Physical-Layer Attacks Against Pulse Width Modulation-Controlled Actuators

Gökçen Yılmaz Dayanıklı
Qualcomm

Sourav Sinha
Virginia Tech

Devaprakash Muniraj
IIT Madras

Ryan M. Gerdes
Virginia Tech

Mazen Farhood
Virginia Tech

Mani Mina
Iowa State University

Abstract

Cyber-physical systems (CPS) consist of integrated computational and physical components. The dynamics of physical components (e.g., a robot arm) are controlled by actuators via actuation signals. In this work, we analyze the extent to which intentional electromagnetic interference (IEMI) allows an attacker to alter the actuation signal to jam or control a class of widely used actuators: those that use pulse width modulation (PWM) to encode actuation data (e.g., rotation angle or speed). A theory of False Actuation Injection (FAI) is developed and experimentally validated with IEMI waveforms of certain frequencies and modulations.

Specifically, three attack waveforms, denoted as *Block*, *Block & Rotate*, and *Full Control*, are described that can be utilized by an attacker to block (denial of service) or alter the actuation data encoded in the PWM signal sent by an actuator's legitimate controller. The efficacy of the attack waveforms is evaluated against several PWM-controlled actuators, and it is observed that an attacker can implement denial-of-service attacks on all the tested actuators with *Block* waveform. Additionally, attackers can take control of servo motors from specific manufacturers (Futaba and HiTec) with reported *Block & Rotate*, and *Full Control* waveforms. A coupling model between the attack apparatus and victim PWM-based control system is presented to show that the attacker can utilize magnetic, resonant coupling to mount attacks at an appreciable distance. 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 said UAV, e.g., change in the flight trajectory. Additionally, the denial of service attacks are demonstrated on other actuators such as DC motors, the rotational speed of which is controlled with PWM, and possible countermeasures (such as optical actuation data transmission) are discussed.

This work was supported by the National Science Foundation (NSF) under Grant No. CNS-1801611.

1 Introduction

A cyber-physical system (CPS) is a complex combination of computation, communication, and control elements. A generic CPS includes actuators, sensors, and a controller as illustrated in Figure 1. The sensors convert a system variable (e.g., acceleration) to electric (digital or analog) signals and send them to the controller. The controller processes the sensor data and makes a decision for how to influence the future state of the system and sends actuation signals to actuators (e.g., a servo motor) which perturbs the CPS state.

The attackers can utilize EM waves to obstruct or manipulate the actuation data, sensor data, or communication signal which are illustrated as Point 1, 2, and 3 in Figure 1, respectively [1]. Our interest in this work is the FAI attacks in which the attacker aims to obstruct or manipulate the actuation control with IEMI. Pulse width modulation (PWM) signals, to which the actuation data (such as speed or rotation angle of a motor) is encoded, are commonly used for actuation control. The integrity of PWM signals is thus very important because any blockage or alteration of the actuation data results in the loss of control of the physical components. For instance, during an attack on a fixed-wing UAV, if the attacker prevents the actuation of the control surfaces (e.g., ailerons), the victim UAV can easily crash. Even with specific actuators, an attacker can take control of the control surfaces (e.g., ailerons) to force the UAV to follow an unsafe trajectory. This paper is concerned with how such an effect may be obtained by an attacker at a distance and without breaking traditional digital protections, e.g., encrypted communication between controller and actuator.

1.1 Related Work

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 [2]. An attacker can exploit this phenomenon by using specific waveforms to affect the circuitry conveying PWM signals (e.g., traces on printed circuit boards or cables) to manipulate the operation of a tar-

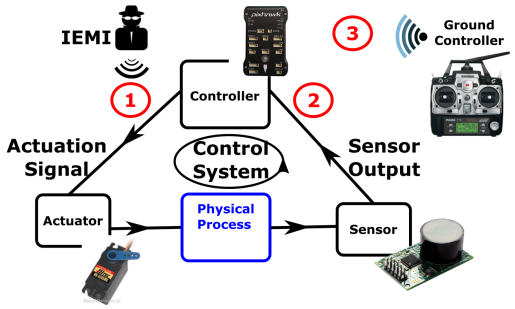


Figure 1: An IEMI attack can target a variety of attack points in a cyber-physical system: Actuation Signal (1), sensor output (2), and radio control signal (3) can be manipulated or blocked (i.e., jammed) by IEMI.

geted actuator by changing the voltage representing the PWM signal. In certain conditions (e.g., when the attacker exploits the victim resonance), the induced voltage is large enough to block or manipulate the actuation data (Point 1 Figure 1).

Unlike FAI attacks (Point 1 in Figure 1), sensor data manipulation (Point 2 in Figure 1) with IEMI has been well-documented in the literature. Kune et al. reported IEMI attacks to inject false data into microphones and implantable cardiac devices [3]. An IEMI attack on magnetic speed sensors of an anti-lock braking system was reported in [4]. Kasmi and Esteves show false voice commands to mobile phones can be injected through headphone cables with IEMI [5]. It is shown that a few-100 mVs of induced voltage [6] is more than sufficient to manipulate analog sensor data through ADC-clipping effect [6, 7] and device-nonlinearities [3, 8]. The reader is referred to [9, 10] for a systematic description of mechanisms such as 'ADC clipping and 'device nonlinearity' exploited in sensor data manipulation. However, as the amplifiers or ADCs are not used in the actuation system, the attacker can't exploit these mechanisms. To manipulate the actuation data (FAI), the attacker needs to induce a voltage comparable to the amplitude of the victim PWM, (e.g., 5 V for a UAV [11]) and spoof the victim controller, the mechanism of which is explained in Section 2.

Although sensor data manipulation is applicable with less power, it poses a less significant threat for the victim system because the robust state estimators can detect, filter, and correct the false sensor data injected by the attacker [12]. Nevertheless, the state estimators are not effective against FAI, because even the robust state estimator detects a faulty state due to the induced false actuation data and sends a 'recovery' actuation signal, the attacker overrides this 'recovery' signal, as the attack point is between the state estimator (in the controller) and actuator (Figure 1). The ability of FAI attacks to override the state estimator control makes them a severe threat for secure CPS operation. A low–frequency (50 Hz) sawtooth waveform that generates an 'artificial' voltage drop to depreciate the actuation data is demonstrated in [6]; however, the attack with low–frequency waveform has some limitations: first, the attacker radiator (toroid) should be placed around the victim PWM cables (i.e., attack distance is limited to a few cms.); second, the induced servo rotation is limited to one direction because the attacker can only decrease the PWM width; third, the attacker is assumed to be synchronized to the victim PWM signal which requires a receiver system to analyze the victim EM leakage. In this work, high–frequency (e.g., VHF–band) amplitude modulated attack waveforms are reported that increase the attack distance to multiple meters, force the servo rotation to both directions, and do not require synchronization or a receiver system to eavesdrop on the victim EM leakage.

Another class of attacks that utilize EM interference is 'communication jamming' that targets the communication link between the ground/radio controller and the system (Point 3 in Figure 1) [13]. Attacks are shown with malicious Wi-Fi signals to take control of the commercial drones [14, 15]. Unlike FAI, the 'communication jamming' is not effective if the victim device is in autonomous mode. Additionally, controllers with robust state estimators can mitigate communication jamming similar to sensor manipulation attacks unlike the attacks on actuation signal [12].

1.2 Contributions

To the best of the authors' knowledge, this is the first study solely focused on the threat IEMI poses to PWM–controlled actuators. Our 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 (Futaba and HiTec). Additionally, the efficacy of attacks is tested on other PWM-based actuators such as DC motors, the speed of which is controlled by the PWM.
- An electromagnetic coupling 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 model, the (resonant) frequency at which power from the attack setup can be delivered with the greatest efficiency can be found, thereby lowering the overall cost of attack. Two methods, an analytical and an experimental, are reported to estimate and determine the victim resonant frequency.
- The FAI attacks are demonstrated on a fixed-wing UAV during flights. For demonstration, an attacker system that consists of an RF module and an antenna is designed and mounted on the victim UAV. The *Block* and *Full Control* attacks are implemented during flights and the effect of the

attacks to the trajectory of the UAV is reported with the flight data (e.g., aileron rotation, roll angle, and trajectory).

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

A Zero Phase Shift Line (ZPSL) antenna with a uniform field distribution is designed and produced for the attack demonstrations, which is believed to be useful to other researchers investigating IEMI attacks (Appendix B).

2 Adversarial Control of Actuators

PWM signals control actuators through the information encoded in the signal, e.g., rotation angle or speed. An attacker aims to prevent successful transmission of, or change, this information to manipulate actuator movement.

Actuator Control with PWM: A PWM signal is a rectangular waveform with a fixed period, t_{PWM}, of 20 ms as illustrated in Figure 2a. The time duration, t_{high}, varies between 1 ms and 2 ms and carries the actuation information which is the actuation data like rotation angle or speed. In this section, the PWM operation is explained for a servo motor application for 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 for 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, $t_{high} = 1$ ms, 1.5 ms, and 2 ms corresponds to the rotation angles $-45°$, 0°, and 45° respectively, as illustrated in Figure 2b, 2c and 2d. There are two options for an actuator to process the actuation data encoded to a PWM signal. First, by checking the rising and falling edges the PWM pulse; second, take the average of the PWM possibly with a low pass filter. It is experimentally observed that the actuators are non-responsive to low-amplitude DC signals applied to PWM input, which shows that the duration between rising and falling edges of the PWM is used to determine the actuation data.

2.1 Threat Model

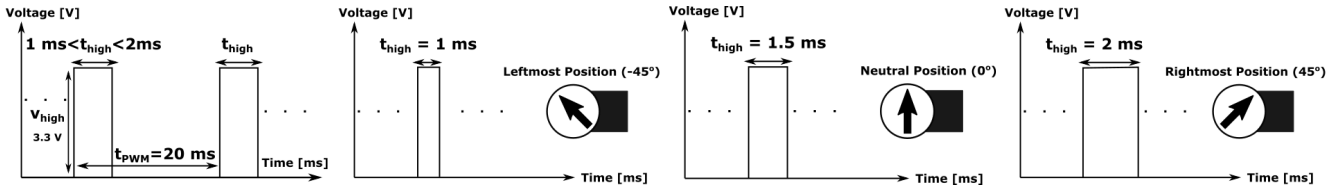
The threat model assumes an attacker aims to block or take over the control of PWM-based actuators with EMI. For an EM coupling discussion specific to attack scenario based on Faraday's law of induction [16], the reader is referred to Section 3. Throughout the attacks, there is no physical contact between 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 [17], 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.

2.2 Previously Reported Attack Waveforms

A 50 Hz sawtooth waveform that generates an 'artificial' voltage drop on a PWM signal to depreciate the actuation data is reported in [6]. Although the low-frequency waveform is capable of rotating servo counterclockwise, the attack has certain limitations, which we addressed with high-frequency attack waveforms with amplitude modulation. Firstly, the 50 Hz sawtooth waveform is effective from a few cm*s* and the attacker needs to wrap the PWM coils of the victim around the attacker toroid because the induced voltage is proportional to the time derivative of the attacker current, i.e., attack frequency ($dsin(\omega t)/dt = \omega cos(\omega t)$) [6, 18]. The reader is referred to Appendix A for a detailed discussion about the induced voltage and attacker frequency relationship. A relatively low-frequency (10 MHz) *Pulsed Sinusoid* is suggested in [19] to increase the t_{high} and rotate the servo to clockwise direction. However, each of these waveforms assume the attacker can synchronize the attack signal with the victim's PWM signal (i.e., the exact timing of victim PWM pulses), which requires an additional receiver (e.g., an antenna, low-noise amplifier (LNA), and a signal processing unit). Adding to that, as the previously discussed attacks do not exploit any special coupling mechanism, the attacks are limited to a short distance, i.e., the attacker radiator should be placed around the victim cables [6, 19]. In the following sections, three attack waveforms, namely *Block*, *Block & Rotate*, and *Full Control*, will be reported to address the distance and the synchronization limitations.

2.3 Wired Experimental Setup

A wired setup (Figure 3), 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 necessary for a wireless setup. The victim side is a UAV system with a Futaba Ground Radio Controller that relays the control from the operator to a UAV Autopilot (e.g., Pixhawk) which converts the control information to a PWM signal and sends it to the servo motor. A voltage buffer is used to eliminate loading that might distort the waveform of the PWM. 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 generation.



(a) (b) (c) (d)

Figure 2: PWM and servo motor control (a) Legitimate PWM signal (b) $t_{high} = 1$ ms, servo motor rotates to leftmost position. (c) $t_{high} = 1.5$ ms, servo motor rotates to center position. (d) $t_{high} = 2$ ms, servo motor rotates to rightmost position.

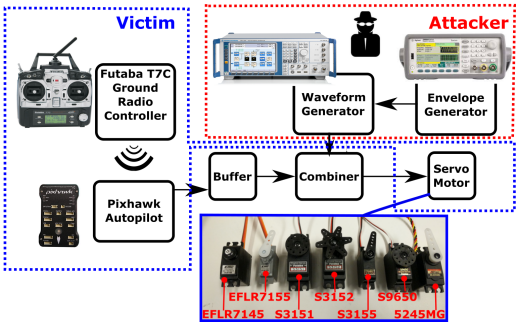


Figure 3: The reported attack waveforms are tested in a wired experimental setup on different servo models.

2.4 Attack Waveform I: Block

A *Block* attack is a continuous wave signal at the frequency f_a (Figure 4a), which induces a voltage in the victim PWM circuitry, 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 frequencies to increase attack distance. Analytical and experimental approaches are discussed in Section 3 to detect the victim resonance.

Wired Setup Results for Block: A *Block* waveform with a peak value (V_p) and frequency (f_a) (Figure 4a) is applied to the servo models in the wired setup (Figure 3). 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 fixed-wing UAV on which the attacks will be demonstrated.

1. Establish servo control through ground radio controller.
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 red boxes (Table 1) display the successful attacks (i.e., the control of servo motor is 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 of the instant the attack is initiated. 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 1.

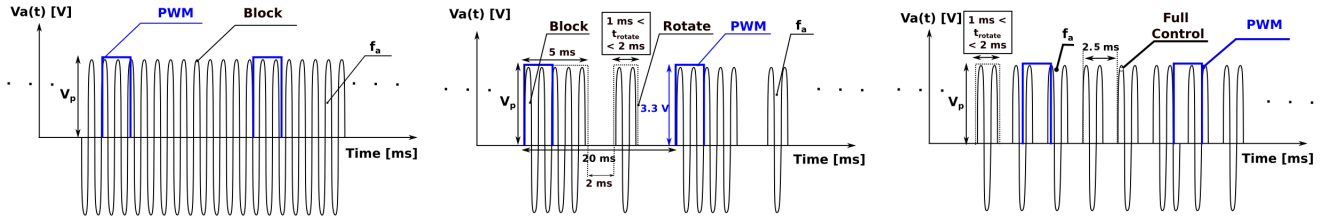
2.5 Attack Waveform II: Block & Rotate

The *Block* waveform blocks the transmission of the rotation angle data to the actuators; however, an advanced waveform, with which the attacker to masks/erases the original rotation data encoded in t_{high} and injects false actuation data, is needed to control an actuator. An attacker can use a wide pulse ($t_{high} > 2$ ms) to override the original angle data.

To observe how a servo responds to a wide pulse ('Block' pulse in Figure 4b) on top of the original pulse, each servo is rotated to the neutral position (Figure 2c) and then a PWM signal with an out of range t_{high} is applied and the servo rotation is observed. During all 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. 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 might be a precaution to keep the servo rotation stable under conditions when rotation angle data is not available in the PWM channel. This observation also shows a weakness of servo motor control with PWM. An attacker can inject a wide 'Block' pulse on top of t_{high} and block the original actuation

Table 1: Block Attack is successful on all servo models (red 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)



(a) (b) (c)

Figure 4: 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}.

data. However, an additional sinusoidal pulse should be used to inject the false rotation angle information ('Rotate' pulse in Figure 4b). The duration of the rotate pulse (t_{rotate}) determines the false rotation angle injected into the victim system. For instance, the attacker can use a *Block & Rotate* waveform with $t_{rotate} = 1$ ms (Figure 4b) to rotate the servo to -45°.

Wired Setup Results for Block & Rotate: The test procedure in Section 2.4 is followed with the wired setup (Figure 3). The *Block & Rotate* waveform is synchronized to the original PWM with an oscilloscope. The grey boxes in Table 2 shows the successful attacks in which the attacker can control the rotation with t_{rotate} (Figure 4b). The Eflite models respond to *Block and Rotate* by locking to a rotation angle depending on the servo model and f_a. However, it is observed t_{rotate} cannot determine the victim rotation. The authors think that the microcontroller of Eflite models is saturated due to *Block & Rotate* and can not detect the rising and falling edges of the 'Rotate' pulse which the false rotation angle information.

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 successful attacks. The HiTec model can be controlled by applying an attack waveform with $V_a = 3$ V and $f_a = 8.75$ MHz; however, at higher frequencies, the attacks were not successful within the setups' power level. All of the Futaba models can be controlled by *Block & Rotate* at $f_a = 70$ MHz and $f_a = 140$ MHz and attacks at $f_a = 70$ 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 requires the attacker to synchronize or align the 'Block' pulse to the victim PWM. Despite being theoretically possible with the detection of magnetic fields emanated from rising and falling edges of the victim PWM, practically synchronization is difficult. Firstly, multiple PWM signals controlling the servo motors emanate a combination of fields, and picking the desired fields requires a sensitive receiver system. Additionally, even though a sensitive receiver is employed, the magnetic field measurements will be highly dependent on the antenna orientation and PWM cable position. Although *Block & Rotate* applies to stable systems like production lines or solar tracking systems with PWM-controlled actuators, it is hard to implement synchronization on a mobile system like a UAV.

Table 2: *Block & Rotate* is successful on Futaba and HiTec models (red 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°)

2.6 Attack Waveform III: Full Control

In an actuation control application, PWM has a fixed duty cycle in between $\%5 < \frac{t_{high}}{t_{PWM}} < \%10$ (Figure 2a, $t_{PWM} = 20$ 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}), so the question arises: *What happens when an attacker applies a PWM with a larger duty cycle?*

As the t_{high} range is fixed for actuation control, the attacker can only modify the t_{PWM} to alter the duty cycle. t_{PWM} is decreased to 2.5 ms and the servo operation is observed by varying the t_{high} in between 1 ms and 2 ms and it is observed that each servo model can be controlled with the increased duty cycle PWM. Note that the t_{PWM} value is chosen slightly larger than the maximum t_{high} value to maximize the duty cycle without losing the rising/falling edges. This observation is the basis for *Full Control* waveform which consists of frequent sinusoidal pulses with period 2.5 ms and varying t_{rotate} (Figure 4c). 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* does not need synchronization to the victim PWM unlike the *Block & Rotate*. Adding to that, the high duty cycle *Full Control*, with frequent rising and falling edges, masks the original PWM signal and takes control of the victim actuator.

Wired Setup Results for Full Control: Table 3 shows the effect of *Full Control* attack on servo models for varying

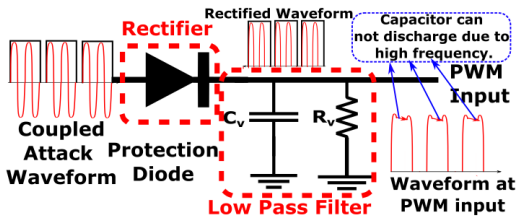


Figure 5: The protection diode rectifies the attack waveform. The victim capacitance (C_v) is charged up to the peak but not able to discharge which results in the appearance the attack waveform envelope at the PWM input.

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 4c) 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 3.3.

2.7 Attack Mechanism

Diode-based protection circuits are simple and cost-effective in protecting the ports of controllers from excessive voltage, electrostatic discharge, and reverse currents [20, 21]. However, the diodes combined with the inherent capacitance and resistance of the victim circuitry can behave as an 'envelope detector' [22] which enables the use of amplitude-modulated attack waveforms such as *Full Control* and *Block & Rotate*. In Figure 5, a reverse-current protection diode is shown to illustrate the attack mechanism. The R_v and C_v in Figure 5 models the terminal impedance, the by-pass capacitors and input capacitance of the victim input. The attack waveform coupled through the PWM cables is rectified by the diode, which leaves only the positive cycles. With the first rectified cycle, the capacitor is charged up to the voltage peak; however, the capacitor can not discharge between the cycles due to the high frequency/low period nature of the attack waveform and relatively high time constant of the parallel $R-C$ circuit [23]. Additionally, the overall circuitry including the diode and R_v, C_v is nothing but an envelope detector widely used as an AM demodulator in the early radios [22, 24]. For the success of the attacks, the rectification of the diode is the key, because the rectification introduces the low-frequency component of the attacker, i.e., the envelope. We observed that Futaba and HiTec servo controller boards consist of diode protection which is the reason for the successful control of these servos.

Table 3: Full Control is successful on Futaba models (red 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)

2.8 Comparison of Attack Waveforms

A comparison of attack waveforms is given in Table 4. *Block* waveform is prevents the transmission of actuation data transmission at each tested frequency and observed to be effective on all tested servo models. The previously reported *Sawtooth* [6] and *Pulsed Sinusoid* [19] waveforms can rotate the Futaba servo to one direction, but limited in terms of the attack distance, rotation direction and require synchronization which necessitates a sensitive receiver (an LNA, filter matched filter, and possibly a signal processing unit) to detect the EM leakage of the victim PWM. *Block & Rotate* and *Full Control* enable the attacker to fully control specific servo models by injecting rotation angle data to the PWM channel. *Block & Rotate* is applicable to tested Futaba and HiTec servos models (Table 2 and 3). As a side note, *Full Control* exploits the low duty–cycle nature of the original PWM and injects the false actuation data very frequently to take control of the victim actuator without a need for synchronization. *Full Control* applies to all Futaba models and gives the attacker the 'full control' of the servo rotation i.e., clockwise and counter-clockwise rotation.

3 Enabling Attacks at Distance

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 [25]. 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 [26]. To mitigate this threat, a tracker/defender UAV with the attack system onboard can be deployed to intercept the intruder UAV and launch FAI attacks against the intruder to safely drive it towards the capture region or outside the geofence that defines the boundary of the restricted airspace. However, for a successful attack, the tracker is required to be in close proximity to the intruder for

a certain period of time. Reliable and consistent detection of the intruder UAV can enable the tracker to pursue the intruder UAV and gain sufficient proximity to it. This problem has received significant attention over the years; see [27] for a review. In restricted airspaces, the tracker can rely on onboard detection sensors in coordination with ground-based sensors such as radars, acoustic sensors, vision sensors, etc., for accurate detection of the intruder. Many techniques have also been proposed to pursue and intercept unauthorized UAVs for the deployment of countermeasures in [28–30]. For these strategies to work, the defenders' capabilities are considered to be superior to those of the intruder. This assumption is not limiting, as tracker UAVs of different sizes and classes can be equipped with the attack mechanism, and the intruder UAV can be identified and classified using ground-based sensors before an appropriate tracker UAV is directed to intercept it. A challenge may arise when the intruder becomes aware of the tracker and tries to evade it. In these scenarios, strategies based on pursuit-evasion games [31] can be developed to intercept the evaders. Note that, even when continuously maintaining close proximity to the intruder is not possible, the tracker can still compromise the trajectory of the intruder UAV by launching intermittent attacks. In this work, we do not consider the detection and tracking problem and focus only on devising the FAI attacks. Without loss of generality, the 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 [2] to induce a voltage in the victim PWM circuitry; however, as observed in the wired setup (Table 1, 2, and 3), 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 mV*s* of induced voltage can result in significant changes in the sensor readings [6], so the attacker needs to utilize an additional coupling mechanism to induce more voltage. In the following section, the mutual coupling between the attacker and the victim is determined analytically to find an optimal attack frequency that ensures the maximum induced voltage.

Table 4: Comparison of Attack Waveforms

	Block	Sawtooth [6]	Pulsed Sinusoid [19]	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	✓	✓	✓	✓	✓

3.1 Electromagnetic Coupling Model

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: The far-field of an antenna lies in the region $R > \frac{2D^2}{\lambda}$ where D is the maximum dimension of the antenna and λ is the wavelength of the signal [32, 33]. The far field EM waves are plane waves and the electric and magnetic fields can be shielded with metal surfaces (e.g., aluminum foil) easily due to the coupled nature of electric and magnetic fields.

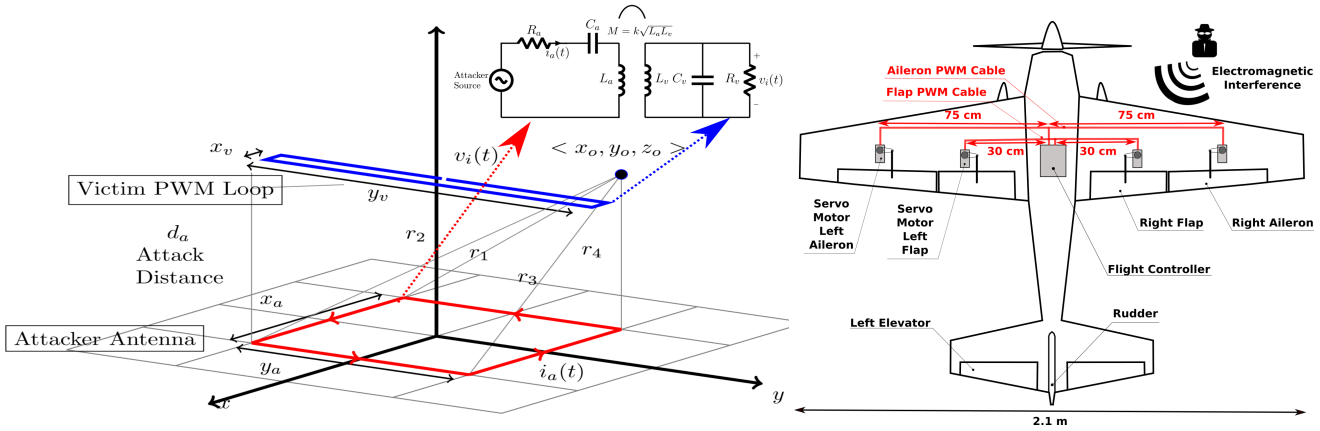
Near Field Region: The near field region lies in the vicinity of the antenna (e.g., $R < \frac{\lambda}{2\pi}$ for an electrically small dipole [34]) where magnetic and electric fields have a complex relationship unlike the plane waves in the far field. Depending on the antenna type, capacitive or inductive energy may be dominant (e.g., inductive 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 can easily be attenuated and reflected by the metals. However, low–frequency magnetic near fields generated by loop antennas are known to penetrate much more easily to the system because of their decoupled nature from the electric fields [35]. Adding to that, magnetic resonant coupling (i.e., coupling through magnetic fields in the near field between resonant components) is an efficient way of transferring power over medium distances even in weakly coupled scenarios (i.e., Wireless Power Transfer) [36]. The magnetic near field region of an inductive antenna is an efficient way of inducing high voltages in the PWM circuitry.

For the derivation of the coupling ratio between the attacker antenna and the victim loop, the model illustrated in Figure 6a 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 may not align during attacks. The reported scenario, in which the surface normals of the antenna and victim circuitry are parallel, provides maximum coupling and induced voltage to the victim.

The coupling ratio, k, is the ratio of the flux captured by the victim 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. The detailed derivation for the coupling coefficient, k, can be found in Appendix A.

$$k = \frac{\psi_v}{\psi_a} = \frac{\iint_{S_v} \mathbf{B} \cdot d\mathbf{S}}{\iint_{S_a} \mathbf{B} \cdot d\mathbf{S}} \tag{1}$$

The UAV flap and aileron PWM cable lengths are 60 cm and



(a) (b)

Figure 6: 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.

Table 5: Coupling coefficients (k) for aileron and flap loops: $x_a = 35\,\text{cm}$, $y_a = 35\,\text{cm}$, $d_a = 1\,\text{m}$, $i(t) = 1\,\text{A}$ at 61 MHz

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

150 cm as shown in Figure 6b. The coupling ratio (k) between antenna and PWM cables is found with (1) and (8). The attacker antenna size ($x_a = 35\,\text{cm}$, $y_a = 35\,\text{cm}$) and the attack distance ($d_a = 1\,\text{m}$) are fixed. The analytically found coupling ratios for cables are very small and on the level of 10^{-4} (Table 5), which means the attacker and victim is weakly coupled and an additional approach is required to induce multiple *Volts* reported in Table 1, 2 and 3.

3.2 Circuit Model for the Attack

Kurs *et al.* showed that magnetic resonant coupling (MRC) can be utilized efficiently to transfer power wirelessly with distances up to eight times of the coil radius even in weakly coupled scenarios [36]. 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 highly–efficient Wireless Power Transfer (WPT) applications, up to 75.7% for weakly coupled scenarios [37], possible [38]. A magnetic resonant coupled series to parallel circuit model is provided in Figure 6a for the attack scenario, in which L_v, C_v, and R_v are the inductance, capacitance, and resistance of the victim circuitry, e..g., PWM cables. L_v and C_v are determined by the length of the cables and parasitic capacitances, respectively. R_v is the resistance of victim circuitry that includes copper loss and the load termination. The resonant frequencies of the victim loop (f_v) and attacker antenna (f_a) are:

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

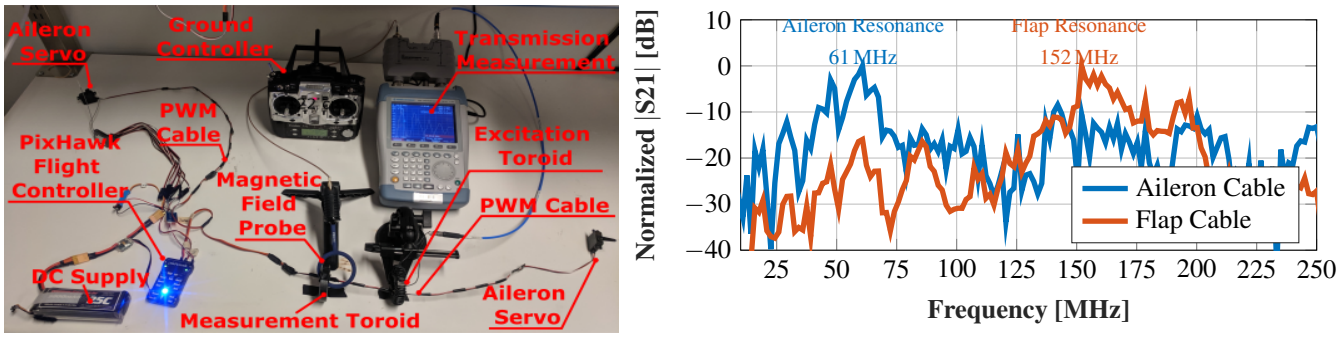
According to the threat model, the attacker can not physically modify the victim system and alter the victim resonance (f_v); however, a resonant attacker antenna can be adopted that has the same resonant frequency with the victim ($f_a = f_v$). Especially for Tesla coils, magnetic resonant coupled circuits have been investigated through Kirchoff's circuit law [39], 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.

$$f_{s+} = \frac{f_v}{\sqrt{1-k}} \quad , \quad f_{s-} = \frac{f_v}{\sqrt{1+k}} \tag{3}$$

where the optimum attack condition is $f_s = f_a = f_v$. However, as analytically we found that k is very small ($k << 1$) (Table 5), f_{s+} and f_{s-} in (3) converge. 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.

3.3 Detection of the Victim Resonance

To detect the victim resonant frequency, f_v, the attacker can use an analytical or an experimental approach. While the analytical approach gives an estimation of the victim resonance



(a) (b)

Figure 7: 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.

with limited information about the victim (e.g., cable length), the experimental approach, that requires a measurement on the victim circuitry, presents a more accurate resonant frequency detection.

3.3.1 Analytical Detection of the Resonance

The resonant frequency of a cable is determined by the length, parasitic capacitance, and termination of the victim PWM cable. Depending on the termination, the resonant frequency can be at quarter-wavelength (for short termination) or half-wavelength (for open termination) frequency [41]. As the PWM cables are terminated by the high impedance loads such as controller outputs and servo motor input, an open termination is a proper representation that corresponds to a resonant frequency at the half-wavelength frequency for PWM cables. f_v can be found as follows:

$$f_v = A\frac{c}{(2*L_{PWM})} = 0.7\frac{c}{(2*L_{PWM})} \quad (4)$$

where L_{PWM} is the length of the cable, c is the speed of light in a vacuum, and A is a constant that compensates for the reduced speed of light due to the cable insulators. The cable insulators (e.g., PVC) have relative dielectric constants between $\varepsilon_r = 2$ and $\varepsilon_r = 3$ [42, 43], which can be introduced with $A = 0.7$ accurately [41, 44]. (4) 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.

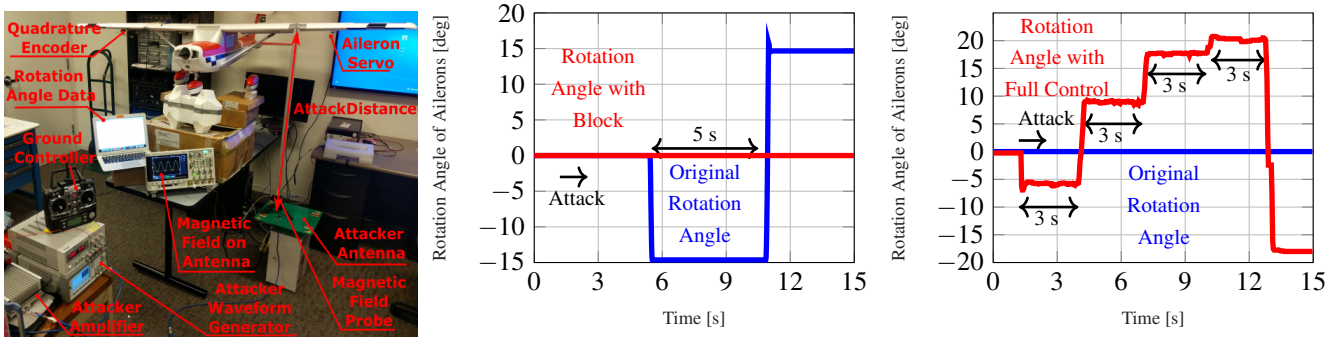
3.3.2 Experimental Detection of the Resonance

Although the analytical approach provides a resonance estimation with limited information about the victim, an experimental approach can be used to measure f_v. Smith reports a method in which a transmission measurement is implemented through current clamps located around the cables under test [41]. The method reported here is similar but employs ferrite toroids and a field probe instead of the current clamps. The experimental setup (Figure 7a) 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 7a. The measurement toroid picks up the field generated in the cable, and the resonance frequency is detected when the maximum transmission occurs.

Figure 7b 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 6). 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 analytical approach estimates a resonance frequency at 70 MHz and 175 MHz for aileron and flap cables, respectively (Table 6).

4 Indoor Attack Demonstrations on a UAV

For indoor attack demonstrations, a Cessna 150 (C150) fixed-wing UAV with a wingspan of 2.1 m is used as an in-



(a) (b) (c)

Figure 8: The *Block* and *Full Control* attacks are demonstrated indoors. The effect of the attacks is measured through quadrature encoders located on the right aileron servo shaft. (a) The experimental setup includes a fixed-wing UAV and 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) *Block* demonstration: The original rotation angle (blue) sent from the ground controller can not control the servo during the attack; The servo is 'blocked' at the neutral position (red). Attack distance is 50 cm. (c) *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 victim tries to keep the ailerons at neutral position (blue). The attack distance is 25 cm.

Table 6: Detected victim PWM cable resonances, f_v.

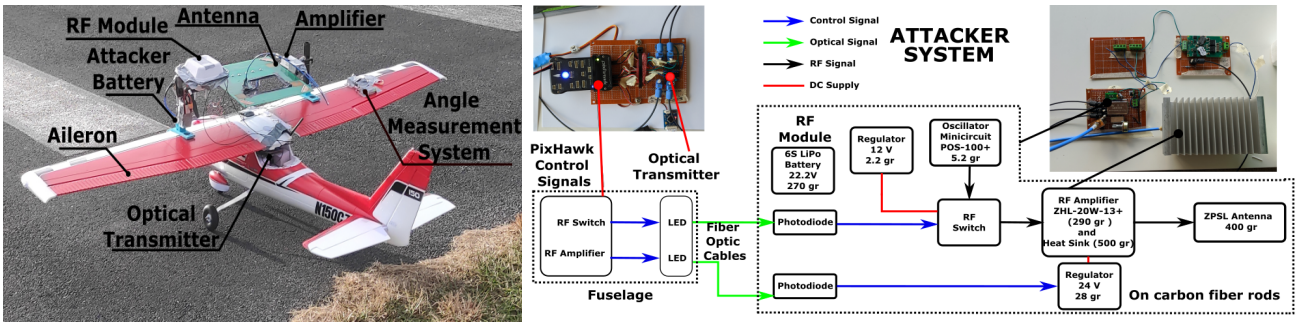
	Aileron PWM Cable (150 cm)	Flap PWM Cable (60 cm)
Experimental	61 MHz	152 MHz
Analytical	70 MHz	175 MHz

truder/victim [45] as shown in Figure 8a. The ailerons of the intruder are selected through the use of resonant frequency for aileron PWM cables 61 MHz measured in the previous section (Table 6). As the left and right aileron cables are electrically connected and carry the same PWM, attacks are effective on both right and left ailerons. The attacker system consists of a waveform generator, a 20 W RF amplifier, and a Zero Phase Shift Line (ZPSL) antenna. The ZPSL antenna resonates at the attack frequency, and details about the design and production of the antenna are presented in Appendix B. The victim UAV (Figure 8a) is fully operational for the *Block* and *Full Control* demonstrations except for the DC motor and propeller for safety reasons. The radio ground controller sends control signals for actuators. The rotation angle of the right aileron is measured with a quadrature encoder [46] located on the shaft of the Futaba S3155. The encoder converts the rotation angle of the servo (and also the aileron) to a quadrature signal and sends it to a TIVA C microcontroller for angle detection. The antenna is located under the left-wing deliberately to eliminate the EMI on angle measurements.

Indoor Block Demonstration: In the wired experiments, it is observed that *Block* prevents the servo control. To observe this, an attack with a duration of 15 s is applied, and during the attack, the victim system attempts to control the servos by sending neutral (0°), left (-15°), and right (15°) rotation command. 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 8b demonstrates the rotation angle of ailerons with (Red) and without (Blue) *Block* attack. While the IEMI attack is not applied, the ailerons follow the commands of the victim system (blue); however, when the *Block* attack is initiated, the ailerons stop following the commands of the victim and stays at the neutral position. When the attack stops, the ground controller retakes the control of the ailerons. 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 (e.g., cable) position.

Indoor Full Control Demonstration: In section 2.6, it is observed that Futaba models can be controlled by varying the pulse duration (t_{rotate}) of the *Full Control* waveform (Figure 4c). To observe this, it is assumed that the intruder/victim system sends a neutral command to keep the ailerons at neutral position (0°) during the attack demonstration. The attacker applies a *Full Control* waveform with an incrementally increasing t_{rotate} to rotate the ailerons clockwise $[1.4\,\text{ms}, 1.6\,\text{ms}, 1.8\,\text{ms}, 2\,\text{ms}]$ at every 3 s. In the end of the sequence, a $t_{rotate} = 1.2\,\text{ms}$ 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 8c, even though the actual PWM signal carries a neutral position command. *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 assume that there is a legitimate PWM in the channel (unlike *Block* attack during which 'erasing' the original PWM in the channel is sufficient.).



(a) (b)

Figure 9: In-flight attacker system and the victim UAV (a) The attacker system including the battery, RF module, amplifier, and the antenna is mounted on the UAV with carbon-fiber rods for in-flight demonstrations. Attack distance is 15 cm. The overall weight is decreased by carving out a section from the antenna. (b) Victim Pixhawk generates the attack control signals which are converted to optical signals and sent through fiber cables to the RF module to ensure the control in high EMI. The CW signal at the victim resonance is modulated with an RF switch and the amplified waveforms are radiated through a ZPSL antenna.

5 In-flight Attack Demonstrations on a UAV

For demonstration purposes, we mount the attacker system on top of the intruder UAV (see Figure 9a) to try to recreate the intruder-tracker interception scenario. The overall platform has a gross take-off weight of 6 kg to which the attacker system contributes 1.4 kg, the setup required to mount the attacker system contributes 320 g, and the angle measurement unit contributes 150 g. C150 is a standard fixed-wing UAV with a propeller and three control surfaces, namely, the elevator, the aileron, and the rudder. The propeller generates the thrust, and the control surfaces are used to maneuver the UAV. The elevator primarily affects the pitching motion/pitch attitude (θ), the aileron affects the rolling motion/roll attitude (ϕ), and the rudder affects the yawing motion/yaw attitude (ψ) (Figure 10a).

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 [47] for details on UAV dynamics and control.

5.1 Attacker System

The attacker system consists of an optical transmitter and receiver, battery, RF module, amplifier, and a ZPSL antenna as shown in Figure 9b. The victim Pixhawk is programmed to initiate the attacks upon request of the ground controller. Attack control signals are sent in as optical signals to ensure the reliable control even under high EMI, e.g., to halt the attack in an emergency. The RF Switch modulates the continuous wave signal to generate *Block* or *Full Control* waveforms. The attack waveform from the RF switch is fed to the RF amplifier with an output power of 20 W and the attack waveform is radiated from the ZPSL antenna which resonates at the attack frequency and matched to 50 Ω.

The victim UAV uses a Pixhawk autopilot running on PX4 firmware which is modified to control the duration and waveform of the IEMI attacks from the ground/radio controller. To robustly measure the aileron rotation in high-EMI, a quadrature encoder is attached to the right aileron servo with an isolated Pixhawk (i.e., with a separate DC supply) mounted on the right-wing of the UAV. A firmware module is developed for the PX4 firmware that acts as an interface for the quadrature encoder and records the aileron rotation angle. For the flights, Pixhawk's stabilized flight mode is utilized during which the pitch and roll setpoint is supplied by the pilot from the radio/ground controller. The autopilot then calculates the required elevator and aileron rotation, respectively, to achieve the setpoint. The rudder rotation and the thrust are commanded directly from the radio/ground controller.

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 1) 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 10d), and UAV tracks the setpoint roll attitude as shown in Figure 10f. 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 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. Af-

ter 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 10b 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: During *Full Control* demonstration, the pilot sends a zero roll setpoint. As the attack starts ($t = 0$), the aileron rotates to the false value of -36° ($t_{rotate} = 1.8$ ms) injected by the attacker system (Figure 10e) resulting in a negative rolling motion. The autopilot commands a positive aileron rotation to recover the orientation of the UAV, but the aileron does not respond as it is under attack. The attack is turned off after 1.7 s at which point the roll attitude is close to -180° (Figure 10g). 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° turn. The UAV completed the full aileron roll in less than 2.6 s, and the altitude dropped by only 10 m 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 10c.

6 Attack Distance and Power Relationship

Indoor demonstrations show that a power of 20 W is sufficient for 25 cm-*Full Control* and 50 cm-*Block* attacks. However, the attack distance and minimum power relationship is not clear from these observations. To determine this relationship, the field distribution of the attacker antenna is simulated with an EM simulator (ANSYS HFSS). Adding to the ZPSL antenna with 35 cm-by-35 cm planar dimensions (used in indoor and in-flight attacks), a 'large' ZPSL antenna with 70 cm-by-70 cm planar dimensions is simulated as well. The field distributions of antennas with varying attack distance through the z-axis is combined with the indoor results to determine the attack distance and power relationship shown in Figure 11. Some of our observations are as follows: The *Full Control* requires more power than *Block* regardless of the antenna size. The large antenna requires significantly less power than the smaller antenna. 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 the near field is a known phenomenon. For Transcranial Magnetic Stimulation (TMS) applications, in which magnetic fields stimulate particular regions of the brain, larger loops are preferred for better field 'penetration' to the inner brain layers [48]. To increase the attack distance, adding to increasing the antenna dimension, metamaterial–artificial magnetic conductors [49], which functions as magnetic reflectors, can be utilized to improve the field power by 3 dB which decreases the attack power and protect the tracker from its own attack field.

In scenarios, where the victim system is not RF-shielded, the far field antennas with high directivity improve the attack distance. Assuming lossless and matched antennas for both the attacker and the targeted circuitry, i.e., victim loops, the power transferred to the victim, P_{tgt}, can be determined with the Friis transmission formula [32]:

$$\begin{aligned} P_{tgt} &= P_{atk} + D_{atk} + D_{tgt}\left(\theta_{tgt}, \phi_{tgt}\right) \ldots \\ &+ 20\log_{10}\left(\frac{\lambda}{4\pi d}\right) + 20\log_{10}(|\hat{\rho}_{atk} \cdot \hat{\rho}_{tgt}|) \end{aligned} \tag{5}$$

where P_{atk}, D_{atk} and $\hat{\rho}_{atk}$ are attacker power, antenna directivity and polarization, respectively. $D_{tgt}\left(\theta_{tgt}, \phi_{tgt}\right)$ is the directivity of a particular loop in the victim, e.g., PWM cables. (5) shows that the increase in the D_{atk} of the antennas directly improve the transferred power to the victim, Yagi-Uda antennas with multiple resonant dipoles can have directivities around 9.2 dBi [50]. This means an attack power reduction of ≈ 7.44 dB compared to a small loop with a theoretical directivity of 1.76 dBi [32]. 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. However, as the boresight and polarity of the far-field antennas should be aligned with the victim loop to maximize $D_{tgt}\left(\theta_{tgt}, \phi_{tgt}\right)$, using far field antennas on moving victim systems (e.g., UAVs) is challenging. For those scenarios, the near field attacks with loop antennas should be used (Section 5).

7 Attacks on DC Motors and Speed

Another type of widely used actuator in CPS applications (from drones to robots) is 'DC motors' the rotational speed (rpm) of which is controlled by PWM. Similar to servo control (Figure 2), when t_{high} is minimum (i.e., 1 ms), the rotation speed is minimum (i.e., rpm=0 and the motor 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 DC motor at the desired rpm.

As over-the-air coupling mechanism is the same regardless of the actuator and consists of the victim cable resonant frequency detection and a resonant antenna design, and contributes additional experimental parameters, the attacks on the DC motor speed is tested in a wired setup (Figure 12a).The attack waveform is added to the victim PWM ($t_{high} = 1.5$ ms) with a wideband combiner (Minicircuits ZFRSC-42-S+) and fed to the ESC, and the rpm of the DC motor is observed with varying attack frequency and voltage. The motor-ESC pair is powered with a 22.2 V 6S LiPo battery, and the PWM input to the system is commanded through the Pixhawk flight controller. Three ESC models are tested: Eflite 60 A Pro [51],

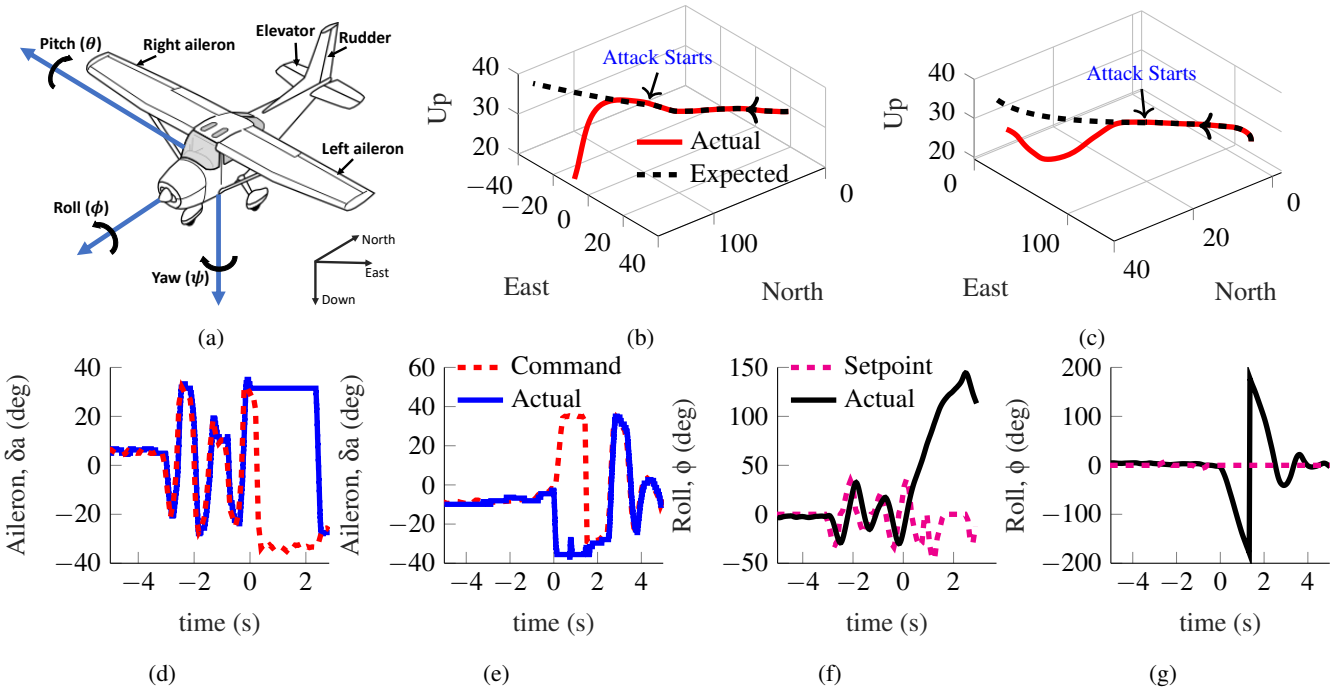


Figure 10: Results of in-flight demonstration of the attack. The attack starts at $t = 0$. (a) Axes of motion and control surfaces of a fixed-wing UAV. (b) The trajectory of the UAV during *Block* attack demonstration (Block Video). (c) The trajectory of the UAV during *Full Control* attack demonstration (Full Control Video). (d) The *Block* waveform locks the aileron servo (at $t = 0$, blue curve). (e) The *Full Control* waveform ($t_{rotate} = 1.8$ ms) rotates the aileron to $-36°$ (at $t = 0$, blue curve). (f) The roll attitude tracking during *Block* attack demonstration. (g) The roll attitude tracking during *Full Control* attack demonstration.

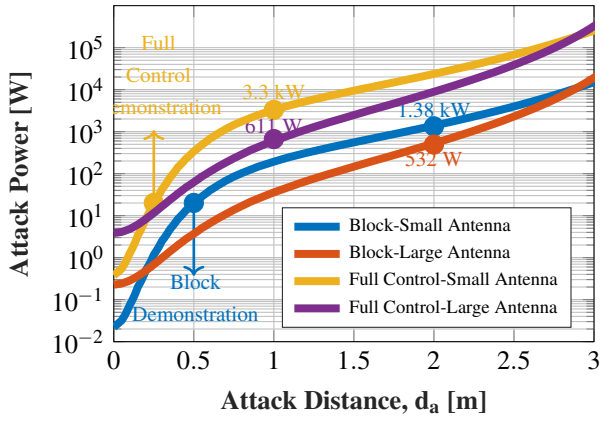
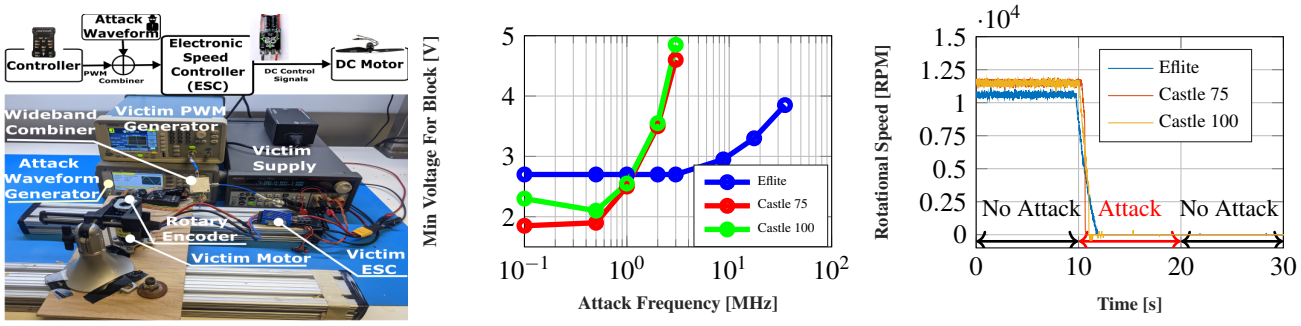


Figure 11: The field distribution of small and large ZPSL antennas are found with EM simulation, and indoor demonstrations are used as a benchmark. Generally, large antenna and *Block* attacks require less power; however, the required attack power increases significantly above 2 m.

Castle Phoenix Edge 75 A [52], and Castle Phoenix Edge 100 A [53] with an Eflite BL50 525 kV DC motor [54].

It is observed that at certain attack frequency and voltages, *Block* waveform prevents the rotation of each ESC-DC motor combination (Figure 12b and 12c). However, depending on the models, the attack frequency and power differ. While Castle models are vulnerable to *Block* at frequencies below 3 MHz within the attack voltage range (max 5 V), the Eflite models can be attacked with frequencies up to 35 MHz. Similar to the results observed with servos (Table 1), the higher frequency attacks require higher power. This 'Low Pass' characteristic is because of the ferrite beads on the PWM cables utilized for EM interference. However, ferrite beads are observed to be ineffective at relatively low frequencies of the attack waveforms. Additionally, even after the attack stops at $t = 20$ s (Figure 12c), the DC motor fails to reattain the rpm instructed by the victim PWM as it goes back to the 'disarmed' state. To prevent any action before the system is fully configured, the Pixhawk requires the motor to be armed manually by the user through the ground/radio controller. In the 'disarmed' state, no power is sent to the motor, and an armed motor disarms automatically if it is left idle for a certain amount of time. The Block attack stops the rotation of the DC motor for 10 s, resulting in the automatic disarming of the motor; hence, after the attack ends, the manual arming of the DC motor is necessary to ensure its recovery from the attack. *Full Control* waveform is applied to the tested ESC-DC motor couples. Although *Full Control* has a similar effect as *Block* and results in the full stop of the motors when the attack is initiated, the control of the victim rpm through *Full Control* waveform is not observed within the tested voltage (<5 V) and



(a) (b) (c)

Figure 12: PWM–controlled DC motors are tested in a wired setup. The change in the speed (rpm) of DC motors is recorded. (a) The experimental setup for wired tests (b) The minimum peak voltages to stop the DC motor rotation. *Block* stops the rotation of all tested ESC and DC motor couples; however, the attack frequency should be lower (< 3 MHz) for Castle models. (c) The attack is initiated at $t = 10$ s, ended at $t = 20$ s. None of the tested ESC-DC motor combinations 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.

frequency (<100 MHz) range. It can be said that as the PWM inputs of the tested ESCs do not have a similar protection circuitry (i.e., a diode in series to a capacitor behaves as an envelope detector) as the servo motors, they are more resilient to the precise speed control. Unfortunately, the denial of service attacks is observed on each tested ESC-DC motor couple with both *Block* and *Full Control* waveforms.

8 Countermeasures

The attacker uses a magnetic field to couple to the victim circuitry, and as the magnetic fields exist in nature as complete circles 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 [55, 56]. However, high permeability materials like MuMetal lose their magnetic properties with increased frequency and become inefficient magnetic shields above 100 kHz [56]. As the frequency goes roughly above 100 kHz the magnetic or non-magnetic conductors like steel or aluminum perform better than MuMetal [57, 58]. However, high-frequency magnetic shielding highly depends on the shield thickness, and thick conductor plates are needed unlike the far-fields which can be shield with thin metal layers, e.g., aluminum foil [57]. Magnetic shielding 'efficiency' also relies on how much the shielding material encloses the protected system or component. Frika et al. showed that even small openings (e.g., cable holes) in the magnetic shielding deteriorates the shielding efficiency significantly [57, 59]. This is the most concerning issue about IEMI attacks using inductive coupling, because it is practically challenging to cover all moving parts of a CPS with magnetic shielding. For instance, completely covering the control surface of a UAV with magnetic shielding is not practical due to cost, weight, and disrupted flight dynamics. The authors think that shielding can be a solution for some IEMI scenarios (e.g., far field attacks [8]); however, it can not be the sole countermeasure against attacks with inductive coupling. A PWM signal with a changing frequency is suggested as a countermeasure [60] for the attacks using voltage drops to manipulate PWM [6]. As the *Block & Rotate* and *Full Control* waveforms override the rotation angle information regardless of the victim PWM frequency, varying frequency–PWM is not effective for the reported attacks in this paper.

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 [61, 62], the optical transmission is a viable and reliable defense against FAI. During in-flight tests, the optical transmission works without disruption under high EMI.

9 Conclusion

Intentional Electromagnetic Interference (IEMI) is a significant threat to the secure operation of PWM–controlled actuators. The results demonstrate that the actuation control of all tested servo and DC motors are vulnerable to *Block* attack, which prevents the data transmission and paralyzes the actuators. The amplitude modulated attack waveforms, namely *Block & Rotate* and *Full Control* inject false data to specific servo models (e.g., Futaba) and give the attacker the control of the actuators. The attacks are demonstrated on the control surfaces of a fixed-wing UAV, and the flight data shows that the *Block* and *Full Control* attacks result in the

disruption of the UAV trajectory control. While *Block* attack prevents the aileron control of the UAV and results in a crash, *Full Control* waveform rotates the ailerons to one extreme and results in an 'aileron roll' of the victim UAV. Other actuators, such as DC motors, the speed of which is controlled by PWM, are not secure either. Although IEMI on actuators can be utilized as an offensive measure (e.g., against an intruder UAV), defenses such as optical transmission and magnetic field shielding should be utilized for secure operation.

References

[1] A. Cardenas, "Cyber-physical systems security knowledge area issue 1.0," tech. rep., www.cybok.org, October 2019.

[2] C. Balanis, *Advanced Engineering Electromagnetics*. Wiley, 1989.

[3] D. Kune, J. Backes, 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*, pp. 145–159, May 2013.

[4] Y. Shoukry, P. Martin, P. Tabuada, and M. Srivastava, "Non-invasive spoofing attacks for anti-lock braking systems," in *Cryptographic Hardware and Embedded Systems* (G. Bertoni and J.-S. Coron, eds.), vol. 8086 of *Lecture Notes in Computer Science*, pp. 55–72, 2013.

[5] C. Kasmi and J. Lopes Esteves, "Iemi threats for information security: Remote command injection on modern smartphones," *IEEE Transactions on Electromagnetic Compatibility*, vol. 57, no. 6, pp. 1752–1755, 2015.

[6] J. Selvaraj, G. Y. Dayanikli, N. P. Gaunkar, D. Ware, R. M. Gerdes, and M. Mina, "Electromagnetic induction attacks against embedded systems," in *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, ASIACCS '18, (New York, NY, USA), pp. 499–510, ACM, 2018.

[7] I. Giechaskiel, Y. Zhang, and K. B. Rasmussen, "A framework for evaluating security in the presence of signal injection attacks," *Computer Security – ESORICS 2019*, pp. 512–532, 2019.

[8] Y. Tu, S. Rampazzi, B. Hao, A. Rodriguez, K. Fu, and X. 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, (New York, NY, USA), p. 2301–2315, Association for Computing Machinery, 2019.

[9] 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)*, pp. 233–248, 2020.

[10] I. Giechaskiel and K. Rasmussen, "Taxonomy and challenges of out-of-band signal injection attacks and defenses," *IEEE Communications Surveys Tutorials*, vol. 22, no. 1, pp. 645–670, 2020.

[11] "Pixhawk 1 flight controller." https://docs.px4.io/en/flight_controller/pixhawk.html. [Online; accessed 15-May-2019].

[12] M. Pajic, I. Lee, and G. J. Pappas, "Attack-resilient state estimation for noisy dynamical systems," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 82–92, 2017.

[13] S. Capkun, "Physical layer & telecommunications security knowledge area issue 1.0," tech. rep., www.cybok.org, October 2019.

[14] 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*, pp. 1213–1218, Nov 2016.

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

[16] D. Pozar, *Microwave Engineering*. Wiley, 1997.

[17] 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*, vol. 2006, no. 318, pp. 6–12, 2006.

[18] M. Leone and H. Singer, "On the coupling of an external electromagnetic field to a printed circuit board trace," *IEEE Transactions on Electromagnetic Compatibility*, vol. 41, no. 4, pp. 418–424, 1999.

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

[20] A. K. Zachary Stokes, "Reverse current protection in load switches," Tech. Rep. SLVA730 Application Report, Texas Instruments.

[21] J.-H. Chun and B. Murmann, "Analysis and measurement of signal distortion due to esd protection circuits," *IEEE Journal of Solid-State Circuits*, vol. 41, no. 10, pp. 2354–2358, 2006.

[22] R. Turner, *Diode Circuits Handbook*. A Howard W. Sams photofact publication, Foulsham, 1963.

[23] J. Nilsson and S. Riedel, *Electric Circuits*. Mastering Engineering Series, Prentice Hall, 2011.

[24] R. Ziemer and W. Tranter, *Principles of Communications: Systems, Modulation, and Noise*. Wiley, 1995.

[25] R. J. Bunker, *Terrorist and insurgent unmanned aerial vehicles : use, potentials, and military implications*. Strategic Studies Institute, US Army War College, 2015.

[26] D. Gettinger and A. H. Michel, "Drone sightings and close encounters: An analysis," 2015.

[27] I. Güvenç, O. Ozdemir, Y. Yapici, H. Mehrpouyan, and D. Matolak, "Detection, localization, and tracking of unauthorized uas and jammers," in *2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC)*, pp. 1–10, IEEE, 2017.

[28] S. Buerger, J. R. Salton, D. K. Novick, R. Fierro, A. Vinod, B. HomChaudhuri, and M. Oishi, "Reachable set computation and tracking with multiple pursuers for the asap counter-uas capability.," tech. rep., Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), 2016.

[29] S. Tolman and R. W. Beard, "Counter uas using a formation controlled dragnet," in *2017 International Conference on Unmanned Aircraft Systems (ICUAS)*, pp. 1665–1672, IEEE, 2017.

[30] R. Strydom and M. V. Srinivasan, "Uas stealth: target pursuit at constant distance using a bio-inspired motion camouflage guidance law," *Bioinspiration & biomimetics*, vol. 12, no. 5, p. 055002, 2017.

[31] T. H. Chung, G. A. Hollinger, and V. Isler, "Search and pursuit-evasion in mobile robotics," *Autonomous robots*, vol. 31, no. 4, pp. 299–316, 2011.

[32] C. Balanis, *Antenna theory: analysis and design*. Harper & Row series in electrical engineering, Wiley, 1982.

[33] R. A. Salvatore Celozzi and G. Lovat, *Electromagnetic Shielding*, ch. Appendix B : Magnetic Shielding, pp. 282–316. Wiley, 2008.

[34] R. Johnson and H. Jasik, *Antenna Engineering Handbook*. Electronics Electrical Engineering, McGraw-Hill, 1993.

[35] J. R. Moser, "Low-frequency low-impedance electromagnetic shielding," *IEEE Transactions on Electromagnetic Compatibility*, vol. 30, no. 3, pp. 202–210, 1988.

[36] A. Kurs, A. Karalis, R. Moffatt, J. D. Joannopoulos, P. Fisher, M. Soljacic, and M. Soljac, "Wireless power transfer via strongly coupled magnetic resonances," *Science*, vol. 83, no. 5834, pp. 83–86, 2007.

[37] 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*, vol. 56, no. 5, pp. 1801–1812, 2009.

[38] 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*, vol. 58, no. 2, pp. 544–554, 2011.

[39] M. Denicolai, "Optimal performance for tesla transformers," *Review of Scientific Instruments*, vol. 73, no. 9, pp. 3332–3336, 2002.

[40] D. Finkelstein, P. Goldberg, and J. Shuchatowitz, "High voltage impulse system," *Review of Scientific Instruments*, vol. 37, no. 2, pp. 159–162, 1966.

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

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

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

[44] K. Wyatt, "Measuring resonance in cables." https://www.edn.com/measuring-resonance-in-cables/. Accessed: 2021-05-12.

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

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

[47] R. W. Beard and T. W. McLain, *Small unmanned aircraft: Theory and practice*. Princeton university press, 2012.

[48] Z. D. Deng, S. H. Lisanby, and A. V. Peterchev, "Electric field depth-focality tradeoff in transcranial magnetic stimulation: simulation comparison of 50 coil designs," *Brain Stimulation*, vol. 6, no. 1, pp. 1–13, 2013.

[49] D. Sievenpiper, L. 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*, vol. 47, no. 11, pp. 2059–2074, 1999.

[50] H. Sun, Y. Guo, M. He, and Z. Zhong, "A dual-band rectenna using broadband yagi antenna array for ambient rf power harvesting," *IEEE Antennas and Wireless Propagation Letters*, vol. 12, pp. 918–921, 2013.

[51] "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.

[52] "Phoenix edge 75 amp esc." https://www.castlecreations.com/en/phoenix-edge-75-esc-010-0101-00. Accessed: 2021-07-12.

[53] "Phoenix edge 100 amp esc." https://www.castlecreations.com/en/phoenix-edge-100-esc-010-0100-00. Accessed: 2021-07-12.

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

[55] H. Ott, *Electromagnetic Compatibility Engineering*. Wiley, 2011.

[56] "Mumetal high permeability magnetic shielding: Frequently asked questions." http://www.mu-metal.com/faqs.html.

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

[58] R. B. Schulz, "Elf and vlf shielding effectiveness of high-permeability materials," *IEEE Transactions on Electromagnetic Compatibility*, vol. EMC-10, no. 1, pp. 95–100, 1968.

[59] 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*, vol. 51, no. 3, pp. 1–4, 2015.

[60] D. Muniraj and M. Farhood, "Detection and mitigation of actuator attacks on small unmanned aircraft systems," *Control Engineering Practice*, vol. 83, pp. 188 – 202, 2019.

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

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

[63] M. 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*, vol. 105, no. 4, pp. 557–564, 2000.

[64] Y. Zeng, Z. N. Chen, X. Qing, and J. Jin, "Design of a near-field nonperiodic zero phase shift-line loop antenna with a full dispersion characterization," *IEEE Transactions on Antennas and Propagation*, vol. 65, no. 5, pp. 2666–2670, 2017.

A Derivation of Attacker Magnetic Field and Induced Voltage

An electromagnetic field solution is used to determine the coupling coefficients reported in Table 5 [63]. The model shown in Figure 6a is used for the solution, and the distance between the attacker and the victim, d_a, is 1 m. $< x_o, y_o, z_o >$ is any point on which the time-varying magnetic field, **B**, is found. As the attacker 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, in which 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 factor [63]. The x, y, and z components of **B** are obtained from magnetic vector potentials A_x and A_y:

$$\mathbf{B} = \nabla \times \mathbf{A}\ ,\ B_x = -\frac{\partial A_y}{\partial z}\ ,\ B_y = \frac{\partial A_x}{\partial z}\ ,\ B_z = \frac{\partial A_y}{\partial x} - \frac{\partial A_x}{\partial y} \quad (6)$$

Note that $A_z = 0$ because the attacker current only has x and y components (Figure 6a). Magnetic vector potential (**A**) is found by line integral of the attacker current (7). **dl** and μ are differential length vector of the attacker current (I_a) and permeability of the medium, respectively.

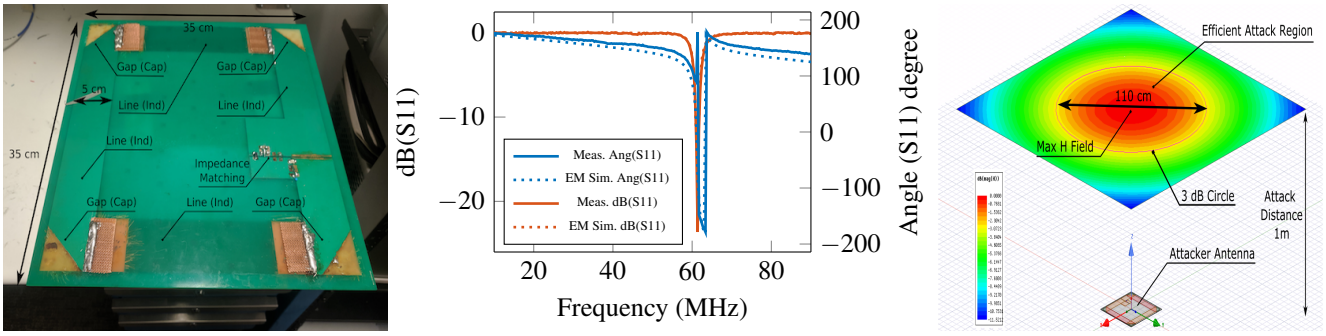
$$\mathbf{A} = \frac{\mu}{4\pi}\int \frac{I_a\,\mathbf{dl}}{|\mathbf{r}-\mathbf{r}'|} \quad (7)$$

where $\mathbf{r}$ and $\mathbf{r}'$ are position vectors for the attacker field (B) and current (I_a). As the victim loop normal is through z-axis, only B_z contributes to the induced voltage. After the calculation of A_x and A_y with (7), B_z is found as [63]:

$$B_z = \frac{\mu I_a}{4\pi}\sum_{n=1}^{4}\left[\frac{(-1)^n D_n}{r_n\left(r_n + (-1)^{n+1} C_n\right)} - \frac{C_n}{r_n\left(r_n + D_n\right)}\right] \quad (8)$$

where the position variables C, D, and r (Figure 6a) are:

$$\begin{aligned} C_1 &= -C_4 = x_a/2 + x_o \quad & r_1 &= \sqrt{C_1^2 + D_1^2 + d_a^2} \\ C_2 &= -C_3 = x_a/2 - x_o \quad & r_2 &= \sqrt{C_2^2 + D_2^2 + d_a^2} \\ D_1 &= D_2 = y_a/2 + y_o \quad & r_3 &= \sqrt{C_3^2 + D_3^2 + d_a^2} \\ D_3 &= D_4 = -y_a/2 + y_o \quad & r_4 &= \sqrt{C_4^2 + D_4^2 + d_a^2} \end{aligned} \quad (9)$$



(a) (b) (c)

Figure 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 $z = 1$ m, a wide attack region with a Half Power Beam Width diameter of 110 cm

The field distribution of the attacker antenna on the victim loop (Figure 6a) is determined with a Matlab script using (8), and the coupling coefficients reported in Table 5 are determined with (1). Faraday's law of induction states that the induced voltage, v_{ind}, to a victim loop is the time derivative of the normal magnetic flux captured by the coil surface, so the relationship of B_z and v_{ind} is:

$$v_{ind} = -\frac{d}{dt}\iint_{S_v} B_z \cdot dS \tag{10}$$

where S_v is the victim loop surface and its normal is assumed to be aligned with the z-axis. With the introduction of (8), (10) becomes:

$$v_{ind} = -\frac{\mu}{4\pi}\left(\frac{d}{dt}I_a\right)\iint_{S_v} P(x_o,y_o,z_o)\cdot dS \tag{11}$$

where $P(x_o,y_o,z_o)$ is the position variable which does not vary with time:

$$P(x_o,y_o,z_o) = \sum_{n=1}^{4}\left[\frac{(-1)^n D_n}{r_n\left(r_n+(-1)^{n+1}C_n\right)} - \frac{C_n}{r_n\left(r_n+D_n\right)}\right] \tag{12}$$

(11) demonstrates that the induced voltage on the victim loop is linearly proportional to the time derivative of the attacker current, $d/dt(I_a)$. If we assume a pure sinusoidal current such that $I_a = sin\omega t$, the induced voltage is proportional to $d/dt(sin\omega t) = \omega cos\omega t$. Thus, the induced voltage, v_{ind}, is linearly proportional to the frequency of the attacker, and the attack waveforms that utilize very low frequencies (e.g., as 50 Hz) [6] induces significantly less voltage compared to VHF frequencies. It should be noted that this characteristic is observed up to the first resonance frequency of the victim loop, and the reader can refer to [18] for a detailed discussion for above–resonance v_{ind} characteristics.

B Attacker Antenna Design and Production

It is concluded in Section 2.1 that a magnetic resonant coupling can be utilized by a tracker for efficient attacks (i.e., same power longer attack distance or less power same attack distance). This requires an attacker antenna that resonates at the same frequency with the victim PWM cables. As the relative position of the intruder is not constant during the flight, the magnetic field should be strong enough in a large enough area; i.e., a 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 [64]. However, the large electrical size of these antennas results in non-uniform 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 make the magnetic field more uniform in the near field.

A ZPSL antenna is designed for the ailerons resonating at $f_v = 61$ MHz. ANSYS HFSS is used for EM simulations and fine-tune the antenna dimension to the victim resonance at $f_v = 61$ MHz. A lumped L-C impedance matching circuit for 50 ohm is employed to eliminate back power to amplifier and transmit maximum possible power to the antenna. The planar size of the antenna is 35 cm by 35 cm (Figure 13a). The inner dielectric section of the PCB antenna is removed to decrease the air drag in the flight tests. The simulation and measurements are aligned as shown in Figure 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 is a sign of good impedance match. ZPSL antenna has a bidirectional magnetic near field which has local maximums through + and - z-axis of the antenna. In Figure 13c, $|H|$ distribution of the antenna is shown on a 2 m by 2 m plane at an attack distance of 1 m. It is observed that the Half Power Beam Diameter of the antenna is 110 cm.