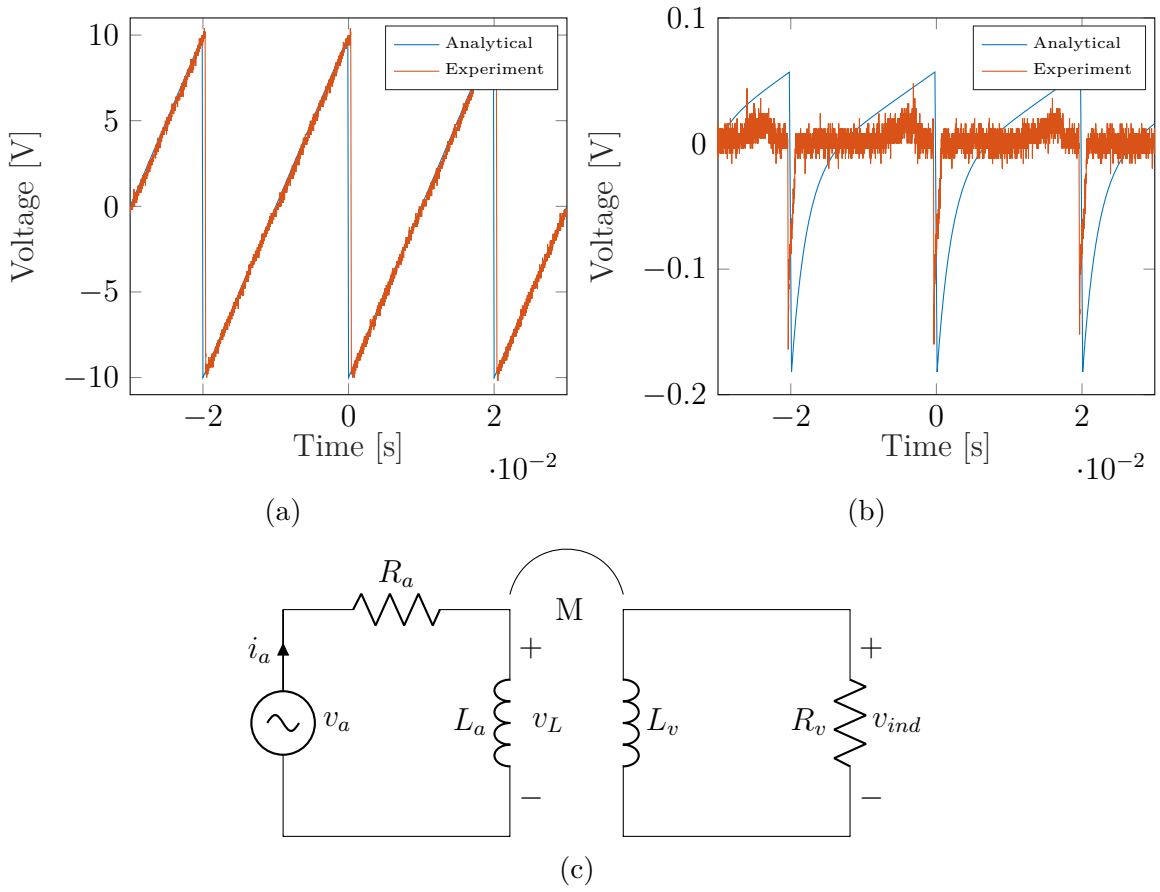


Figure 2.5: The results for the validation of v_a and v_{ind} relationship (2.6) is reported. (a) A sawtooth waveform is an efficient way of inducing voltage drops. (b) Analytically found (2.6) and measured induced voltages are aligned. A sawtooth waveform induces a voltage drop with a short duration in the victim coil. (c) The lumped circuit models assume that the attacker and victim are inductively coupled, which is the case in practice due to the magnetically–dominant nature of the attacks.

where κ is the mutual inductance between the attacker toroid and victim PWM cable. (2.1) shows that the induced voltage v_{ind} is linearly related to the time derivative of the attacker current, i_a. Thus, an attack waveform, v_a with a sharp decrease in a very small amount of time, is a good candidate to produce voltage drops at the target. A sawtooth waveform is just such a waveform and selected as the attack waveform, v_a, in the following sections

(Figure 2.5a). The mutual inductance, κ, in (2.1) is found as follows for the attacker toroid:

$$\kappa = \frac{\mu_f \, N \, t}{2 \, \pi} \, \ln\left(\frac{r_{outer}}{r_{inner}}\right) \tag{2.2}$$

where μ_f is the permeability of the toroid material (e.g., ferrite), N is the coil number, r_{outer}, r_{inner}, and t are the outer radius, inner radius, and thickness of the ferrite toroid with a rectangular cross section, respectively.

(2.1) provides the relationship between the attacker current, i_a, in toroid coils and induced voltage in the victim PWM cables (v_{ind}). i_a in terms of v_a can be derived using an R–L circuit model shown in Figure 2.5c. The attacker resistance, R_a, represents the copper losses and any additional series resistor to the toroid. L_a is the inductance of the toroid. The parasitic capacitance of the coils in the toroid is ignored because of the low attack frequency. On the other side, R_a should be included, because at low frequencies the reactance due to toroid is relatively small and copper losses become comparable to the reactance. The time–varying voltage, v_L, across the inductance representing the toroid is related to the attacker current i_a as follows:

$$v_L\,(t) = L_a \, \frac{d}{dt} i_a\,(t) \tag{2.3}$$

The relationship between the time varying attacker voltage (e.g., at the output of the atatcker waveform generator), v_a, and voltage on the toroid, v_L, can be found with the impulse response of an R-L circuit [12]:

$$v_L(t) = \int_{-\infty}^{+\infty} v_A(t-\tau)\, h_{RL}(t) d\tau \tag{2.4}$$

where h_{RL} is the transfer function for the attacker circuitry (Figure 2.5c).

$$h_{RL}(t) = \delta(t) - \frac{R_a}{L_a} e^{-\left(\frac{R_a}{L_a}\right)t} u(t) \tag{2.5}$$

where $u(t)$ is the step function. By combining (2.1), (2.4), and (2.5), the voltage induced at the victim circuitry is as follows:

$$v_{ind}(t) = \frac{\kappa}{L_a} \int_{-\infty}^{+\infty} v_a(t-\tau)\, h_{RL}(\tau) d\tau \tag{2.6}$$

(2.6) is numerically evaluated in MATLAB and is validated with the experimental setup shown in Figure 2.4. A single coil PWM cable is wrapped around a 60 coil toroid with an air gap and a sawtooth waveform is applied as attack waveform v_a (Figure 2.5a). It is observed that the analytical (2.6) and experimental results are aligned. While the sharp voltage drop of sawtooth waveform v_a results in a sharp voltage drop in the victim coil, the slowly increasing section of sawtooth has a negligible effect (Figure 2.5b). A square wave can be chosen as an attack waveform as well with voltage drops and peaks induced on the victim PWM. Additionally, inverting the sawtooth waveform (i.e., with a very steep increase) results in a voltage peak instead of a drop. The discrepancy in the recovery times of the waveforms can be due to the limited current supply capability of the attacker waveform generator (Agilent 33600A).

2.3.3 Demonstration of Short-Distance False Actuation Injection

In order to observe the efficacy of sawtooth waveform for false actuation injection, the experimental setup shown in Figure 2.6 is used. One coil of the PWM cable that transfers the PWM signal to servo motor is wound around the toroid, and the servo motor response is observed. Although it is not necessary to wound the PWM cable around the toroid (less in amplitude but similar in pattern v_{ind} is observed when the PWM cable is 'only' positioned inside the toroid), adding a coil increases v_{ind}. As the attacker H field drops off sharply outside the air gap of the toroid, producing an effect at a distance requires the

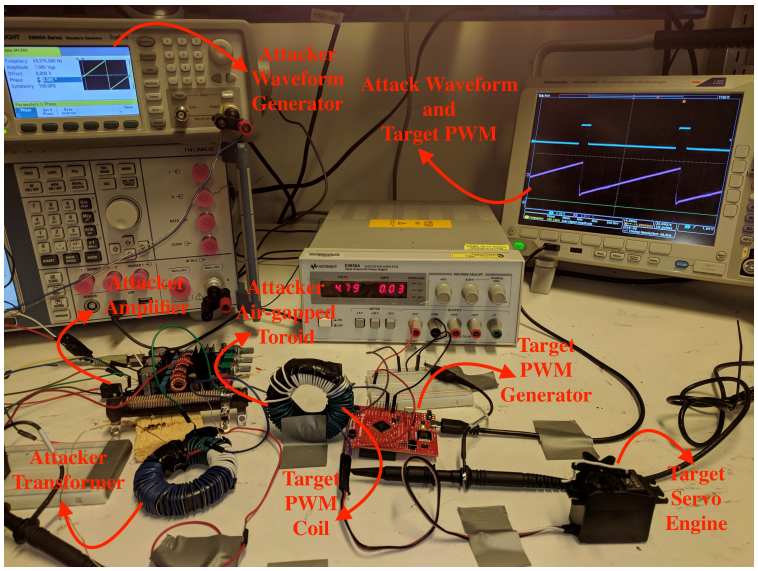
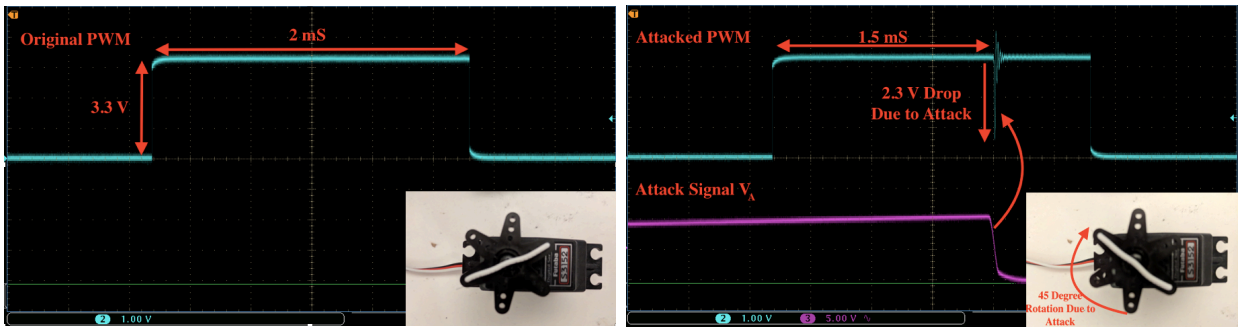


Figure 2.6: The experimental setup is used for attack demonstrations with a sawtooth waveform.One coil of the victim PWM cable is wound around the toroid, and the servo motor response is observed.

proper selection of a magnetic field directivity element, which is practically challenging due to the divergence free nature of magnetic field ($\nabla \cdot B = 0$). However, the limitation on the attack distance can be relieved with higher frequency attack waveforms which is disccussed in Section 2.4. The attacker waveform, which is in sawtooth form with a 5 Vpp at 50 Hz, is amplified with an audio amplifier with a rated power of 4 W. The induce voltage drop is 2.3 V, as measured at the PWM input of the servo motor as shown in Figure 2.7b. As this voltage drop caused the signal observed by the servo engine to exceed the thresholds for a legitimate downward transition (edge), the apparent PWM duration was decreased to 1.5 ms. This resulted in a clockwise rotation of the servo by 45°. To hold the servo at this angle, the frequency of v_a was locked to that of the legitimate PWM signal and the phase of v_a is adjusted to the desired t_{high} , i.e., rotation angle. Changing the phase of the attacker waveform rotates the victim servo to other rotation angles as well (Attack Video). In a subsequent experiment, the frequency of $V_A(t)$ is increased to 60 Hz while leaving the PWM signal at 50 Hz. When the attacker waveform is not synchronized to the victim



(a) (b)

Figure 2.7: The short distance actuation control is achieved through an induced voltage drop. Attack Video (a) When the attack is not implemented and $t_{high} = 2\,\text{ms}$, the servo rotates to the leftmost position. (b) When the voltage drop is positioned 1.5 ms after the rising edge, the servo rotates to the neutral position which corresponds to a compromised pulse duration of 1.5 ms, while the victim pulse duration, t_{high} is 2 ms.

PWM, the servo changes positions randomly because of the sweeping nature of voltage drop in the high voltage section of victim PWM. The short-distance FAI demonstration shows that an attacker, with low cost hardware like audio amplifier and toroid, can manipulate servo motor rotation by injecting voltage drops to PWM signal. However, due to the low frequency nature of the attack waveform, some limitations exist. First of all, the attacker radiator (e.g., toroid) should be placed very close to the victim circuitry. Secondly, the attacker is limited to rotate the servo motor to one direction (clockwise) because the voltage drop has only the effect of decreasing t_{high}. However, an inverted sawtooth waveform, which induces voltage peaks instead of drops, is observed to be a possible way to increase t_{high} and consequently to rotate the servo to other direction (i.e., counterclockwise). In Section 2.4, higher frequency modulated attack waveforms and more efficient coupling scenarios will be reported for long-distance attacks.

2.4 Long–Distance False Actuation Injection

In Section 2.3, a low–frequency (50 Hz) sawtooth waveform that generates an 'artificial' voltage drop on a PWM signal to depreciate the actuation data is reported. The sawtooth waveform has three main drawbacks: first, the attack distance is limited to a few cm*s*; second, the induced rotation is to one direction (e.g., clockwise) because the attacker can only decrease t_{high} with a voltage drop; third, the attacker needs to 'synchronize' to the victim to align the induced voltage drop. In this section, these limitations will be addressed with high–frequency (e.g., VHF–band) attack waveforms that exploit the victim resonance through magnetic resonant coupling (MRC).

2.4.1 Threat Model for Long–Distance False Actuation Injection

The threat model assumes an attacker aims to block or take over the control of PWM-based actuators with EMI. For an EM coupling discussion specific to attack scenario based on Faraday's law of induction [82], the reader is referred to Section 2.4.3. Throughout the attacks, there is no physical contact between the attacker and the victim hardware. Unlike high power EM attacks, in which the attacker aims to damage the victim circuitry and operation with excessive EM power [49], the FAI attacks are low–power and untraceable, and only intend to alter the victim PWM signal through EM coupling. The maximum attack power is limited to 20 W, which is obtainable with COTS amplifiers. In the first attack scenario which requires less–power, the attacker aims to block the actuation data to incapacitate the victim actuation control but not to inject false commands. In the second attack scenario, the attacker also aims to inject false actuation data to take control of victim actuators. The attacker has access to RF components like amplifiers and antennas, as well as information about the topology of the victim system, e.g., the estimated length of PWM

cables.

2.4.2 Waveforms for Long–Distance False Actuation Injection

A wired setup (Figure 2.8), in which the attack waveforms are added to the victim PWM and fed to the actuators, is adopted to test the response of the actuators to the reported attack waveforms. The wired–setup (i.e., conducted) minimizes the noise and the effect of the antenna pattern, which is essential for a wireless setup. Additionally, the wired setup renders the accurate measurement of minimum attack voltage and frequency levels for successful attacks possible. The victim side is a fully-operational UAV– motion surface control system with Futaba S3155 servo motors (Figure 2.8). A Futaba Ground/Radio Controller that relays the control from the operator to a UAV Autopilot (e.g., Pixhawk) is employed. Autopilot converts incoming control information to an actuation signal and sends the PWM signals to the servo motors. The attack waveform is added to the PWM with a DC–4200 MHz combiner. A voltage buffer is added to keep intact the victim PWM form. The attack waveform carrier is generated by a Rohde & Schwarz SMU 200 Vector Signal Generator during all attack scenarios. In the *Block & Rotate* and *Full Control* attacks, a Keysight 33600A Waveform Generator is added to the setup for envelope signal generation.

Previously Reported Attack Waveforms

A relatively low–frequency (10 MHz) *Pulsed Sinusoid* is suggested to extend the pulse duration, t_{high}, and rotate the servo to one direction [92]. However, like the sawtooth waveform in Section 2.3, the attack is limited to one-direction, requires synchronization (i.e., an additional receiver to detect the EM leakage of the victim PWM), and limited to short–distance as none of the resonant coupling mechanisms are utilized.

Attack Waveform I: Block

A *Block* attack is a continuous wave signal at the frequency f_a as shown in Figure 2.9a. This waveform induces a voltage in the victim PWM cable, which prevents the servo from detecting the rising and falling edges of the original PWM. The efficiency of the attack depends on the attacker frequency (f_a) and victim resonant frequency (f_v). The attacker can use victim resonant frequency (e.g., aileron PWM cable) to increase attack distance significantly. An analytical and experimental approach to estimate or measure the resonant frequency of the victim PWM circuitry will be provided in Section 2.4.3.

Wired Setup Results for Block Waveform: A *Block* waveform with a peak value (V_p) and frequency (f_a) (Figure 2.9a) is applied to the servo models in the wired setup (Figure 2.8). The following procedure is followed with frequencies (f_a) of 8.75 MHz, 17.5 MHz, 35 MHz, 70 MHz, and 140 MHz. The frequencies are chosen close to the resonance of the PWM cables of the fixed-wing UAV.

1. Establish servo control through ground radio controller.

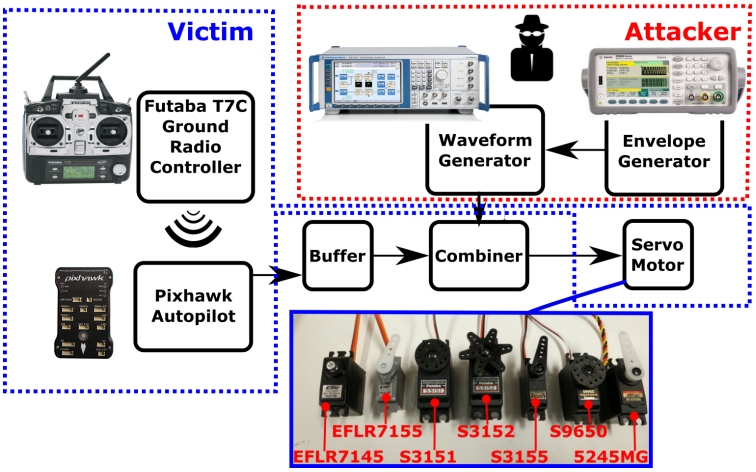


Figure 2.8: The reported attack waveforms are tested in a wired experimental setup on different servo models.

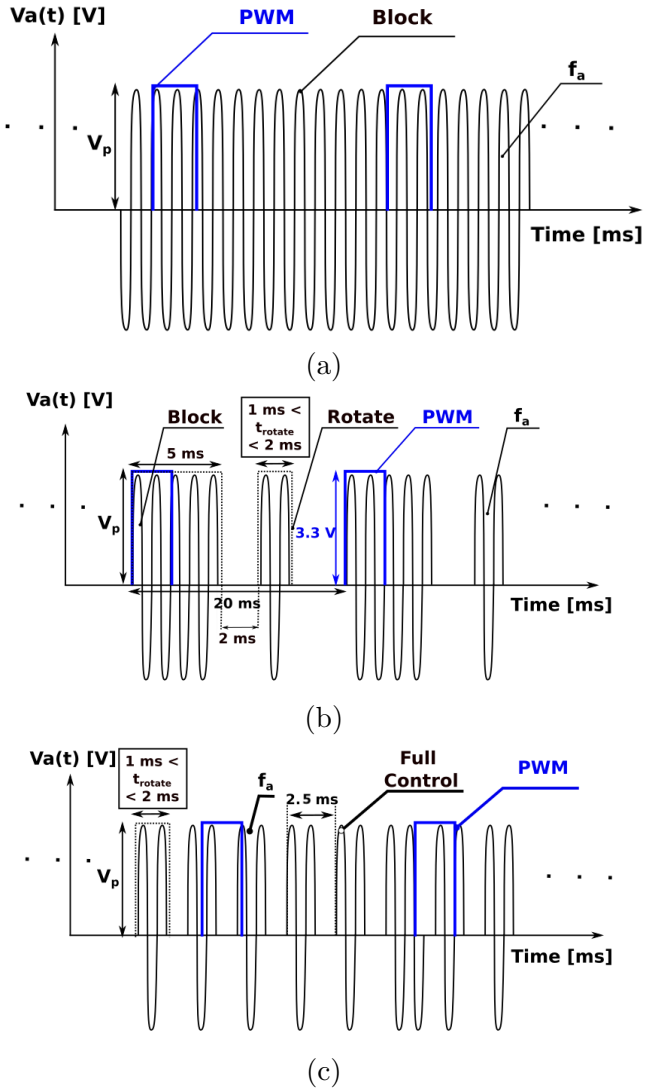


Figure 2.9: Attack waveforms (a) *Block* waveform disables the legitimate PWM (blue) (b) *Block & Rotate* waveform consists of two pulses: *Block* pulse eliminates the victim PWM and *Rotate* pulse injects the false rotation angle. (c) *Full Control* injects frequent pulses with a false rotation angle encoded in t_{rotate}.

2. Inject *Block* waveform starting from -30 dBm with 1 dBm increments.

3. Detect minimum V_p for successful attack (i.e., ground controller is not able to control servo rotation).

The gray boxes (Table 2.1) display the successful attacks (i.e., the control of servo motor is

Table 2.1: Block Attack is successful on all servo models (gray boxes). Minimum peak voltage V_p for varying frequencies is reported for successful attacks. (MF: Moves Freely, L: Locks)

f_a	8.75 MHz	17.5 MHz	35 MHz	70 MHz	140 MHz
Eflite EFLR 7145	1.14 V (L)	1.48 V (L)	0.69 V (L)	2.10 V (L)	7.20 V (L)
Eflite EFLR 7155	0.56 V (L)	1.01 V (L)	1.14 V (L)	2.14 V (L)	6.50 V (L)
Futaba S3151	0.51 V (MF)	2.88 V (MF)	1.32 V (MF)	6.55 V (MF)	10.11 V (MF)
Futaba S3152	0.52 V (MF)	1.55 V (MF)	1.30 V (MF)	6.70 V (MF)	9.10 V (MF)
Futaba S3155	0.57 V (MF)	1.83 V (MF)	1.26 V (MF)	5.45 V (MF)	4.12 V (MF)
Futaba S9650	0.74 V (MF)	2.04 V (MF)	1.18 V (MF)	5.50 V (MF)	3.76 V (MF)
HiTec HS5245MG	2.28 V (L)	2.12 V (L)	2.68 V (L)	7.35 V (L)	4.28 V (L)

lost). It is observed that all servo models can be blocked with varying attack powers (V_p); however, some servo models are more sensitive to the *Block* waveform. The Eflite models can be blocked with lower V_p values up to 70 MHz; another observation is that Futaba servos move freely (i.e., an external torque can move them.) during an attack, while Eflite and HiTec servos lock to the rotation angle before the attack begins. Especially lower frequencies around $f_a = 8.75$ MHz requires lower V_p for successful attacks, the authors believe this is due to the low pass characteristic introduced by the shunt capacitance at the input of the servo microcontroller pin. It should be noted that the efficient attack frequency is a combined effect of victim resonance and servo frequency response given in Table 2.1.

Attack Waveform II: Block & Rotate

The *Block* waveform, discussed in Section 2.4.2, prevents the transmission of the rotation angle data to the actuators. However, a more advanced waveform is required to inject false rotation angle information into the PWM signal. To achieve this, the attacker needs to eliminate (i.e., mask) the original rotation angle data encoded in t_{high} and then inject the false data to the PWM channel. An attacker employs a wide–pulse ($t_{high} > 2$ ms) to override the original rotation angle data.

To test this hypothesis, the following test procedure is followed. Each servo is rotated to the

Table 2.2: Servo motor response when t_{high} is longer than standard maximum duration 2 ms. t_{PWM} is fixed and 20 ms .

Servo Type	$t_{high} > 2$ ms
Eflite EFLR 7145	Locks
Eflite EFLR 7155	Locks
Futaba S3151	Moves freely
Futaba S3152	Moves freely
Futaba S3155	Moves freely
Futaba S9650	Moves freely
HiTec HS5245MG	Locks

neutral position (Figure 2.1c) and then a PWM signal with an out of range t_{high} is applied and the servo rotation is observed. During measurements, t_{PWM} and V_{high} are kept constant at 20 ms and 3.3 V, respectively. It is observed that all tested servo models stay at their position when t_{high} is larger than 2 ms (Table 2.2). While Eflite and Hitec servos lock (i.e., an external torque can not move them.), it is observed that Futaba servos move freely. The response of Eflite and Hitec is possibly a precaution to keep the servo rotation stable in high-noise situations when rotation angle data is distorted. This observation also points to a weakness of servo motor control with PWM. An attacker can inject a long enough *Block* pulse on top of t_{high} and simply block the original rotation angle as illustrated in Figure 2.9b. However, an additional sinusoidal pulse should be used to inject the false rotation angle information. The duration of the rotate pulse (t_{rotate}) determines the false rotation angle injected into the channel. For instance, the attacker can adjust t_{rotate} to 1 ms, 1.5 ms, and 2 ms to rotate the actuator to -45°, 0°, and 45°, respectively.

Wired Setup Results for Block & Rotate Waveform: The test procedure explained in Section 2.4.2 is followed in the wired setup (Figure 2.8). The attack waveform is synchronized to the original PWM with an oscilloscope by adjusting the attack waveform delay. The grey boxes in Table 2.3 correspond to the successful attack cases in which the attacker can control the rotation of the servo with varying t_{rotate} (Figure 2.9b). The Eflite–make servos respond to the applied attack waveform by locking to a rotation angle depending on the servo model

and f_a. However, changing t_{rotate} does not result in a change in the servo position. The author thinks that the microcontroller of Eflite servo is saturated due to the waveform and can not detect the rising and falling edges of the Rotate pulse which carries the false rotation angle information (Figure. 2.9b).

Futaba and HiTec servo models can be controlled by the *Block & Rotate* attack. A clear correlation between the increasing f_a and V_p is observed for attack success. In the applied power range, the HiTec can be controlled by applying an attack waveform with $V_a = 3\,\text{V}$ and $f_a = 8.75\,\text{MHz}$; however, at higher frequencies, the attacks are not successful. All of the Futaba models can be controlled by *Block & Rotate* at $f_a = 70\,\text{MHz}$ and $f_a = 140\,\text{MHz}$, and the attacks at $f_a = 70\,\text{MHz}$ require significantly less attack power on Futaba models. *Block & Rotate* enables the injection of false rotation angle information to the PWM channel, but it also requires the attacker to synchronize the *Block* pulse to the victim PWM signal. Although synchronization is possible through the detection of the magnetic field leakage from rising and falling edges of the victim PWM, practically it is difficult. First of all, multiple PWM signals controlling the servo motors emit a combination of fields and it is computationally demanding to select the desired PWM signals. Adding to that, the EM leakage power from the rising and falling edges is significantly low due to the limited peak voltage of PWM (5 V for TTL). Finally, even though near field magnetic antennas are utilized efficiently, the

Table 2.3: Block & Rotate is successful on Futaba and HiTec models (gray boxes). The minimum peak voltage V_p for varying frequencies is reported. (FC: Full Control, RM: Random Movement, LA: Locks At, NC: No Control)

f_a	8.75 MHz	17.5 MHz	35 MHz	70 MHz	140 MHz
Eflite EFLR 7145	1.64 V (LA 0°)	1.74 V (LA 0°)	1.66 V (LA 0°)	1.3 V (LA 0°)	6.6 V (RM)
Eflite EFLR 7155	NC	1.46 V (LA 30°)	NC	6 V (LA 30°)	5.5 V (LA 60°)
Futaba S3151	1.84 V (FC)	NC	NC	5.35 V (FC)	12.30 V (FC)
Futaba S3152	1.20 V (FC)	1.94 V (FC)	NC	4.82 V (FC)	14.00 V (FC)
Futaba S3155	NC	NC	NC	4.08 V (FC)	12.10 V (FC)
Futaba S9650	1.09 V (FC)	NC	NC	4.83 V (FC)	12.7 V (FC)
HiTec HS5245MG	3.22 V (FC)	NC	NC	NC	11.6 V (LA 120°)

measurements are highly dependent on the antenna orientation and PWM cable positions, which is practically difficult e.g., in a UAV scenario. However, synchronization is possible on immobile victims like production lines and solar tracking systems with PWM–controlled actuators.

Attack Waveform III: Full Control

In a servo motor application, the PWM has a fixed duty cycle in between $\%5 < \frac{t_{high}}{t_{PWM}} < \%10$ (Figure 2.1a, $t_{PWM} = 20\,\text{ms}$). An attacker can exploit the low duty cycle nature of the PWM by injecting an attack PWM with a significantly larger duty cycle (i.e., the same t_{high} with lower t_{PWM}). The question arises: *What happens when an attacker applies a PWM with a larger duty cycle?*

As t_{high} is fixed and in the range of 1 ms to 2 ms for all servo models, the attacker can only decrease the t_{PWM} to increase the duty cycle. t_{PWM} value is decreased to 2.5 ms and the servo operation is observed by varying the t_{high} in between 1 ms and 2 ms. It is observed that, all seven servo models can be controlled with the increased duty cycle PWM, i.e., t_{PWM} does not affect the actuation data. Note that the t_{PWM} value is chosen as slightly larger than maximum value of t_{high} in order not to lose the rising and falling edges of the PWM signal. This observation is the basis of *Full Control* attack which gives an attacker the control of Futaba servos. The *Full Control* waveform consists of frequent periodic sinusoidal pulses with period 2.5 ms and varying t_{rotate} (Figure 2.9c). The attacker chooses the t_{rotate} in the range [1 ms 2 ms] to inject false rotation angle information to the PWM channel. The *Full Control Attack* is practically an advanced version of *Block & Rotate Attack* because the adversary does not need to synchronize to the victim PWM (i.e., no need for a receiver system). On the other side, the high duty cycle attack waveform masks the PWM signal and the frequent rising and falling edges of the attack waveform injects the false rotation angle

information to the channel.

Table 2.4: Full Control is successful on Futaba models (gray boxes). Eflite and HiTec models move randomly; however, it is not possible to control them. (FC: Full Control, RM: Random Movement)

f_a	8.75 MHz	17.5 MHz	35 MHz	70 MHz	140 MHz
Eflite EFLR 7145	0.45 V (RM)	1.33 V (RM)	1.57 V (RM)	1.12 V (RM)	4.16 V (RM)
Eflite EFLR 7155	0.87 V (RM)	1.39 V (RM)	1.21 V (RM)	2.04 V (RM)	4.28 V (RM)
Futaba S3151	0.77 V (RM)	2.54 V (RM)	1.84 V (RM)	3.80 V (FC)	12.40 V (FC)
Futaba S3152	1.20 V (FC)	1.86 V (FC)	1.06 V (FC)	4.54 V (FC)	11.90 V (FC)
Futaba S3155	1.58 V (RM)	2.75 V (RM)	3.44 V (RM)	3.92 V (FC)	11.10 V (FC)
Futaba S9650	1.11 V (FC)	2.94 V (RM)	0.94 V (RM)	4.16 V (FC)	9.10 V (FC)
HiTec HS5245MG	2.76 V (RM)	2.06 V (RM)	2.20 V (RM)	3.72 V (RM)	6.90 V (RM)

Wired Setup Results for Full Control Waveform: Table 2.4 shows the effect of *Full Control* attack on servo models for varying attack frequencies. It is observed that Eflite EFLR 7145 and 7155 servos respond to *Full Control* waveform by moving randomly to a variety of angles. HiTec HS5245MG has also a very similar response, it randomly moves or locks at some random angle. Although *Full Control* waveform prevents the Pixhawk Autopilot to control the servo, it is not possible to inject false rotation angle data to fully control the Eflite and HiTec servos. On the other side, all tested Futaba models can be controlled with *Full Control* waveform at reported attack frequencies. For instance, Futaba S3152 can be controlled by an attack waveform at $f_a = 70\,\text{MHz}$ with a 4.54 V peak voltage in the PWM channel. The control can be achieved by adjusting the t_{rotate} (Figure 2.9c) in between 1 ms and 2 ms. Especially, $f_a = 70\,\text{MHz}$ is a significant attack frequency for a UAV system because it is close to the resonance of the aileron PWM cable as will be explained in Section 2.4.3.

Comparison of Attack Waveforms

A comparison of attack waveforms is given in Table 2.5. *Block Waveform* is the simplest and disables the victim actuation control. Although *Block* waveform is not able to inject

false rotation angle to the PWM channel, it is effective on all tested servo models because the digital servo models rely on the detection of rising and falling edges of the PWM signals which are masked by the *Block* waveform. The previously reported *Pulsed Sinusoid* [92] waveforms is able to rotate the Futaba servo to one direction and is applicable from close distances but requires a synchronization hardware (e.g., magnetic field probe and LNA) to synchronize to the victim PWM. *Block & Rotate* and *Full Control* are waveforms which enable the attacker to fully control certain servo models by injecting rotation angle data to the PWM channel. *Block & Rotate* is applicable to tested Futaba and HiTec servos models (Table 2.3 and 2.4). However, it requires synchronization to the victim PWM. Practically, for a successful attack, the attacker needs a sensitive receiver to detect the victim PWM rising edges which requires additional hardware like an LNA, filter, matched filter, and possibly a signal processing unit. On the other side, *Full Control* exploits the low–duty cycle nature of PWM signals used in servo motor applications and does not require synchronization and a receiver system. *Full Control* injects false data very frequently to override the original rotation angle data in the PWM channel. *Full Control* is applicable to Futaba servo models and provides the full position control of the actuator. A comparison of attack waveforms is given in Table 2.5. *Block Waveform* is the simplest and disables the victim actuation control. Although *Block* waveform is not able to inject false rotation angle to the PWM channel, it is effective on all tested servo models because the digital servo models rely on the detection of rising and falling edges of the PWM signals which are masked by the *Block* waveform. The previously reported *Pulsed Sinusoid* [92] waveforms is able to rotate the Futaba servo to one direction and is applicable from close distances but requires a synchronization hardware (e.g., magnetic field probe and LNA) to synchronize to the victim PWM. *Block & Rotate* and *Full Control* are waveforms which enable the attacker to fully control certain servo models by injecting rotation angle data to the PWM channel. *Block & Rotate* is applicable to tested Futaba and HiTec servos models (Table 2.3 and 2.4). However, it requires synchronization to

the victim PWM. Practically, for a successful attack, the attacker needs a sensitive receiver to detect the victim PWM rising edges which requires additional hardware like an LNA, filter, matched filter, and possibly a signal processing unit. On the other side, *Full Control* exploits the low–duty cycle nature of PWM signals used in servo motor applications and does not require synchronization and a receiver system. *Full Control* injects false data very frequently to override the original rotation angle data in the PWM channel. *Full Control* is applicable to Futaba servo models and provides the full position control of the actuator.

Table 2.5: Comparison of Attack Waveforms

	Block	Sawtooth[93]	Pulsed Sinusoid[92]	Block & Rotate	Full Control
Block Data	✓	✓	✓	✓	✓
Inject False Data	✗	✓	✓	✓	✓
No need for Synchronization	✓	✗	✗	✗	✓
Actuation Control One Direction	✗	✓	✓	✓	✓
Actuation Control Two Directions	✗	✗	✗	✓	✓
Applicable to Eflite Servos	✓	No Data	No Data	✗	✗
Applicable to HiTec Servos	✓	No Data	No Data	✓	✗
Applicable to Futaba Servos	✓	✓	✓	✓	✓

2.4.3 Enabling Long–Distance False Actuation Injection

We propose to demonstrate the FAI attacks on servo motors of the UAVs which control the moving surfaces of the system such as ailerons or flaps. The intrusion of unauthorized UAVs to restricted air spaces provokes many security issues and results in halting operations in military/civilian air spaces [23]. Between 2013–2015, a total of 921 UAV and manned aircraft encounters have been recorded in the U.S. national airspace, with the majority of these encounters within five miles of an airport, resulting in a halt in flights [44]. To mitigate this threat we consider that an intruder UAV can be met by a tracker UAV that—when sufficient proximity is gained to the intruder—launches FAI attacks against the intruder to guide its trajectory away from the restricted airspace (Figure 2.10). Without loss of generality, the

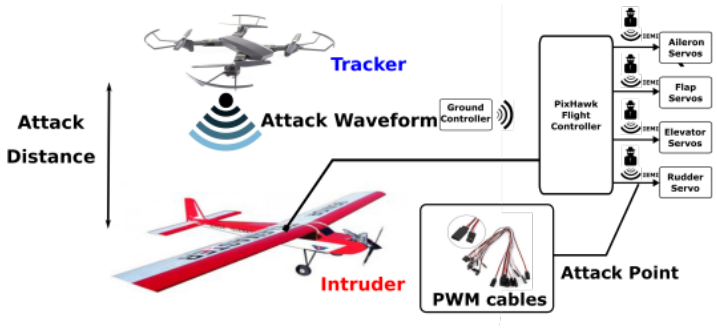


Figure 2.10: The attack scenario includes two UAVs, namely an intruder and a tracker. The tracker uses FAI to block or manipulate the actuation control of the intruder to defend the safe air–space.

intruder is assumed to be a fixed-wing UAV, while the tracker is either a fixed-wing UAV or a drone equipped with an attack setup capable of generating FAI to block or take control of the intruder's PWM signals. In the following sections, the terms intruder/victim and tracker/attacker will be used interchangeably.

The attacks rely on Faraday's law of induction [16] to induce a voltage in the victim PWM circuitry; however, as observed in the wired setup (Table 2.1, 2.3, and 2.4), the induced voltage should be a few $Volts$ for successful attacks. These values are relatively large considering the analog false data injection scenarios in which a few 100 mVs of induced voltage can result in significant changes in the sensor readings [93], so the attacker needs to utilize an efficient coupling mechanism to induce more voltage. In Section 2.4.3, the mutual coupling between the attacker and the victim is determined analytically to find an optimal attack frequency that ensures the maximum induced voltage.

An Electromagnetic Coupling Model for the Attack Scenario

An adversary can use either the near or far-field region produced by the attacker antenna to induce voltages in the PWM circuitry. The appropriate region for FAI attacks will be revealed after the explanation of antenna fields.

Far Field Region: Far field of the anntenas is utilized by most of the antenna applications like communication, satellite, WiFi, and radar in which the radiation distances are much larger than the wavelength of the carrier signal and antenna dimension. The region approximately lies in $R > \frac{2D^2}{\lambda}$ where D is the maximum overall dimension of the antenna and λ is the wavelength of the signal [15]. The electric ($\mathbf{E}$) and magnetic ($\mathbf{H}$) fields are coupled to each other i.e., they are sources of each other. The field in the far–field follows the plane wave characteristic with a constant ratio of $Z_0 = 120\pi = \frac{|\mathbf{E}|}{|\mathbf{H}|}$ in free space or air [86].

Near Field Region: The near field of the antenna lies in the vicinity of the antenna (e.g., $R < \frac{\lambda}{2\pi}$ for an electrically small dipole [55]), and in this region, the magnetic and electric fields have a complex relationship unlike the plane waves in the far field. Depending on the antenna type, an electric or magnetic field may be dominant (e.g., the magnetic field for a loop antenna). An efficient attack waveform should penetrate the victim system without significantly attenuated or reflected by metal components/wires and induce enough voltage to the victim PWM circuitry. The far field waves are attenuated and reflected by the metals; however, low frequency magnetic near fields are known to penetrate more easily to the system because of their decoupled nature from the electric fields [71]. Adding to that, magnetic resonant coupling (i.e., coupling through magnetic fields in the near field between resonant components) is reported as an efficient way of transferring power over medium distances even in weakly coupled scenarios (i.e., long attack distance) [62]. The near field region of a magnetic antenna is an efficient way of inducing high voltages to a PWM circuitry.

For the coupling ratio detection between the attacker square loop antenna and the victim PWM circuitry, the parameters and model given in Figure 2.11a are used. The attacker antenna is excited with a time–varying attacker current, $\mathbf{i_a} = I_a sin(wt)$, and consequently generates a magnetic field. This magnetic field is captured by the victim PWM loop which results in induced voltages. The orientation of the antenna and PWM loop is assumed to

be through z-axis throughout the analysis. However, it should be noted the surface normal of the antenna and victim cable are not aligned during attacks. The reported scenario, in which the surface normals of the antenna and victim circuitry are parallel, provides maximum coupling. The attack distance (d_a) is assumed to be 1 m and $< x_o, y_o, z_o >$ is any point on which the time–varying magnetic field, $\mathbf{B}$, is calculated (Figure 2.11a). As the antenna is an electrically small loop (i.e., maximum antenna dimension is smaller than the attack signal wavelength), a magneto–quasistatic (MQS) solution can be used [69]. In MQS approach, the problem is solved as a static problem at once, and then the time-varying term (e.g., $sin(\omega t)$) is introduced as a multiplication. Magnetic vector potential, $\mathbf{A}$, and magnetic field density, $\mathbf{B}$, are related to each other as follows:

$$\mathbf{B} = \nabla x \mathbf{A} \tag{2.7}$$

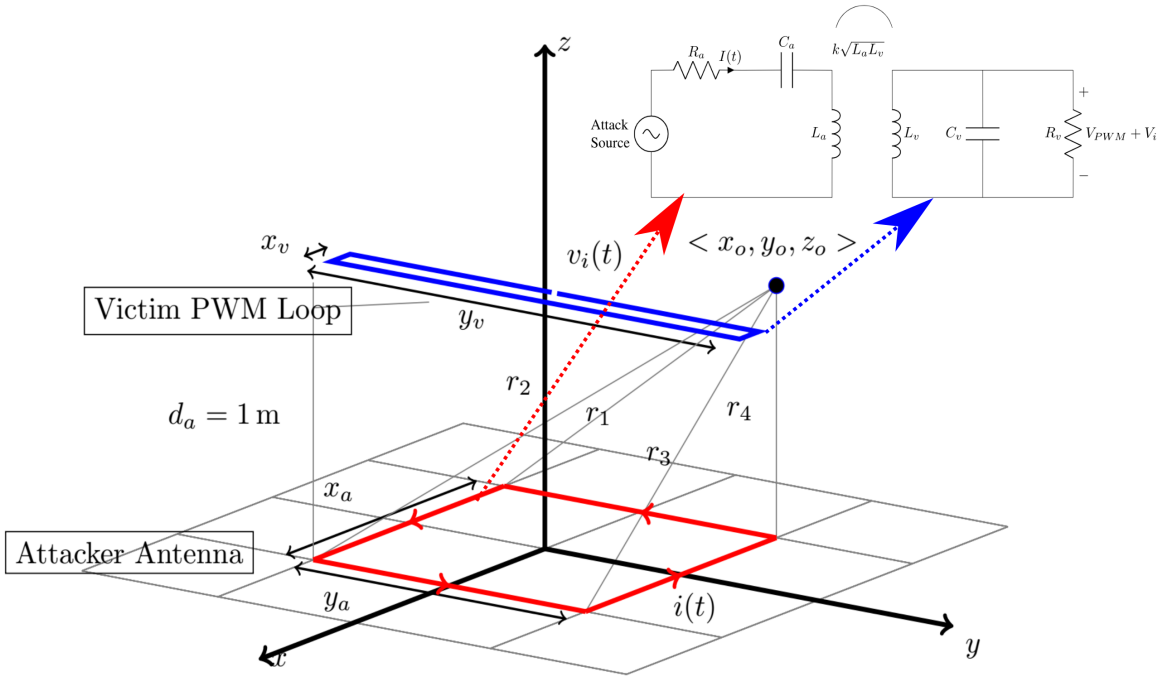
The x, y and z component of $\mathbf{B}$ can be found from magnetic vector potentials through x–axis and y–axis vector potentials (A_x and A_y) as follows [69]. As $\mathbf{i_a}$ current has no z directed component, there is no z directed magnetic vector potential ($A_z = 0$).

$$B_x = -\frac{\partial A_y}{\partial z} \ , \ B_y = \frac{\partial A_x}{\partial z} \ , \ B_z = \frac{\partial A_y}{\partial x} - \frac{\partial A_x}{\partial y} \tag{2.8}$$

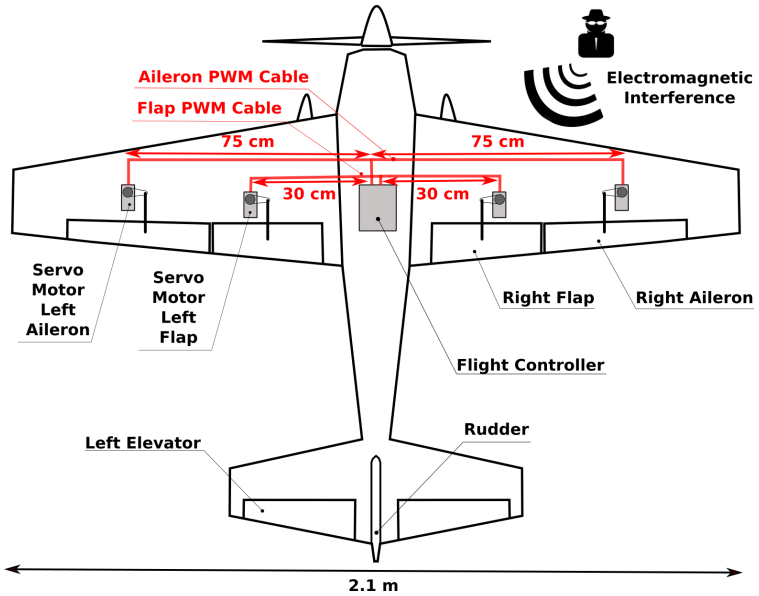
Magnetic vector potential ($\mathbf{A}$) is found by the line integral of the attacker current (2.9). $\mathbf{dl}$ and μ are differential length vector of the current and permeability of the medium, respectively. MQS assumption makes it possible to calculate the magnetic vector potential with current amplitude, I_a.

$$\mathbf{A} = \frac{\mu}{4\pi} \int \frac{I_a \, \mathbf{dl}}{|\mathbf{r} - \mathbf{r}'|} \tag{2.9}$$

where $\mathbf{r}$ and $\mathbf{r}'$ are position vectors for the field and attacker current ($\mathbf{i_a}$) as shown in Figure 2.11a. As the victim loop surface normal is through z–axis, only z directed magnetic field



(a)



(b)

Figure 2.11: The coupling between the attacker antenna and the victim PWM circuitry is found analytically. (a) The model used for analytical electromagnetic solution and the circuit model for the magnetic resonant coupling (b) The victim PWM cables connect the controller and servo motors of the UAV. PWM circuitry have different lengths and positions.

(B_z) contributes to the induced voltage. After the calculation of A_x and A_y with (2.9), B_z is [69]:

$$B_z = \frac{\mu I_a}{4\pi} \sum_{n=1}^{4} \left[\frac{(-1)^n D_n}{r_n \left(r_n + (-1)^{n+1} C_n\right)} - \frac{C_n}{r_n \left(r_n + D_n\right)} \right] \tag{2.10}$$

where the location dependent variables C, D, r are (Figure 2.11a):

$$\begin{aligned} C_1 = -C_4 = x_a/2 + x_o \quad , \quad r_1 = \sqrt{C_1^2 + D_1^2 + d_a^2} \\ C_2 = -C_3 = x_a/2 - x_o \quad , \quad r_2 = \sqrt{C_2^2 + D_2^2 + d_a^2} \\ D_1 = D_2 = y_a/2 + y_o \quad , \quad r_3 = \sqrt{C_3^2 + D_3^2 + d_a^2} \\ D_3 = D_4 = -y_a/2 + y_o \quad , \quad r_4 = \sqrt{C_4^2 + D_4^2 + d_a^2} \end{aligned} \tag{2.11}$$

The coupling ratio, k, is the ratio of the flux captured by the victim PWM loop (ψ_v) to the total flux generated by the attacker antenna, ψ_a. S_a and S_v are areas of attacker antenna and PWM loop, respectively.

$$k = \frac{\psi_v}{\psi_a} = \frac{\iint_{S_v} \mathbf{B} \cdot d\mathbf{S}}{\iint_{S_a} \mathbf{B} \cdot d\mathbf{S}} \tag{2.12}$$

The UAV flap and aileron cable lengths are 60 cm and 150 cm as shown in Figure 2.11b. The coupling ratio (k) between antenna and PWM cables is found with (2.10) and (2.12) with a Matlab script. The attacker antenna size ($x_a = 35\,\text{cm}$, $y_a = 35\,\text{cm}$) and the attack distance ($d_a = 1\,\text{m}$) are assumed to be the fixed for aileron and flap cable. The coupling ratio for cables are found to be very low on the level of 10^{-4} as shown in Table 2.6. This is a weakly coupled scenario and the attacker needs an additional approach to induce voltage levels reported in Table 2.1, 2.3 and 2.4.

Table 2.6: Coupling coefficient(k) between attacker antenna and victim aileron/flap PWM loops is small which shows the attack scenario is a weakly coupled one. $x_a = 35\,\text{cm}$, $y_a = 35\,\text{cm}$, $d_a = 1\,\text{m}$, $i(t) = 1\,\text{A}$ at 61 MHz

Victim Loop Size	ψ_a (Wb)	ψ_v (Wb)	k
Flap Loop ($x_v = 1\,\text{cm}$ $y_v = 60\,\text{cm}$)	9.58×10^{-7}	1.27×10^{-10}	1.32×10^{-4}
Aileron Loop ($x_v = 1\,\text{cm}$ $y_v = 150\,\text{cm}$)	9.58×10^{-7}	2.32×10^{-10}	2.42×10^{-4}

Circuit Model for the Attack Scenario

The coupling ratio found by EM solution (Table 2.6) shows that the attacker antenna and victim loop is weakly coupled. Kurs et al. showed that magnetic resonant coupling (MRC) can be used efficiently to transfer power wirelessly with distances up to eight times of the coil radius even in weakly coupled scenarios [62]. MRC is a specific coupling scenario where the receiver and transmitter resonate at the same frequency and coupling is inductive (i.e., dominantly via magnetic fields). This phenomenon makes high efficiency Wireless Power Transfer (WPT) applications possible [67, 87]. Power transfer efficiencies up to 75.7% is reported for weakly coupled transmitter and receivers [67]. A magnetic resonant coupled series to parallel circuit model is provided in Figure 2.11a for the attack scenario. L_v, C_v, and R_v are the inductance, capacitance, and resistance of the victim PWM cable. L_v is determined by the length of the victim PWM cables. The victim PWM connection is a three conductor cable with PWM, ground, and V_{cc} and the parasitic capacitance C_v is due to the interaction between PWM–ground and PWM–V_{cc} cables. R_v is the resistance of victim loop that includes copper loss and termination load. The resonant frequency of the victim loop (f_v) and attacker antenna (f_a) can be found as follows:

$$f_v = \frac{1}{2\pi\sqrt{L_v C_v}} \quad , \quad f_a = \frac{1}{2\pi\sqrt{L_a C_a}} \tag{2.13}$$

According to the threat model, the attacker can not physically modify the victim system and alter the victim resonance (f_v); however, a resonant attacker antenna can be adopted that has the same resonant frequency with the victim ($f_a = f_v$). Especially for Tesla coils, magnetic resonant coupled circuits have been investigated through Kirchoff's circuit law [35], and it is concluded, regardless of the coupling strength (e.g., weakly), the attacker and victim circuits should have the same resonant frequencies to transfer maximum energy, i.e., $f_a = f_v$ [40]. If k is above a value called critical coupling, a phenomenon called resonance splitting occurs due to the loading effect of the secondary coils (victim side) and the attacker waveform frequency (f_s) should be adjusted to one of the two operating frequencies which are above f_{s+} and below f_{s-} the uncoupled resonance frequencies of victim or attacker, i.e., f_a and f_v.

$$f_{s+} = \frac{f_v}{\sqrt{1-k}} \quad , \quad f_{s-} = \frac{f_v}{\sqrt{1+k}} \tag{2.14}$$

where the optimum attack condition is $f_s = f_a = f_v$. However, analytically it is found that k is negligibly small ($k << 1$) (Table 2.6), and f_{s+} and f_{s-} in [2.14] converges. Thus, for an efficient attack (e.g., the same attack power with larger attack distance), the attacker needs to have a resonant antenna at victim resonant frequency (f_v) and also the attack waveform frequency, f_s, should be tuned to the victim resonant frequency, f_v.

Detection of the Victim Resonance

The victim resonance can be determined analytically or experimentally. While the analytical approach provides a resonance estimate of the victim with the victim dimension information (e.g., wing size), the experimental method provides a more accurate resonant frequency detection with the requirement of reverse engineering of the victim.

Analytical Detection of the Resonance The resonant is of the victim PWM cable is

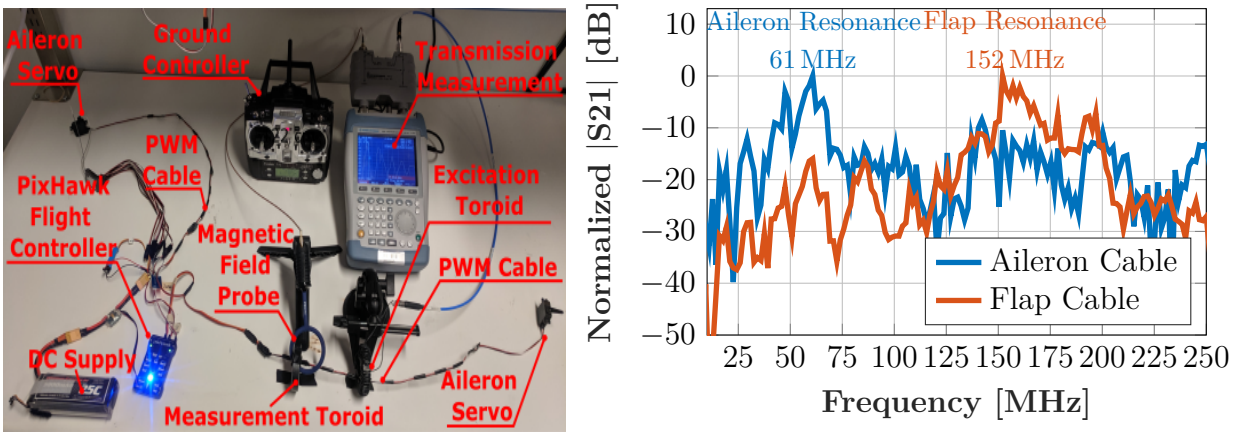
determined by the length of the cables, parasitic capacitances, and terminations. The cables resonate at quarter-wavelength or half-wavelength frequency for short and open termination (both ends), respectively [98]. In the PWM scenario, as the PWM cables are terminated by the high-Z loads like servo motor input and autopilot pins, open termination is a proper representation that corresponds to resonance at half-wavelength frequency. The analytical formula for the resonant frequency is:

$$f_{res} = A\frac{c}{(2 * L_{PWM})} = 0.7\frac{c}{(2 * L_{PWM})} \tag{2.15}$$

where L_{PWM} is the length of the cable, c is the speed of light in vacuum, and A is a constant that compensates the decreased speed of light in the wires, For a copper wire with an insulator material with a dielectric constant between 2 and 3 (e.g., PWM cables) [75, 116], $A = 0.7$ is a proper approximation [98, 117]. [2.15] can be used to generate a database of attack frequencies, e.g., a UAV attack frequency database with the UAV dimensions publicly available. If the analytically found frequency differs from the actual resonance due to, e.g., loading effect and parasitic capacitance, the attacker could use a narrow band-attack signal centered around the analytical resonant frequency to increase the probability that resonant coupling is achieved. Conversely, the attacker could vary the frequency of the attack signal around the analytically found resonant frequency and detect the exact resonant frequency by the induced effect on the victim.

Experimental Detection of the Resonance Although the analytical approach provides a simple way of resonance estimation, an experimental approach can be used for more accurate resonance detection. Smith reports a method in which a transmission measurement is implemented through current clamps located around the cables under test [98]. The method reported here is similar but employs ferrite toroids and a field probe instead of the current clamps. The experimental setup (Figure 2.12a) includes a Rohde & Schwarz spectrum

analyzer with a tracking generator that sweeps the frequency band in between 1 MHz and 499 MHz to make a transmission measurement, i.e., S_{21}. The excitation port (Port 1) of the spectrum analyzer is connected to a toroid with 60 coils, and the measurement port (Port 2) of the spectrum analyzer is connected to a field probe which measures the field of the measurement toroid. The system under test includes a battery, flight controller, ground controller, PWM cables, and servos, which are fully operational during measurements. The left and right-wing PWM cables are positioned inside the excitation and measurement toroids as displayed in Figure 2.12a. The measurement toroid picks up the field generated in the cable, and the resonance frequency is detected when the maximum transmission occurs.



(a) (b)

Figure 2.12: The aileron and flap PWM cable resonances are experimentally determined with a transmission measurement (S_{21}). (a) The test setup includes toroids, magnetic field probe and a spectrum analyzer. (b) At the cable resonant frequency, the transmission makes a peak. Aileron cable has a lower resonant frequency (61 MHz) as expected because of its larger length.

Table 2.7: Victim PWM cable resonances are detected experimentally and analytically.

	Aileron PWM Cable (150 cm)	Flap PWM Cable (60 cm)
Experimental	61 MHz	152 MHz
Analytical	70 MHz	175 MHz

Figure 2.12b provides the normalized transmission measurement of aileron (150 cm) and flap (60 cm) PWM cables. The loading effect due to servos and flight controller exists but does not significantly affect the position of the resonant frequency. The aileron measurement makes a peak around 61 MHz which is the resonant frequency for the aileron cable. Additionally, the flap cable has a resonance at 152 MHz (Table 2.7). The measurements show that the attacker can use a resonant frequency to attack a specific control surface (e.g., 61 MHz for ailerons), and cable length is inversely proportional to the resonance frequency. For comparison, the analytically found resonances (2.15) for aileron and flap cables are at 70 MHz and 175 MHz, respectively (Table 2.7).

Attacker Antenna Design and Production

It is concluded in Section 2.4.3 that magnetic resonant coupling can be utilized by a tracker for efficient attacks (i.e., same power longer attack distance or less power the same attack distance). This requires an attacker antenna that resonates at the same frequency with the victim PWM cables,f_v. As the relative position adn orientation of the intruder is not constant during the flight, the magnetic field should be strong enough in a large enough area; i.e., a relatively non–directive antenna pattern is needed in the near field. In RFID applications, where a tag attached to a vehicle or a person, a very similar problem is addressed with electrically large loop antennas [124]. However, the large electrical size of these antennas results in nonuniform magnetic field distribution. Zero phase shift line loop (ZPSL) antenna is a modified version of electrically large loops which utilizes distributed capacitors on the antenna to hove a more uniform magnetic field distribution in the near field region.

A ZPSL antenna is designed for the aileron resonating at $f_v = 61$ MHz. ANSYS HFSS is used for EM simulations and fine–tune the antenna dimension to the victim resonance, f_v. A lumped L–C impedance matching circuit for 50 ohm is employed to eliminate back power

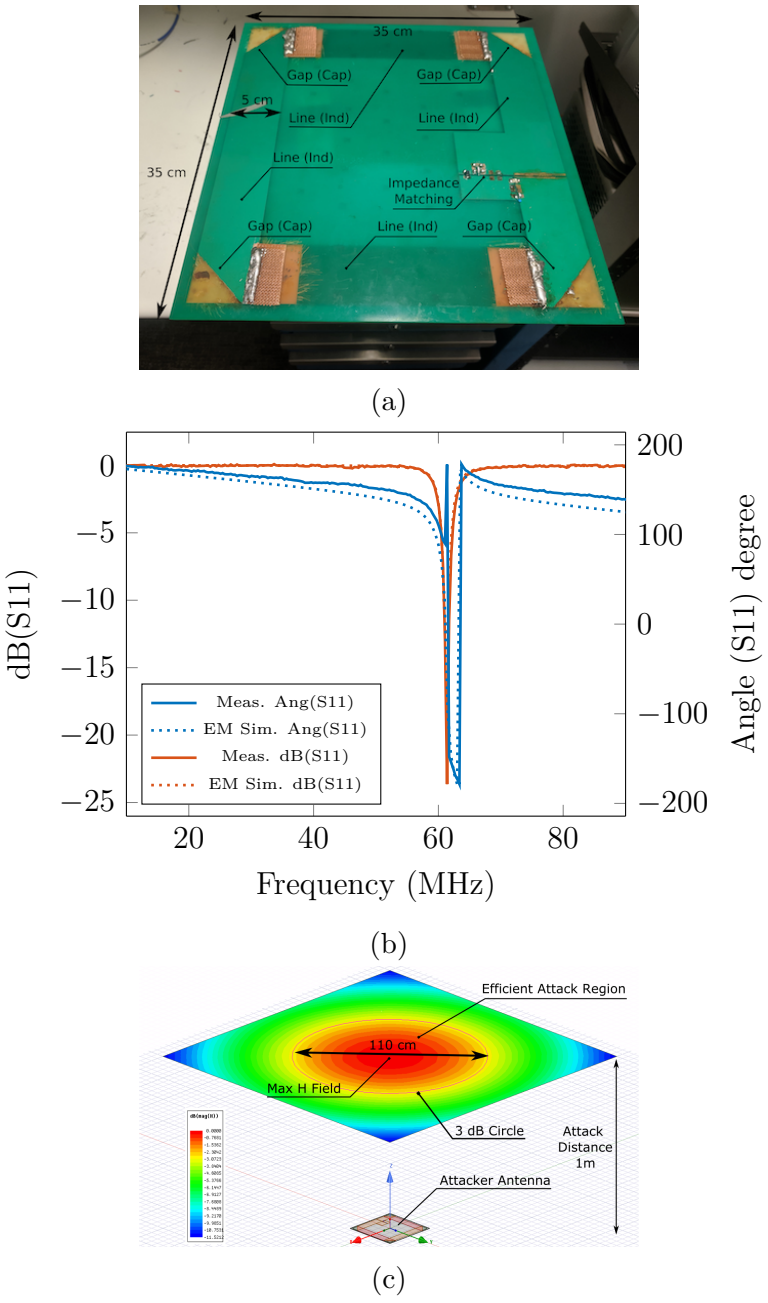


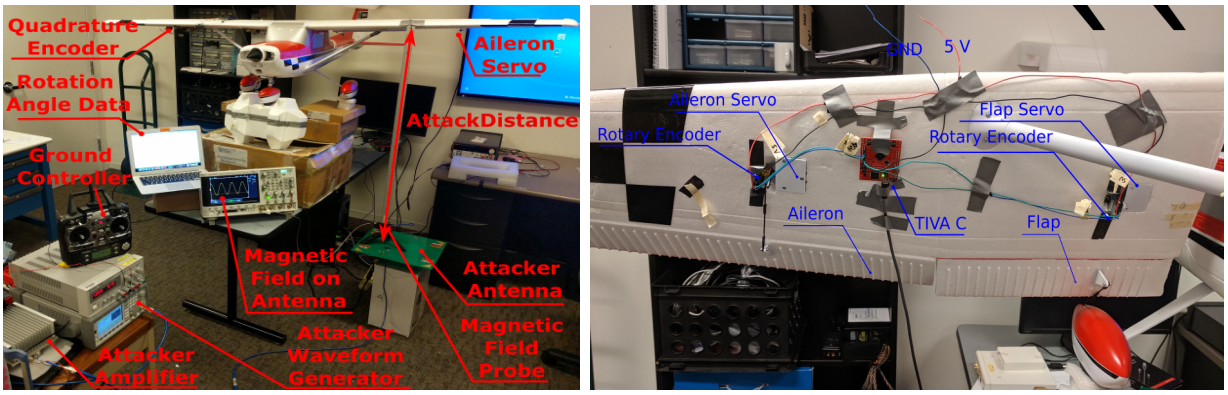
Figure 2.13: A resonant near field antenna is designed and produced for attacking ailerons. (a)Zero Phase Shift Line (ZPSL) Antenna, distributed capacitances, inductances and antenna dimension (b) S_{11} comparison of EM simulation and measurement; antenna resonates at 61 MHz (c) Normal Magnetic field distribution $|H_z|$ at $z = 1\,\text{m}$, a wide attack region with a Half Power Beam Width diameter of 110 cm

to amplifier and transmit maximum possible power to the antenna. The planar size of the antenna is 35 cm by 35 cm as shown in Figure 2.13a. The inner dielectric section of the PCB

antenna is removed to decrease the air drag and weight for the flight tests. The simulation and measurements are well matched as shown in Figure 2.13b. At 61 MHz, the reflection (S_{11}) phase of the antenna is observed to be 0° which points the resonance. The S_{11} is below -15 dB in the vicinity of 61 MHz which points that antenna is matched to 50 Ω. ZPSL antenna has a bidirectional radiation pattern which has local maximums through + and - z–axis. In Figure 2.13c, $|H|$ distribution of the antenna is shown on a 2 m by 2 m plane at a distance of 1 m. It is observed that the Half Power Beam Diameter of the antenna is 110 cm on the plane.

2.4.4 Indoor Demonstration of Long–Distance False Actuation Injection on a Victim UAV

For indoor attack demonstrations, a Cessna 150 (C150) fixed-wing UAV with a wingspan of 2.1 m is employed as an intruder/victim [1] (Figure 2.14a). The ailerons of the intruder are selected through the experimentally determined resonant frequency 61 MHz (Table 2.7). As the left and right aileron cables are electrically connected and controlled by the same PWM, attacks affect both the right and left aileron. The attacker system consists of a waveform generator, a 20 W RF amplifier, and a Zero Phase Shift Line (ZPSL) antenna, the design and production procedure of which is explained in the previous section. The rotation angle of the ailerons is measured with an AMT10 quadrature encoder [28] located on the shaft of the right aileron servo as shown in Figure 2.14b. AMT10 encoder converts the rotation angle of the servo to quadrature signals which are transmitted to a TIVA C microcontroller that records the angle data in its flash memory. The quadrature encoder is located on the right aileron servo while attacks are applied from the left–wing side (Figure 2.14a) to prevent the effect of EMI on angle measurements (Figure 2.14b).



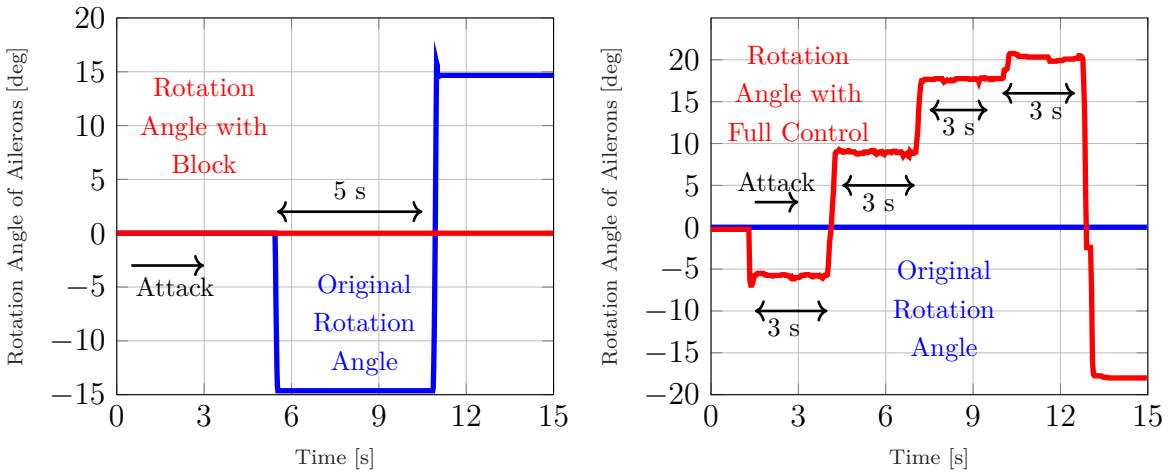
(a) (b)

Figure 2.14: The attacks are demonstrated indoors. (a) The experimental setup includes a fixed-wing UAV and an attacker system. The attacker antenna is located under the left-wing of the UAV and the efficacy of the attacks are measured with varying attack distances at fixed attack power 20 W. (b) Quadrature encoders are mounted on the right aileron servo for rotation angle measurement.

Indoor Block Demonstration

During wired tests in Section 2.4.2, it is observed that *Block* waveform paralyzes the servo control. To observe this effect, it is assumed that the attack is applied for 15 s and during the attack, the victim/intruder system tries to control the servos by sending neutral (0°), left (-15°), and right (15°) rotation commands. The attack power, frequency, and distance are 20 W, 61 MHz, and 50 cm, respectively. The antenna orientation is adjusted for maximum attack distance.

Figure 2.15a demonstrates the rotation angle of ailerons with (Red) and without (Blue) *Block* attack. In both cases, the ground controller sends neutral, left, and right rotation commands with 5 s durations. It is observed that when there is no IEMI, the ailerons follow the commands as shown with blue plot in Figure 2.15a. However, when the *Block* waveform is radiated, the ailerons stop following the commands sent from the ground controller and stays at the neutral position. When the attack stops, the ground controller retakes the control of the ailerons.



(a) (b)

Figure 2.15: The *Block* and *Full Control* attacks block or control the victim aileron rotation. (a) *Block* demonstration: The original rotation angle (blue) sent from ground controller can not control the servo during the attack; The servo is 'blocked' at neutral position (red). Attack distance is 50 cm. (b) *Full Control* demonstration: The attacker increases t_{rotate} (at every 3 s) and the control surfaces (i.e., ailerons) rotate with varying t_{rotate} while the system tries to keep the ailerons at neutral position (blue). The attack distance is 25 cm.

During measurements, it is observed that the *Block* waveform is efficient from a distance up to 50 cm with an attack power of 20 W; however, the attack distance is observed to be highly dependent on the antenna orientation and the PWM circuitry positions.

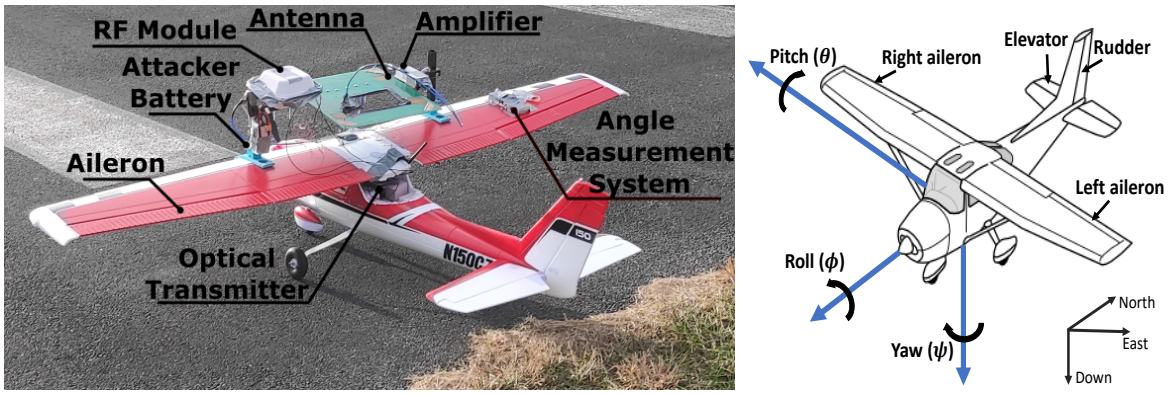
Indoor Full Control Demonstration

In Section 2.4.2, it is observed that Futaba make servos can be controlled by varying the pulse duration (t_{rotate}) of the *Full Control* waveform (Figure 2.9c). To observe this phenomenon on a victim UAV with Futaba servos (S3155), it is assumed that the intruder/victim system sends a neutral command to keep the ailerons at neutral position (0°) throughout the attack demonstration. The attacker applies a *Full Control* waveform with an incrementally increasing t_{rotate} to rotate the ailerons clockwise [1.4 ms, 1.6 ms, 1.8 ms, 2 ms] at every 3 s. In the end of the sequence, a $t_{rotate} = 1.2$ ms is applied to observe that the attack is applicable

for counterclockwise rotation as well. The attack distance, power, and frequency are 25 cm, 20 W, and 61 MHz, respectively. It is observed that the attack waveform moves the ailerons with increasing t_{rotate} from left to right as in Figure 2.15b, even though the actual PWM commands a neutral position. It is also observed in the end, by sending a smaller $t_{rotate} = 1.2$ ms, the right to left rotation (counter–clockwise) is also possible. Another observation is that *Full control* is applicable from a smaller attack distance than *Block* because the induced waveform in the *Full Control* scenario should be large enough to make the servo think that there is a legitimate PWM in the channel (unlike *Block* attack during which 'erasing' the original PWM in the channel is sufficient.)

2.4.5 In–flight Demonstration of False Actuation Injection Attacks on a Victim UAV

The intruder, Eflite Cessna C150, is a standard fixed–wing UAV with three control surfaces, namely the aileron, the elevator, and the rudder which primarily controls the the rolling motion/roll attitude (ϕ), the pitching motion/pitch attitude (θ), and the yawing motion/yaw attitude (ψ), respectively (Figure 2.16b). During the attacks, both left and right ailerons are affected as they are controlled by the same PWM; however, their sense of rotation is opposite because of their placement. The aileron rotation (δa) is positive when the right aileron is trailing edge up & the left aileron is trailing edge down. Thus, a positive aileron rotation produces a positive rolling motion that increases the roll attitude of the UAV. The reader is referred to [20] for details on UAV dynamics and control.



(a) (b)

Figure 2.16: The attacks are demonstrated on a victim/intruder fixed–wing UAV. (a) The attacker system including a battery, an RF module, an amplifier, and a ZPSL antenna is mounted on the UAV with carbon–fiber rods for in–flight demonstrations. Attack distance (i.e., the distance between the UAV fuselage and attacker antenna) is 15 cm. The system weight is decreased by carving out a section from the antenna and employing a lightweight battery and mount material. (b) The intruder fixed-wing UAV has three control surfaces: the aileron, elevator, and rudder which control the roll (ϕ), pitch (θ), and yaw attitude(ψ), respectively.

Attacker System

In order to demonstrate the *Block* and *Full Control* attacks during a flight on an intruder, an attacker system, consists of an optical transmitter, an optical receiver, an RF module, a battery and a ZPSL antenna, is mounted on the intruder UAV with a carbon fiber frame as shown in Figure 2.16a. The two practical concerns, which is excessive weight and additional air drag due to attacker system, are addressed with low weight mount materials, smaller capacity batteries, and cutting out a nonfunctional PCB section from the attacker antenna. The test system, that includes the intruder UAV and attacker hardware, has an weight of 6 kg to which the attacker system contributes 1.4 kg, the mount system (carbon–fiber rods and 3-D printed parts) contributes 320 gm, and the angle measurement system(a battery, a PixHawk, and a quadrature encoder) contributes 150 gm.

The attacker system consists of an optical transmitter, an optical receiver, battery, RF

module, amplifier, and a ZPSL antenna. The victim Pixhawk is programmed to initiate the attacks upon request of the ground controller with control signals as illustrated in Figure 2.17. The control signals are converted to optical signals and sent through fiber–optic cables to the RF module. The optical receiver in the RF module converts the control signals back to voltage values. The 'RF Switch control' modulates the continuous wave signal to generate *Block* or *Full Control* waveforms, and 'RF amplifier control' is employed to turn on the amplifier DC supply during attacks to eliminate battery drain.

Optical signals, which are naturally resilient to electromagnetic interference, are utilized to send control signals from victim Pixhawk which is located in the fuselage to the RF module located on the fiber rod frame (Figure 2.16a) to securely end the attack. The fiber optic cables, which lack free electrons, are nonmetal mediums, and EM waves do not affect them because of the lack of electrons. The attack waveform envelope is fed to the RF switch to generate the *Block* or *Full Control* waveform. The amplifier with a rated power of 20 W amplifies the attack waveform, and a ZPSL antenna (2.4.3), resonating at victim resonant frequency, radiates the attack field. The intruder UAV controller is a Pixhawk autopilot and is running on PX4 firmware. The firmware is modified such that the radio controller is able to start or end the attacks from the ground. To robustly measure the aileron rotation, a quadrature encoder (QE) is positioned on the right aileron servo. Another Pixhawk is mounted on the right–wing of the UAV that processes the rotation angle data from the QE. The additional PixHawk module is used to safely measure the aileron servo response (i.e., rotation angle) even in a highly EM–contaminated environment (Figure 2.16a).In inflight demonstrations, PixHawk is adjusted to a 'stabilized' mode, which means the pitch and roll 'setpoint' is supplied by the radio/ground controller, and required actuator positions (e.g., servo motor rotation angles) are calculated by the PixHawk and sent to the actuators in PWM form.

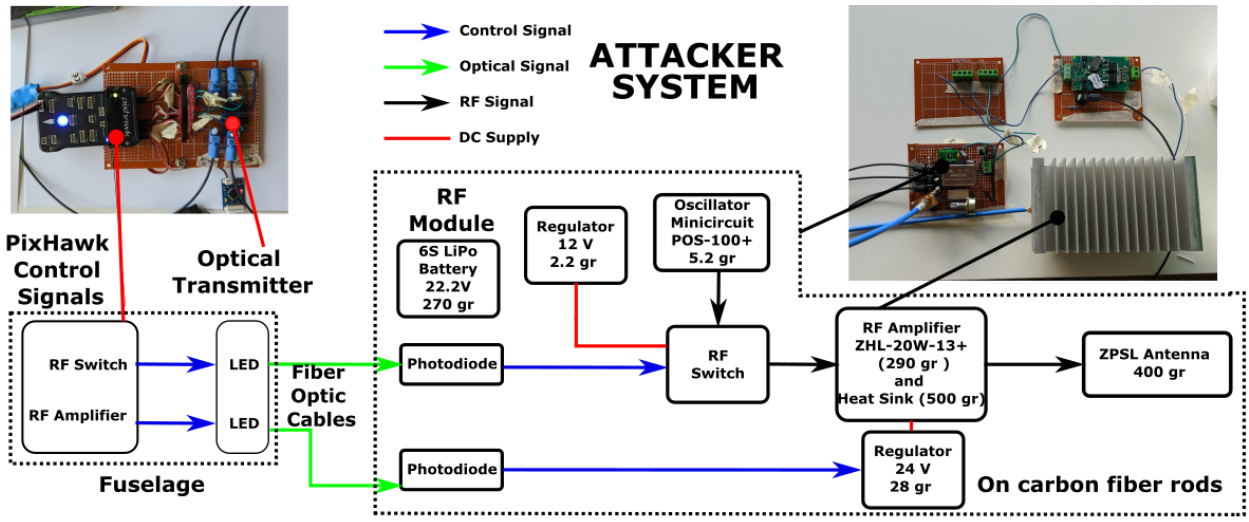


Figure 2.17: Victim controller Pixhawk generates the attack control signals. Control signals are converted to optical signals and sent through fiber cables to the RF module to be able to control the attack waveform under EM interference: The optical signals converted back to control signals by photodiode receivers and the amplified attack waveforms are radiated though ZPSL antenna.

In–flight Block Demonstration

Block waveform prevents the transmission of original actuation data, and servo motors respond to that by staying (locking or moving freely as summarized in Table 2.2) at their angular position just before the attack. To observe the effect of *Block* during a flight, the pilot (i.e., ground controller) sends a continuously varying roll setpoint, which is used by the autopilot to determine the required aileron rotation angle. When there is no attack ($t < 0$), the aileron rotation is equal to what is commanded by the autopilot (Figure 2.18c), and UAV tracks the setpoint roll attitude as shown in Figure 2.18e. As the attack starts ($t = 0$), the aileron locks at its current position of 32°, which results in a continuous positive rolling motion that increases the roll attitude of the UAV beyond the setpoint. The autopilot commands a negative aileron rotation to compensate for the effect of attack; however, no reduction in roll angle is observed as the aileron is locked due to the *Block*. The attack is

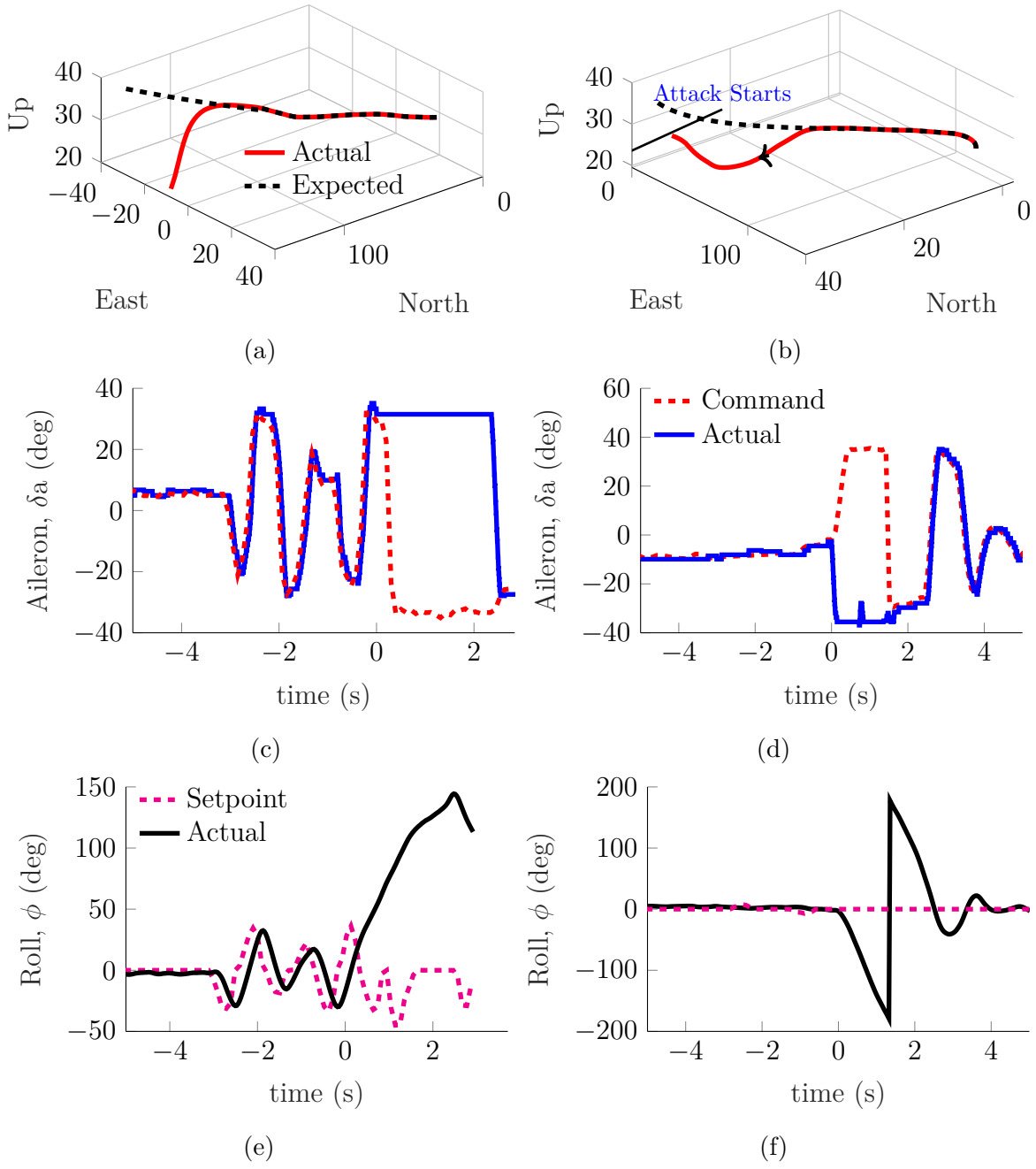


Figure 2.18: Results of in–flight demonstration of the attack. The attack starts at $t = 0$. (a) The trajectory of the UAV during *Block* attack demonstration (Block Video). (b) The trajectory of the UAV during *Full Control* attack demonstration (Full Control Video). (c) The *Block* waveform locks the aileron servo (at $t = 0$, blue curve). (d) The *Full Control* waveform ($t_{rotate} = 1.8\,\text{ms}$) rotates the aileron to $-36°$ (at $t = 0$, blue curve). (e) The roll attitude tracking during *Block* attack demonstration. (f) The roll attitude tracking during *Full Control* attack demonstration.

stopped after 2.4 seconds at which point, the roll attitude of the UAV rises to 150° , and the altitude of the UAV drops by 10 m. After the attack is stopped, the aileron rotates to the commanded negative position required to reduce the roll attitude. The roll attitude starts to decrease, but the altitude keeps dropping because of the high roll attitude. In 2.8 s, the altitude of the UAV dropped by almost 17 m, and the autopilot failed to recover the nominal orientation of the UAV in time, resulting in a crash (Block Video). Figure 2.18a presents the measured trajectory of the UAV under attack and the predicted trajectory without attack. The predicted trajectory is obtained by extrapolating the trajectory before the attack begins.

In–flight Full Control Demonstration

Full Control does not only prevent the transmission of original rotation angle to the actuators, but also injects a false actuation data to the PWM channel to manipulate the actuator rotation. In order to observe *Full Control* during a flight, the ground controller sends a zero roll setpoint which means a straight trajectory without any roll motion, and *Full Control* is applied to rotate the ailerons to an extreme i.e., $t_{rotate} = 1.8$ ms Figure 2.9c. Before *Full Control* ($t < 0$), the roll attitude is stable at 0° (Figure2.18f) and aileron rotation is around -10° to keep the roll attitude at 0° (Figure2.18d). As soon as the attack begins ($t = 0$), the aileron rotates to the false value of -36° which is injected by a *Full Control* waveform with $t_{rotate} = 1.8$ ms as shown in Figure 2.18d. The autopilot commands a positive aileron rotation to recover the orientation of the UAV, but the aileron does not respond as the original PWM is overriden by the *Full Control* waveform. The attack is turned off at $t = 1.7$ s at which point the roll attitude is -180° (Figure 2.18f). The autopilot, instead of commanding positive aileron rotation, commands a negative aileron rotation to recover the UAV by doing a 'full aileron roll' i.e., a 360°. The UAV completed the full aileron roll in less than 2.6 seconds, and the altitude dropped by about 10 meters before the UAV is recovered (Full Control Video).

The measured and the predicted trajectory of the UAV during *Full Control* demonstration is shown in Figure 2.18b.

2.5 Attack Distance and Attack Power Relationship

Indoor demonstrations show that an attack power of 20 W is sufficient for 25 cm-*Full Control* and 50 cm-*Block* attacks. However, the attack distance should be in the range of 1 m to 2 m for a practical scenario in which a tracker UAV approaches an intruder. To determine the attack distance and attack power relationship, the attacker ZPSL antenna is simulated in ANSYS HFSS to determine the field with varying attack distance. Adding to the ZPSL antenna which is produced for indoor and inflight demonstrations, a 'large' ZPSL antenna with 70 cm-by-70 cm planar dimensions is modeled. The simulated field distributions of antennas are combined with the indoor results to determine the minimum attack power required for varying attack distance (Figure 2.19). With both small and large antennas, the *Full Control* requires more power. For the attack distances up to 3 m, the large antenna requires significantly less power. For *Full Control* at $d_a = 1$ m, the required powers are 611 W and 3.3 kW for large and small antenna, respectively. However, if the attack distance is 2 m for the *Block*, required powers are 532 W and 1.38 kW for large and small antenna, respectively. The ability of large antennas in generating high magnetic fields in long radiation distances is a known phenomenon. For TMS applications, in which magnetic fields are used to stimulate particular regions of the brain, larger loops are preferred for better field 'penetration' to the inner brain layers [34]. For those scenarios in which attack distance should be increased, adding to increasing the antenna dimension, metamaterial– artificial magnetic conductors [97], which functions as magnetic reflectors, can be utilized to improve the field directivity by 3 dB which decreases the attack power and protect the tracker from

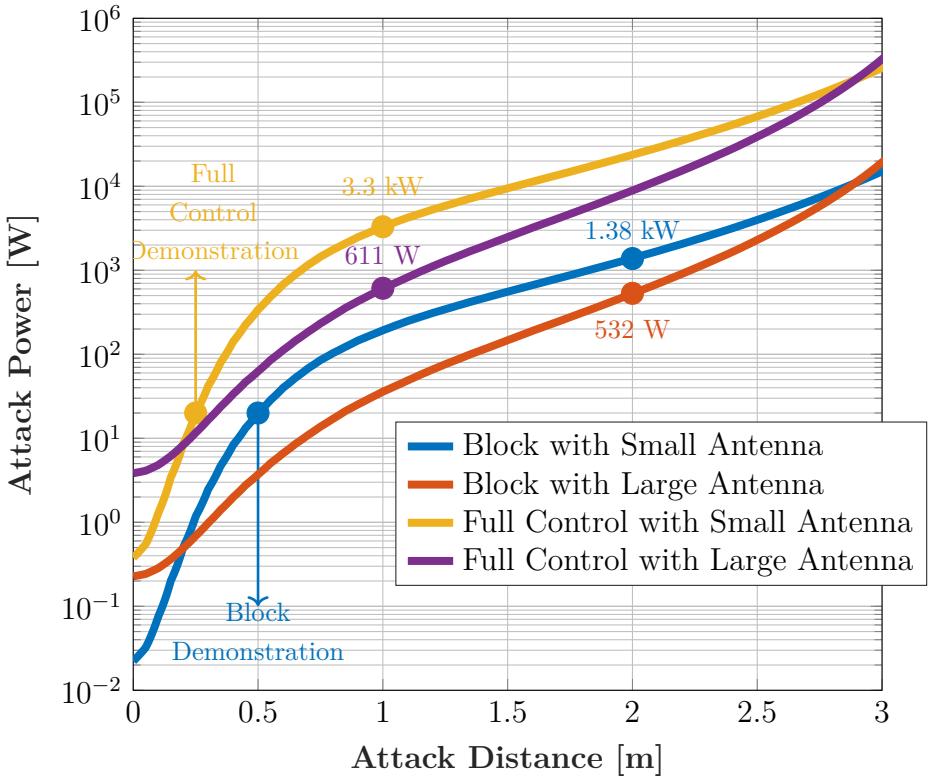


Figure 2.19: The field distribution of small and large ZPSL antennas are found with EM simulation, and indoor demonstrations are used as a benchmark. Large antenna requires less power for *Block* and *Full Control*. Generally, large antenna and *Block* attacks require less power; however, the required attack power increases significantly above 2 m.

its own attack field.

In scenarios, where the victim system is not shielded, the authors think that far-field antennas with high directivity can be employed to improve the attack distance. Unlike the near field loop antennas, the far field antennas can be highly directive. For instance, Yagi-Uda antennas with multiple resonant dipoles can have directivities around 9.2 dBi [101]. This means an attack power decrease by ≈ 7.44 dB (The directivity for an electrically small loop is 1.76 dBi [15]). Additionally, far field antennas do not require the tracker to be protected by the attack field because the radiation is diminutive out of the antenna boresight. The boresight of the antennas should be accurately aligned with the victim system which can be achieved with

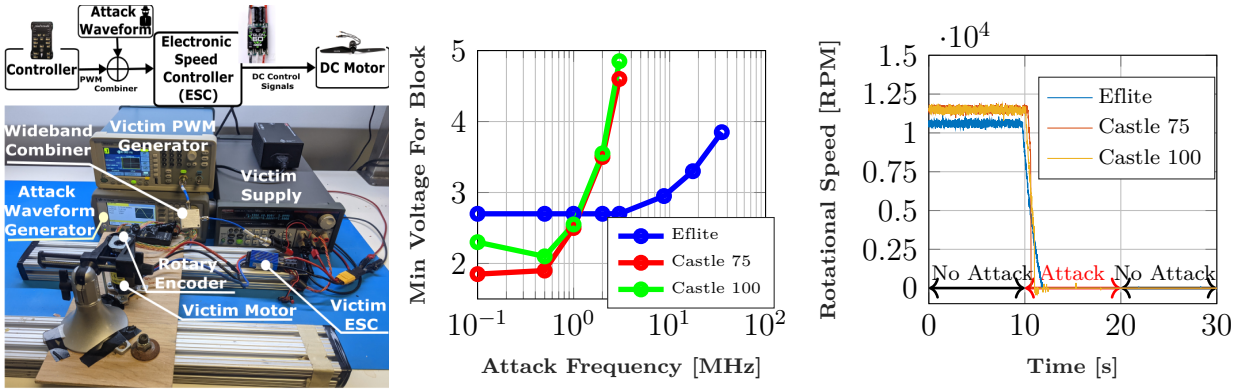
phased array antennas with controllable boresight.

2.6 Efficacy of Attacks on Other PWM–Controlled Actuators: DC Motors

DC motors are widely used in CPS applications for rotational motion, i.e., propeller rotation of a UAV. DC motors are PWM–controlled actuators, the rotational speed (i.e., rotation per minute-rpm) of which is controlled by the PWM pulse duration. Similar to servo control (Figure 2.1), when t_{high} is minimum (i.e., 1 ms), the rotation stops, and when t_{high} is maximum (i.e., 2 ms), the motor rotates with full speed. An Electronic Speed Controller (ESC) converts the speed data in the PWM to varying frequency current pulses that rotate the motor at the desired rpm.

To observe the effect of attack waveforms on the PWM-controlled DC motors, the wired setup in Figure 2.20a is used. The attack waveform is added to the original PWM with a wideband combiner and fed to the PWM input of the ESC, and the response of the DC motor is observed with varying attack frequency and voltage. The DC motor is powered with a 22.2 V supply which corresponds to the voltage level of a 6S LiPo battery which is used to power UAV outrunners. Three ESC models are tested: Eflite 60 A Pro [5], Castle Phoenix Edge 75 A [4], and Castle Phoenix Edge 100 A [3] with an Eflite BL50 525 kV brushless DC motor [2]. While an original PWM with a $t_{high} = 1.5$ ms is applied to the DC motor, the *Block* waveform with varying frequency and voltage is applied, and the motor rpm is recorded with a quadrature encoder located on the shaft of the DC motor (Figure 2.20a).

It is observed that at certain attack frequency and voltages, *Block* stops the rotation of each ESC-DC motor combination. However, depending on the models, the attack frequency and



(a) (b) (c)

Figure 2.20: PWM–controlled DC motors are tested in a wired setup against IEMI. The rpm change with attacks is observed. (a) The experimental setup for wired tests (b) The minimum peak voltages for successful attacks are shown. *Block* stops the operation of all tested ESC and DC motor couples; however, the attack frequency should be lower (< 3 MHz) for Castle models. (c) When the attack is initiated at $t = 10$ s, the rotation stops for each model. None of the tested ESC-DC motors recover from the attacks ($t > 20$ s). Attack frequency and voltage is 35 MHz and 4 V for Eflite ESC; and 3 MHz and 5 V for Castle ESCs.

power differ significantly. While Castle models are immune to *Block* at frequencies above 3 MHz within the setup voltage range (max 5 V), the Eflite model can be attacked with frequencies up to 35 MHz. Similar to the results observed with servos (Table 2.1), the higher frequency attacks require higher power. This 'Low Pass' characteristic is because of the ferrite beads on the ESC PWM cables for high frequency interference which is limited on frequencies below 3 MHz for Castle ESCs, and below 35 MHz for Eflite ESCs. Figure 2.20c shows the rpm of ESC–DC motor couples, with *Block* applied for 10 s at $t = 10$ s. The rotation stops in all models when the attack begins and none of them continue rotation after the attack stops, which means a permanent block in DC motor application. The reason for this is the 'arming PWM protocol' that initiates the DC motor is not launched after the attack, e.g., during a flight.

The *Full Control* is applied to the tested ESC-DC couples, and it is observed that although

the attacks stop the rotation as *Block*, the waveform is not injecting false rpm data to the motors. *Full Control* can be used to decrease the overall attack power (due to the pulse attack waveform); however, it is observed to be not effective in manipulating the speed data within the tested voltage (<5 V) and frequencies (<100 MHz).

2.7 Countermeasures

The attacker utilizes magnetic fields to couple to the victim PWM circuitry, and as the magnetic fields exist in nature as complete loops because of their divergence free nature ($\nabla \cdot B = 0$), the proper way to shield them is to redirect them with magnetic materials like MuMetal or steel plates [6, 76]. However, high permeability materials like MuMetal lose their magnetic properties with increased frequency and become inefficient above 100 kHz [6]. As the frequency of the magnetic field goes roughly above 100 kHz the magnetic or non–magnetic conductors like steel or aluminum perform better than MuMetal [79, 91]. However, high–frequency magnetic shielding highly depends on metal thickness and requires thicker conductor plates compared to the ones applied in far–field shielding [79]. Magnetic shielding 'efficiency' also depends on how much the shielding material encloses the victim system. Frika et al. showed that even small openings, such as cable holes, in the magnetic shielding deteriorates the shielding efficiency significantly [42]. This is the most concerning issue about shielding IEMI with inductive coupling, because it is practically demanding to cover all moving sections of a CPS with shielding material. For instance, completely covering the control surface of a UAV with magnetic shielding is not practical due to cost, weight, and disrupted flight dynamics. Although shielding is a solution for some scenarios such as the analog sensor attacks through far-field coupling [111], it can not be the sole countermeasure against attacks with inductive coupling using near field coupling.

A PWM signal with a changing frequency is suggested as a countermeasure [72] for the attacks with sawtooth waveform discussed in the short–distance section. Although the countermeasure is efficient for an attack scenario, in which the attacker detects the victim PWM pulse and assumes a constant PWM period, if the attacker is capable of detecting each rising edge of the victim PWM pulse, the attacks with sawtooth waveform would still apply. As the *Block & Rotate* and *Full Control*, which are discussed in the long–distance attacks, override the rotation angle information regardless of the victim PWM frequency, varying frequency selection is not effective.

Optical transmission is a resilient way to transmit information through channels exposed to high EMI. As the optical fibers are non-metallic, the fields can not interact with the electrons as they do in conventional copper cables. The actuation signals can be transferred through fiber cables; however, one drawback of optical transmission is increased complexity in hardware. Optical transmission requires light-emitting diodes (LEDs) and phototransistors which operate as transmitters and receivers that complicates the circuitry; however, only a limited number of actuation signals (e.g., aileron, flap) should be sent through fiber cables and by considering the availability of small, low cost and lightweight optical transmitter and receivers [53, 54], the optical transmission is a viable and reliable defense against FAI. During in-flight tests, the optical transmission works without disruption under high EMI.

2.8 Conclusion

Intentional Electromagnetic Interference (IEMI) is a significant threat to the secure control of actuators with PWM. The results demonstrate that the actuation data in the PWM circuitry can be blocked or manipulated with certain waveforms at victim resonant frequencies. It is also analytically shown that an attacker can use a magnetic resonant antenna to utilize

magnetic resonant coupling for efficient attacks (i.e., higher attack distance with the same power). Three attack waveforms, namely *Block & Rotate* and *Full Control* which give the attacker the precise control of certain servo models, e.g., Futaba S3155. The *Block* and *Full Control* attacks are demonstrated on a fixed-wing UAV in indoor and in-flight scenarios. For indoor demonstrations an attack power of 20 W suffices for distances up to 25 cm and 50 cm for *Full Control* and *Block* attacks, respectively. The in-flight attacks are demonstrated on a fixed-wing UAV and the flight data captured during the attack shows that the *Block* and *Full Control* attacks applied on the control surfaces of the UAV results in significant consequences. While *Block* attack prevents the aileron control of the UAV which results in a crash, *Full Control* waveform rotates the ailerons to one extreme which results in an 'aileron roll' of the victim. Although IEMI on actuators can be utilized as an efficient offensive tool against adversaries (e.g., an intruder UAV), defenses like optical signal transmission and magnetic shielding can be cooperatively employed to mitigate inductively coupled IEMI as well.

Chapter 3

Bit–Flip Attacks on Serial Communication Systems

Wired serial communication (e.g., UART, SPI, I2C) is widely used to exchange information between sensors, actuators, and controllers in cyber-physical systems. In this work, it is demonstrated that intentional electromagnetic interference (IEMI) can be utilized to not only induce spurious serial communications but to also alter legitimate communications, arbitrarily and at a distance, through attacks that cause controlled, bidirectional bit flips. A successful modification attack is carried out in three phases: in the *detection* phase the attacker monitors the electromagnetic (EM) leakage of the victim data to be alerted to the fact that data is being transmitted; in the *signal processing* phase the EM leakage is analyzed to synchronize the generation of the attacker's IEMI to have a desired effect on the communication channel at the instance the victim is performing the reception of the data, and in the *transmission* phase the IEMI is generated and transmitted to the victim circuitry during the interval where it will override the original data.

To prove the efficacy of bit–flip attacks with IEMI, a narrowband attack signal, which utilizes the baud rate of the victim communication system as the main attack frequency, is suggested and evaluated against a universal asynchronous receiver-transmit (UART) communication system. The narrowband waveform enables the use of low frequency and inexpensive hardware and does not require any specific information about the victim system except for the

baud rate. However, due to the low frequency nature of the attacks, the attacks require relatively large power which can be addressed with audio amplifiers. The narrowband waveform is shown to be over 98% effective at inducing a desired bit sequence (e.g., 0xAA or 0x00) into randomly transmitted UART frames, which indicates that an attacker could also choose to inject spurious UART frames, at will. Countermeasures such as twisted cables and optical transmission are recommended and experimentally analyzed during attack scenarios.

3.1 Introduction

Digital data transmission can be wired or wireless; serial or parallel; and synchronous or asynchronous [41]. In serial communication, data is sent one bit at a time, unlike the parallel, in which multiple bits of data are sent synchronously. Synchronous communication (e.g., Ethernet[10]) employs a common clock to synchronize transmitter and receiver, and data transfer is continuous (i.e., at each clock cycle); however, in asynchronous communication, the data transmission is started when data is available in the channel, and there is no need for a master clock. In the reported attacks, the victim system is assumed to utilize wired UART communication, which is a serial and asynchronous communication method.

Cyber-physical systems (CPS) depend on the integrity of data transmitted between sensors, actuators, and controllers. Wired serial digital communication is widely used in these systems because it is less susceptible to EM interference than wireless communication, is straightforward from a protocol perspective, and, unlike parallel communication, requires only one to three wires. Serial communication standards, such as SPI, UART, and I2C [31], connect controllers to a multitude of sensors[13, 107, 108] and even GPS receivers [9]. An attacker with the ability to manipulate the bits that are transmitted by sensors could easily mount, for example, a false-data injection attack against a CPS to cause it to enter an unsafe

state. For example, it is known that if the position or speed data obtained by an onboard GPS of an unmanned ariel vehicle (UAV), or the wheel speed measurement of a vehicle, can be manipulated by an attacker then such systems can be made to crash.

While much work has focused on attacks that digitally manipulate information, we examine the possibility that an attacker could alter digital information (i.e., bits) through analog means. Intentional electromagnetic interference (IEMI) against analog sensors, such as light, temperature, and speed sensors, implantable cardiac devices, and microphones have been extensively reported in security literature [61, 93, 95, 111]. The attacker induces a relatively low-voltage on the analog output of a sensor and, due to the nonlinearities of the Analog to Digital Converter (ADCs) [93] or amplifier [61, 111] used by the measuring system, the sensor data is altered significantly. The reader is referred to [45, 121] for a review of existent analog manipulation mechanisms. Manipulation of digital data, however, is substantially different and has not received as much attention. First of all, the attacker needs to induce a voltage comparable to the logic level of the transmitter (e.g., 3.3/5 V for CMOS/TTL), which is significantly larger than the induced voltage commonly reported in in analog data manipulation [61, 93]. Secondly, the attacker needs to determine when data is being transmitted and alter it in-flight (i.e., synchronize with the targeted system). Synchronization requires that the attacker acquire the timing characteristics of the victim system; for example, to flip a zero to one, the attacker needs to replace a 0 V signal with a 3.3 V one (assuming CMOS logic) at the instant the victim receiver samples the signal. An additional difficulty in obtaining required timing information is that wired communications are considerably more difficult to eavesdrop upon than wireless ones (notwithstanding beamforming and directional antennas).

In [93] a non-synchronized attack against a serial communication system was demonstrated. The authors report that without synchronization, and with using an attack waveform of

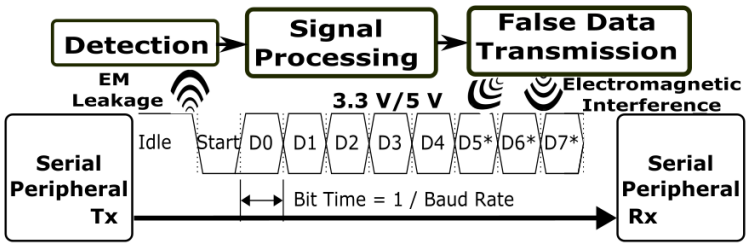


Figure 3.1: The attacker monitors (detection) and analyzes (signal processing) the EM leakage of the victim data. The false data is injected to the victim system with reported narrowband and wideband waveforms (transmission).

only a single frequency, the maximum bit-flip ratio cannot exceed a theoretical limit of 50%, because the signal that couples to the targeted device is sinusoidal and can never increase (or decrease) the voltage measured by the serial receiver more than 50% of the time. In this work, we introduce a synchronized bit-flip attack that leverages three phases (Figure 3.1) to exceed this limit and allow for arbitrary injection of modification to data in serial communication. In the first phase, *detection*, the attacker listens for electromagnetic (EM) leakage from a victim transmitter that signals the start of a serial transmission; in the second phase, *signal processing*, the EM leakage is processed to uncover the necessary timing information to allow the attacker to manipulate the information when it is being received by the victim; in the final phase, *transmission*, the attacker radiates a specially crafted signal that will ensure that a desired bit is read by the victim receiver.

3.1.1 Contributions

A bit-flip attack on serial communication that exceeds the current best 50% theoretical bit-flip limit [93] is reported. In contrast to existing work, the timing information about the victim transmitter/receiver, gathered from the EM leakage, is utilized to ensure that an attacker increases (`0->1` flip) or decreases (`1->0` flip) the apparently transmitted voltage when the victim receiver is sampling (measuring) the communication line. The contributions

are as follows:

- The analytical explanations are provided for the minimum necessary attack phases to effect controlled bit-flips in serial communication.
- The design of a narrowband attack signal (at the victim baud rate) that enable bidirectional bit-flips is reported with experimental validation. It is shown that the attacker can inject a 'desired' bit sequence into the victim frames over 98% accuracy with the suggested attack phases and waveform design approach.
- Passive countermeasures, such as twisted cables, are proposed which do not require additional signal processing/burdensome attack mitigation circuitry and are easy for designers to implement.

The effect of distance between the attacker and victim circuitry is analyzed to determine power requirements for a successful attack.

3.1.2 Related Work

Faraday's law of induction states that a time-varying magnetic field normal to the surface of a conductor loop generates a voltage between the terminals of the conductor [16]. Considering also Ampere's law, which states that any time-varying current generates a time-varying magnetic field [16], there are two common ways that an adversary can leverage EM waves to attack a system. Firstly, the adversary can adopt a 'passive' approach and listen to the EM leakage (with an antenna or field probe) of a victim system to extract information (e.g., data timing), which are classified as 'eavesdropping' or 'side–channel' attacks. Secondly, the attacker can choose an 'active' approach and induce a voltage through IEMI to manipulate the victim device.

From the early days of World War II, it has been known that electronic devices emanate acoustic, optical, thermal, and electromagnetic waves largely correlated to their operation [26]. The time-varying currents in an electronic system (e.g., cryptographic hardware) generates a magnetic field which can be eavesdropped on by an attacker with a field probe or an antenna, and the captured field can be processed to extract secret information, e.g., cryptographic key [60, 88, 112]. This attack vector, commonly referred to as a side-channel (with historical instances such as 'TEMPEST'), is recognized by organizations like NATO, and official guidelines are publicly shared to protect safety-critical systems from eavesdropping attacks [7]. Sayakkara et al. review a variety of eavesdropping attacks on Internet of Things (IoT) devices [88]. Previous work has shown that EM leakage from computer screens (or TV screens with cathode ray tubes) can be used to extract the image or text displayed on the screen [38, 51, 112].

Although row hammer attacks, which exploit the electrical interaction between densely spaced DRAM cells [84, 85], are classified as bit-flip attacks, they exploit a hardware vulnerability and do not use IEMI. Attackers can use EM pulses to inject transient faults to encryption applications which have similarities with the transmission phase of the bit-flip attacks[17, 33, 70], though these attacks lack the precision of our attack, do not occur at a distance, and require more control over the targeted device. Various IEMI attacks on analog sensors have been demonstrated: Kune et al. show that electrocardiogram machines, cardiac implementable electric devices (CIEDs), and microphones can be attacked with IEMI. Using, e.g., an attack power of 10 W and a monopole antenna, an attacker could induce an artificial pacing inhibition on CIEDs from a distance of '1 m to 2 m' [61]. Kasmi and Esteves demonstrate that an amplitude–modulated FM–band signal can inject spurious voice commands to a mobile phone [57]. Shoukry et al. present two types of IEMI attacks on the magnetic speed sensors of anti-lock braking systems (ABSs) [95]. The first attack, which is

called 'disruptive' and 'uncontrollably' distorts the speed data; the second attack, which is called 'spoofing', senses and erases (with active shielding) the original magnetic field that carries the speed information, and injects false speed data with a specially crafted magnetic field. Although the 'disruptive' and 'spoofing' attacks have certain superficial similarities with bit-flip attacks, they target the magnetic field measured by a magnetic speed sensor and not digital data represented by line voltage (the latter requiring application of both Ampere's law and Faraday's law while the former uses only Ampere's law, with consequent lower attack difficulty and constraints).

In general, analog data manipulation requires lower power relative to bit-flip attacks on digital systems. In analog sensor attacks, an attacker can exploit nonlinearities of ADCs and amplifiers with a small induced voltage (e.g., 100 mV) [93]; however, a bit-flip requires an induced voltage comparable to the logic level, e.g., 3.3 V for CMOS [32, 93]. False Actuation Injection (FAI) attacks also require high voltages to be induced on the victim circuitry like the reported bit-flip attacks of [32, 93]; however, FAI and bit-flip attacks have discrepancies because the targeted data is transmitted differently. For example, while actuation data is encoded in the duty cycle of the actuation signal, the communication data is sent through bits (i.e., FAI requires manipulation of duration while we target a signal's value at a particular instance in time).

3.2 Threat Model

The attacker attempts to alter serial data by targeting the output(s) of serial communication peripherals operating at CMOS/TTL logic levels (i.e., 3.3/5 V). Serial communications that use physical layer signaling with higher voltages (e.g., RS-232) or differential signaling (e.g., RS-422) are still vulnerable to our attack, as such systems are typically implemented using,

for example, a UART peripheral connected to a line driver that translates CMOS/TTL output signals of the peripheral to the required line voltages.

The attacker system has no physical connection to the victim hardware and the communication signal(s) are manipulated solely through wirelessly conducted IEMI. The attacker is in the vicinity of the victim and leverages COTS hardware (e.g., an arbitrary waveform generator, amplifier, low pass filter, low noise amplifier, and a magnetic field probe) to eavesdrop upon the victim and generate IEMI. The term 'false data' is used generically to refer to bits that are flipped in an uncontrollable manner, while the term 'desired false data' is used to refer to bits flipped in a controllable manner. The attacker effects injected data through a narrowband waveform. It is assumed that the attacker knows the nominal bit duration (i.e., baud rate) of the serial frames in advance (and that the duration is constant within a frame), as well as knowing the length of frames (also constant), which is practically implemented in most serial protocols. An attacker can obtain these parameters (bit duration and frame length) through eavesdropping upon communications before initiating the attack (Section 3.4.1).

The receiver of a serial communication system samples the incoming data at the center of each data bit [31]. An attacker, with the information of the victim sampling time, can generate a specific waveform to increase or decrease the victim voltage at the sampling instants to flip bits in a controllable manner. The reported narrowband is designed such that the victim voltage is increased or decreased at the sampling times to flip bits.

Finally, it is assumed that the attacker is utilizing magnetic near-field coupling to make the attack effective in the presence of radio–frequency (RF) shielding [93]. Requisite structures to generate and direct such fields include electrically small loops, solenoids, and toroids.

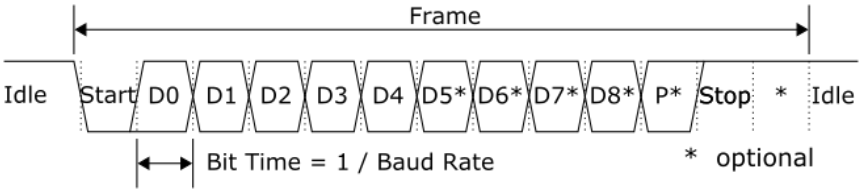


Figure 3.2: UART data frame has 8 data bits. The channel is high in idle mode (i.e., when there is no data transmission), and the start bit is low which starts the data transfer.The stop bit can be 1 1.5, and 2 bit long, and the last 4 bits of the data frame is optional.

3.3 Universal Asynchronous Receiver–Transmitter Communication

A UART device has two ports which are Tx and Rx, for transmitting and receiving data (Figure 3.1). UART device is also responsible for converting parallel data to serial for Tx or vice versa for Rx. The data transmission is asynchronous, which means that there is not a master clock to synchronize Tx and Rx, and the data transfer starts when there is data in the channel (i.e., triggered by the high to low transition for the start bit). A UART data frame always starts with a zero bit (Figure 3.2) which results in a high-to-low transition as the channel is high in idle mode, i.e., no data mode. This high-to-low transition at the beginning of the data frame triggers the receive operation, and the Rx port starts to sample the data multiple times (e.g., 16 times) of the universally defined baud rate (e.g., 9.6 kbps). A UART data frame includes a start bit, 5 to 8 data bits, one or no parity bit (i.e., optional), and 1, 1.5, or 2 stop bits [31]. The attacks will be shown on frames with 8 bit ($D0$-$D7$) data and one stop bit without parity check (Figure 3.2). The reported attacks are applicable to UART frames with parity check option as well.

The receiver module samples the incoming data in the center of each data bit. A common method is to adjust the receiver clock frequency to 16 times the baud rate (e.g., 153.6 kSPS for 9.6 kbps). After the high-to-low transition of the start bit (Figure 3.2), The first sampling

is made in the middle of the start bit (i.e., at the 8th clock cycle) to guarantee that there is data in the channel, and the detected high to low transition is not because of noise [31]. Then, the sampling is done for every 16 clock cycles which are in the middle of data bits to detect the data.

3.4 Mechanism of Bit–flip Attacks

With the information of the victim sampling time, an attacker can synchronize the attack waveform to the victim data to increase or decrease the victim voltage at the victim sampling times, and flip certain bits to inject the desired data. Bit-flip attacks have three phases: *detection*, *signal processing*, and false data *transmission* (Figure 3.1). In the detection phase, the EM leakage of the original data is monitored by a receiver system. In the *signal processing* phase, the victim EM leakage is digitized, and the exact timing of the victim data is detected through a threshold detector. After the detection of the victim data, the *transmission* phase

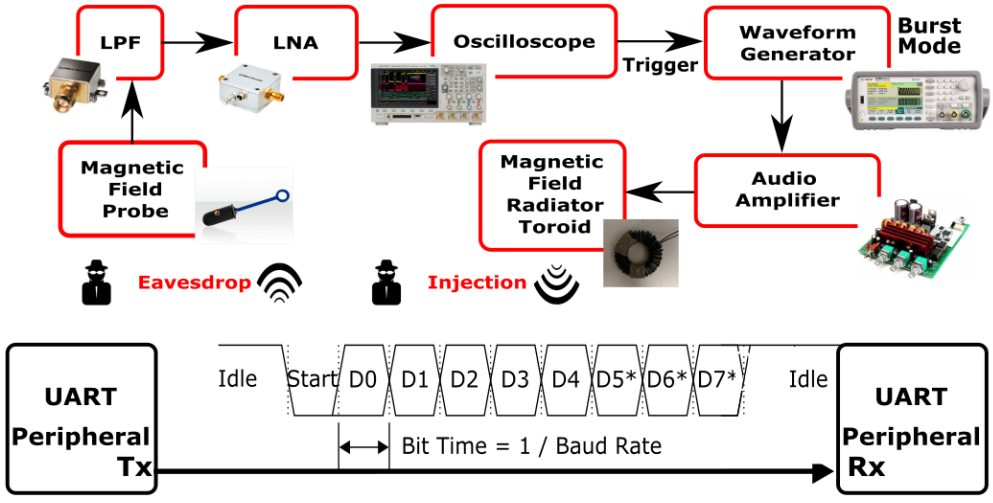


Figure 3.3: Attacker hardware includes components to eavesdrop the EM leakage to detect the victim data in the channel. The attack waveforms are injected to the channel through a magnetic field radiator (e.g., toroid) .

starts in which the desired data is injected into the system with the attack waveforms.

3.4.1 Phase I: Detection

In the *detection* phase, the attacker passively listens to the EM leakage of the victim circuitry. When the data transmission begins, the high voltage in the idle UART channel is taken to 0 V for the low start bit (Figure 3.2), and a small but detectable time-varying victim current, i_v, which radiates a magnetic field, B_v, circulates in the UART circuitry. B_v is captured by a field probe as illustrated in Figure 3.4a.

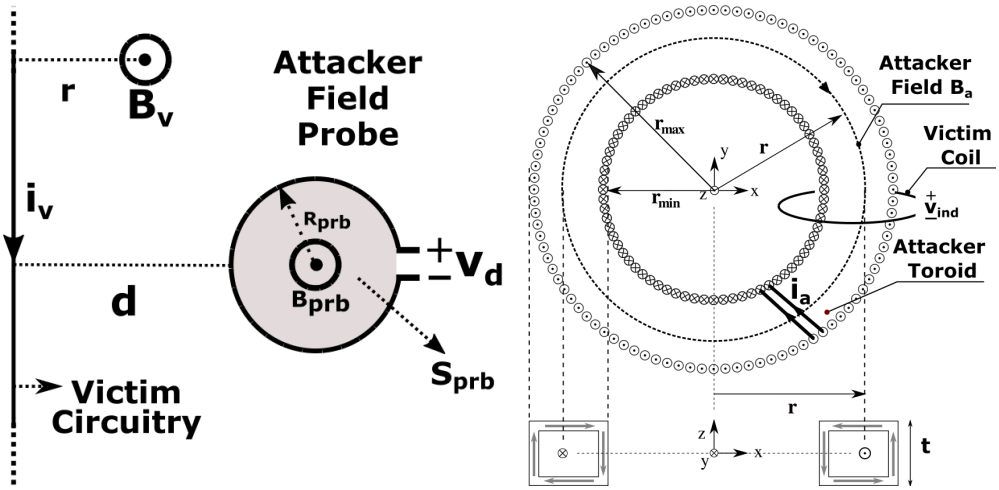
Faraday's law of induction states that a time-varying magnetic field normal to a conductor loop results in an electromotive force (emf) on the free electrons of the conductor, and generates a potential difference between the terminals of the conductor [16]. To determine the relationship between the victim current, i_v, and detected voltage from a field probe, v_d, the model in Figure 3.4a is used. A circular field probe is located at a distance d from the victim signal line. The victim current, i_v, is assumed to be infinitely long, which holds for the signal lines with a much larger length than the probe radius, R_{prb}.

$$B_v = \frac{\mu_o \, i_v}{2\pi r} \tag{3.1}$$

where μ_o is the free space permeability and B_v is the victim circuit normal to the attacker probe surface (Figure 3.4a). The induced voltage, v_d, on the terminals of the field probe is the time derivative of the flux captured normal to the field probe surface.

$$v_d = -\frac{d}{dt} \iint_{S_{prb}} B_v \cdot dS = -\mu_o \frac{d}{dt} \iint_{S_{prb}} \frac{i_v}{2\pi r} \cdot dS \tag{3.2}$$

If the field probe radius is small compared to the eavesdropping distance ($R^2_{probe} < d^2_{eav}$), the



(a) (b)

Figure 3.4: The *detection* and *transmission* phases are analytically analyzed with models. (a) Detection Phase: The magnetic field, B_v, due to the victim current, i_v, is captured by an attacker with a magnetic field probe. The detected voltage, v_d, includes the voltage peaks due to the rising and falling edges in the victim circuitry, which enable the attacker to synchronize to the victim system. (b) Transmission Phase: The ferrite toroid, with high permeability, provides a low reluctance path for attacker magnetic field, B_{atk}. This enables the attacker to generate high magnetic fields to manipulate the voltage in the victim UART coil.

victim EM leakage, B_v, on the probe surface is approximately uniform and equal to the field at the center of the probe, $r = R_{prb} + d$.

$$B_v = \mu_o \frac{i_v}{2\pi(d + R_{prb})}, \text{ on probe surface} \tag{3.3}$$

The detected voltage, v_d, is found with (3.2) and (3.3):

$$v_d = -\mu_o \frac{R_{prb}^2}{2(d + R_{prb})} \frac{d}{dt} i_v \tag{3.4}$$

Theoretically, a larger loop captures more flux, and consequently more v_d is generated in the field probe terminals; however, in practice, a larger loop introduces additional noise to the system. On the other side, the detected voltage, v_d, is linearly proportional to the time rate

of the victim current, i_v. Thus, the attacker detects abrupt changes, such as the high-to-low transition at the beginning of the start bit (Figure 3.2), in the victim circuitry relatively easily.

To observe the effect of detection distance on the monitored EM leakage, an experimental setup, which includes a victim–UART communication system and a low noise receiver, is employed (Figure 3.5a). The victim UART devices, which are connected with a 30 cm signal cable, send and receive a data frame of '`10101010`' to maximize the transition numbers. The attacker receiver, which consists of a magnetic field probe with a radius of 2.5 cm (Aaronia PBS), a Low Noise Amplifier (Minicircuits ZFL-500LN), and a Low Pass Filter (Minicircuits ZX75LP-83+), monitors the EM leakage with a digital oscilloscope at a sampling rate of 100 Msps.

It is observed that the voltage peaks due to the bit transitions in the victim data are detectable up to a distance of 30 cm. Figure 3.5b shows 10 voltage peaks, which points the high-to-low and low-to-high transitions at $d = 10$ cm. Another observation is that the voltage peaks have reversed polarity for high-to-low and low-to-high transitions of the victim because of the inverted direction of i_v. Figure 3.5c demonstrates the EM leakage of a single transition with varying attack distance, and it is observed that the leakage has a damped sinusoid characteristic. Figure 3.5d compares the measured and analytically found (3.4) peak voltage values with varying d. It is observed that analytical and measured values fit when $max(di_v/dt) = 8 \times 10^6\,\mathrm{A\,s^{-1}}$ (Figure 3.5d), which means a peak current of 80 mA circulates in the victim cable assuming a victim rise time of 10 ns.

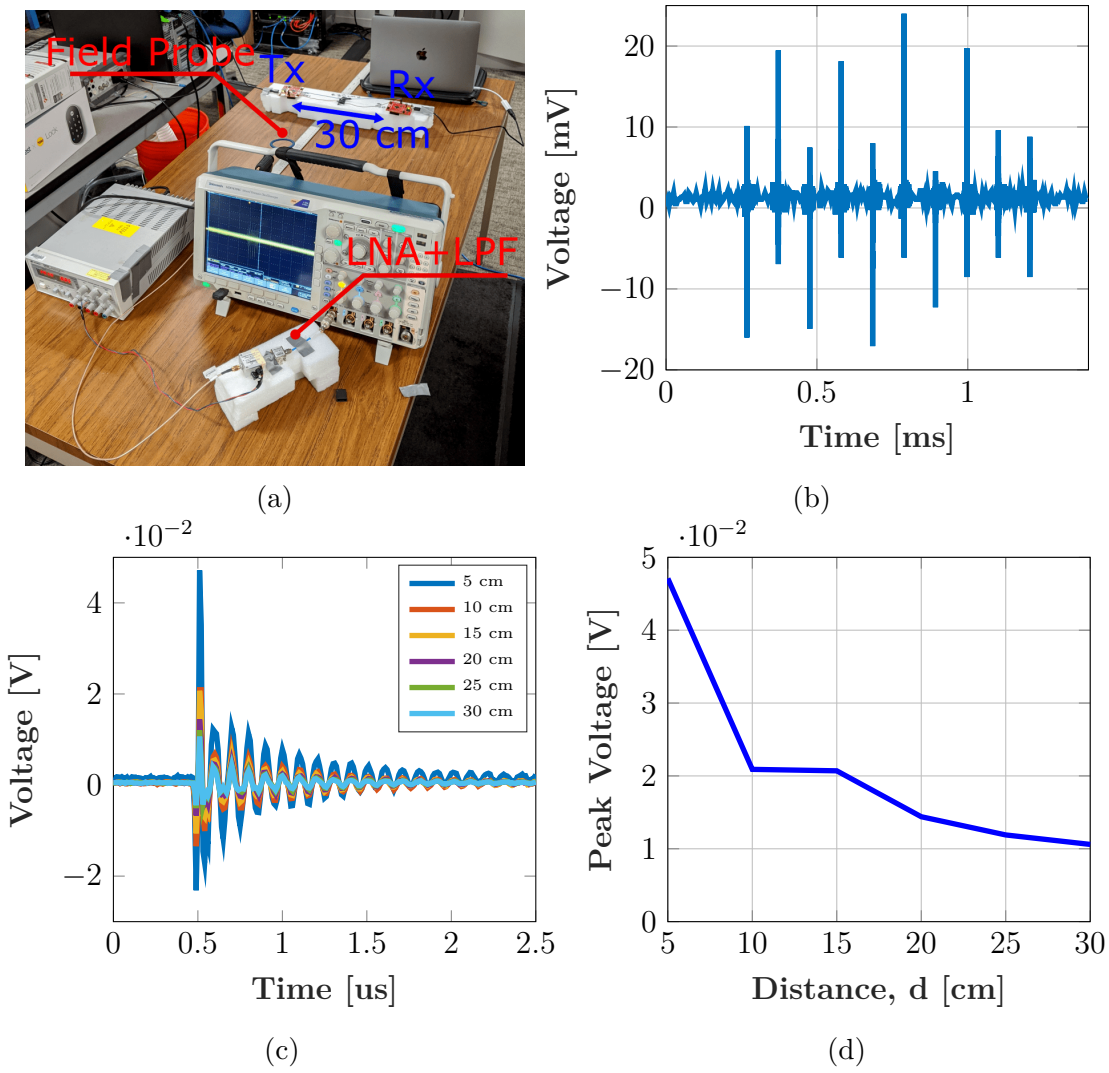


Figure 3.5: For victim data detection, a low noise receiver with a magnetic field probe (Aaronia PB4), an LNA (Minicircuits ZFL-500LN), and an LPF (Minicircuits ZX75LP-83+), is used. The detection distance, d, between the field probe and victim cables is varied. (a) Experimental setup (b)The EM leakage for the UART frame '1010 1010' at $d = 10\,\text{cm}$ is shown. 10 voltage peaks are detected due to the transitions of the start bit and data. The sampling rate is 100 Msps and the average of 16 measurements is shown. (c)The detected traces (average of 16) for a single peak is shown with varying d. (d)The maximum voltage of the EM leakage decreases with increasing detection distance, d; however, it is still possible to detect the frames from $d = 30\,\text{cm}$. Analytically found peak (3.4) values align with the measurements ($max(di_v/dt) = 80 \times 10^6\,\text{A}\,\text{s}^{-1}$).

3.4.2 Phase II: Signal Processing

In the *signal processing* phase, the analog EM leakage is digitized and voltage peaks due to transitions (e.g., low-to-high) in the victim data are detected with a threshold operation to send the attack waveform. The *signal processing* process should have low latency to ensure that even the first bit after the start bit, e.g., `D0` in the UART frame, can be altered with the EMI after the detection (Figure 3.2). For instance, the attack waveform should be transmitted in 156.25 µs, which is the duration of 1.5 bit, for flipping `D0` in a 9.6 Kbps UART system. The maximum allowable latency becomes more stringent as the baud rate of the communication increases; however, higher frequency attack waveforms can be used in those scenarios which improve the coupling to the victim and increase the attack distance. The latency of digital oscilloscopes and waveform generators which will be used in the attack demonstrations is measured and found to be below 150 ns.

A variety of processors like Software Defined Radios (SDR), Field Programmable Gate Arrays(FPGA), or Digital Signal Processors (DSP) can be used for the *signal processing* phase. Due to the simplicity of application development and portability, an SDR is a viable option for the *signal processing*. However, SDRs are known to have high latency [90] because the radio front-end and the general-purpose computer, in which most of the *signal processing* is done, communicates through an interface like ethernet, USB, or PCIe. Schmid et al. reported that the round trip time (i.e., receive and transmit) of an IEEE 802.15.4 implementation without any *signal processing* application is 3 ms for an SDR application at a sampling rate of 4 Msps [90], which is higher than the maximum allowable latency 156.25 µs for a 9.6 Kbps UART bit–flip attack. On the other side, the EM leakage has frequency components up to 80 MHz which corresponds to a Nyquist rate of 160 Msps which is relatively high for many SDR devices, but there are options like USRP X300/310 from Ettus Research which supports 200 Msps operation with a PCIe interface [8]. To detect the latency of high-sampling

rate SDRs with a fast interface like PCIe, a USRP X300 with a 100 Msps sampling rate, and a PCIe interface is programmed for a round trip time measurement in GNURadio. For the round trip measurement, the X300 is programmed to detect (i.e., threshold) the transition of an inputted square wave and generate a square waveform as soon as the transition is detected. The receive port of X300 is connected to a square wave generated by a waveform generator, and when the input signal is above the threshold which is adjusted to the half of the input square wave amplitude, the SDR outputs the square wave (which resembles the attack waveform), and the time difference, i.e., latency, between the input and output square waves is detected with an oscilloscope.

The latency of the USRP X300 with a PCIe connection is measured to be between 8 ms and 15 ms in three consecutive measurements. The SDR latency is not consistent throughout the measurements, which makes an SDR a poor choice for bit–flip attacks that require precise synchronization to the victim data. Additionally, the minimum SDR latency even with high-end USRPs such as X300 and fast interfaces like PCIe is at least 8 ms, which is significantly higher than the maximum allowable latency (156.25 µs) for a 9.6 Kbps UART system.

Digital oscilloscopes, with sampling rates up to 5 Gsps, can be utilized for the digitization of the victim EM leakage and trigger the attack waveform. The latency of the digital oscilloscope is defined as the time delay between the instance the signal detected at the oscilloscope input and trigger transmission from the oscilloscope trigger output. The oscilloscope trigger output sends a low-to-high signal when the oscilloscope detects a peak above a certain threshold, which is adjusted manually during the attacks. To measure the latency of the oscilloscope, a pulse signal, which is generated by a waveform generator, is sent to the first oscilloscope input, and the trigger output of the oscilloscope is connected to the second oscilloscope input, and the time difference, i.e., oscilloscope delay, between the two signals is measured three times for each oscilloscope. The measurement procedure is applied to two

digital oscilloscopes, namely Keysight DSOX3024T and Tektronix MDO4104C, and it is observed that the latencies are 24 ns and 40 ns for Tektronix and Keysight models, respectively (Table 3.1). The first conclusion is that the latency of each oscilloscope is significantly lower than the required latency (e.g., 156.25 µs for a victim with a baud rate of 9.6 kbps). Additionally, the oscilloscope latencies are very consistent, unlike the SDR latencies. As soon as the oscilloscope detects the voltage peak (e.g., the peak due to the start bit of the UART data frame) in the victim EM leakage, the trigger signal of the oscilloscope is sent to the waveform generator to start the attack waveform injection (Figure 3.3, so the latency of the waveform generator, which is the time delay between the reception of the trigger signal (from the oscilloscope) and transmission of the attack waveform, also adds to the overall latency of the *signal processing* phase. To detect the latency, the waveform generator (Agilent 33600A) is programmed to a 'burst mode' in which a sinusoidal signal is triggered by the external signal i.e., oscilloscope trigger output. A pulse signal, which is generated by another waveform generator and triggers the 33600A, and the waveform generator output are connected to a digital oscilloscope, and the latency between the trigger and waveform generator output is measured. It is observed that the latency of Agilent 33600A is consistent and 150 ns (Table 3.1). Even though the latency of the waveform generator is higher than the latency of the tested digital oscilloscopes (Table 3.1), it is still far below the required latency. This shows that an oscilloscope and a waveform generator, with a total latency of approximately 200 ns can be utilized as the *signal processor* as displayed in Figure 3.3.

Table 3.1: The latencies of the digital oscillators and the waveform generator are measured.

	Measurement 1	Measurement 2	Measurement 3
Keysight DSOX3024T	40 ns	40 ns	40 ns
Tektronix MDO4104C	24 ns	24 ns	24 ns
Agilent 33600A	150 ns	150 ns	150 ns

3.4.3 Phase III: False Data Transmission

As soon as the victim data is detected, the *transmission* phase is initiated to radiate the attacker waveform to the victim circuitry. The attacker uses a magnetic field radiator like a toroid, a solenoid, or a loop antenna to efficiently generate a magnetic field and induce a voltage on the victim circuitry (Section 3.2). To find the relationship between the attacker current, i_a, and the induced voltage, v_{ind}, a ferrite toroid model, which is wound by a single victim coil, is derived as shown in Figure 3.4b. The attacker current, i_a, produces a magnetic field, B_a, the interaction of which with the free electrons of the victim circuitry, results in an induced voltage, v_{ind}. The relationship of i_a and B_a is found with Ampere's law [16]:

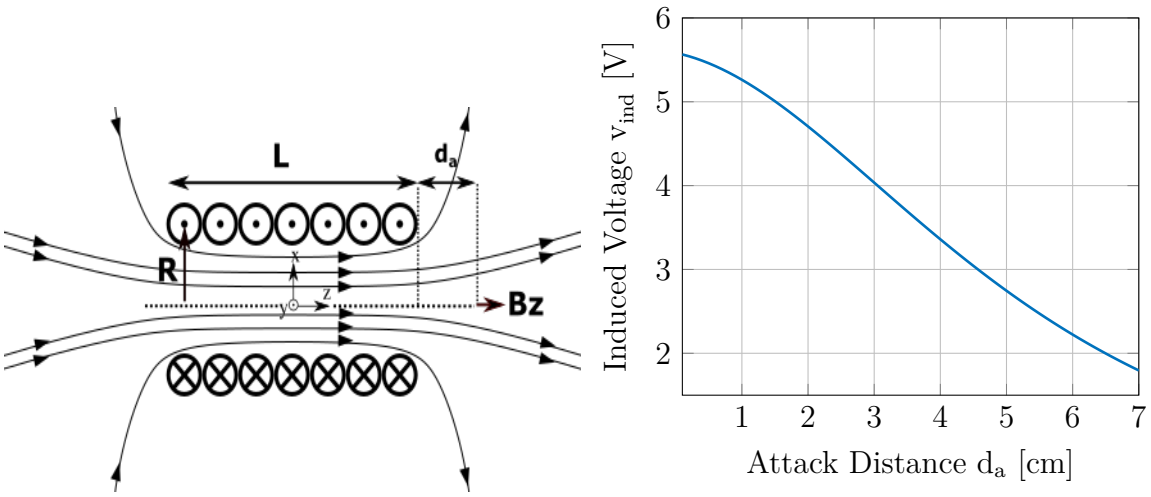
$$B_a(r) = \begin{cases} \frac{\mu N i_a}{2\pi r}\hat{a}_r, & r_{min} < r < r_{max}, \quad |z| < t/2 \\ 0, & \text{elsewhere} \end{cases} \tag{3.5}$$

where t, r_{min} and r_{max} are the thickness, minimum radius, and maximum radius of the toroid (Figure 3.4b). The attacker magnetic field, B_a, has a radial orientation ($-\hat{a}_\phi$) and only exists inside the toroidal coils because the enclosed current is zero out of the toroidal coils. If one coil of the victim cable (e.g., UART cable) is positioned around the toroid as shown in Figure 3.4b, the magnetic flux, ϕ_a, captured by the victim is:

$$\phi_a = \iint_{S_{toroid}} B_a \cdot dS = \frac{\mu N t}{2\pi} \ln\left(\frac{r_{max}}{r_{min}}\right) i_a \tag{3.6}$$

Faraday's law of induction states that the induced voltage, v_{ind}, in a conductor coil is the time derivative of the normal magnetic flux captured by the coil surface, so the relationship of i_a and v_{ind}:

$$v_{ind} = -\frac{d}{dt}\phi_a = \frac{\mu N t}{2\pi} \ln\left(\frac{r_{max}}{r_{min}}\right) \frac{d}{dt} i_a \tag{3.7}$$



(a) (b)

Figure 3.6: (a) The ferrite toroid, with high permeability, provides a low reluctance path for attacker magnetic field, B_{atk}. This enables the attacker to generate high magnetic fields to manipulate the voltage in the victim UART coil. (b) A solenoid or a loop, with magnetic fields radiating outside the coils, can be used for attacks from a distance. (c) The induced voltage on a 1 cm^2 victim loop, by a 100-coil victim loop antenna with a radius of 7 cm. The current is continous with 20 A amplitude at 500 kHz. B_z is detected with (2.10)

3.4.4 Bit–Flip Attacks from Distance

Although ferrite toroid is an efficient magnetic field generator, the field is confined in the ferrite material (3.5) which requires the toroid to be positioned around the victim cable. However, the attacker can utilize a solenoid (or a loop) as illustrated in Figure 3.6a with an outward magnetic field to flip bits from a distance. The z-axis magnetic field, B_z, of a solenoid is [24]:

$$B_z = \frac{\mu N i_a}{2}\left(\frac{L/2-z}{L\sqrt{R^2+(L/2-z)^2}}+\frac{L/2+z}{L\sqrt{R^2+(L/2+z)^2}}\right) \tag{3.8}$$

where μ is the permeability of the medium, i.e., air. A victim loop with an area of 1 cm^2, the normal of which is aligned and centered to the z-axis, is assumed to find v_{ind} with varying attack distance, d_a between solenoid and victim loop. The captured magnetic flux is found

Table 3.2: Attacker dimension and current for induced voltages reported in Figure 3.6b

Coil Number	Radius(R)	Length(L)	i_a	Frequency(f)
100	7 cm	1 cm	20 A	500 kHz

analytically (3.6), and v_{ind} is detected with a time derivative (3.7). Induced voltage, v_{ind}, with varying attack distance, d_a, is shown in Figure 3.6b. The attacker generates 3.36 V at $d_a = 4$ cm and achieves bit flips in a digital channel (3.3 V logic) with the current and loop parameters given in Table 3.2. However, the relatively high current (20 A) and coil number (100) show that generating a large enough v_{ind} with a continuous signal (i.e., sinusoidal) at sub-MHz frequency is practically challenging. This is expected because, at sub-MHz frequencies where the wavelengths are larger than 300 m (assuming the propagation medium is air), the victim resonance (e.g., cable), which is at a higher frequency [61, 93], can not be exploited as discussed in [61, 93]. Adding to that, as v_{ind} is linearly proportional to the attack frequency in a continuous waveform (i.e., time–derivative of a sinusoid), the low–frequency attacks suffer from low coupling efficiency as well. To overcome this, current waveforms like a sawtooth with abrupt changes and large time derivatives as suggested in [93] can be utilized. Another option is the pulsed current generators, which generate a high current for a very short amount of time, as practiced in Transcranial Magnetic Stimulation (TMS) applications [29, 39].

3.5 Narrowband Attack Waveform Design

The relationship in (3.7) shows that the induced voltage to the victim coil has the same form as the time derivative of the attacker current. On the other side, a ferrite toroid acts as an ideal inductor at frequencies below its self-resonance frequency where the parasitic capacitance between the coils is negligible [104]. Due to this inductive characteristic, the

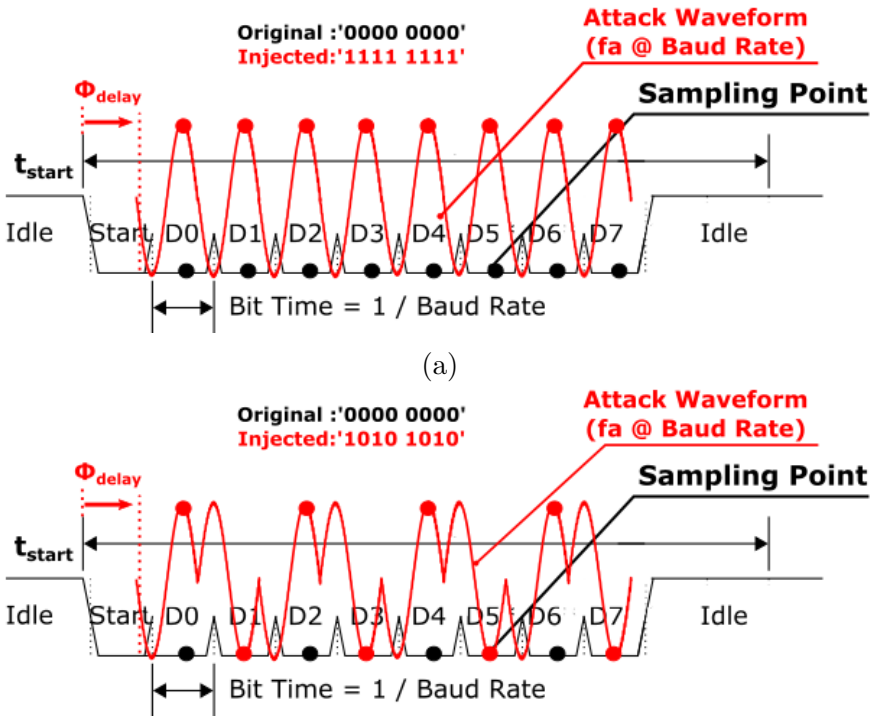


Figure 3.7: Attack waveforms to inject false data frames. The original data frame is 0x00. (a)The attack waveform is synchronized to the victim sampling points (block dots) by adjusting the ϕ_{delay} and tuning the attacker frequency to f_a (e.g., 9.6 kHz for 9.6 kbps baud rate) (b)To inject 0xAA (i.e., induce 0s and 1s), inverted cycles should be used. The attack waveform does not affect the bit values which are already desired values by the attacker (D1, D3, D5 and D7).

attacker voltage, v_a applied to the toroid (e.g., from the attacker amplifier) and the attacker current, i_a has the relationship:

$$v_a = L_a \frac{d}{dt} i_a \tag{3.9}$$

where L_a is the attacker or toroid inductance which is a constant at the attack frequency. The comparison of 3.7 and 3.9 shows that the induced voltage, v_{ind}, and attacker voltage, v_a, has the same forms, i.e., the attacker induces a voltage which is a copy of the attacker waveform with varying magnitude depending on the coupling between attacker and the victim. This relationship is used to decide an optimum attacker waveform to inject false data frames.

To flip a bit, an adversary needs to increase or decrease the victim voltage by a value comparable to the logic level of the victim, e.g., 3.3 V. For instance, input-high voltage threshold for a TIVA C microcontroller GPIO pin is $0.65 \times V_{DD}$ [106], which means v_{ind} should be at least $0.65 \times 3.3\,\text{V} = 2.145\,\text{V}$ to flip a zero to one. As the UART receiver samples data with the baud rate at the center of each bit [31], a sinusoidal attack waveform at the baud rate can be used to flip bits and inject the desired false data. The attacker aligns the attack waveform to the original data by adjusting the delay (ϕ_{delay}) as shown in Figure 3.7, and the polarity (i.e., phase) of each cycle determines whether a `0` or `1` is injected. Figure 3.7a illustrates an attack waveform to flip all bits to `1` in the victim frame.

While the attack waveform applies to any victim data, the victim frame is assumed to be `0x00` (i.e., all `0`s) for illustration purposes. As the ϕ_{delay} is adjusted so that maximums of v_{ind} are aligned with sampling instants, the attacker flips all the bits to `1` (Figure 3.7a). In Figure 3.7b, the attacker induces a waveform with inverted sinusoidal cycles (180^o out of phase) to inject '`10101010`' (`0xAA`).

Assuming the original data frame is `0x00`, the attacker only flips the `D0`, `D2`, `D4`, and `D6` from `0` to `1`, while inducing a negative voltage but not affecting the `D1`, `D3`, `D5`, and `D7` which are already low. This shows that to inject a desired frame into the victim, the adversary does not need to determine the original data. The attack waveform can be generated with sinusoidal *cycles* as follows where $T = \frac{1}{baudrate}$:

$$cycle(t_c) = \begin{cases} sin(2\pi t_c/T) & 0 < t_c < T \\ 0 & elsewhere \end{cases} \tag{3.10}$$

The attack waveform, v_a, is the sequence of the *cycles* the polarity (i.e., phase) of which is determined by the false data, F, to be injected. The attack waveform for an 8 bit UART

frame has the form (3.11):

$$v_a(t) = \sum_{n=0}^{7} cycle(t - nT - F[n]180^\circ) \tag{3.11}$$

Binary Phase Shift Keying (BPSK) utilizes two phases which are separated by 180° to modulate data [118]. The reported attack waveform has the same form with BPSK modulated injected data at the attack frequency, i.e., baud rate. For instance, the red attack waveform in Figure 3.7b is nothing but BPSK modulated false data, `0xAA`. With a BPSK modulator, the generation of the attack waveform is straightforward.

3.6 Bit–Flip Attack Demonstrations on a UART Communication System

In this section, the efficacy of bit-flip attacks will be demonstrated on a victim system communicating with UART using narrowband attack waveforms. We then discuss the computation of frequency response and the generation of wideband attack waveforms.

3.6.1 Victim System Description

The victim system consists of two TIVA C microcontrollers communicating through UART (Figure 3.8). The transmitter device sends an 8-bit frame with a baud rate of 9600 bps at every 1 s period. The Tx and RX devices are connected with 30 cm ground and UART cables as demonstrated in Figure 3.8. The receiver sends the detected (and possibly attacked) data to a personal computer through a Universal Serial Bus (USB) connection to record and observe the attack.

3.6.2 Attacker System Design

The attacker system, illustrated in Figure 3.3, is used for the attack demonstration shown in setup Figure 3.8. The EM leakage of the original victim frame is detected (i.e., *detection* phase) with a magnetic field probe, which is located 1 cm away from the UART circuitry, a Low Noise Amplifier (Minicircuits ZFL-500LN), and a Low Pass Filter (ZX75LP-83+). The amplified and filtered EM leakage is fed to a digital oscilloscope to digitize and detect the data frame with a threshold. The threshold voltage level for peak detection, which varies with the orientation and distance of the field probe to the victim circuit, is empirically adjusted.

The waveform generation is initiated by the trigger output of the digital oscilloscope, Tektronix MDO4104C, which is connected to the trigger input of the arbitrary waveform generator (AWG), Agilent 33600A. When the peak is detected (i.e., the victim data is transmitted.), the oscilloscope generates a low-to-high trigger signal and the narrowband attack waveform is transmitted.

The AWG has a limited output power (1 W), and the attack waveform should be amplified to induce sufficient voltage in the victim circuitry, e.g., UART cable. Due to the relatively low attack frequency ((9.6 kHz or 19.2 kHz), an audio amplifier is used for amplification. The output of the low-cost (20$) mono channel audio amplifier with a rated power of 420 W is connected to a 70-coil air-gapped ferrite toroid. The air gap is employed to conveniently locate the ferrite toroid around UART or ground cables (i.e., without unplugging the victim cables), and the air gap can be filled with a ferrite piece after placement of the toroid to enhance the attack field.

As the audio amplifier is matched to a 4 Ω load, the toroid, with an inductance of 550 µH, is put in series with a capacitor 500 nF to minimize the imaginary impedance of the load at

the attack frequency, i.e., 9.6 kHz. However, at the resonance, as the series capacitor and toroid have a low real impedance which is 2 Ω, an additional series resistance is added to match the load to 4 Ω.

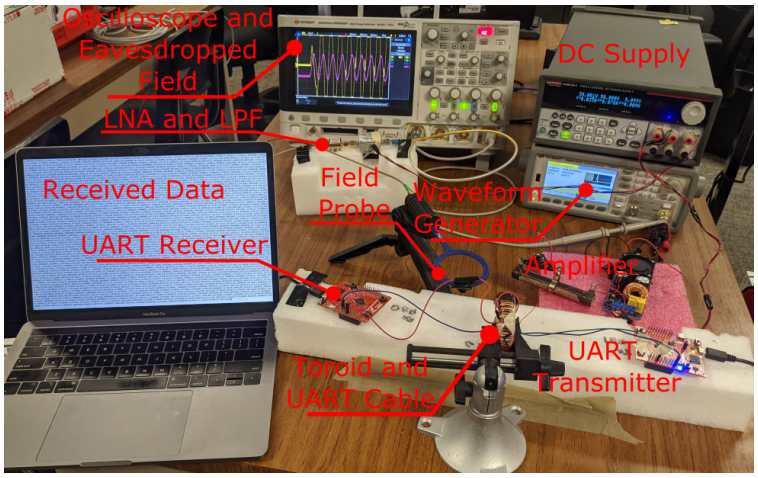


Figure 3.8: The experimental setup for UART bit-flip attacks. The original UART frame is detected by the receiver circuitry that consists of a magnetic field probe, LNA, and LPF. The oscilloscope triggers the arbitrary waveform generator which is programmed to generate the BPSK attack waveform designed for the desired frame to be injected. The attack waveform is amplified and transmitted to the victim circuitry through an audio amplifier and a toroid. One coil of the victim UART cable is wound around the toroid to increase the induced voltage.

3.6.3 Results

To flip bits and inject false data, the attacker needs to synchronize the induced waveform v_{ind} to the victim frame by adjusting ϕ_{delay} (Figure 3.7). To observe the effect of ϕ_{delay}, two attack scenarios are demonstrated with varying ϕ_{delay} (Figure 3.9). In the first scenario, the attacker aims to inject a data frame of all 1s (0xFF) to a chosen data frame in the channel. The transmitter device is programmed to send frames of all 0s (0x00) once every second. To test the attacker's ability to manipulate chosen data frames, the attack waveform illustrated in Figure 3.7a is applied periodically at every 8 victim frames with a varying ϕ_{delay}. The

second scenario is similar to the first one, but the attacker injects all 0s (0x00) to a channel with original frames of all 1s (0xFF).

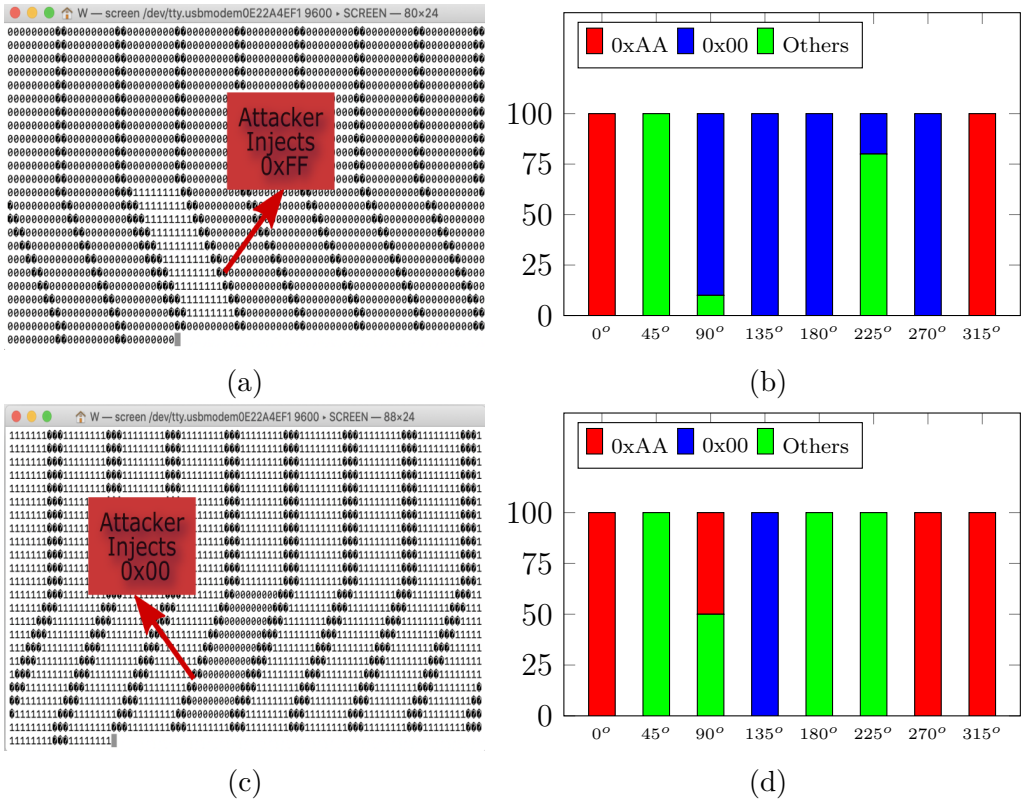


Figure 3.9: The relationship of the attack waveform delay (ϕ_{delay}) and attack success is tested. (a)The attacks are applied 10 consecutive times with a period of 8 data frames. The attacker can inject the false frame (`0xFF`) in each trial when the delay, ϕ_{delay}, is $\phi_{delay} = 0°$. (b) The success of the attacks depends on ϕ_{delay}. When ϕ_{delay} is $\phi_{delay} = 0°$ or $\phi_{delay} = 315°$, each of the 10 attacks is able to inject desired data frame (`0xFF`); however, the attacker is not able to flip bits when ϕ_{delay} $\phi_{delay} = 135°$ or $\phi_{delay} = 180°$. (c) The attacker aims to inject all 0s (`0x00`) when the original data is all 1s (`0xFF`). (d) The injected data bits to the victim with varying ϕ_{delay} values are shown. The attacker can inject all 0s when the ϕ_{delay} is $\phi_{delay} = 135°$.

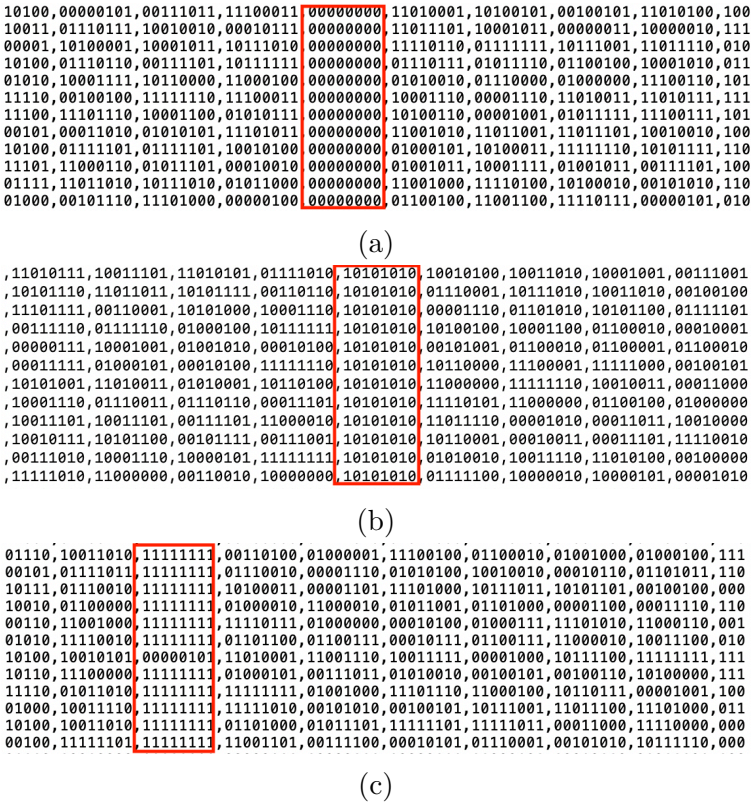
The received data for the first scenario is shown in Figure 3.9a for $\phi_{delay} = 0°$. The first observation is that the attacker is successful in flipping bits and injecting a false frame of all 1s (0xFF). However, the attack success relies on the ϕ_{delay} (Figure 3.9b). While all ten consecutive attacks are successful at $\phi_{delay} = 0°$ and $\phi_{delay} = 315°$, the attacker has no effect

when $\phi_{delay} = 135°$ and $\phi_{delay} = 180°$ which are the inverted version of the successful delay , i.e., 180° difference. This observation validates the theory that if the waveform is shifted $\phi_{delay} = 180°$ (i.e., inverted) the polarity of v_{ind} is reversed. For other ϕ_{delay} values like $\phi_{delay} = 45°$ and $\phi_{delay} = 225°$, false frames other than 0xFF are injected which means that the attack waveform randomly flip bits but not successful in injecting data in a controllable manner (Figure 3.9b). In the second scenario, in which the attacker aims to flip 0s to 1s and inject an all 1s (0xFF) frame, the ϕ_{delay} is adjusted to 0°, and it is observed that the attacks are not successful unlike the previous scenario ((Figure 3.9d)). However, when ϕ_{delay} is adjusted to 135°, the attacker can inject the false frame with a %100 success rate (Figure 3.9c).

To assess the efficacy of FDI attacks, repetitive attacks are applied to inject '0x00', '0xFF', and '0xAA' to the UART channel. The success rates are summarized in Table 3.3. The attacks can be implemented for any desired false frame with the waveform design process explained in the Section 3.5; however, 0xAA ('1010 1010') is chosen to have maximum inverted sinus cycles and discontinuities as illustrated in Figure 3.7b. The transmitter device is programmed to send pseudo-random frames to the channel, and the attacker chooses to attack one frame in every nine frames (Figure 3.10). The attacker achieves a success rate of %100 while injecting 0x00 and a section of the received attacked data is shown in Figure 3.10a. While injecting 0xAA and 0xFF, the success rate is observed to be %99.04 and %98.30 in 1146 and 707 trials, respectively (Figure 3.10b and 3.10c). It is observed that the attacker can flip bits and inject false data to the UART channel with a significantly high success rate ($>$ %98.30) (Table 3.3). The near field coupling can be in the form of inductive or capacitive in which magnetic or electric fields are used to transfer power, respectively. While capacitive coupling can be mitigated significantly with a grounded conductor (e.g., aluminum foil), low-frequency magnetic fields are very hard to shield and penetrate easily

Table 3.3: Multiple attacks to inject false frames `0x00`, `0xAA`, and `0xFF` are applied, and success rates of more than 98.30% are observed.

Injected Frame	Attack Number	Success	Success Rate
0x00	683	683	100.00%
0xAA (Attack Video)	1146	1135	99.04%
0xFF	707	695	98.30%



(a)

(b)

(c)

Figure 3.10: Samples from the attacked frames (a)The attacker injects 0x00 to the UART channel with a success rate of %100 in 683 trials. (b)The attacker injects 0xAA with a success rate of %99.04 in 1146 trials. (c)The attacker injects 0xFF; however, one of the attacks is not successful and injects 0x05 instead. The success rate is %98.30 in 707 trials.

to the electric field shields. The induced voltage by inductive coupling is proportional to the loop area of the victim loop. In the reported UART attack demonstration, the attacker positions the air gap of the ferrite toroid (where the magnetic field is maximum) between the UART and ground cable to enhance the induced voltage.

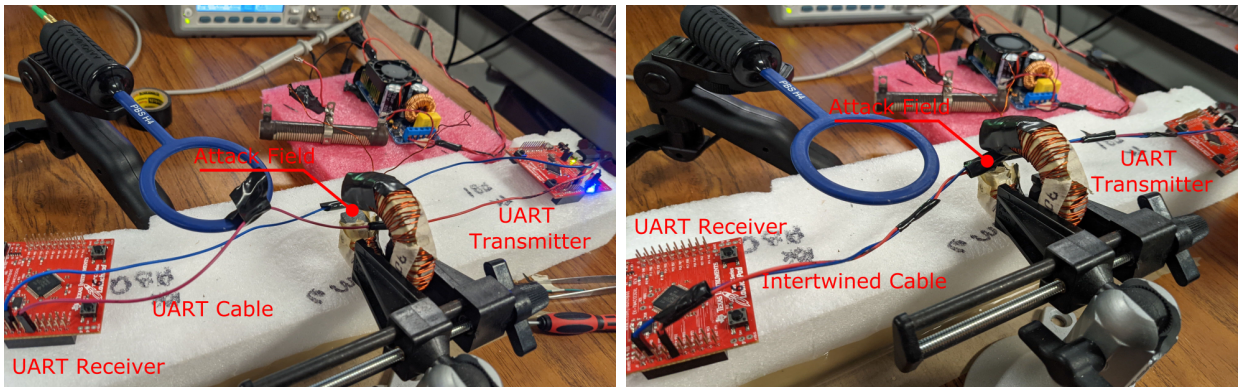
In the attack scenarios where the victim signal is not carried in a cable but in a PCB, the attacker can exploit the already established conductor loops between traces and layers [32]. The most efficient way to eliminate IEMI with inductive coupling is to minimize the loop area of the victim. In a PCB scenario, the layout design should be done accordingly by placing the ground and 'significant' signal traces (e.g., UART) as close as possible to eliminate large loops. For the scenarios in which the 'significant' signal is carried through cables, twisted cables should be used to decrease the victim area and mitigate the induced voltage and attack efficiency.

3.6.4 Twisted Cables

Twisted cables, in which two or more cables (e.g., signal and ground) are intertwined, are used to minimize the EM radiation from the cables[18]; however, twisted cables are also resilient to EMI from an outer source, e.g., a toroid. The twisted cables (Figure 3.11b) mitigate the induced voltage in two ways. First, due to the close spacing between twisted cables, the victim loop exploited by the attacker is minimized, which decreases the captured magnetic and the induced voltage. Induced voltage in a rectangular victim loop with dimensions a and b by an infinite current is found as follows in [93]:

$$v_{ind} = -\mu \left[\frac{b}{2\pi} \ln \left(\frac{d+a}{d} \right) \right] \frac{d}{dt} i_a \tag{3.12}$$

where μ is the permeability of the medium and d is the distance between loop and attacker current.(3.12) shows that as the victim loop area (a and/or b) is minimized, v_{ind} decreases significantly. On the other side, a twisted cable is a chain of small victim loops with opposite surface normals, this means that even though the attacker induces a voltage on one loop, in the next loop, assuming the magnetic field magnitude does not change significantly, the same



(a) (b)

Figure 3.11: Twisted cables decrease the attack success rate from 97.2% to 0%. (a)Signal (i.e., UART) and ground cables are not intertwined, i.e., twisted, and the attacker injects EMI into the loop in between signal and ground cables. (b) The twisted cables minimize the loop and mitigate the induced voltage significantly.

voltage is induced with an opposite sign which cancels the induced voltage in the previous loop.

To observe the efficacy of twisted cables against IEMI, the attacks are applied to regular cables and twisted cables (Figure 3.11), and the success rates are measured. Unlike the attacks in proo-of-concept demonstrations, the victim cable is not wrapped around the toroid and left inside the toroid air gap to have a fair comparison with the twisted cable (Figure 3.11a). 861 attacks are applied consecutively to the regular cable (Figure 3.11a), and it is observed that the attacker can flip 'one or more bit' in the victim frame in 837 trials with a success rate of 97.2% (Table 3.4). However, when the attacks are applied to twisted cables which are placed in the toroid air gap where the attack field is maximum (Figure 3.11b), the attacker is unsuccessful in each of the 930 trials (Table 3.4).

These results show that twisted cable is an efficient and simple way to eliminate IEMI attacks through inductive coupling when the data is transmitted through a cable. However, in scenarios where the data is sent through PCB traces, the victim is still vulnerable to the reported attacks because twisted cables are not an option.

Table 3.4: Twisted cables provide a secure data transmission channel during IEMI attacks with inductive coupling.

Cable Type	Attack Number	Success	Success Rate
Regular-Figure3.11a	861	837	97.2%
Twisted-Figure 3.11b	930	0	0%

In those scenarios, we suggest the designers determine the 'significant' signals like digital communication signals, analog sensor outputs, and actuation signals, and minimize the signal loops with closely spaced ground connections and short traces during the layout design, this will minimize the captured magnetic flux and induced voltage, and increase the resonant frequency of the traces, which makes the attacks more expensive for the attacker (e.g., more power and higher frequencies are needed for similar effects.). Another approach in a PCB scenario is twisted transmission lines designed in the PCB with vias and multilayer traces.

3.6.5 Fiber-Optic Transmission

A fiber-optic communication system converts a voltage signal (analog or digital) to light, transfers the light over a fiber-optic cable, and then reconstructs the signal from light [74]. Some advantages of fiber-optic transmission are low latency, high data rate, and resilience in EMI-rich environments [18]. Fiber-optic communication is a reliable way of transmitting data within a rich-EMI because the data is sent in the form of light through a fiber cable, which is a form of glass, in which free electrons do not exist unlike conventional transmission lines (e.g., cables, PCB traces).

We suggest transmitting 'significant' digital signals through fiber cables which void the EMI attack. One drawback of fiber-optic transmission, which requires transmitters (i.e., light-emitting diodes) and receivers (i.e., phototransistors) that convert electric signals to light and vice versa, is hardware complexity and cost. However, in relatively low-data rate

applications like UART communication, low-cost optical LEDs and phototransistors can be utilized as transmitters and receivers. For example, the cost for a low-performance fiber optic Tx-Rx couple is around $10. The fiber-optic transmission is by far the safest way (among the countermeasures discussed in this work) to transmit 'significant' signals in an EMI-rich environment because light theoretically does not interact with EMI [18, 74].

3.7 Conclusion

Serial digital communication is widely used to transfer data in cyber-physical systems between sensors, peripheral devices, and controllers. However, in this work, it is shown that the data carried in the digital communication channel can be altered in a controllable manner with intentional EMI. In this chapter, we look at the security of a widely used serial communication system, i.e., UART, and determine the weaknesses of the system in an EMI attack scenario. It is shown that an attacker can override the original data with the desired data by combining eavesdropping, signal processing, and signal injection phases with low-cost components like an audio amplifier and lab equipment like an oscilloscope. It is observed that the attacker can replace the original data with desired data with success rates of more than %98.3. As a countermeasure, the twisted cables are experimentally investigated and observed to be quite efficient. Although attacks to conventional cables are mitigated with twisted cables, the victim systems which carry digital data in PCB systems are nevertheless vulnerable due to the structural loops between communication lines and ground planes/traces, and approaches like minimizing victim trace length in the PCB are suggested.

Chapter 4

Physical–Layer Attacks on Power Converters for Electric Vehicle Chargers

With a low–carbon footprint and decreasing cost, electric vehicles (EV) become an appealing alternative to vehicles with internal combustion engines. However, the comparatively limited range of EVs is always a concern for buyers while transitioning to an EV. Lately, extremely fast EV chargers (XFC) are proposed to compensate for the limited– range of EVs with short charging times. Although XFC has become a standard technology in EV charging applications, a security analysis of these systems under physical layer attacks (such as EM interference) is lacking in security literature. In this part of the dissertation, a state–of–art extremely fast charger (XFC) combined with a Battery Management System (BMS), which is designed by SELECT (Sustainable Electrified Transportation Center) group in Utah State University [122], will be assessed in varying Electromagnetic Interference (IEMI) scenarios. Possible attack points such as current sensors and switches are examined, and attack mechanisms specific to the attack points are reported. Possible PCB–level countermeasures such as via–fenced lines are discussed, which will be examined in detail in Chapter 5.

4.1 Introduction

The security of XFC chargers and BMS are of great importance since attacks on these systems could result in the overcharging and thermal runaway of the battery fire which can turn into a fire in the system, i.e., EV. Larger scale synchronized attacks on EV chargers, since they connect the EV to the power grid, could cause instability in the grid leading to blackouts. Until now the security of power converters XFC chargers has been largely ignored. In this work, we seek to enhance the security of EVs by examining the potential vulnerabilities of XFC chargers and BMSs. To this end, simulation and experimental results are reported for attacks against critical components of the systems, namely their sensor and actuator (switching) capabilities. For the first time, electromagnetic-based attacks are demonstrated on XFC chargers, which compromises sensors and actuators in XFC chargers, and possible defense approaches are reported.

4.1.1 Contributions

A state–of–art power converter system is examined from a perspective of an IEMI attacker. To the best of the author's knowledge, this is the first study that focuses on power converter security from the perspective of IEMI attacks. The contributions of this section are:

- Showing that the voltage and current sensor outputs of power converters can be manipulated with low–cost and low–power amplifiers and radiators (e.g., ferrite toroids or rods) by an attacker. The mechanism of the attacks on sensors are explained.
- Demonstrating that, and proving an analytical model that explains how drivers/switches can be controlled (i.e., open or closed) via difficult to shield IEMI. Such drivers/switches are ubiquitous in hardware and cyber–physical systems, this work is the

first to show and explain how actuators that control the output current of the EV chargers,can be affected.

- Proposing several hardware–PCB level design cghanges to mitigate IEMI attacks.

4.1.2 Related Work

Low–power IEMI induces an undesired voltage on the victim circuitry (e.g., PCB trace that transmits analog sensor output) to manipulate the sensor data without leaving any physical trace after the attacks. Security researchers reported IEMI attacks on light, temperature, speed sensors, implantable cardiac devices, and microphones [61, 93, 95, 111]. Although each attack involves the radiation of an electromagnetic wave, each attack differs in terms of the attack mechanism employed like device–specific nonlinearities, due to amplifiers [61, 111] and ADCs [93]. The reader is referred to [46] for a comprehensive review of such attacks. Because amplifiers and ADCs are commonly used in power converters for sensing and feedback control, IEMI is an efficient tool to attack XFC power converters with relatively low–cost and low–power hardware, e.g., amplifier, toroid radiator.

4.2 Threat Model

The threat model assumes an attacker aiming to manipulate or disrupt the operation of an EV charger through the manipulation of sensor and actuation data with IEMI. The attacker can approach the victim circuitry (e.g.. PCB of the BMS), and place an EM radiator (e.g., antenna). There is no physical connection between the attacker hardware and victim circuitry, and all the interaction happens through air with EM coupling. The attacker has access to low-cost COTS RF components and devices, e.g., waveform generators, RF

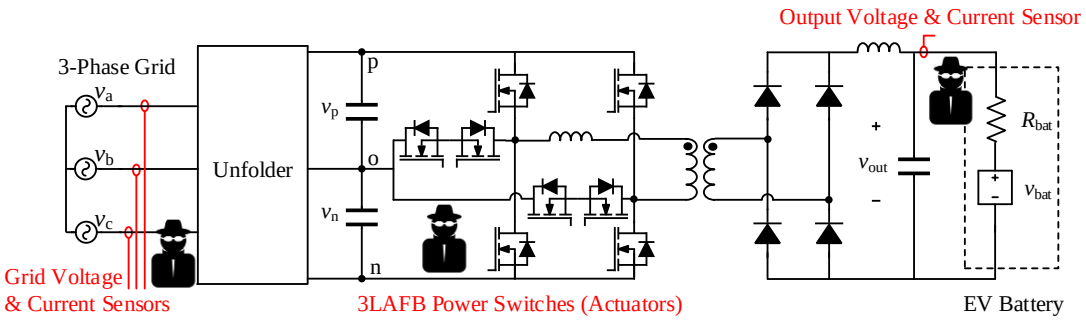


Figure 4.1: The victim power converter: The secure operation of the system relies on the integrity voltage and current sensor outputs. An advanced attacker can also attack the gate signals that control current (power) switches EV batteries. [32]

amplifiers, and EM radiators like toroids and antennas (Figure 4.3b). The attacker targets weak points of the victim system with magnetic near field radiators (e.g., a toroid) or a loop antenna with a directive near field radiation pattern.

4.3 Victim–Electric Vehicle Charger Description

The victim system consists of a high power 350 kW AC–DC power converter and a Battery Management System (BMS). The AC–DC conversion is achieved with an unfolder and a 3–Level Asymmetric Full Bridge (3LAFB) structure Figure 4.1. The current and voltage sensors are positioned at the input (i.e., grid side) and output (i.e., EV side) of the power converter as shown in Figure 4.1. The analog current and voltage sensor outputs are transmitted through PCB traces or cables to the controller, which is digitized and processed to determine the system's required output current for the current state. The power switches (i.e., the actuators that control the output current) in the 3LAFB structure (3–Level Asymmetric Full Bridge) are controlled by varying duty cycle gate control signals (i.e., PWM) sent from the controller. From the attacker's viewpoint, the low voltage analog current and voltage sensor outputs and gate signals pose the most vulnerable attack points as shown in Figure 4.1. The analog sensor

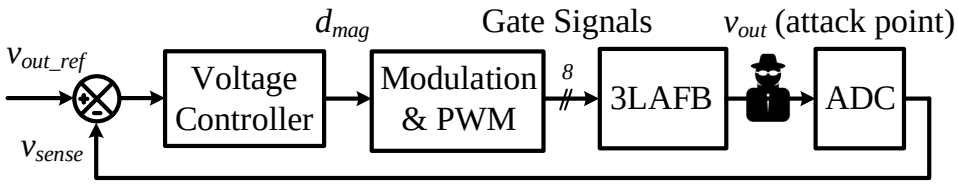


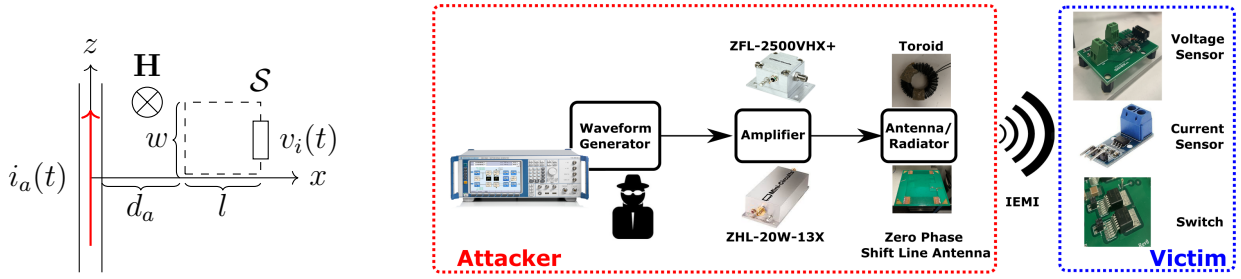
Figure 4.2: The controller digitizes the output voltage data and depending on the next state determines the output current through the gate signals which are in the form of PWM. The attacker manipulates the sensor data (e.g., v_{out}) which results in over or under–supply of the output current [32]

outputs, which are manipulated by IEMI, results in the assumption of wrong voltage/current data by the victim controller which means a larger/lower current supplied to the EV battery. Additionally, an attacker with the ability to control the current switches (i.e., actuators), can drive an excessive current to the EV even without the sensor output manipulation.

4.4 Mechanism of Sensor and Actuator Attacks on EV Chargers

IEMI attacks with inductive coupling rely on Faraday's law of induction, which declares that a time–varying magnetic flux captured by a conductor loop results in a voltage induced in the conductor terminals [82]. An attacker can exploit Faraday's law of induction to change sensor data through sensor output manipulation or output current through gate signal change. To observe how a time–varying current, i_a, supplied by an attacker, induces a voltage, v_i, on a victim loop, an infinitely long, z–directed current is assumed to be located at a distance, d_a, from a rectangular victim loop with dimensions w and l as illustrated in Figure 4.3a [93]. By Faraday's and Ampere's laws the relationship between the attacker signal, i_a, and the induced voltage, v_i, is:

$$v_i(t) = -\mu \left[\frac{w}{2\pi} \ln \left(\frac{d_a + l}{d_a} \right) \right] \frac{d}{dt} i_a(t) \tag{4.1}$$



(a) (b)

Figure 4.3: (a) IEMI attack model [93] (b) Attacker hardware and attack points for power converters

where μ is the permeability of the medium . The amplitude and shape of the induced voltage, v_i, is defined by a geometry coefficient (square brackets) and the time derivative of atatcker current, i_a, (4.1). During the attack demonstrations, the attacker excites the field radiators with a continuous sinusoidal current, i_a, so the induced voltage, v_i, is sinusoidal with a phase shift.

4.4.1 Attack Point I – Voltage Sensor Output

The voltage sensors at the input (i.e., grid side) and output (i.e., EV side) of the power converter (4.2) transmit the analog sensor data (v_{out}) to the controller which is sampled by an Analog–to–Digital (ADC) for further processing. The attacker radiates EM interference to the victim circuitry (e.g., PCB traces that carry the sensor outputs). The attack has two phases: the first phase is the efficient EM coupling to the victim circuitry through the exploitation of victim resonance [61], and before the attack, a frequency sweep is implemented to find the victim resonant frequency. The second attack phase is the manipulation of the sensor data through 'clipping' effect [93]. An ADC digitizes an analog voltage in the range which is called ADC input range which spans voltage values from v_{min} to v_{max}, and a common practice to filter out noise in the analog data is to average the digitized data. It

is addressed in [93] how a generic ADC transfer function and electrostatic discharge (ESD) diodes result in the phenomenon called 'clipping'. We assume that the input voltage of the ADC is compromised and a time–varying voltage v_{ADC} is fed into the ADC:

$$v_{ADC}(t) = V_s + v_i(t) \tag{4.2}$$

where V_s is the low–frequency sensor output which is assumed as a DC offset, and v_i is the purely sinusoidal signal induced by the attacker with frequency f and amplitude V_i. For very small sensor output scenarios (e.g., $V_s = 0\,\mathrm{V}$), only the sinusoidal attack waveform (v_i) is measured by the ADC, and as the min voltage an ADC accepts is 0 V, and negative voltages are assigned as 0 V digitally, the ADC samples and averages a half–wave rectified signal in practice. The mean value (DC) of a half–wave rectified sinusoidal waveform with amplitude V_i and period $T = 1/f$ is:

$$V_{DC} = \frac{1}{T}\left(\int_0^{\frac{T}{2}} V_i sin(2\pi f t)\mathrm{d}t + \int_{\frac{T}{2}}^{T} 0\mathrm{d}t\right) = \frac{V_i}{\pi} \tag{4.3}$$

Note that (4.3) assumes an infinite sampling frequency and ignores the effects observed when the attack frequency is a perfect multiple of sampling frequency in which cases the relative phase of the attacker to the victim becomes important. Other effects also render (4.3) an approximation that works well in practice; the reader is referred to [47, 93] for a detailed treatment of ADC manipulation mechanisms.

4.4.2 Attack Point II – Current Sensor Output

The second attack point is the output of the current sensors which measures the current and transmits it in analog form to the victim converter (Figure 4.2). The victim controller

samples the data with an ADC similar to the attacks on analog voltage sensors. The attacker places a magnetic field radiator (e.g., an air gap toroid) to induce a voltage on the victim circuitry. The two–phase attack mechanism that includes the efficient coupling and manipulation of the ADC, which is discussed in the Attack Point I applies to this scenario, too. However, this case has a fundamental difference: the attack point is a PCB trace (unlike cables in Attack Point I) which requires the manipulation of smaller victim loops than *Attack I* and necessitates higher attack fields and powers.

4.4.3 Attack Point III – Gate Control of Current Switches

The high–power SiC switches at the full-bridge (3LAFB) circuit are controlled by gate signals (Figure 4.1). The attacker aims to manipulate the switch and the output current of the victim by inducing a voltage on the gate signal, V_{IN}, as illustrated in Figure 4.4. To activate the gate driver and turn on the switch, the induced voltage v_i should exceed the threshold of the gate drive (4.4) 4.4:

$$v_i(t) = V_i sin(2\pi f t) > V_{th} \text{ Switch ON} \tag{4.4}$$

The voltage at the gate driver input, V_{IN}, is equal to induced voltage, v_i, as the gate control is 0 V for a turned-off switch.

4.5 Attack Demonstrations on EV Chargers

In this section, the IEMI attacks, which target three attack points, namely voltage sensor output, current sensor output, and gate signal, will be demonstrated. Although attacks targeting the sensors are classified as false data injection (FDI) attacks, the gate signal

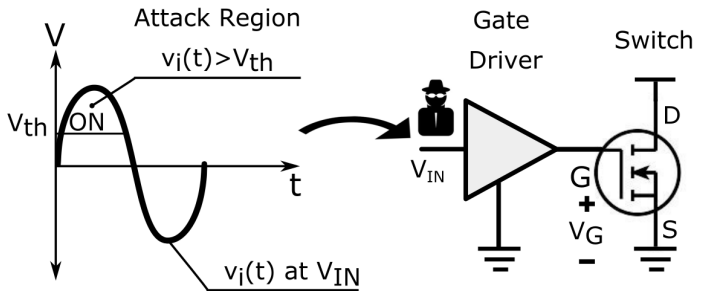


Figure 4.4: The induced voltage, v_i, should exceed the gate driver threshold, V_{th}, to turn on the current switches.

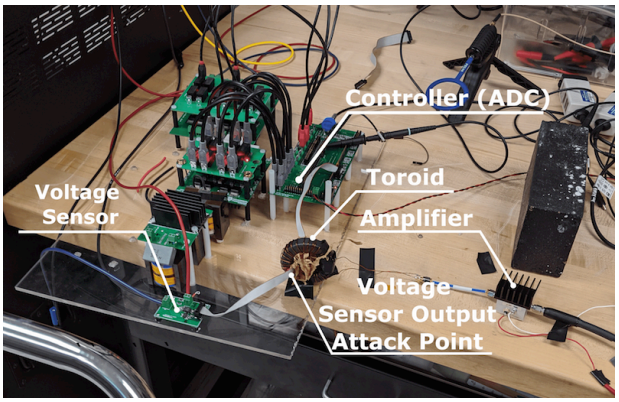
attacks, which manipulates the output current switches, are classified as False Actuation Injection (FAI) attacks because of the ability of the attacker to control a physical device (i.e., current switches) in the victim.

4.5.1 Attack I: False Voltage Sensor Data Injection

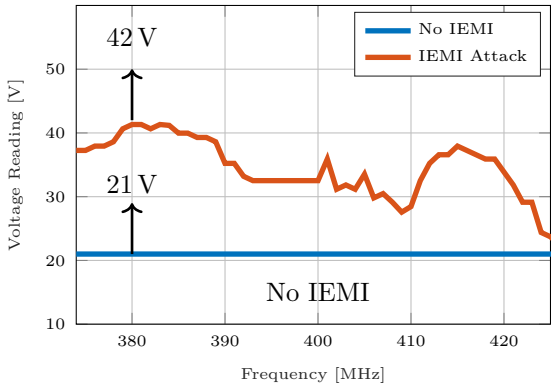
The attacker positions the toroid around the victim cable that carries the voltage sensor output as shown in Figure 4.5a. The toroid has an air–gap that can be filled with a ferrite piece which eliminates the need for the attacker to unplug the victim cables. The attacker system includes a Mini-Circuits ZFL–2500VHX+ RF amplifier and a 30 coil toroid (Figure 4.3b). The attack power is fixed at 200 mW throughout the attack.

Measurement Methodology

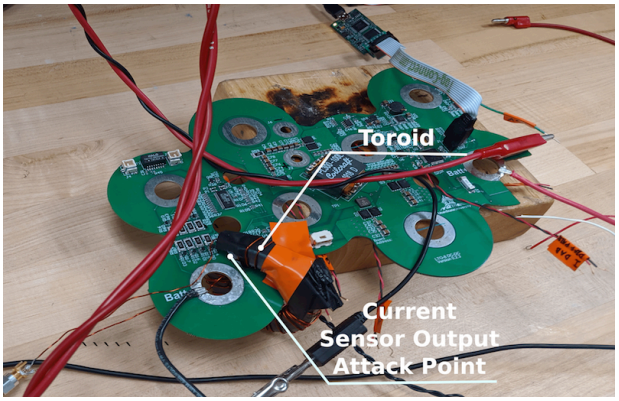
The voltage output of a DC supply is adjusted to 21 V and connected to the voltage sensor as the measured/reference voltage. The sensor is observed to be measuring the reference accurately before the attack implementation. To magnify the effect of the attack (i.e. less power same data manipulation or same power more data manipulation), an attacker can exploit the resonance of the victim circuitry [61]. At the resonance, the attacker induces



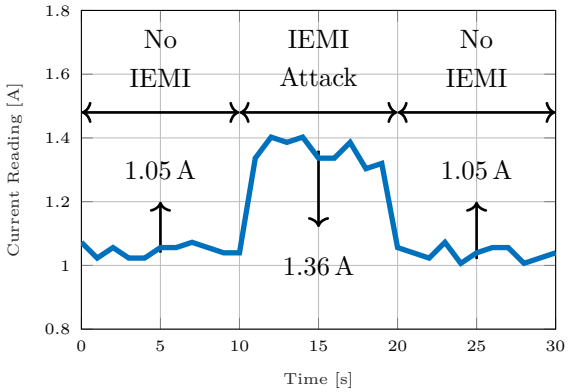
(a)



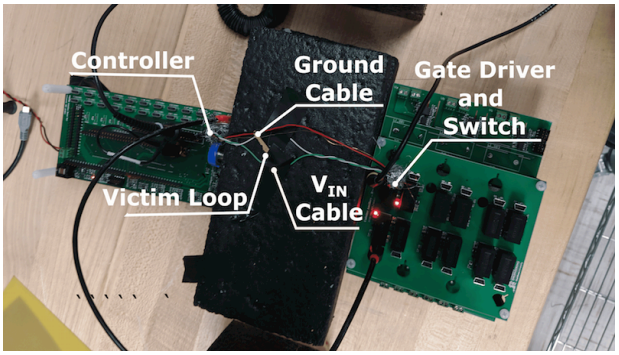
(b)



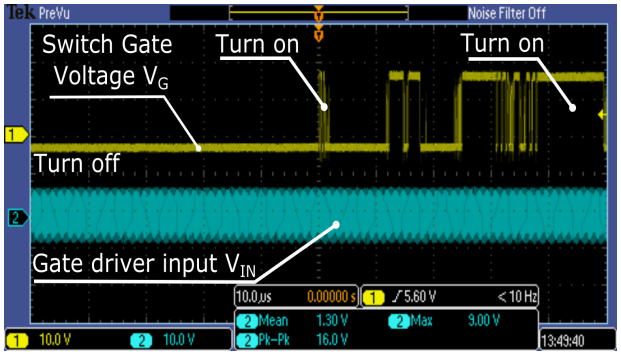
(c)



(d)



(e)



(f)

Figure 4.5: The attacker targets three points in the victim: voltage sensor output, current sensor output, and gate signal of the current switches. (a) Experimental setup for voltage sensor output manipulation (b) Voltage sensor output manipulation with attack frequency: measured voltage increased by 21 V under IEMI (c) Experimental setup for current sensor output manipulation (d) Current readings during the attack, when IEMI is applied between $t = 10\,\text{s}$ and $t = 20\,\text{s}$, the average of current readings increased from 1.05 A to 1.36 A. (e) Experimental setup for the attacks on current switches (f) The attacker induces a strong sinusoidal to the gate driver (V_{IN}–blue curve) and turns on the switch (V_G–yellow curve).

larger voltages at the terminals of the victim cables, e.g., at the input of the victim ADC. To detect the victim resonance, a frequency sweep between 100 MHz and 500 MHz is implemented with 10 MHz increments while observing the change of the voltage sensor data. Although all tested frequencies increase the measured voltage (as expected with 'clipping effect' because the original sensor output is closer to the minimum input voltage, v_{min}, of the ADC), it is observed that between 380 MHz and 420 MHz, the effect is more pronounced.

Results

Figure 4.5b summarizes how the attacks affect the voltage readings of the victim. Depending on the frequency, the voltage readings increased up to the range between 28 V and 42 V, while the original voltage measured by the sensor is 21 V. Specifically, at 380 MHz, the voltage reading is increased to 42 V which doubles the original sensor output. Another observation is that the IEMI injection increases the voltage readings at all attack frequencies. This observation is parallel to the ADC nonlinearity and 'clipping' effect discussion in [93], as the reference 21 V corresponds to a sensor output at the lower half of the ADC input range, the effect of the attack is to increase the voltage data. The IEMI attack on voltage readings is a significant threat for an EV charger because the attacks are achievable with low–cost and low–power hardware.

Simulated Effects of False Voltage Sensor Data Injection

To explore the effects of false voltage data injection on the output voltage (e.g., EV side) of the victim system, a system with the hardware parameters provided in [122] is simulated in Matlab–Simulink in Utah State University [32]. An attacker is assumed to induce an undesired voltage on v_{out} and change the digital v_{sense} through ADC clipping effect (Figure

4.2). The attacker can result in a faulty over-voltage and over–current situation which results in decreased battery capacity and lifespan, and an increase in cell temperatures which could lead to thermal runaway in which the battery pack would ignite and create a self-sustaining fire. In the simulation the results of which are shared in Figure 4.6, an IEMI attack is

Table 4.1: Parameters for Matlab–Simulink results shared in Figure 4.6

Parameter	**Value**	**Parameter**	**Value**
V_{bat}	500 V	R_{bat}	0.5 Ω
$V_{out,ref}$	502 V	ϕ_{grid}	45°
V_p	480 V	V_n	176 V

assumed to be initiated at 10 ms; the attacker reduces the feedback signal, v_{sense}, by 1 V that causes the control system to compensate by increasing the output voltage of the system and consequently the current driven to the EV. This alteration represents the average voltage distortion that is induced on an ADC sensor used to measure output voltage during an IEMI attack. The attack duration is 30 ms.

When the v_{sense} decreased by 1 V by the attacker, the output voltage of the system is increased by 1 V from 502 V to 503 V. Despite the small increase of the voltage, as the battery voltage is kept at 500 V by the BMS, the current supplied to the battery increases

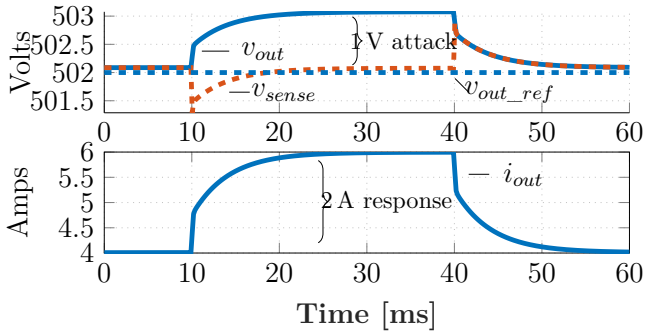


Figure 4.6: An increase of 1 V in v_{sense} signal cause the charging current to increase from 4 to 6 A, which indicates that a small change in sensed voltage can lead to a substantial increase in current (and thus heating of a battery)[32].

from 4 A to 6 A. The charging current is extremely sensitive to changes in v_{out} due to the small battery resistance (<1 Ω), which implies that small manipulations in sensed voltage (e.g., through IEMI) result in a significant increase in current and can cause physical damage.

4.5.2 Attack II: False Current Sensor Data Injection

In this scenario, the attacker aims to manipulate the current sensor data on the printed circuit board (PCB) of the Battery Management System (BMS). The air–gapped toroid is located on the PCB trace as displayed in Figure 4.5c, and the attacker hardware consists of a 20 W RF amplifier (Mini-Circuits ZHL–20W–13X) and the toroid. The amplifier output power is adjusted to 2.5 W to eliminate any impedance mismatch due to the dominantly imaginary impedance of the toroid.

Measurement Methodology

The current sensor is measuring a reference current of 1 A which is supplied by a DC supply, and the sensor output is observed to make measurements accurately before the attacks. Then, an IEMI frequency sweep between 10 MHz and 500 MHz with 10 MHz increments is applied, and it is observed that in the vicinity of 100 MHz, the current reading manipulation is more pronounced. The attack frequency is chosen as 100 MHz.

Results

In Figure 4.5d, the current sensor readings of the victim is shared with a temporary IEMI attack between $t = 10$ s and $t = 20$ s. It is observed that when the attack initiates at $t = 10$ s, the mean value of current readings increase by % 30 from 1.05 A to 1.36 A, while the reference current of 1 A is unchanged during before, during and after the attack. Adding to this, the

attack increases the current sensor readings, which is parallel with the discussion made in Section 4.4. This demonstration proves that PCB traces can be attacker by IEMI as well as wires/cables; however, relatively large attack powers are required for PCB traces than wires/cables.

4.5.3 Attack III: Turning on Current Switches with IEMI

The attacker hardware consists a 20 W RF amplifier (Mini–Circuits ZHL–20W–13X) and a Zero–Phase–Shift Loop (ZPSL) antenna (Figure 4.3b). ZPSL antenna is a near field resonant antenna with a strong magnetic field at 72 MHz directed through antenna normal. The attacker positions the ZPSL antenna 10 cm above intertwined and shielded cables that carry V_{IN} and ground of the gate driver. We will use the terminology where V_{IN} is the gate driver input or voltage and V_G is switch gate voltage (Figure 4.4).

Measurement Methodology

Attack frequency is 72 MHz, which is the resonant frequency of the loop antenna, and the attack power is increased by 1 dB increments from 100 mW to 20 W while the gate input, V_{IN} , and transistor gate voltage, V_G (Figure 4.5f) are observed with an oscilloscope. V_{IN} is set to low during the attacks to ensure that the switch stays off. If the attack is successful (i.e., the switch is turned on by the induced voltage to gate driver, V_{IN}), the gate voltage V_G is expected to increase to 18 V by the gate driver. To capture the turn-on characteristic for V_G and V_{IN}, the oscilloscope is set to a single–trigger mode for a low to high transition at V_G.

Results

When the 20 W IEMI is applied from a distance of 10 cm, it is observed that the attacker is not able to turn on the switch. This is an expected result because the loop area between cables that carry ground and V_{IN} connection is small and the differential voltage between V_{IN} and ground is not high enough to satisfy the condition (4.4). Although this reveals that sending V_{IN} and ground cables through intertwined cables are relatively secure, in PCB–based systems, the V_{IN} and ground traces/pads are not always close due to the minimum spacing requirements of the manufacturing process. To observe this phenomenon, the green V_{IN} and the white ground cables are physically separated and a loop of 4 cm^2 is exposed as demonstrated in Figure 4.5e. When the attack power is adjusted to 20 W, it is observed that the V_G increases which means that the switch is turned on due to the attack (Figure 4.5f). The first observation is that the switch turns on and off (i.e., a transient characteristic) until it stabilizes at turn-on condition. As the oscilloscope is triggered for a very short time window of 100 µs, the power increase is not observable at the input of the gate (blue) which can be explained by the relatively small increase of attack power (and induced voltage) as the amplifier operates in saturation.

4.6 A Discussion of Defenses

Every sensor data and actuation signal in an EV charger is a point that should be defended for secure system operation. The attacker can manipulate the sensor readings to supply an excessive current to the victim EV, which can easily damage batteries or start a fire due to overheating. On the other side, the third attack point (i.e., gate driver signal) gives the attacker direct control of the output current and eliminates any state estimation algorithm that might be effective in analog sensor output attacks. The digital gate signals are not as

sensitive to the IEMI as the sensed, analog signals; however, if the victim loop of the gate signal is large enough, the attackers can even turn on output switches that are intended to be closed. If this event occurs on live hardware, a short–circuit event is likely to occur in the bridge topology; the incredible currents and heat generated in a short–circuit are likely to cause system-wide device failure or at least system shutdown and a fire hazard.

Although RF shielding (e.g., conductive sheet or foam) is effectively used against relatively high–frequency signals [76], the relatively low frequency (<100 MHz) and magnetic nature of the reported attacks makes it very difficult to shield fast chargers. Adding to that, none of the magnetic field shielding options (e.g., MuMetal or Faraday cage) are employed in commercial fast chargers. To protect PCB traces transmitting sensitive signals (e.g., analog sensor outputs and gate/switch control signals), hardware designers should be aware of IEMI threats from the first moment of layout generation and eliminate large loops between significant traces and ground pad/traces. However, due to minimum spacing restrictions of the PCB manufacturing process and complex layout designs with many components, eliminating large loops may not always be possible. In those situations, we suggest using via–fenced striplines for analog sensor outputs and gate driver signals. Although via–fenced stripline is used for eliminating crosstalk between traces, it can also be used to eliminate high–frequency IEMI from outside sources.

4.7 Conclusion

The secure operation of fast electric vehicle chargers and Battery Management systems rely on the integrity of the sensing and actuation data in the system. In this work, it is demonstrated that an attacker can target voltage sensor outputs and gate control signals of an EV charger with low–cost hardware and can cause physical damage due to the excessive

currents supplied to the battery. The attackers can control the output current of the system by manipulating the feedback signals from the analog sensors and can cause damage to the EV, XFC, and BMS systems with one or a combination of attacks. Furthermore, the control signals from the microcontroller to the gate drivers can also be manipulated, which gives the attacker direct control of the current supplied to the EV, given the victim loop and attacker power level is large enough to induce sufficient voltage. In Chapter 5, physical layer countermeasures against IEMI will be assessed with simulation results.

Chapter 5

Physical Layer Countermeasures

Electromagnetic interference is a largely analyzed problem in consumer and military electronic systems [76, 115]. However, in the regular EM interference cases, the interference is assumed to be sourced from a nearby component or system, unintentionally. This approach limits the designers to concentrate on certain EMI frequency bands, power levels, and source positions. Nevertheless, as happens in IEMI scenarios, an attacker can utilize any frequency, waveform. and position to manipulate a victim system. Additionally, an attacker with sufficient resources can apply high powers with a specific coupling mechanism (e.g., magnetic resonant coupling) to manipulate the analog, digital, and actuation data as described in Chapter 2, 3, and 4. To mitigate IEMI, an extensive hardware design approach, that starts with the PCB layout, is required. First of all, the designer needs to detect the 'significant' signals, which are analog sensor outputs that carry sensor data, actuation signals that transfer the actuation data, and digital signals that convey information between components like processors and sensors. With the detection of critical signals, the physical layer countermeasures discussed in the following parts can be implemented to the circuitry (e.g., traces) that conveys 'significant' signals.

In this section, the focus is on shielding, PCB-level countermeasures, and optical transmission of 'significant' signals to mitigate IEMI. In the first part, the pros and cons of shielding and optical transmission of 'significant' signals are discussed as a defense for IEMI. In the next section, PCB-level countermeasures are discussed after analytically solving the induced

voltage, V_{ind}, due to EM interference on a victim PCB trace. Then, based on the analytical solution and EM simulations, the efficacy of PCB-level countermeasures will be reported.

5.1 Shielding

Shielding is the general term for reducing the electromagnetic interference on a device through the EM blocking effect of specific materials (e.g., aluminum foil) and structures (e.g., Faraday cage). The coupling between the attacker and the victim can be 'inductive', 'capacitive', and 'radiation' which utilize the 'magnetic', 'electric', and 'radiation' field as the coupling modality, respectively. 'Electric', 'magnetic', and 'radiation' field shielding rely on different natural phenomena and are treated accordingly with diverse material and approaches as summarized in Table 5.1.

In 'electric' and 'magnetic' field coupling, the victim is in the near field of the attacker antenna, and the coupling type is determined by the antenna characteristics. For instance, the ZPSL loop antenna in Chapter 2 generates a highly magnetic near field that manipulates the victim voltage through inductive coupling. On the other hand, the attacker can use a directive, far-field antenna to utilize 'radiation' coupling. In such a scenario, as the victim is in the far-field of the attacker antenna, the voltage is induced by the interaction of plane waves with the free electrons in the victim circuitry which defines a 'radiation' coupling. The 'radiation' coupling can be shielded relatively easily with thin conductor layers (e.g., aluminum foil) as well as the electric fields in the near field [79].

Due to the penetration capability of magnetic fields to metal surfaces(e.g., electric field shielding), the inductive coupling, which transfers energy through magnetic fields, poses a significant threat. Although 'radiation' coupling is applied from far distances like 10s of meters [111], the attacks can be shielded relatively easily with thin layer conductors like alu-

minum foils, and the induced voltages are significantly lower than a near-field scenario. As the magnetic fields exist in nature as closed loops represented by Gauss's law for magnetism ($\nabla B = 0$), it is impossible to hinder them. The only magnetic field shielding approach is to redirect a magnetic field with magnetic field 'guides' with magnetic materials such as MuMetal (an alloy of nickel, iron, copper, and molybdenum) [6, 76]. However, the high permeability materials lose magnetic properties with elevated frequencies and become inefficient above 100 kHz [6]. As the frequency of the magnetic field goes roughly above 100 kHz, the eddy currents become the main field mitigation principle, and the magnetic or non-magnetic conductors like steel or aluminum perform better than MuMetal [79, 91]. Additionally, high-frequency (above 100 kHz) magnetic shielding highly depends on the thickness of the metal and requires thick plates [79]. For instance, for attenuating 10 kHz magnetic field by 20 dB, a 60 mil thick steel plate is needed (Figure 6-23 at [76]). Magnetic field shielding 'efficiency' also relies on how much the shielding material encloses the protected system or component. Frika et al. desscribed that even small openings on the magnetic shielding deteriorate the shielding with increasing frequency [42].

> The shield must completely enclose the electronics and must have no penetrations such as holes, seams, slots, or cables. Any penetrations in a shield unless properly treated may drastically reduce the effectiveness of the shield [79].

This is the most alarming issue about magnetic field shielding because it is practically challenging to cover all physically moving parts of a CPS (e.g., a UAV) with thick and heavy shielding, e.g., steel plates. For instance, in Chapter 5.2 an inductively coupled IEMI attack at 72 MHz is applied to the moving surface of a UAV. To eliminate the magnetic field at that frequency, the UAV wings should be enclosed by metal shielding which is practically unattainable for a UAV application due to weight and agility considerations. The author thinks that shielding can be a solution for some scenarios (e.g., against attacks

Table 5.1: The efficient shielding is determined by the coupling type and the attack frequency. While low–frequency magnetic coupling requires high μ materials, higher frequencies require conductor plates. Radiation coupling utilizes the far-field of the attacker antenna and can be shielded with thin and lightweight conductor sheets.

Victim Position [76, 79]	Coupling Type	Low Frequency (< 100 kHz)	High Frequency
Near Field (Attack Dist. $< \lambda/2\pi$)	Electric	Conductor Plate	Conductor Plate
Near Field	Magnetic	High μ Material [6, 76, 91]	Conductor Thin Plate (Cu,Steel etc.) [76, 91]
Far Field	Radiation	Conductor Sheet	Conductor Sheet (e.g., copper aluminum)

with 'radiation' coupling); however, it can not be the sole countermeasure against attacks employing inductive coupling.

5.2 Optical Transmission

A fiber-optic communication system converts a voltage signal (analog or digital) to light, transfers light over a fiber-optic cable, and then reconstructs the signal from light [74]. Some advantages of fiber-optic communication are low latency, very high data rate, and resilience in EMI-rich environments [18]. Fiber-optic communication is a reliable way of transmitting data within a rich-EMI environment because the data is sent in an optical form through a fiber cable, which is a form of glass, in which free electrons do not exist unlike metals e.g., conventional transmission lines and PCB traces. However, one drawback of fiber-optic transmission, which requires transmitters (i.e., light-emitting diodes) and receivers (i.e., phototransistors) that convert electric signals to optical waves and vice versa, is hardware complexity and cost. However, in applications such as actuation control in Chapter 2 which do not require high-performance (e.g., high data rate, low latency), low-cost optical transmitters/receivers can be employed. For example, the cost for a low-performance fiber optic transmitter/receiver couple is $10 as of October 2020. The fiber-optic transmission is by far the safest way (among the countermeasures discussed in Chapter 5) to transmit 'significant' signals in an EMI-rich environment because light does not interact with EMI. In

Chapter , fiber-optic transmission function propelry in a highly EMI-contaminated region, i.e., 20 cm away from a ZPSL antenna excited by a power of 20 W.

5.3 Countermeasures at the Printed Circuit Board

The PCB traces that carry the 'significant' signals are occasionally targeted by attackers to manipulate actuation, sensor, and communication data. In Chapter 4, the PCB traces that convey the current sensor data are targeted by the attacker. The bit–flip attack discussed in Chapter 3 applies to the data carried in PCB traces as well. Thus, defense approaches integrated with PCBs have utmost significance for secure CPS operation.

To reveal which parameters of the victim PCB traces determine the induced voltage to the victim, the analytical relationship [65] between an attacker field and induced voltage to the victim is analyzed.

5.3.1 Induced Voltage on a PCB trace by Electromagnetic Interference

The induced voltage on a PCB trace, due to an external EM field (Figure 5.1), can be analytically derived by combining a lumped transmission line model and Maxwell equations. Rachidi [83] compares three analytical coupling model that relates the induced voltage on a general transmission line. Although each model, namely Taylor [103], Agrawal [11], and Rachidi [83], use different field components (electric, integral of the magnetic field, or a combination of both), in each solution the analytically found V_{ind} is equivalent [83].

All solutions model the external field as an excitation source on the transmission line, and then solve the lumped transmission line model to detect the induced voltage, V_{ind}, in the

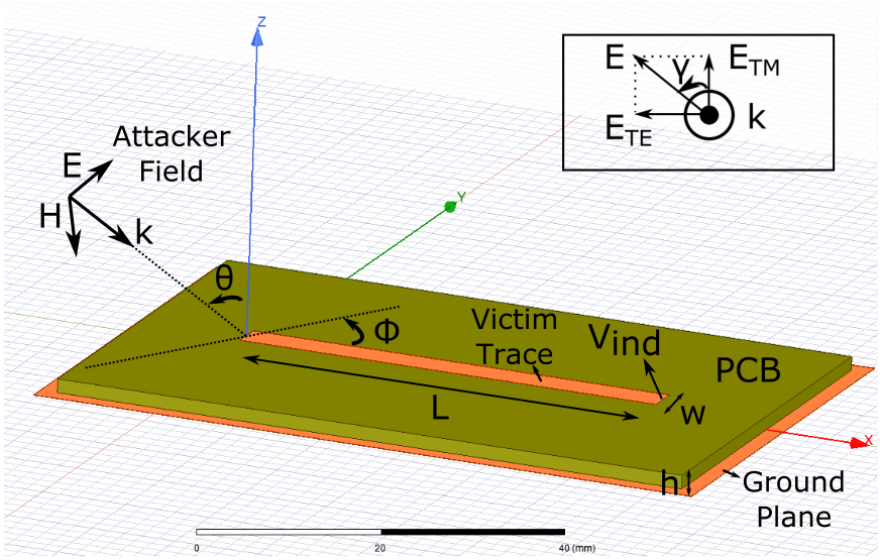


Figure 5.1: The adversary radiates a TEM wave to induce voltage V_{ind} at the output terminal of the PCB trace. The attack waveform direction is characterized by θ, ϕ and γ angles. A ground backed PCB trace with a length L is assumed. V_{ind} at the output terminal at $x = L$ plane is found analytically

line terminals. Unlike Rachidi [83] and Taylor [103], which uses position integral of the electric and magnetic fields, Agrawal solution is based on the tangential electric field of the excitation and does not require any differentiation or integration on the field which simplifies the derivation. Leone and Singer expand upon the Agrawal model, which is for a general transmission line, and report a solution for a ground-backed PCB (i.e., microstrip line with an infinite ground layer) excited by an external plane wave [65].

The scenario Leone and Singer reported is a proper representation of an attacker wave targeting a PCB trace (Figure 5.1). The orientation of the attack waveform is described by angles θ, ϕ, and γ where θ is the angle between the propagation vector (k) and z-axis, γ is the polarization angle that defines Transverse Magnetic (TM) and Transverse Electric (TE) wave components (Figure 5.1), and ϕ is the angle between the incident plane (i.e., the plane that includes the propagation vectors of the incident and reflected wave from the ground) and the x-axis. The left ($x = 0$) and right ($x = L$) terminals are defined as input and

output terminals of the victim trace where the input terminal is connected to a device that transmits a 'significant' signal (e.g., sensor output) and the output terminal is connected to a device that receives a 'significant' signal (e.g., ADC). As the attacks aim to manipulate output voltage (Figure 5.1), the induced voltage, V_{ind}, at the output terminal is derived.

The solution is based on the Agrawal model which requires the total tangential E_x field on the trace (i.e., this field consists of the incident and reflected E field from the ground plane.). Additionally, the z-directed E field, E_z, is required to find the excitation on each terminal [11]. As the solution is only interested in the V_{ind} at the output terminal of the trace, the simplified Baum–Liu–Tesche (BLT) (5.1) is used [65, 105].

$$V_{ind} = \frac{1}{e^{j2\beta L} - \Gamma_{in}\Gamma_{out}}(1 + \Gamma_{out})(e^{j\beta L}S_1 + \Gamma_{in}S_2) \tag{5.1}$$

where Γ_{in} and Γ_{out} are reflection coefficients of input and output terminals. Z_{in}, Z_{out} and Z_o are input, output, and characteristic impedance of the line, respectively.

$$\Gamma_{in} = \frac{Z_{in} - Z_o}{Z_{in} + Z_o} \quad , \quad \Gamma_{out} = \frac{Z_{out} - Z_o}{Z_{out} + Z_o} \tag{5.2}$$

where S_1 and S_2 are the excitation sources to model the coupling of the EM field generated by the attacker [65].

$$\begin{pmatrix} S_1 \\ S_2 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} v_{in} + v_x^+ - v_{out}e^{j\beta L} \\ -v_{in}e^{j\beta L} - v_x^- e^{j\beta L} + v_{out} \end{pmatrix}$$

v_{in} and v_{out} are the terminal voltages due to the z directed E field (Figure 5.1)

$$v_{in} = \int_0^h E_z(x = 0, z)dz \quad , \quad v_{out} = \int_0^h E_z(x = L, z)dz \tag{5.3}$$

The excitation terms, v_x^+ and v_x^-, model the effect of the tangential electric field, E_x, on the PCB trace (Figure 5.1).

$$v_x^+ = \int_0^L E_x(x) e^{j\beta x} dx \quad , \quad v_x^- = \int_0^L E_x(x) e^{-j\beta x} dx \tag{5.4}$$

It should be noted that the E_x and E_z values in (5.3) and (5.4) are the total electric field, that includes the incident electric field E and its reflection from the PCB-air boundary and ground plane while assuming the trace does not exist (i.e., the tangential E_x is not 0 due to the conductor material.). Assuming that the PCB thickness, h, is much smaller than the wavelength in the PCB ($k_z t << 1$), the induced voltage V_{ind} at the output is found for matched input and output loads ($Z_o = Z_{in} = Z_{out}$) as provided in (5.5). For the details of the derivation, the reader is referred to [65].

$$V_{ind} = jk_o hE \frac{e^{j(\beta - k_x)L} - 1}{j(\beta - k_x)} \left(sin\phi \, sin\gamma \, cos\theta \; + \; cos\phi \, cos\gamma \; - \; \frac{\sqrt{\epsilon_{eff}}}{\epsilon_r} \, sin\theta \, cos\gamma \right) \tag{5.5}$$

where k_o, k_x, and β are free space wave number, its x component and line propagation constant and λ_o is the free-space wavelength.

$$k_o = \frac{2\pi}{\lambda_o} \quad , \quad k_x = k_o sin\theta cos\phi \quad , \quad \beta = k_o \sqrt{\epsilon_{eff}} \tag{5.6}$$

The resonant frequencies can be found by detecting the local maximums of (5.5 [65]), where c_o is the speed of light in free space.

$$f_{res,n} = \frac{c_o}{2L} \frac{n}{\sqrt{\epsilon_{eff}} - sin\theta cos\phi} \qquad where \quad n = 1, 2, 3, 4... \tag{5.7}$$

The resonant frequencies, $f_{res,n}$, of the trace are determined by the trace length, L, effective dielectric constant ϵ_{eff}, and the angles of the incident waveform (Figure [65]). For the low-

frequency excitation, i.e., the trace length is much smaller than the attacker wavelength, the exponential term in (5.5) approximates to the line length, L.

$$\frac{e^{j(\beta-k_x)L}-1}{j(\beta-k_x)} \approx L \quad while \quad |\beta-k_x|L \ll 1 \tag{5.8}$$

With the low frequency relation given in (5.8) (i.e., Assumption is $|\beta-k_x|L \ll 1$), (5.5) reduces to

$$V_{ind} = j2\pi\left(\frac{f}{c_o}\right) hLE(sin\phi\, sin\gamma\, cos\theta \;+\; cos\phi\, cos\gamma \;-\; \frac{\sqrt{\epsilon_{eff}}}{\epsilon_r}\, sin\theta\, cos\gamma) \tag{5.9}$$

(5.9) provides the induced voltage, V_{ind}, in the victim trace terminal for low-frequency and thin PCB assumption (which is almost always the case in this dissertation as the attack frequencies are below S-Band and lower than the resonant frequency of the attacker traces.). (5.9) provides an insight for which parameters determine the induced voltage, V_{ind}.

- **Victim Loop Area (h L):** The induced voltage, (V_{ind}), is linearly proportional to the area of the loop between the trace and ground plane (Figure 5.1). This phenomenon can be explained with Faraday's Law of Induction which states that induced voltage in the terminals of a conducting loop is proportional to the time derivative of the 'overall' magnetic flux captured normal to the loop surface [82].

- **Attack Frequency (f):** If the attacker frequency is below the resonant frequency of the trace (5.7), V_{ind} linearly increases with increasing attack frequency, f. This result can again be explained with Faraday's Law of Induction which states that V_{ind} in a conducting loop is proportional to the time derivative of the magnetic flux captured normal to the loop surface [82]. With an increasing attack frequency, as the time derivative increases proportionally (e.g., $\frac{d}{dt}sin2\pi ft = 2\pi f sin(2\pi ft)$), V_{ind} also

increases.

- **Incidence and Polarization Angles of the Attack Waveform:** The incidence (θ, ϕ) and polarization angle (γ) of attacker waveform (Figure 5.1) have an effect on V_{ind}. V_{ind} is maximum when $\theta = 90^o$ and each of γ and ϕ are 0^o or 180^o. This corresponds to an attacker waveform directed $\pm x$ direction and the H field is directed $\pm y$. This is an expected result because the induced voltage is maximized when the H field is normal to the victim loop area according to Faraday's Law of Induction [82].

As the main parameters that determine the induced voltage, V_{ind}, are found, possible ways to decrease the induced voltage can be discussed.

5.3.2 Minimizing the Length of the Signal Trace

To observe the effect of line length, L, on the induced voltage, two ground–backed PCB traces with length 5 cm and 10 cm are analyzed. (5.5) is solved with a Matlab script. The traces are on an FR-4 PCB with a thickness of 1.6 mm and dielectric constant of 4.4.

The induced voltage, V_{ind}, is illustrated in Figure 5.2 with varying attacker frequency. Firstly, it is observed that the longer PCB trace has a lower resonant frequency (Table 5.2). By the resonant frequency, the frequency at which the attacker can induce the maximum voltage is meant. For instance, for the trace with $L = 10$ cm, the first resonance is at 810 MHz, while resonance is at 1.62 GHz for the $L = 5$ cm trace (Figure 5.2). Secondly, if the attacker radiates lower attack frequencies than the resonance of the victim trace, it is observed that V_{ind} is directly proportional to the trace length, L (assuming all other parameters like h are the same.). For instance, at 100 MHz, the induced voltage on the PCB trace with 10 cm length doubles the induced voltage on 5 cm one (i.e., 6 dB difference as shown in Figure 5.2).

If the attacker is to exploit the resonance of the victim trace to induce a maximum V_{ind}, the attack frequency should be doubled for the shorter trace. From the attacker's viewpoint, attacking a shorter victim circuitry is more expensive in terms of design complexity and cost because of the relatively complex amplifier and antenna designs needed for higher frequencies. Additionally, the attack efficiency suffers because higher frequency signals can be shielded comparatively easy. The attacker can try to induce voltage with smaller frequencies

Table 5.2: The first and second resonant frequencies of PCB traces with lengths 5 cm and 10 cm, the propagation is towards the PCB plane (-z axis $\theta = 0$, $\phi = 0$), the wave is assumed to be fully Transverse Magnetic (TM) $\gamma = 0$

Structure	First Resonant Frequency $n = 1$	Second Resonant Frequency $n = 2$
Trace Length = 5 cm	1.62 GHz	3.24 GHz
Trace Length = 10 cm	810 MHz	1.62 GHz

than victim resonance (Chapter 3); however, still, in that case, the attack power should be quadrupled to induce the same voltage for 5 cm trace. While designing the PCB traces, the length of traces that carry 'significant' signals should be minimized to make the attacks expensive for the attacker. A suggested approach is to lay traces that carry 'significant' signals (e.g., analog sensor outputs, digital communication signals, actuation signals) in a small area at once and then lay the other traces that carry other 'insignificant' signals (e.g., DC supply lines) during the PCB design.

5.3.3 Minimizing PCB Thickness

(5.9) concludes that V_{ind} is linearly proportional to the loop area (Lh) between the victim trace and the ground plane. This statement is intuitive considering that the induced voltage on a conductor loop is proportional to the time derivative of the 'overall' captured magnetic flux. Figure 5.3 shows the comparison of V_{ind} for two same-length PCB traces with different PCB thicknesses. The PCB material is assumed to be FR-4 and $L = 10$ cm for both traces.

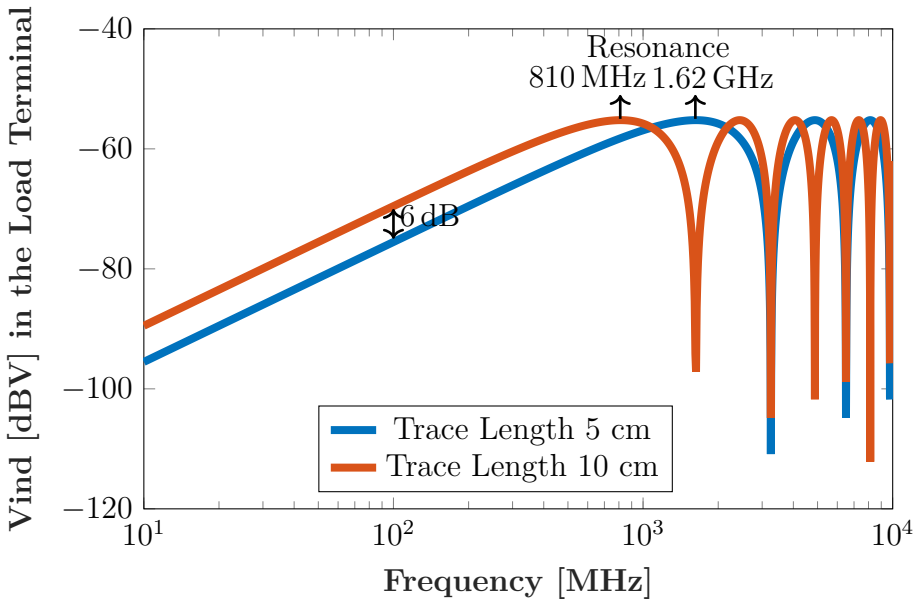


Figure 5.2: The induced voltage, V_{ind}, on the victim terminal, for traces with length $L = 5\,\text{cm}$ and $L = 10\,\text{cm}$. For frequencies below resonance, V_{ind} to long trace doubles the V_{ind} to the short trace. V_{ind} becomes maximum at resonant frequencies of the cables. The propagation is towards -z axis and $\theta = 0$, $\phi = 0$), $\gamma = 0$ and the attacker E field is $1\,\text{V}\,\text{m}^{-1}$.

It is observed that V_{ind} is doubled when the PCB thickness is doubled in the low-frequency region which shows that the PCB designer can choose a thinner PCB and mitigate the effect of IEMI significantly. For instance, choosing an FR-4 thickness of 0.8 mm instead of 1.6 mm simply halves the induced voltage which requires the attacker to double the field and quadruple the power to have the same V_{ind} on the same length trace. It is observed that PCB manufacturers like OSH Park (US) provide thin layer FR-4 PCBs $t = 0.8\,\text{mm}$ with the same per/square inch price of the standard FR-4 ($t = 1.6\,\text{mm}$). Designers should prefer thinner substrates if it is practically possible. Another option is to employ multilayer PCBS and using a thin substrate between the ground plane and the 'significant' trace layer to minimize the victim loop.

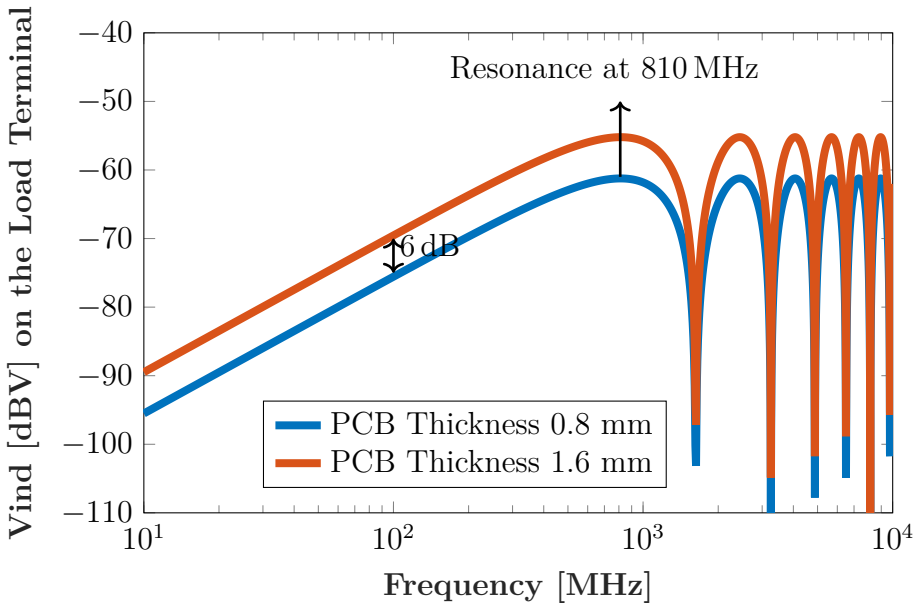
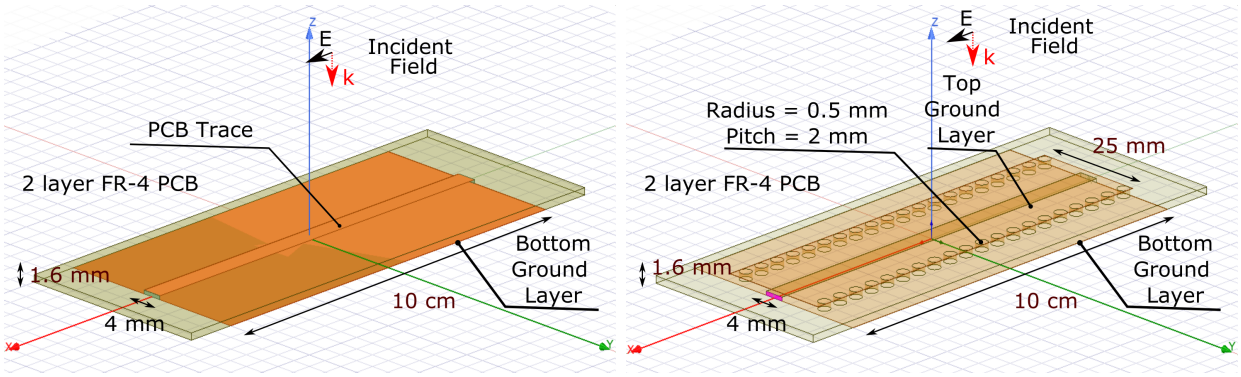


Figure 5.3: The induced voltage, V_{ind} for same-length traces ($L = 10\,\text{cm}$) with different substrate thickness ($t = 0.8\,\text{mm}$ and $t = 1.6\,\text{mm}$). For below-resonance frequencies, V_{ind} to trace with thick PCB doubles the V_{ind} to the trace with thin PCB. V_{ind} becomes maximum at resonant frequencies of the cables. The propagation is towards -z axis and $\theta = 0$, $\phi = 0$, $\gamma = 0$, while the attacker E field is $1\,\text{V}\,\text{m}^{-1}$.

5.3.4 Via Fenced Lines

In high-speed PCBs, via-fenced lines are widely used to decrease the EM interference between neighboring traces which is called 'crosstalk' in EMI community [102]. The microstrip or stripline transmission lines are guarded by vias and ground planes (Figure 5.4b) which behave as a solid conductor enclosing (i.e., shielding) up to an approximate frequency inversely proportional to the via spacing ($\lambda/8$) [66]. Ponchak et al. compared the isolation effectiveness of via-fenced microstrip and stripline transmission lines in a Low-Temperature Cofired Ceramic (LTCC) multilayer substrate. As the via fenced stripline is completely covered by ground planes and closely spaced vias, better isolation is achieved compared to a via-fenced microstrip line (approximately 15 dB improvement in isolation) [81]. The 'significant' signals (i.e., sensor, actuation, or digital communication signals) can be transmitted

through via-fenced striplines to mitigate the effect of an external electromagnetic field like IEMI. To observe the efficiency of the via fence lines against IEMI, a 10 cm PCB trace with



(a) (b)

Figure 5.4: The induced voltage, V_{ind}, is compared for a PCB trace and via-fenced PCB trace. (a)The HFSS model for PCB trace (b)The HFSS model for via-fenced PCB trace

and without a via fence (Figure 5.4b) under a plane wave excitation is simulated in ANSYS HFSS. The PCB is a two-layer FR-4 with a dielectric constant of 4.4. Each layer has a thickness of 0.8 mm and the trace is positioned on the first layer, i.e., the ground to trace distance is 0.8 mm.

Before analyzing the via fence effectiveness against IEMI, the correlation of the simulation and analytical solution (5.5) is tested on a 10 cm PCB trace. Figure 5.5 shows that the zeros and poles (resonance) of the analytical solution matches with the ANSYS HFSS. The resonances are found to be at 780 MHz and 800 MHz with analytical solution and EM simulation, respectively.

Induced voltage, V_{ind}, comparison of a regular and via-fenced line is given in Figure 5.6. The via-fenced line is effective in mitigating the induced voltage on the victim terminals by around 22 dB in the frequency region below the resonance. The isolation improves at around the first resonance of the PCB trace at 700 MHz. Although the via fence mitigates the IEMI at low-frequency region and compels the attacker to use a higher frequency which

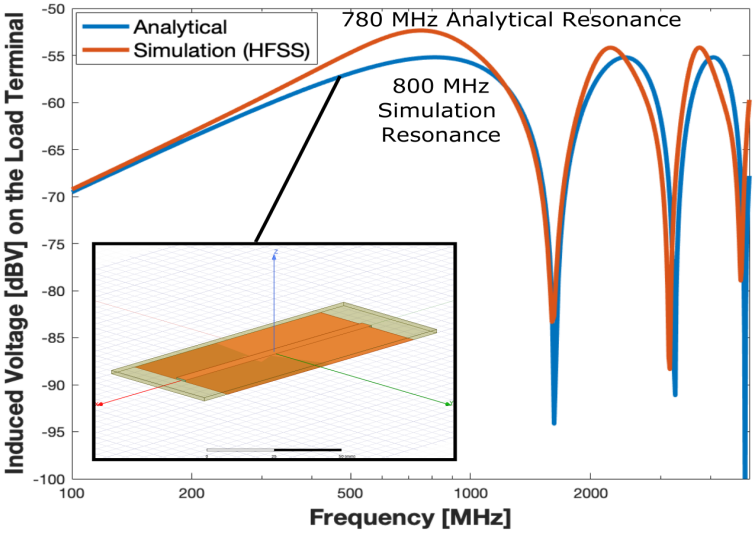


Figure 5.5: The analytical solution (5.5) and EM simulation is used to detect the induced voltages on the terminals of a 10 cm trace, and it is observed that 3-D EM simulation and analytical solution results correlate.

means more expensive attacks (i.e., higher cost, complex hardware design), as the frequency increases the via fence becomes less efficient as shwon in Figure 5.6.

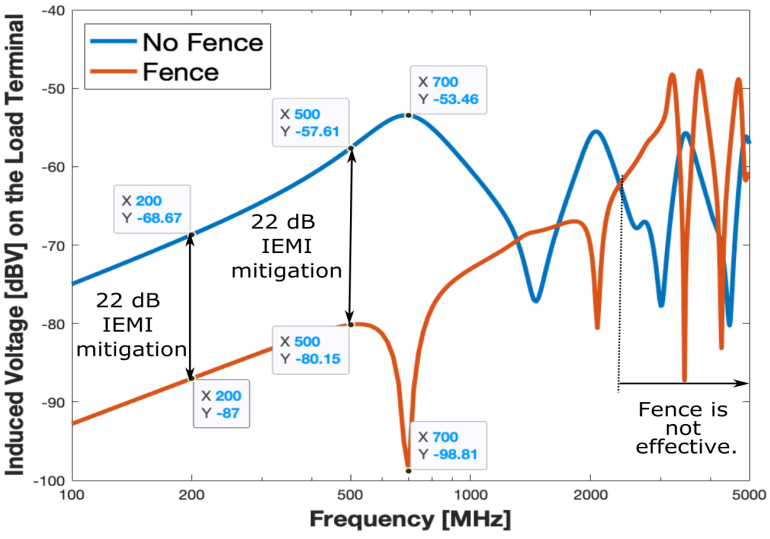


Figure 5.6: The via fence mitigates the IEMI and decreases V_{ind} by 22 dB in the frequency region below resonance. However, as the frequency increases, via-fence isolation becomes ineffective.

5.4 Conclusion

In the previous chapters, it is concluded that attackers can use IEMI, specifically with inductive coupling, to manipulate sensor outputs, actuation information, and digital data. In this Chapter, possible defense mechanisms are reported. The first suggestion is magnetic field shielding; which requires specific magnetic materials like MuMetal for frequencies below 100 kHz or thick aluminum steel metal plates for higher frequencies. However, as the magnetic shield should enclose the protected system (e.g., UAV wings) and requires heavy material, it is concluded that magnetic field shielding can not be a practical defense for every scenario. Then, optical transmission, which is observed to function properly in a high EMI situation in Chapter 2, is reported as a way of reliable signal transmission in EMI-rich environments. In the last part, the induced voltage on a PCB trace due to an attack wave is analytically derived to provide PCB-level countermeasures. First of all, the 'significant' signals of the system should be detected,and the length of the traces that carry 'significant' signals should be minimized. Then, thin substrates should be preferred to minimize the loop area between the signal line and ground plane and consequently the induced voltage. Some other PCB level defenses like via fenced lines are discussed, which provide mitigation of induced voltage by 20 dB for a 10 cm PCB trace in a radiation coupling scenario. If the PCB layer countermeasures, shielding, and optical transmission of certain signals are combined, the attacks become notably expensive for the attacker which assures the secure operation of the system.

Chapter 6

A Rogowski Coil Design For Side-Channel Attacks and Design of Magnetic Field Radiators

In Chapter 6, two side-projects are discussed. The first part will explain the design process of a PCB-embedded Rogowski-coil to improve the side-channel attacks on cryptosystems with Correlational Power Analysis, the design procedure with EM simulation will be explained, and the performance of the produced coils will be reported. In the second part, magnetic field radiators are analyzed for IEMI attacks, and the advantage and disadvantages of radiators such as solenoids, loops, and Helmholtz coils are discussed in terms of the attack distance, field strength, and field focus. In the final section, a magnetic field array will be designed through an optimization method to focus the fields to a specific region of a victim system.

6.1 A Rogowski Coil Design for Side Channel Attacks

Side channels, which are physical attributes of systems such as power consumption or EM leakage, are exploited by attackers to reveal secret information about the operation. Attackers analyze the power consumption of cryptographic systems to expose the cryptographic key of the system with Simple Power Analysis (SPA) [60] and Correlational Power Analysis

(CPA) [22] attacks. To measure the victim power consumption, a small value–sense resistor is inserted between the crypto-device and the supply or ground, and the voltage traces (also called current traces) on the sense resistor is recorded [60]. After the detection of the current traces, a Hamming weight, which correlates the victim system bit changes (i.e., transistor actions) and instant power consumption, is applied to current traces to reveal the cryptographic key [68]. However, researchers look for innovative ways to combine side channels such as EM leakage and power consumption to improve the CPA attacks, i.e., decrease the minimum number of current traces required to reveal the key. Schena suggested an 'EM coupling CPA' attack to combine the EM leakage and power consumption of the victim system through a Kalman filter [89]. In this approach, in addition to the regular current traces, the EM leakage of the victim system, which is proportional to the time derivative of the victim current (di/dt) [16], should be fed to a Kalman filter to improve the attack efficiency. Schena collected the EM leakage of the victim system with a magnetic field probe [89], which does not give accurate results.

Although the 'EM coupling CPA' is a promising approach, Schena experimentally concluded that the regular CPA and EM coupled CPA resulted in "the same number of correct partial key guesses" which means the EM coupled approach does not particularly improve the attack efficacy [89]. However, it is mentioned that this might be due to the limitations of the equipment used to take the records, e.g., EM field measurement.

In this section, to address the limitation for di/dt measurements [89], a small form factor PCB embedded structure will be designed to measure the magnetic field (i.e., di/dt) of the victim system accurately. This approach does not require field probes, a small change in the orientation of which can result in significant measurement errors. The new structure is embedded in an FR-4 PCB and the maximum operating frequency is chosen as 100 MHz, which is above the clock frequency of the victim cryptosystem (16 MHz).

6.1.1 Literature

There are many options to measure current on a transmission line. Magnetoresistive sensors are widely used for relatively low-frequency currents [50]; however, as the goal is to measure time derivative, di/dt, a Rogowski coil, which is a conductor loop located in the vicinity of the current trace to capture the magnetic flux of the current, is a sound option [114, 119]. The output of the Rogowski coil is in the form of di/dt which obviates the use of an integrator which is the case for current measurement scenarios. Wang et al. report a toroidal Rogowski coil designed on a PCB [114]; Hauer compares planar Rogowski coils on PCBs with straight and U-shape current lines[50]. However, the starting point for our design is the folded-dipole Rogowski coil [119] with a small form factor, good noise-immunity, and a high coupling ratio (Figure 6.1a).

6.1.2 Simulation and Measurement Results for the Rogowski Coil

The EM model, which consists of the current line (blue) and the Rogowski coil (pink) as shown in Figure 6.1a, is simulated in HFSS. The current line is placed around the Rogowski coil to maximize the captured magnetic flux (proportional to di/dt) generated by the current, i. The structure is manufactured in an FR-4 PCB with a thickness of 1.6 mm (Figure 6.1b), and the width of the Rogowski conductors are minimized (0.25 mm) to decrease the parasitic capacitance and improve the frequency band of the operation. The dimension of the ten coil-Rogowski structure is 28 mm by 15 mm.

To characterize the coupling between the current line and the Rogowski coil, SMA connectors are added to the input of the current line and the output of the Rogowski coil (Figure 6.1b and 6.2a), and a transmission measurement (i.e., S_{21}) is carried out. The transmission measurement gives the frequency-domain transfer function, $H(f)$, of the operation (i.e., the

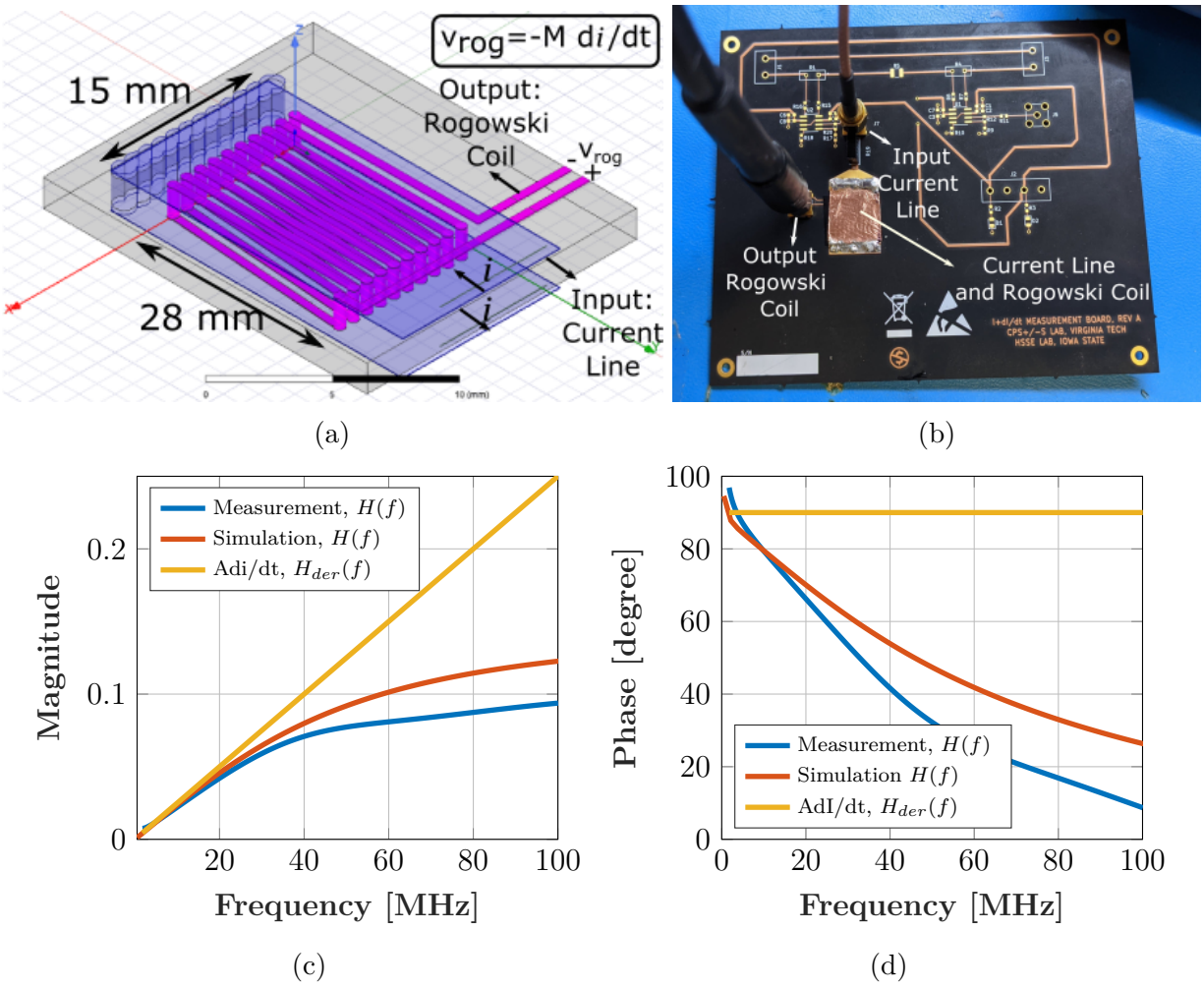


Figure 6.1: A rogowski coil is designed for di/dt measurement, and the simulation and measurement results are compared. (a) The HFSS model for the current line and the Rogowski coil is shown. (b) The overall structure that includes the current line and the Rogowski coil is produced on an FR-4 PCB. (c) The magnitude of $H(f)$ is compared with the transfer function for the ideal time derivation, $H_{der}(f)$. (d) The phase response of $H(f)$ is compared with the transfer function for the ideal time derivation, $H_{der}(f)$.

coupling between the current line and the Rogowski coil) which is defined as:

$$H(f) = \frac{V_{rog}}{V_{in}} \tag{6.1}$$

where $H(f)$ is the frequency domain transfer function of the system, and V_{in} and V_{rog} (Capital

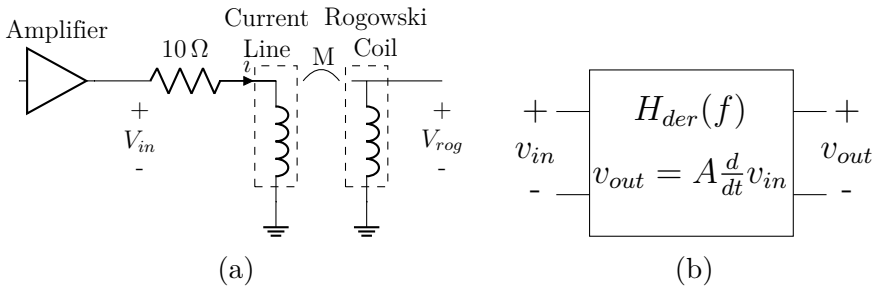


Figure 6.2: (a) The measured structure includes the current line and the rogowski coil and a series resistor. (b) For the Kalman filter, the ideal time-derivative of the v_{in} is needed, the transfer function of which is called $H_{der}(f)$.

letters are used for frequency domain parameters.) are frequency domain representations of the voltage at the input of the current line and the output of the Rogowski coil, respectively (Figure 6.1a). During the measurements, a series 10 Ω resistor is added between the current line and the SMA connector (Figure 6.2a). Figure 6.1c and 6.1d shows the magnitude and phase characteristic of the transfer function, $H(f)$, for simulation and measurement. The measurement (blue) and simulation result (red) are aligned for frequencies up to 30 MHz; however, as the frequency increases the measurement and simulation results start to deviate. This is an expected result because the simulation model does not include the SMA connectors and the series 10 Ω resistor, and also the effect of the parasitic capacitances and dielectric losses can be more pronounced in measurements compared to the simulation results. The yellow plots in Figure 6.1c and 6.1d shows the transfer function for the ideal time derivation (Figure 6.2b), $H_{der}(f)$, which is required for the Kalman filter.

$$H_{der}(f) = \frac{V_{der}}{V_{in}} = jA2\pi f \tag{6.2}$$

where V_{der} is the frequency domain representation of the output. A is a constant and determined by the coupling between the current line and the Rogowski coil.

6.1.3 di/dt Detection with Rogowski Coil Measurements

The orange plots in Figure 6.1c and 6.1d show the $H_{der}(f)$ when A is adjusted to 2.5×10^{-9}, and it is observed that although at low frequencies, the measurements are parallel to the ideal time derivation, as the frequency increases, measurements start to deviate from $H_{der}(f)$. To compensate for this, a compensation transfer function, H_{con}, is defined which should be applied to the output of the Rogowski coil, v_{rog}, such that:

$$H_{com}(f) = H_{der}(f)/H(f) \tag{6.3}$$

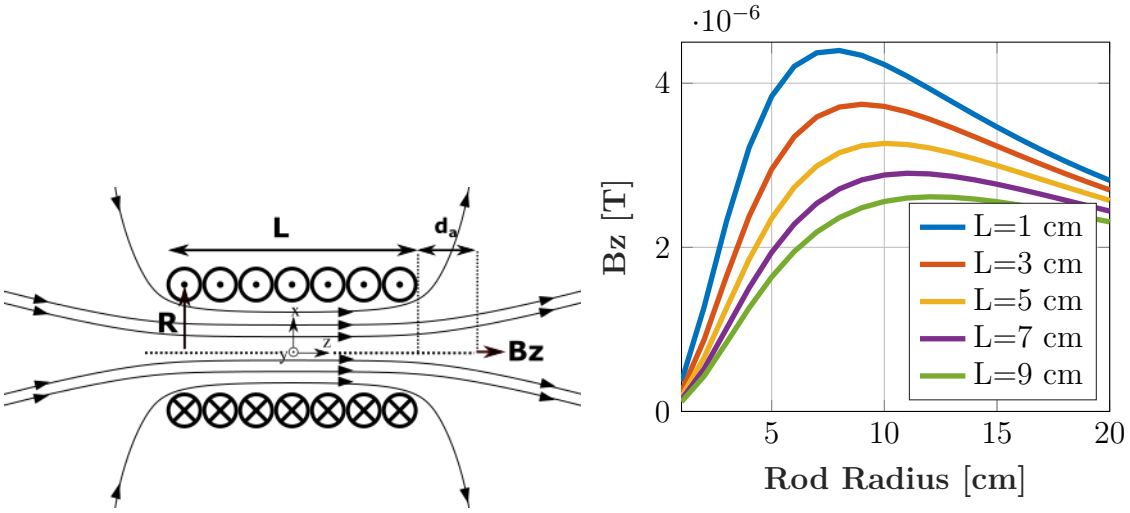
where $H_{con}(f)$ is the division of $H_{der}(f)$ by $H(f)$ and should be applied to the Rogowski output, V_{out}, to get the ideal time derivative:

$$V_{der} = V_{out} H_{com}(f) \tag{6.4}$$

Where V_{der} is the frequency domain representation of di/dt , and can be fed to the Kalman filter after conversion to the time domain.

6.2 Magnetic Field Radiators

In this part, the goal is to assess the field characteristics (e.g., strength and focus) of commonly used radiators such as solenoids and loops (Figure 6.3a). First, the magnetic field of a finite solenoid is discussed with EM simulation results, and then the effect of the radius, length, and core material is analyzed in terms of the field strength and distribution. Structures like planar coils and Helmholtz coils are simulated to determine the magnetic fields generated. For convenience, the attack distance, d_a, is assumed as 5 cm for all results.



(a) (b)

Figure 6.3: The magnetic field of a finite-solenoid is analytically found with (6.5). (a) A finite-solenoid radiate magnetic fields outside the coils, and the attacker wants to maximize the field at $d_a = 5\,\text{cm}$. (b) Z-axis magnetic fields, B_z, of varying size solenoids at $d_a = 5\,\text{cm}$ are generated. The field increases with decreasing solenoid length, L. The maximum field at $d_a = 5\,\text{cm}$ is generated when the radius R of the solenoid is 7 cm. Attacker current (i_a) is 1 A.

6.2.1 Effect of Radiator Radius and Length

The z–axis magnetic field (6.5) of a finite-solenoid for near field (Figure 6.3a) is [24]:

$$B_z = \frac{\mu N i_a}{2}\left(\frac{L/2 - z}{L\sqrt{R^2 + (L/2 - z)^2}} + \frac{L/2 + z}{L\sqrt{R^2 + (L/2 + z)^2}}\right) \tag{6.5}$$

To induce maximum voltage, the attacker needs to maximize B_z at the attack distance of 5 cm; the attacker has the freedom of choosing solenoid length, L, radius, R, and the core material, i.e., μ. The magnetic field of finite solenoids, found with (6.5), with varying L and R is displayed in Figure 6.3b. Each curve corresponds to a fixed length and the the x-axis corresponds to the varying radius of the solenoid.

It is observed that decreasing the radiator (i.e., solenoid) length improves the magnetic

field regardless of the radius value. However, depending on the attack distance, there is an optimum R value at which B_z is maximum. For example, for $L = 1\,\text{cm}$, the radius value that generates the max B_z at $5\,\text{cm}$ is $R = 7\,\text{cm}$ 6.3b. This shows that the attackers, with a known attack distance in mind, can optimize the radius of the loop to maximize the magnetic field on the victim.

6.2.2 Effect of Core Material

Magnetic materials (e.g., ferrites) provide a low-reluctance path for magnetic fields, and are utilized in field radiators to improve the field. To observe the effect of magnetic cores in generated field at an attack distance of $5\,\text{cm}$, B_z of two different size coils (Table 6.1) are simulated with and without ferrite cores (Figure 6.4a). The first structure is a long solenoid with a small radius and the second one is a loop with a large radius and small length (Figure6.4a and Table 6.1). The excitation is $100\,\text{mA}$ at $500\,\text{kHz}$ for each structure.

ANSYS-HFSS results show that B_z of long structures decreases very fast as the attack distance increases regardless of the core material; however, although disc-like (i.e., short) structures do not generate as high a B_z as long structures do in the vicinity, they sustain considerable field at higher attack distances (Figure 6.4b). Another observation is that although a ferrite core improves the B_z of a long solenoid structure, a ferrite core does not provide a significant advantage in the loop structure. Figure 6.4c shows the normalized B_z distribution of the fields on y-axis at $z = 5\,\text{cm}$, and it is observed that long solenoid structure has a narrower beam, i.e., more focused field.

Table 6.1: Solenoid and loop structures are simulated with and without ferrite cores.

Structure	Radius(R)	Length(L)	i_a	Coil Number	Core (Permeability)
Solenoid	1 cm	10 cm	0.1 A@500 kHz	10	Air (μ_o)
Solenoid Ferrite	1 cm	10 cm	0.1 A@500 kHz	10	Ferrite ($600\mu_o$)
Loop	5 cm	2 cm	0.1 A@500 kHz	10	Air (μ_o)
Loop Ferrite	5 cm	2 cm	0.1 A@500 kHz	10	Ferrite ($600\mu_o$)

6.2.3 Improving Field Strength: Helmholtz Coils and Planar Loops

Magnetic field radiators that employ multiple loops with different orientations and positions are preferred in applications that require high and uniform magnetic fields even at distances away from the radiators. Some multiple loop examples are Helmholtz coils and planar loops which are widely used in Transcranial magnetic stimulation [34] and navigation [25] applications. The field distribution of three structures, namely, planar loops, Helmholtz coils, and spiral Helmholtz coils are simulated in ANSYS-HFSS with the models shown in Figure 6.5a. The structures with one-turn coils are excited by 1 A, while the Helmholtz coil with ten-turn spiral is excited by 0.1 A to have a fair comparison.

Figure 6.5b shows the z-axis magnetic field distribution of structures. For comparison, the field distribution of a single loop is included. The first observation is the limited and quickly vanishing field of the single loop with increased z position. It is observed that the planar loop boosts the field in the near field ($z < 3\,\text{cm}$) and then its field vanishes very quickly. Both of the Helmholtz coils generate a uniform and strong field between the coils ($0\,\text{cm} < z < 10\,\text{cm}$). Even though the Helmholtz with spiral coils is excited by 0.1 A, it generates a comparable field to the regular Helmholtz coil with 1 A excitation. It should be noted that the spiral coils have ten-turns unlike the regular Helmholtz coil so they are harder to drive due to increased inductance and resistance. The ultimate choice for the radiator structure can be made with the amplifier characteristics (output impedance, output current, and output voltage rating) that drive the radiators. Series capacitors and Litz wires are used to resonate the radiators

and minimize the AC resistance at resonance, respectively.

Effect of Radius on Helmholtz Coil Field

In practice, AC-excited multiturn coils suffer from the skin depth and proximity effect, which introduces an AC resistance that is significantly higher than the DC resistance even though the structures are resonated with a capacitor [99]. Decreasing the AC resistance is desirable to increase the excitation current, however, the amplifiers are designed/chosen carefully for this relatively low output resistance. One way to decrease the AC resistance is to use Litz wires that alleviate the 'skin depth' and 'proximity' effect. Another way to reduce the AC resistance is to lower the coil radius. However, decreasing the coil radius also decreases the magnetic field because the inductance of the loop is lessened as well. In this section, the coil radius, R, for a Helmholtz coil (Figure 6.4a), is varied and the field distribution is analyzed to find an optimal structure with a small radius (i.e., less AC resistance) and adequate attack field.

Figure 6.6a and 6.6b shows the magnetic field distribution of a Helmholtz coil (Figure 6.5a) with varying coil radius, R and fixed coil separation (10 cm). It is observed in both y and z-axis B_z decreases significantly as the coil radius goes below 6 cm; however, radius values above 7 cm generate similar fields. Additionally, it is observed that, as the radius decreases, the uniformity of the field through the x, y and z-axis degrades significantly. Although in some applications a uniform magnetic field is desirable, in the IEMI attacks, maximizing the magnetic field is the priority, not the uniform field distribution. In scenarios the attacker wants to focus the magnetic field on a specific region of the victim circuitry, the non-uniform magnetic field distribution can even be desirable.

6.2.4 Improving Field Focus: An Optimal Magnetic Field Array

For specific attack scenarios, the attackers desire to manipulate only a certain region in the victim circuitry with a focused magnetic field. For instance, the attacker might need to manipulate only one input of an H-bridge to control an electric motor, or the attacker might want to change only the output of a particular sensor while not affecting the others. In this section, a magnetic field array is designed with an optimization process to analyze the field focusing capabilities of an attacker.

In Section 6.2, finite–solenoids with varying dimensions and core material (e.g., ferrite) are examined in terms of the magnetic field distribution and strength. In an array, elements (e.g., ferrite rods) are placed horizontally, and a small–radius solenoid is much more preferable than a large–radius loop which limits the possible array configurations. Additionally, it is concluded in Section 6.2 that a ferrite core in a small–radius structure enhances the field strength significantly (Figure 6.4b). Due to these reasons, a ferrite solenoid/rod is chosen as the array element with the parameters provided in Table 6.2. Magnetic field distribution,

Table 6.2: The parameters of the ferrite rod used as the array element.

Coil Number	Rod Diameter	Rod Length	Permeability μ	Permittivity ϵ
10	0.25”	1.25”	1000	12

B_z, of the array element (i.e., the ferrite rod Table 6.2) is determined at an attack distance of $d_a = 5\,\text{cm}$ on a 20 cm-by-20 cm plane (Figure 6.7b), and this field is used to optimize the excitation and position of the unit elements in the array. A matlab code, which optimizes the excitations (i.e., currents) for each array element for the most focused field, is used. The field of the single rod is fit to a Gaussian pulse [36] with a variance of 7 (6.6 Figure 6.7a), and inputted to the optimizer.

$$B_z(x,y) = e^{-\left[\frac{x^2}{2var}+\frac{y^2}{2var}\right]} \quad , \quad var = 7 \tag{6.6}$$

Table 6.3: 3-by-3 array current values are optimized for the focused magnetic field at $d_a = 5\,\text{cm}$. The element separation is 3 cm.

I_1	I_2	I_3	I_4	I_5	I_6	I_7	I_8	I_9
$-0.3406\,\text{A}$	$0.0377\,\text{A}$	$-0.3406\,\text{A}$	$0.0377\,\text{A}$	$1\,\text{A}$	$0.0377\,\text{A}$	$-0.3406\,\text{A}$	$0.0377\,\text{A}$	$-0.3406\,\text{A}$

A smaller variance ($var_{obj} = 1$) Gaussian pulse, which has a significantly smaller half-power beamwidth (HPBW), is assigned as the objective field for the optimizer. The symmetric configurations like 3–by–3, 4–by–4, and 5–by–5 arrays with varying element separations are analyzed in terms of the field focusing ability. It is observed that a 3–by–3 array with a separation of 3 cm results in the most focused field with the minimum total current at $d_a = 5\,\text{cm}$ (Figure 6.7b). The excitations, I_n, for each array element is found with the optimizer (Table 6.3). HPBW is defined as the distance between the half-power points of the field distribution and gives the diameter of the beam at the attack distance. The desired beam shape is assumed to be symmetric around the z-axis (i.e., circular), so the HPBW does not change on the x or y axis.

Table 6.3 shows that currents of corner elements (I_1, I_3, I_7, and I_9) should be negative (i.e., 180^o phase difference) and small compared to the to the main excitation at the center, i.e., I_5 (Figure 6.7b). This current distribution demonstrates that the central element, I_5 , generates the majority of the field strength in the focused region, and the corner elements (I_1, I_3, I_7, and I_9) suppress the tails of the field distribution for a more focused field. Additionally, it is observed that the edge elements (I_2, I_4, I_6, and I_8) need significantly small currents compared to the other elements. An attacker can take advantage of this observation and remove the edge elements (I_2, I_4, I_6, and I_8) which result in a 5 element plus-array. Table 6.4 summarizes the field focus properties for 3-by-3 and Plus-array. Both structures significantly decrease the HPBW and improve the field focus. For instance, while the HPBW for a single rod is 40 mm, the HPBW of 3-by-3 and plus-array are 34.5 mm and 31 mm, respectively, which

Table 6.4: The 3-by-3 array and Plus-array improve the field focus; however, more current is needed to generate the same magnetic field.

Structure	Separation	Normalized Total Current	Normalized Field	Half Power Beamwidth	Half Power Area
Single Rod	NA	1	1	40 mm	1256 mm^2
3-by-3 Array 9 elements	3 cm	2.51	0.70	34.5 mm	934 mm^2
Plus Array 5 elements	3 cm	2.36	0.62	31 mm	753 mm^2

corresponds to a %40 improvement (i.e., decrease) in the field focus in terms of the focus area. However, both array structures require significantly higher total current compared to a single rod does to generate similar magnetic field strengths. In conclusion, the array structures found with the optimization method provide an improvement of %40 in the focus area with the expense of increased attacker current.

6.3 Conclusion

In the first part of Chapter 6, a Rogowski coil design is reported which addresses the measurement inaccuracies in a novel side-channel attack, i.e., EM coupling Correlational Power Analysis [89]. The device is characterized with EM simulation and measurements, and a transfer function is provided to determine the time-derivative of the victim current which is required for the attacks. In the next part, magnetic field radiators are assessed in terms of field strength and field focus ability. It is observed that loops with relatively large radius generate more field at increased attack distance, and there is an optimum loop radius for each attack distance (e.g., a loop with radius 7 cm at an attack distance of 5 cm generates the most field.). In the last part, a magnetic field array is designed with optimization to focus the magnetic field. Although it is concluded that the field focus can be improved by 40%, the attacker current should be significantly increased (relative to a single–coil radiator) to generate the same field strength.

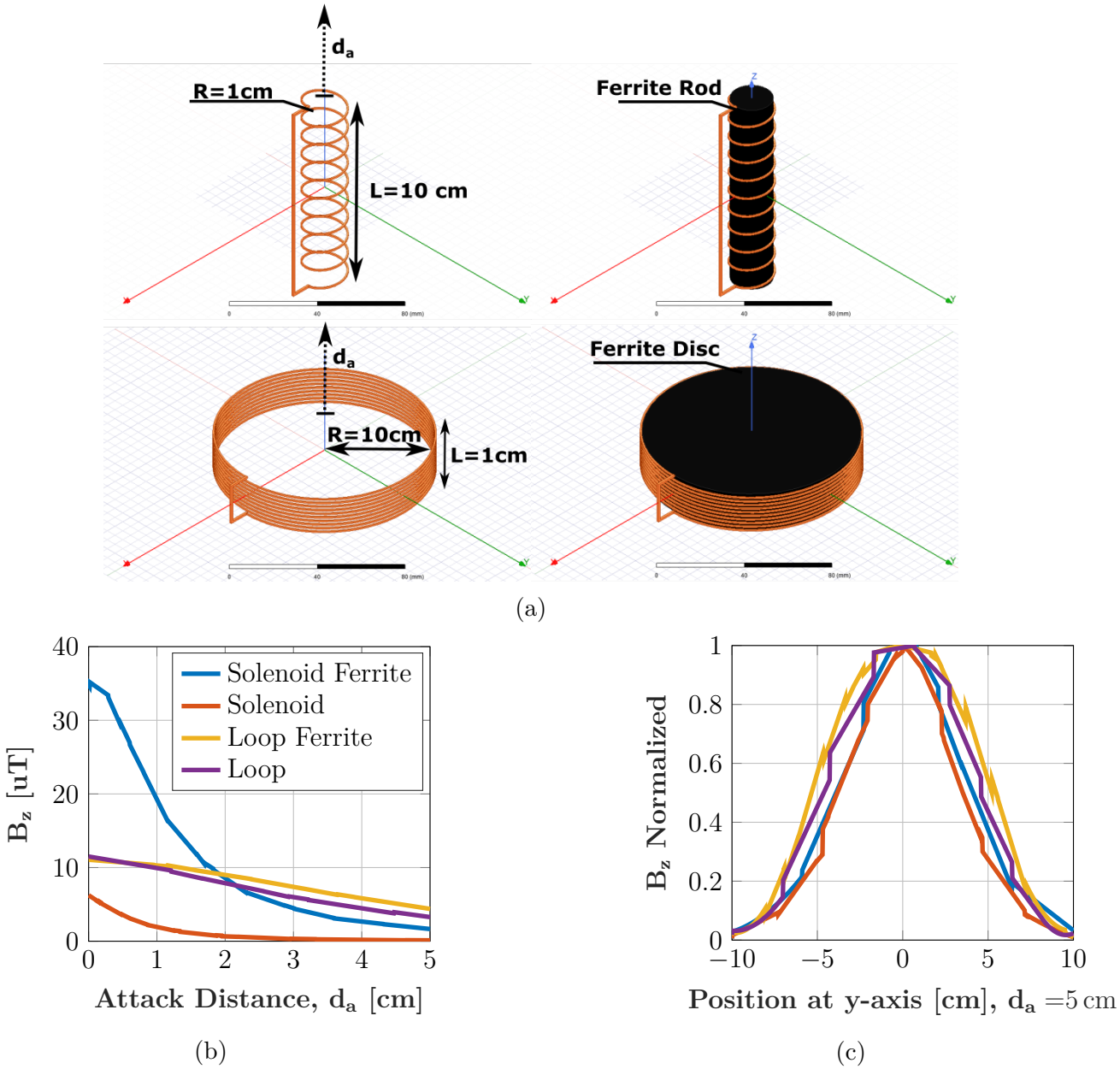
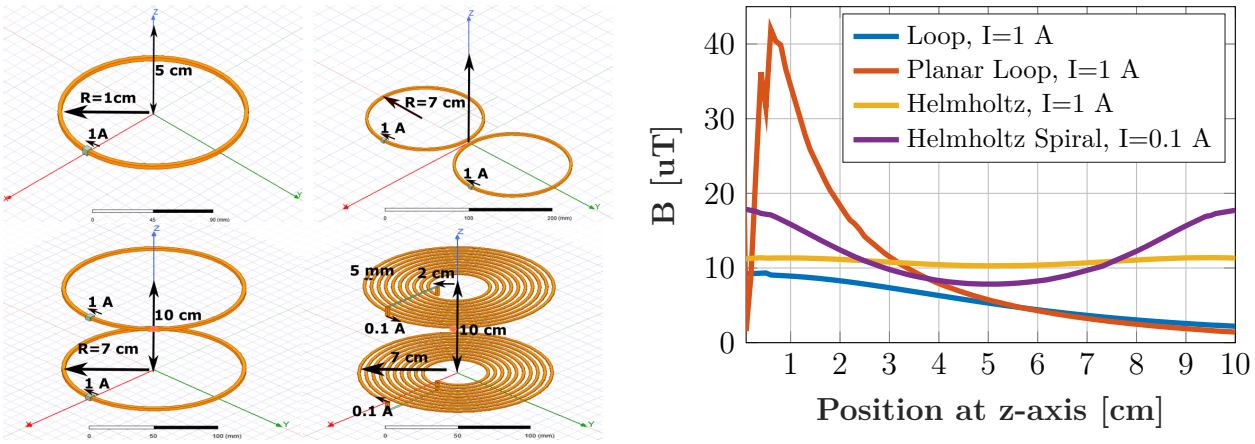
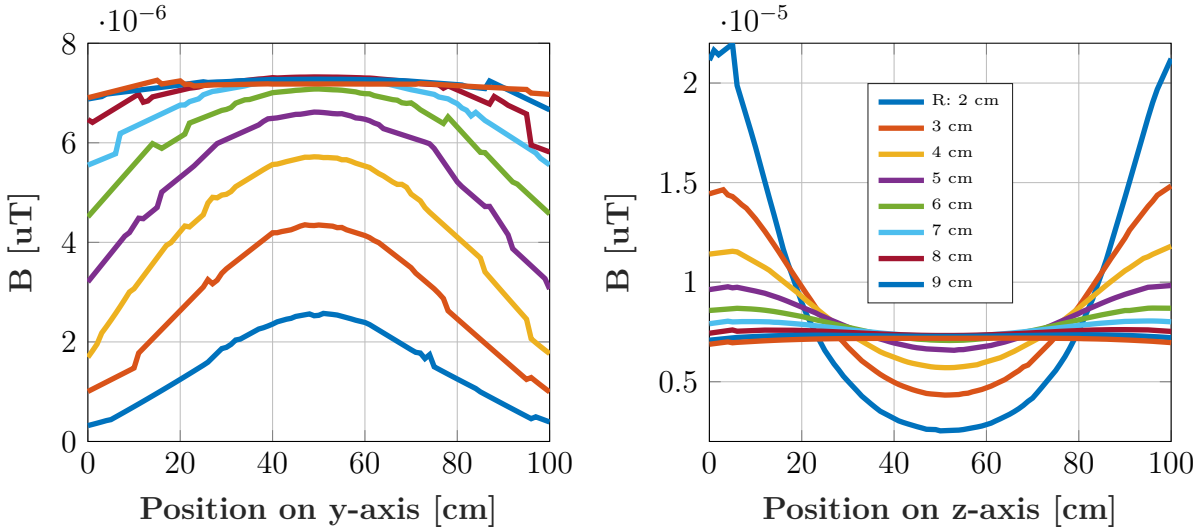


Figure 6.4: Solenoid and loop structures with different dimensions and with and without ferrite cores are simulated in ANSYS HFSS to detect z directed magnetic fields. (a) EM Models are shown for solenoid, solenoid with ferrite core, loop and loop with ferrite core. (b) B_z decreases as the attack distance increases; however, large-radius loop structures generate significantly higher B_z for larger attack distance $d_a > 2\,\text{cm}$. (c) The normalized field distribution at $d_a = 5\,\text{cm}$ are shown; solenoids (orange and blue) have a more focused field. (d) The HP beamwidth of the single rod and Plus-Array is compared with varying attack distance, d_a. The array improves the HPBW for an attack distance of 3 cm or higher.



(a) (b)

Figure 6.5: The magnetic field distribution of different structures are compared. (a) EM simulation models for Helmholtz coil, Helmholtz with spiral coils, and planar loops with regular and inverted excitations are demonstrated. (b) Magnetic field B along the z-axis is shown, Helmholtz with spiral coils generate the maximum field at $z = 5\,\text{cm}$; however, in proximity ($z < 1\,\text{cm}$) the planar loops generate a significantly larger fields.



(a) (b)

Figure 6.6: The effect of the radius on Helmholtz coil field is simulated. Frequency is 500 kHz. (a) The field, B_z, distribution on y-axis at $z = 5\,\text{cm}$ (b) The field, B_z, distribution on z-axis

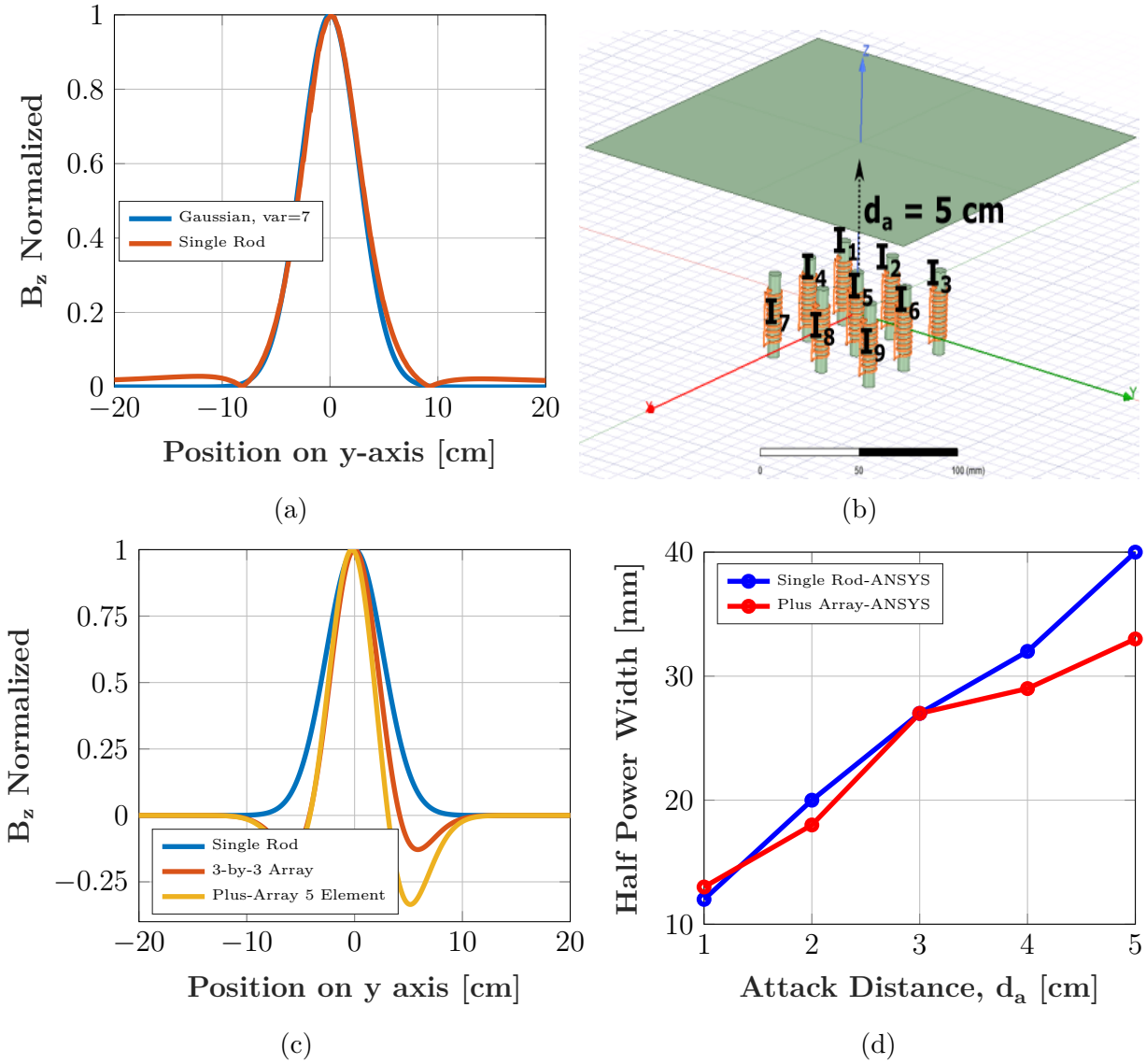


Figure 6.7: An optimization approach is used to find the optimal current and element positions for a focused magnetic field. (a) The single rod field distribution at $d_a = 5\,\text{cm}$ is represented with a Gaussian pulse with a variance of 7. (b) The 3-by-3 array with a separation of 3 cm generates a focused field at $d_a = 5\,\text{cm}$ with the optimal currents given in 6.3. (c) The field distribution at $d_a = 5\,\text{cm}$ are shown. The 3-by-3 and plus-array have more focused fields compared to the single rod; however, the total current should be higher to generate the same affect with arrays.

Chapter 7

Conclusion

In this dissertation, Intentional Electromagnetic Interference (IEMI), as an attack tool on cyber-physical systems, is analyzed and hardware–level defenses are presented. The focus is actuation and digital data manipulation through specially crafted waveforms which are attacks rarely reported in security literature. The attacks are analyzed theoretically with fundamental electromagnetic laws such as 'Faraday's law of Induction'; and the attack mechanisms are discussed. The attacks are demonstrated on real systems such as UAVs, serial communication systems and EV chargers; on analog, digital, and actuation signals which are transmitted in cables or PCBs. The purpose of the attack demonstrations, of course, is not to reveal how the systems can be hacked, but to warn the system designers that IEMI attacks are achievable on different systems (e.g., UAVs), signal types (e.g., actuation), and transmission mediums (e.g., PCBs) with low-cost commercial hardware. However, these attacks can be mitigated with hardware–level defense mechanisms, some of which are discussed in Chapter 5. The designers with IEMI–awareness can make the attacks very 'expensive' (e.g., higher frequency, power, and cost required for attack success), and prevent the majority of the attacks with relatively simple design choices.

The focus of Chapter 2 is the IEMI attacks on actuation control. In the first part of the Chapter, the mechanism of PWM–based actuation control is analyzed, and weaknesses that can be exploited by an attacker with IEMI are discussed. It is concluded that a sawtooth attack waveform that injects voltage drops to a victim PWM signal can control a servo

engine. However, due to the low-frequency nature of the attacks, the attack distance is limited, and the attacker needs the timing information of the victim (i.e., synchronization) which requires an additional receiver system (to eavesdrop on the victim). In the next part, the attack distance is improved with high–frequency (FM–band) amplitude modulated attack waveforms with resonant inductive coupling. The attacks are demonstrated indoor and in–flight on an Unmanned Aerial System, and it is observed that the attacker can prevent the operation of any servo motor through *Block* and take control of the Futaba–make actuators through *Full Control*. The attacks have serious consequences, e.g., the victim UAV crashed due to the *Block* attack during demonstrations. In this dissertation, the focus is to use inductive coupling which is prone to shielding; however, the author thinks that, as a future direction, the far–field antennas can be investigated for FAI attacks which possibly improve the attack range with an increased vulnerability of the attack waveform to the shielding. As a defense mechanism, fiber–optic transmission of actuation signals is suggested which are prone to EMI and utilized effectively during attack demonstrations.

In Chapter 3, the focus is IEMI attacks on digital data and serial communication systems. A widely used serial communication standard, UART, is assessed from an IEMI attacker perspective, and in a proof–of–concept demonstration, it is shown that an attacker can flip-bits in a controllable manner (i.e., inject the desired data) with a success rate of 98% or more with the reported attack phases and waveforms. The low–frequency attack waveform relies on inductive coupling that is immune to EM shielding; however, the attack distance is limited. A parallel research project continues in which higher frequency attacks (vulnerable to RF shielding) with a longer attack range potential are investigated. Countermeasures like twisted cables are suggested for digital transmission, which is validated with experimental results.

In Chapter 4, the focus is IEMI attacks on sensors (e.g., current) and actuators (e.g., current

switches) in state-of-art power converters used in EV chargers. Three attacks, on current and voltage sensors and current switches, are demonstrated to show that both the sensor and actuation signals of power converters can be altered by intentional EMI which can result in extremely high current supply to the EVs with serious physical consequences such as thermal runaway of EV batteries. Considering that many EV chargers are in open spaces approachable by adversaries and lacks magnetic field shielding, attacks on EV chargers have physical consequences, e.g.,a fire from overheated EV battery or a taken-down power grid due to synchronized attacks.

In Chapter 5, the focus is to provide physical layer methods to mitigate IEMI. An analytical model that relates the attacker field and the induced voltage in the victim circuitry (i.e., PCB trace) is reported to lay the basis of suggested countermeasures like choosing shorter traces and thinner PCBs for 'significant' signals, i.e., analog, digital, and actuation signals. The defense methods are validated with EM–based analytical solutions or simulations.

In Chapter 6, two security-related projects are presented. The first one is a design of a Rogowski coil to improve the side-channel attacks on cryptosystems with EM Coupled Correlational Power Analysis, the design procedure and the transfer function of the Rogowski coil is reported with simulation and measurement results. In the second part, the limited attack range of inductively coupled IEMI attacks is addressed with an analysis of magnetic field radiators. Magnetic field radiators such as solenoids, loops, and Helmholtz coils are simulated and their field strength and radiation patterns are compared. At the end of the Chapter, a magnetic field array, with ferrite rod elements, is designed with an optimization approach to improve the field focus.

Bibliography

[1] Carbon-z cessna 150 2.1m bnf basic (efl1450). www.horizonhobby.com. [Online; accessed 14-Jul-2019].

[2] Eflite bl50 brushless outrunner motor, 525kv. https://www.horizonhobby.com/product/bl50-brushless-outrunner-motor-525kv/EFLM7450.html. Accessed: 2021-07-12.

[3] Phoenix Edge 100 Amp ESC, howpublished = https://www.castlecreations.com/en/phoenix-edge-100-esc-010-0100-00, note = Accessed: 2021-07-12, .

[4] Phoenix Edge 75 Amp ESC, howpublished = https://www.castlecreations.com/en/phoenix-edge-75-esc-010-0101-00, note = Accessed: 2021-07-12, .

[5] Eflight 60-amp pro switch-mode bec brushless esc v2: Ec3. https://www.horizonhobby.com/product/60-amp-pro-switch-mode-bec-brushless-esc-v2-ec3/EFLA1060B.html, . Accessed: 2021-07-12.

[6] MuMetal Relative Permeability. URL http://www.mu-metal.com/faqs.html.

[7] Nato-equipment selection process. http://www.ia.nato.int/niapc/tempest/certification-scheme. Accessed: 2021-02-16.

[8] X300/x310. URL https://kb.ettus.com/X300/X310.

[9] Application of uart in gps navigation system -application note. Technical Report AN10353, Philips Semiconductors, March 2005.

[10] Ieee standard for ethernet. *IEEE Std 802.3-2018 (Revision of IEEE Std 802.3-2015)*, pages 1–5600, 2018. doi: 10.1109/IEEESTD.2018.8457469.

[11] A. Agrawal, H. Price, and S. Gurbaxani. Transient response of multiconductor transmission lines excited by a nonuniform electromagnetic field. In *1980 Antennas and Propagation Society International Symposium*, volume 18, pages 432–435, 1980.

[12] Charles Alexander and Matthew Sadiku. *Fundamentals of Electric Circuits*. McGraw Hill Higher Education, 4th edition, 2008. ISBN 9780071284417.

[13] *15V, 1.5A Synchronous Rail-to-Rail Single Resistor Step-Down Regulator*. Analog Devices, 2011. URL https://www.analog.com/media/en/technical-documentation/data-sheets/3600fd.pd. Rev. D.

[14] M. G. Backstrom and K. G. Lovstrand. Susceptibility of electronic systems to high-power microwaves: summary of test experience. *IEEE Transactions on Electromagnetic Compatibility*, 46(3):396–403, 2004. doi: 10.1109/TEMC.2004.831814.

[15] C.A. Balanis. *Antenna theory: analysis and design*. Harper & Row series in electrical engineering. Wiley, 1982. ISBN 9780471603528. URL https://books.google.com/books?id=wARTAAAAMAAJ.

[16] C.A. Balanis. *Advanced Engineering Electromagnetics*. Wiley, 1989. ISBN 9780471503163. URL https://books.google.com/books?id=7u0qGgAACAAJ.

[17] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache. Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures. *Proceedings of the IEEE*, 100(11):3056–3076, 2012. doi: 10.1109/JPROC.2012.2188769.

[18] D. Barnett, D. Groth, and J. McBee. *Cabling: The Complete Guide to Network Wiring*.

Wiley, 2006. ISBN 9780782150872. URL https://books.google.com/books?id=AKDSTYu3nl4C.

[19] Anomadarshi Barua and Mohammad Abdullah Al Faruque. Hall spoofing: A non-invasive dos attack on grid-tied solar inverter. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 1273–1290. USENIX Association, August 2020. ISBN 978-1-939133-17-5. URL https://www.usenix.org/conference/usenixsecurity20/presentation/barua.

[20] RANDAL W. BEARD and TIMOTHY W. McLAIN. *Small Unmanned Aircraft: Theory and Practice*. Princeton University Press, 2012. ISBN 9780691149219. URL http://www.jstor.org/stable/j.ctt7sbc4.

[21] C. Bolton, S. Rampazzi, C. Li, A. Kwong, W. Xu, and K. Fu. Blue note: How intentional acoustic interference damages availability and integrity in hard disk drives and operating systems. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 1048–1062, May 2018. doi: 10.1109/SP.2018.00050.

[22] Eric Brier, Christophe Clavier, and Francis Olivier. Correlation power analysis with a leakage model. In Marc Joye and Jean-Jacques Quisquater, editors, *Cryptographic Hardware and Embedded Systems - CHES 2004*, pages 16–29, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg. ISBN 978-3-540-28632-5.

[23] Robert J. Bunker. *Terrorist and insurgent unmanned aerial vehicles : use, potentials, and military implications / Robert J. Bunker.* 2015. ISBN 978-1-58487-698-4. URL http://login.ezproxy.lib.vt.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsgpr&AN=edsgpr.000995676&site=eds-live&scope=site.

[24] Edmund E. Callaghan and Stephen H. Maslen. The magnetic field of a ferrite solenoid. Technical Report D465, NASA Lewis Research Center, October 1960.

[25] Quanliang Cao, Xiaotao Han, Bo Zhang, and Liang Li. Analysis and optimal design of magnetic navigation system using helmholtz and maxwell coils. *IEEE Transactions on Applied Superconductivity*, 22(3):4401504–4401504, 2012. doi: 10.1109/TASC.2011.2174583.

[26] S. Capkun. Physical layer and telecommunications security knowledge area issue 1.0. Technical report, www.cybok.org, October 2019.

[27] A. Cardenas. Cyber-physical systems security knowledge area issue 1.0. Technical report, www.cybok.org, October 2019.

[28] *AMT10 Mudular Incremental Encoder*. CUI Devices, 11 2019.

[29] K. Davey and M. Riehl. Designing transcranial magnetic stimulation systems. *IEEE Transactions on Magnetics*, 41(3):1142–1148, 2005. doi: 10.1109/TMAG.2004.843326.

[30] Drew Davidson, Hao Wu, Rob Jellinek, Vikas Singh, and Thomas Ristenpart. Controlling uavs with sensor input spoofing attacks. In *10th USENIX Workshop on Offensive Technologies (WOOT 16)*, Austin, TX, 2016. USENIX Association. URL https://www.usenix.org/conference/woot16/workshop-program/presentation/davidson.

[31] Dawoud Shenouda Dawoud and Peter Dawoud. *Serial Communication Protocols and Standards: : RS232/485, UART/USART, SPI, USB, INSTEON, Wi-Fi and WiMAX*. River Publishers, Aalborg, DENMARK, 2020. ISBN 9788770221535. URL http://ebookcentral.proquest.com/lib/vt/detail.action?docID=6300567.

[32] G.Y. Dayanıklı, R. R. Hatch, R. M. Gerdes, H. Wang, and R. Zane. Electromagnetic sensor and actuator attacks on power converters for electric vehicles. In *2020 IEEE Security and Privacy Workshops (SPW)*, pages 98–103, Los Alamitos, CA, USA, may 2020. IEEE Computer Society. doi: 10.1109/SPW50608.2020.00032. URL https://doi.ieeecomputersociety.org/10.1109/SPW50608.2020.00032.

[33] A. Dehbaoui, J. Dutertre, B. Robisson, and A. Tria. Electromagnetic transient faults injection on a hardware and a software implementations of aes. In *2012 Workshop on Fault Diagnosis and Tolerance in Cryptography*, pages 7–15, 2012. doi: 10.1109/FDTC.2012.15.

[34] Zhi-De Deng, Sarah H Lisanby, and Angel V Peterchev. Electric field depth-focality tradeoff in transcranial magnetic stimulation: simulation comparison of 50 coil designs. *Brain stimulation*, 6(1):1—13, January 2013. ISSN 1935-861X. doi: 10.1016/j.brs.2012.02.005. URL https://europepmc.org/articles/PMC3568257.

[35] Marco Denicolai. Optimal performance for tesla transformers. *Review of Scientific Instruments*, 73(9):3332–3336, 2002. doi: 10.1063/1.1498905. URL https://doi.org/10.1063/1.1498905.

[36] Chuong B. Do. The multivariate gaussian distribution, October 2008. URL http://cs229.stanford.edu/section/gaussians.pdf.

[37] Park Donghui and Michael Walstrom. Cyberattack on critical infrastructure: Russia and the ukrainian power grid attacks, Oct 2017. URL https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/.

[38] F. Elibol, U. Sarac, and I. Erer. Realistic eavesdropping attacks on computer displays

with low-cost and mobile receiver system. In *2012 Proceedings of the 20th European Signal Processing Conference (EUSIPCO)*, pages 1767–1771, 2012.

[39] Charles M. Epstein, Eric M. Wassermann, Ulf Ziemann, and Mark Riehl. Tms stimulator design, 11 2012. URL https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780198568926.001.0001/oxfordhb-9780198568926-e-003.

[40] David Finkelstein, Philip Goldberg, and Joshua Shuchatowitz. High voltage impulse system. *Review of Scientific Instruments*, 37(2):159–162, 1966. doi: 10.1063/1.1720117. URL https://doi.org/10.1063/1.1720117.

[41] Louis E. Frenzel. *Handbook of serial communications interfaces: a comprehensive compendium of serial digital input/output (I/O) standards*. Newnes, an imprint of Elsevier, 2016.

[42] A. Frikha, M. Bensetti, F. Duval, N. Benjelloun, F. Lafon, and L. Pichon. A new methodology to predict the magnetic shielding effectiveness of enclosures at low frequency in the near field. *IEEE Transactions on Magnetics*, 51(3):1–4, March 2015. ISSN 1941-0069. doi: 10.1109/TMAG.2014.2362953.

[43] Kevin Fu and Wenyuan Xu. Risks of trusting the physics of sensors. *Commun. ACM*, 61(2):20–23, January 2018. ISSN 0001-0782. doi: 10.1145/3176402. URL https://doi.org/10.1145/3176402.

[44] Dan Gettinger and Arthur Holland Michel. Drone sightings and close encounters: An analysis, 2015.

[45] I. Giechaskiel and K. Rasmussen. Taxonomy and challenges of out-of-band signal injection attacks and defenses. *IEEE Communications Surveys Tutorials*, 22(1):645–670, 2020. doi: 10.1109/COMST.2019.2952858.

[46] Ilias Giechaskiel and Kasper Rasmussen. Taxonomy and challenges of out-of-band signal injection attacks and defenses. *Commun. Surveys Tuts.*, 22(1):645–670, January 2020. ISSN 1553-877X. doi: 10.1109/COMST.2019.2952858. URL https://doi.org/10.1109/COMST.2019.2952858.

[47] Ilias Giechaskiel, Youqian Zhang, and Kasper B. Rasmussen. A framework for evaluating security in the presence of signal injection attacks. In Kazue Sako, Steve Schneider, and Peter Y. A. Ryan, editors, *Computer Security – ESORICS 2019*, pages 512–532, Cham, 2019. Springer International Publishing. ISBN 978-3-030-29959-0.

[48] D. V. Giri and F. M. Tesche. Classification of intentional electromagnetic environments (ieme). *IEEE Transactions on Electromagnetic Compatibility*, 46(3):322–328, 2004. doi: 10.1109/TEMC.2004.831819.

[49] D. V. Giri, F. M. Tesche, and C. E. Baum. An overview of high-power electromagnetic (hpem) radiating and conducting systems. *URSI Radio Science Bulletin*, 2006(318): 6–12, Sep. 2006. ISSN 1024-4530. doi: 10.23919/URSIRSB.2006.7909564.

[50] Sven Hauer. Development of a high-bandwidth current sensor for high-frequency power applications. Master's thesis, Karlsruhe Institute of Technology, 2018.

[51] Zhang Hongxin, Huang Yuewang, Wang Jianxin, Lu Yinghua, and Zhang Jinling. Recognition of electro-magnetic leakage information from computer radiation with svm. *Computers & Security*, 28(1):72 – 76, 2009. ISSN 0167-4048. doi: https://doi.org/10.1016/j.cose.2008.09.009. URL http://www.sciencedirect.com/science/article/pii/S016740480800093X.

[52] M. Hooper, Y. Tian, R. Zhou, B. Cao, A. P. Lauf, L. Watkins, W. H. Robinson, and W. Alexis. Securing commercial wifi-based uavs from common security attacks. In

MILCOM 2016 - 2016 IEEE Military Communications Conference, pages 1213–1218, Nov 2016. doi: 10.1109/MILCOM.2016.7795496.

[53] *Plastic Fiber Optic Phototransistor*. Industrial FIber Optics, 5 2006.

[54] *Fiber Optic Red LED Fiber LED*. Industrial Fiber Optics, 2 2020.

[55] R.C. Johnson and H. Jasik. *Antenna Engineering Handbook*. Electronics Electrical Engineering. McGraw-Hill, 1993. ISBN 9780070323810. URL https://books.google.com/books?id=xTSNJhVlHGgC.

[56] Samy Kamkar. Skyjack:autonomous drone hacking. https://samy.pl/skyjack/, 2013. [Online; accessed 15-June-2019].

[57] C. Kasmi and J. Lopes Esteves. Iemi threats for information security: Remote command injection on modern smartphones. *IEEE Transactions on Electromagnetic Compatibility*, 57(6):1752–1755, Dec 2015. ISSN 0018-9375. doi: 10.1109/TEMC.2015.2463089.

[58] Andrew J. Kerns, Daniel P. Shepard, Jahshan A. Bhatti, and Todd E. Humphreys. Unmanned aircraft capture and control via gps spoofing. *Journal of Field Robotics*, 31(4):617–636, 2014. doi: 10.1002/rob.21513. URL https://onlinelibrary.wiley.com/doi/abs/10.1002/rob.21513.

[59] Alan Kim, Brandon Wampler, James Goppert, Inseok Hwang, and Hal Aldridge. Jun 2012. doi: 10.2514/6.2012-2438. URL https://doi.org/10.2514/6.2012-2438. 0.

[60] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In Michael Wiener, editor, *Advances in Cryptology — CRYPTO' 99*, pages 388–397, Berlin, Heidelberg, 1999. Springer Berlin Heidelberg. ISBN 978-3-540-48405-9.

[61] D.F. Kune, J. Backes, S.S. Clark, D. Kramer, M. Reynolds, K. Fu, Y. Kim, and W. Xu. Ghost talk: Mitigating EMI signal injection attacks against analog sensors. In *Proc. Symp. Security and Privacy*, pages 145–159, May 2013.

[62] André Kurs, Aristeidis Karalis, Robert Moffatt, J D Joannopoulos, Peter Fisher, Marin Soljacic, and Marin Soljac. Wireless Power Transfer via Strongly Coupled Magnetic Resonances. *Science*, 83:83–6, 2007. ISSN 1095-9203. doi: 10.1126/science.1143254. URL http://www.ncbi.nlm.nih.gov/pubmed/17556549.

[63] David Kushner. The real story of stuxnet. *IEEE Spectrum*, Feb. 26 2013.

[64] Jonas Larsson. Electromagnetics from a quasistatic perspective. (June 2006):230–239, 2006. ISSN 00029505. doi: 10.1119/1.2397095. URL http://arxiv.org/abs/physics/0606109{%}0Ahttp://dx.doi.org/10.1119/1.2397095.

[65] M. Leone and H. L. Singer. On the coupling of an external electromagnetic field to a printed circuit board trace. *IEEE Transactions on Electromagnetic Compatibility*, 41 (4):418–424, Nov 1999. ISSN 1558-187X. doi: 10.1109/15.809842.

[66] W. Lindseth. Effectiveness of pcb perimeter via fencing: Radially propagating emc emissions reduction technique. In *2016 IEEE International Symposium on Electromagnetic Compatibility (EMC)*, pages 627–632, 2016.

[67] Z. N. Low, R. A. Chinga, R. Tseng, and J. Lin. Design and test of a high-power high-efficiency loosely coupled planar wireless power transfer system. *IEEE Transactions on Industrial Electronics*, 56(5):1801–1812, May 2009. ISSN 0278-0046. doi: 10.1109/TIE.2008.2010110.

[68] Thomas S. Messerges, Ezzy A. Dabbish, and Robert H. Sloan. Investigations of power analysis attacks on smartcards. In *Proceedings of the USENIX Workshop on Smartcard*

Technology on USENIX Workshop on Smartcard Technology, WOST'99, page 17, USA, 1999. USENIX Association.

[69] Martin Misakian. Equations for the Magnetic Field Produced by One or More Rectangular Loops of Wire in the Same Plane. *Journal of Research of the National Institute of Standards and Technology*, 105(4):557–564, 2000. ISSN 1044677X. doi: 10.6028/jres.105.045.

[70] N. Moro, A. Dehbaoui, K. Heydemann, B. Robisson, and E. Encrenaz. Electromagnetic fault injection: Towards a fault model on a 32-bit microcontroller. In *2013 Workshop on Fault Diagnosis and Tolerance in Cryptography*, pages 77–88, 2013. doi: 10.1109/FDTC.2013.9.

[71] J. R. Moser. Low-frequency low-impedance electromagnetic shielding. *IEEE Transactions on Electromagnetic Compatibility*, 30(3):202–210, Aug 1988. ISSN 1558-187X. doi: 10.1109/15.3298.

[72] Devaprakash Muniraj and Mazen Farhood. Detection and mitigation of actuator attacks on small unmanned aircraft systems. *Control Engineering Practice*, 83:188 – 202, 2019. ISSN 0967-0661. doi: https://doi.org/10.1016/j.conengprac.2018.10.022. URL http://www.sciencedirect.com/science/article/pii/S0967066118306804.

[73] Shoei Nashimoto, Daisuke Suzuki, Takeshi Sugawara, and Kazuo Sakiyama. Sensor con-fusion: Defeating kalman filter in signal injection attack. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, ASIACCS '18, page 511–524, New York, NY, USA, 2018. Association for Computing Machinery. ISBN 9781450355766. doi: 10.1145/3196494.3196506. URL https://doi.org/10.1145/3196494.3196506.

[74] A. Oliviero and B. Woodward. *Cabling: The Complete Guide to Copper and Fiber-Optic Networking*. Wiley, 2009. ISBN 9780470550052. URL https://books.google.com/books?id=CR53cRQtecIC.

[75] Omnicables. Dielectric constant of insulations. https://www.omnicable.com/technical-resources/dielectric-constants-of-insulations. Accessed: 2021-05-12.

[76] H.W. Ott. *Electromagnetic Compatibility Engineering*. Wiley, 2011. ISBN 9781118210659.

[77] M. Pajic, I. Lee, and G. J. Pappas. Attack-resilient state estimation for noisy dynamical systems. *IEEE Transactions on Control of Network Systems*, 4(1):82–92, 2017.

[78] Youngseok Park, Yunmok Son, Hocheol Shin, Dohyun Kim, and Yongdae Kim. This ain't your dose: Sensor spoofing attack on medical infusion pump. In *10th USENIX Workshop on Offensive Technologies (WOOT 16)*, Austin, TX, August 2016. USENIX Association. URL https://www.usenix.org/conference/woot16/workshop-program/presentation/park.

[79] C.R. Paul. *Introduction to Electromagnetic Compatibility*. Wiley Series in Microwave and Optical Engineering. Wiley, 2006.

[80] J. Petit, Bas Stottelaar, and M. Feiri. Remote attacks on automated vehicles sensors : Experiments on camera and lidar. Black Hat Europe, 2015.

[81] G. E. Ponchak, Donghoon Chun, Jong-Gwan Yook, and L. P. B. Katehi. The use of metal filled via holes for improving isolation in ltcc rf and wireless multichip packages. *IEEE Transactions on Advanced Packaging*, 23(1):88–99, 2000.

[82] D.M. Pozar. *Microwave Engineering*. Wiley, 1997. ISBN 9780471170969. URL https://books.google.com/books?id=IDxTAAAAMAAJ.

[83] F. Rachidi. A review of field-to-transmission line coupling models with special emphasis to lightning-induced voltages on overhead lines. *IEEE Transactions on Electromagnetic Compatibility*, 54(4):898–911, 2012.

[84] A. S. Rakin, Z. He, and D. Fan. Bit-flip attack: Crushing neural network with progressive bit search. In *2019 IEEE/CVF International Conference on Computer Vision (ICCV)*, pages 1211–1220, 2019. doi: 10.1109/ICCV.2019.00130.

[85] Kaveh Razavi, Ben Gras, Erik Bosman, Bart Preneel, Cristiano Giuffrida, and Herbert Bos. Flip feng shui: Hammering a needle in the software stack. In *25th USENIX Security Symposium (USENIX Security 16)*, pages 1–18, Austin, TX, August 2016. USENIX Association. ISBN 978-1-931971-32-4. URL https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/razavi.

[86] Rodolfo Araneo Salvatore Celozzi and Giampiero Lovat. *Electromagnetic Shielding*, chapter Appendix B : Magnetic Shielding, pages 282–316. Wiley, 2008.

[87] A. P. Sample, D. T. Meyer, and J. R. Smith. Analysis, experimental results, and range adaptation of magnetically coupled resonators for wireless power transfer. *IEEE Transactions on Industrial Electronics*, 58(2):544–554, Feb 2011. ISSN 0278-0046. doi: 10.1109/TIE.2010.2046002.

[88] Asanka Sayakkara, Nhien-An Le-Khac, and Mark Scanlon. A survey of electromagnetic side-channel attacks and discussion on their case-progressing potential for digital forensics. *Digital Investigation*, 29:43–54, Jun 2019. ISSN 1742-2876. doi: 10.1016/j.diin.2019.03.002. URL http://dx.doi.org/10.1016/j.diin.2019.03.002.

[89] Michael L. Schena. An electromagnetic coupling model for side-channel analysis. Master's thesis, Utah State University, 2016. URL https://digitalcommons.usu.edu/etd/5224.

[90] Thomas Schmid, Oussama Sekkat, and Mani B. Srivastava. An experimental study of network performance impact of increased latency in software defined radios. In *Proceedings of the Second ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization*, WinTECH '07, page 59–66, New York, NY, USA, 2007. Association for Computing Machinery. ISBN 9781595937384. doi: 10.1145/1287767.1287779. URL https://doi.org/10.1145/1287767.1287779.

[91] R. B. Schulz. Elf and vlf shielding effectiveness of high-permeability materials. *IEEE Transactions on Electromagnetic Compatibility*, EMC-10(1):95–100, March 1968. ISSN 1558-187X. doi: 10.1109/TEMC.1968.302912.

[92] Jayaprakash Selvaraj. *Intentional Electromagnetic Interference Attack on Sensors and Actuators*. PhD thesis, Iowa State University, 2018.

[93] Jayaprakash Selvaraj, Gokcen Yilmaz Dayanıklı, Neelam Prabhu Gaunkar, David Ware, Ryan M. Gerdes, and Mani Mina. Electromagnetic induction attacks against embedded systems. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, ASIACCS '18, pages 499–510, New York, NY, USA, 2018. ACM. ISBN 978-1-4503-5576-6. doi: 10.1145/3196494.3196556. URL http://doi.acm.org/10.1145/3196494.3196556.

[94] Hocheol Shin, Dohyun Kim, Yujin Kwon, and Yongdae Kim. Illusion and dazzle: Adversarial optical channel exploits against lidars for automotive applications. In *Cryptographic Hardware and Embedded Systems – CHES 2017*, volume 10529 of *Lecture Notes*

in Computer Science, pages 445–467. Springer, 2017. doi: 10.1007/978-3-319-66787-4_22.

[95] Y. Shoukry, P. Martin, P. Tabuada, and M. Srivastava. Non-invasive spoofing attacks for anti-lock braking systems. In G. Bertoni and J.-S. Coron, editors, *Cryptographic Hardware and Embedded Systems*, volume 8086 of *Lecture Notes in Computer Science*, pages 55–72. 2013.

[96] V Shurenkov and V Pershenkov. Electromagnetic pulse effects and damage mechanism on the semiconductor electronics. *Facta universitatis - series: Electronics and Energetics*, 29(4):621–629, 2016. doi: 10.2298/fuee1604621s.

[97] D. Sievenpiper, Lijun Zhang, R. F. J. Broas, N. G. Alexopolous, and E. Yablonovitch. High-impedance electromagnetic surfaces with a forbidden frequency band. *IEEE Transactions on Microwave Theory and Techniques*, 47(11):2059–2074, Nov 1999. ISSN 0018-9480. doi: 10.1109/22.798001.

[98] Douglas C. Smith. Using current probes to measure cable resonance. http://emcesd.com/tt2008/tt010108.htm. Accessed: 2019-11-28.

[99] G. Smith. Radiation efficiency of electrically small multiturn loop antennas. *IEEE Transactions on Antennas and Propagation*, 20(5):656–657, 1972. doi: 10.1109/TAP.1972.1140293.

[100] Y. Son, H. Shin, D. Kim, Y. Park, J. Noh, K. Choi, J. Choi, and Y. Kim. Rocking drones with intentional sound noise on gyroscopic sensors. In *24th USENIX Security Symposium (USENIX Security 15)*, pages 881–896, Washington, D.C., August 2015. USENIX Association. ISBN 978-1-939133-11-3. URL https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/son.

[101] Hucheng Sun, Yong-xin Guo, Miao He, and Zheng Zhong. A dual-band rectenna using broadband yagi antenna array for ambient rf power harvesting. *IEEE Antennas and Wireless Propagation Letters*, 12:918–921, 2013. doi: 10.1109/LAWP.2013.2272873.

[102] A. Suntives, A. Khajooeizadeh, and R. Abhari. Using via fences for crosstalk reduction in pcb circuits. In *2006 IEEE International Symposium on Electromagnetic Compatibility, 2006. EMC 2006.*, volume 1, pages 34–37, 2006.

[103] C. Taylor, R. Satterwhite, and C. Harrison. The response of a terminated two-wire transmission line excited by a nonuniform electromagnetic field. *IEEE Transactions on Antennas and Propagation*, 13(6):987–989, 1965.

[104] F.E. Terman and McGraw-Hill Companies. *Radio Engineer's Handbook*. McGraw-Hill handbooks. McGraw-Hill Book Company, Incorporated, 1943. URL https://books.google.com/books?id=b7Q8AAAAIAAJ.

[105] F. M. Tesche. Development and use of the blt equation in the time domain as applied to a coaxial cable. *IEEE Transactions on Electromagnetic Compatibility*, 49(1):3–11, 2007.

[106] Texas Instruments. TM4C123GH6PM Microcontroller, 2014. Datasheet.

[107] *TMP116 High-Accuracy, Low-Power, Digital Temperature Sensor With SMBus and I2C Compatible Interface*. Texas Instruments, 2017.

[108] *TMP144 Low-Power, Digital Temperature Sensor With SMAART Wire-UART Interface*. Texas Instruments, 2018.

[109] T. Trippel, O. Weisse, W. Xu, P. Honeyman, and K. Fu. Walnut: Waging doubt on the integrity of mems accelerometers with acoustic injection attacks. In *2017 IEEE*

European Symposium on Security and Privacy (EuroS P), pages 3–18, 2017. doi: 10.1109/EuroSP.2017.42.

[110] Yazhou Tu, Zhiqiang Lin, Insup Lee, and Xiali Hei. Injected and delivered: Fabricating implicit control over actuation systems by spoofing inertial sensors. In *27th USENIX Security Symposium (USENIX Security 18)*, pages 1545–1562, Baltimore, MD, August 2018. USENIX Association. ISBN 978-1-939133-04-5. URL https://www.usenix.org/conference/usenixsecurity18/presentation/tu.

[111] Yazhou Tu, Sara Rampazzi, Bin Hao, Angel Rodriguez, Kevin Fu, and Xiali Hei. Trick or heat?: Manipulating critical temperature-based control systems using rectification attacks. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, CCS '19, pages 2301–2315, New York, NY, USA, 2019. ACM. ISBN 978-1-4503-6747-9. doi: 10.1145/3319535.3354195. URL http://doi.acm.org/10.1145/3319535.3354195.

[112] Wim van Eck. Electromagnetic radiation from video display units: An eavesdropping risk? *Computers & Security*, 4(4):269 – 286, 1985. ISSN 0167-4048. doi: https://doi.org/10.1016/0167-4048(85)90046-X. URL http://www.sciencedirect.com/science/article/pii/016740488590046X.

[113] David Voltmer. *Fundamentals of Electromagnetics*, volume 2. 2007. ISBN 9781598291704. doi: 10.2200/S00077ED1V01Y200612CEM014. URL http://www.morganclaypool.com/doi/abs/10.2200/S00077ED1V01Y200612CEM014.

[114] C. Wang, Y. Chen, G. Zhang, and Z. Zhou. Design of printed-circuit board rogowski coil for highly accurate current measurement. In *2007 International Conference on Mechatronics and Automation*, pages 3801–3806, 2007.

[115] D.A. Weston. *Electromagnetic Compatibility: Methods, Analysis, Circuits, and Measurements, Second Edition*. Taylor & Francis, 2017. ISBN 9781482299502. URL https://books.google.com/books?id=BmCloAEACAAJ.

[116] Wiremasters. Dielectric constants. https://www.omnicable.com/technical-resources/dielectric-constants-of-insulations. Accessed: 2021-05-12.

[117] Kenneth Wyatt. Measuring resonance in cables. https://www.edn.com/measuring-resonance-in-cables/. Accessed: 2021-05-12.

[118] Fuqin Xiong. *Digital Modulation Techniques, Second Edition (Artech House Telecommunications Library)*. Artech House, Inc., USA, 2006. ISBN 1580538630.

[119] Y. Xue, J. Lu, Z. Wang, L. M. Tolbert, B. J. Blalock, and F. Wang. A compact planar rogowski coil current sensor for active current balancing of parallel-connected silicon carbide mosfets. In *2014 IEEE Energy Conversion Congress and Exposition (ECCE)*, pages 4685–4690, 2014.

[120] C. Yan. Can you trust autonomous vehicles : Contactless attacks against sensors of self-driving vehicle. 2016.

[121] C. Yan, H. Shin, C. Bolton, W. Xu, Y. Kim, and K. Fu. Sok: A minimalist approach to formalizing analog sensor security. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 233–248, 2020. doi: 10.1109/SP40000.2020.00026.

[122] D. B. Yelaverthi, R. Hatch, M. Mansour, H. Wang, and R. Zane. 3-level asymmetric full-bridge soft-switched pwm converter for 3-phase unfolding based battery charger topology. In *2019 IEEE Energy Conversion Congress and Exposition (ECCE)*, pages 2737–2743, Sep. 2019.

[123] Qin Yu, Thomas W. Holmes, and Krishna Naishadham. RF equivalent circuit modeling of ferrite-core inductors and characterization of core materials. *IEEE Transactions on Electromagnetic Compatibility*, 44(1):258–262, 2002. ISSN 00189375. doi: 10.1109/15.990733.

[124] Y. Zeng, Z. N. Chen, X. Qing, and J. Jin. An artificial magnetic conductor backed electrically large zero-phase-shift line grid-loop near-field antenna. *IEEE Transactions on Antennas and Propagation*, 65(4):1599–1606, April 2017. ISSN 0018-926X. doi: 10.1109/TAP.2017.2670323.