Paralyzing Drones via EMI Signal Injection on Sensory Communication Channels

Joonha Jang*†, Mangi Cho*†, Jaehoon Kim†, Dongkwan Kim‡, and Yongdae Kim†
†KAIST, ‡Samsung SDS
{*cyber040946, mgcho0608, jaehoon.kim99, dkay, yongdaek*}@kaist.ac.kr

***Abstract*—An inertial measurement unit (IMU) takes the key responsibility for the attitude control of drones. It comprises various sensors and transfers sensor data to the drone's control unit. If it reports incorrect data, the drones cannot maintain their attitude and will consequently crash down to the ground. Therefore, several anti-drone studies have focused on causing the significant fluctuations in the IMU sensor data by resonating the mechanical structure of the internal sensors using a crafted acoustic wave. However, this approach is limited in terms of efficacy for several reasons. As the structural details of each sensor in an IMU significantly differ by type, model, and manufacturer, the attack needs to be conducted independently for each sensor. Furthermore, it can be easily mitigated by using other supplementary sensors that are not corrupted by the attack or inexpensive plastic shielding.**

In this paper, we propose a novel anti-drone technique that effectively corrupts any IMU sensor data regardless of the sensor's type, model, and manufacturer. Our key idea is to distort the communication channel between the IMU and control unit of the drone by using an electromagnetic interference (EMI) signal injection. Experimentally, for a given control unit board, regardless of the sensor used, we discovered a distinct susceptible frequency at which an EMI signal greatly distorted the sensor data. Compared to a general EM pulse (EMP) attack, our work requires considerably less power since it targets the specific susceptible frequency. It can also reduce collateral damage from the EMP attack (*e.g.*, permanent damage to the electric circuits of any nearby devices). For practical evaluations, we demonstrated the feasibility of the attack using real drones, wherein it instantly paralyzed the drones. Lastly, we conclude by presenting practical challenges for its mitigation.

I. INTRODUCTION

Sensors are crucial for the operation of drones, such as attitude control, obstacle avoidance, and navigation. Notably, an inertial measurement unit (IMU), which is an integrated chip consisting of a gyroscope, an accelerometer, a magnetometer, and a barometer, has the primary responsibility for attitude control. If IMU sensors report abnormal values, the drones cannot maintain their attitude and will fall to the ground [73].

Several studies have demonstrated the feasibility of corrupting the IMU output by exploiting the mechanical structure of the sensors [73], [80], [81]. In particular, they corrupted the sensor output by resonating the microelectromechanical system (MEMS) structure of gyroscopes and accelerometers using a crafted acoustic wave. However, these approaches are limited in terms of applicability because they require fine-grained tuning by considering the distinct characteristics of each sensor. Specifically, since the structural details of each sensor largely vary depending on its model, type, and vendor, an adversary must: 1) Figure out an appropriate resonance frequency for each sensor and 2) Conduct an attack independently for each sensor with adjusted environments for the sensor. Further, the approach can be mitigated by using other supplementary sensors that are not corrupted by the attack. For example, Choi *et al.* [14] proposed an approach to make a drone hover (without falling) by using only an accelerometer even though the gyroscope of the drone resonates. Additionally, even inexpensive plastic shielding can prevent the attack by blocking acoustic waves [73], [80], [81].

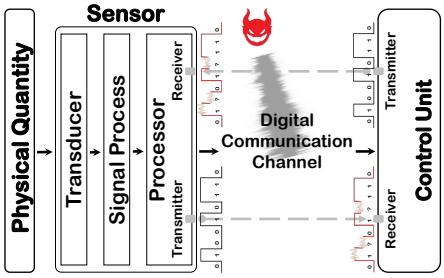

Fig. 1: Simple illustration of our approach. We target the digital communication channel between a sensor and control unit.

Instead of targeting the sensors directly, we propose a novel approach that corrupts the communication channel through which the sensor output is transferred (Fig. 1). Our intuition is that any of the IMU sensor output is transferred to the control unit of the drones through this communication channel. Thus, corrupting the communication channel may prevent the control unit from correctly retrieving any sensor output, regardless of the characteristics of each sensor (§III). If successful, this would effectively incapacitate the drone since the IMU sensor output is necessary for the drone's operation. Additionally, since corrupting the communication channel distorts the original signal itself, it could neutralize existing countermeasures that extract the original signal from the attack signal [83], [94].

Our key idea is to distort the digital signals of the communication channel between the IMU sensor and control unit by leveraging electromagnetic interference (EMI). Despite the advantages mentioned above, attacking the communication channel using EMI has received relatively little attention since

*These two authors equally contributed.

Network and Distributed System Security (NDSS) Symposium 2023
27 February - 3 March 2023, San Diego, CA, USA
ISBN 1-891562-83-5
https://dx.doi.org/10.14722/ndss.2023.24616
www.ndss-symposium.org

Kune *et al*. claimed that distorting digital signals using EMI requires relatively high power [40]. Recently, several studies have shown that EMI could cause a "bit flip" in the original signal of the communication channel [16], [67], [68], [86]. Another study showed that using EMI to overwrite controller PWM commands could compromise a servo motor and make a UAV uncontrollable [17]. However, this method is not applicable to multicopters, as admitted by the authors in their paper. Our approach overcomes most of these limitations, as explained in the rest of this paper.

In §IV, we first investigate the implication of faulty communication channels on transferred sensor data by blocking and disturbing the signals of two representative communication protocols, I2C and SPI, respectively. Consequently, we verified the significance of the communication failure on the transferred sensor data and discovered the required conditions (at a signal level) for communication failure to occur.

Furthermore, we explored whether a remote EMI signal injection could cause communication failure by satisfying the discovered required conditions (§V). First, we empirically analyzed whether the EMI injection could indeed distort a communication channel. To verify this, we shielded each component of the circuit, such as the wires, sensors, and control unit board, with aluminum foil and monitored the communication signals while injecting an electromagnetic (EM) wave. Consequently, we discovered that the control unit board behaved as an unintentional antenna.

Thus, the injected EM wave induced an EMI on the communication channel, thereby distorting the digital signals in it. To precisely investigate this, we conducted a series of experiments using various pairs of IMU sensors and control unit boards and discovered several interesting phenomena. First, *regardless of the paired IMU sensors, each control unit board has a specific frequency which is highly susceptible to EMI*. Thus, an adversary can efficiently launch an attack using an EMI signal at the most susceptible frequency for a given target board. Second, *the power required for channel distortion is determined by both the control unit board model and the sensor model*. By using these properties, we discovered that an adversary can effectively make the target drone crash down to the ground with relatively low power.

We then demonstrated the feasibility of the attack using both 1) PX4 simulation and 2) real drones (§VI). Specifically, we evaluated the relationship between attack distance and required power by radiating EMI up to 100 W with a directional antenna in a shielded chamber. The result shows that the experimental results coincide with the theoretical estimation. In addition, we conducted remote attacks against hovering drones with the same experimental setup (Fig. 17). Notably, we were able to instantly crash the target drone after injecting a malicious EMI signal from several meters away [1], [2].

As an anti-drone technique, our approach has the following advantages compared to an EMP attack and GPS spoofing. First, since it targets a specific susceptible frequency, it requires considerably less power than the EMP attack, which requires hundreds of MW or more in order to burn electronic circuits [41], [46], [51], [63]. Second, it avoids extensive collateral damage as in the other two attack methods. Here, collateral damage refers to unintended damage caused to something other than the intended target, including allies and civilians. The EMP attack affects all electronic circuits causing permanent damage to peripheral devices, while GPS spoofing affects all surrounding GPS receivers causing them to misrecognize accurate location and time [30], [35], [53], [65], [91]. Conversely, our approach disrupts the target system's sensory communication channel only (i.e., it inflicts no permanent damage). Lastly, it instantly crashes drones down to the ground as it fundamentally blocks all sensor data by exploiting the sensory communication channel.

Furthermore, since our attack instantly crashes the target drones, it can also neutralize existing mitigation strategies [4], [14], [22], [42], [60], [65], [84], [92], [93], which we further explain in detail in §VIII. Lastly, our approach can also be applied to other sensors, such as CMOS image sensors that are widely used in autonomous vehicles (§A).

The contributions of our study are summarized as follows:

- We discovered and demonstrated that drones can be crashed through corruption of the communication signals between sensors and the control unit.
- We revealed that an adversary can remotely corrupt the communication signals by injecting an EMI signal.
- We discovered that as each control unit board has a specific frequency that is highly susceptible to EMI. Injecting an EMI signal at the most susceptible frequency for a target board can effectively distort any transferred sensor data.
- Using real drones, we demonstrated that the attack instantly crashed drones down to the ground.
- We manifested the applicability of the attack using CMOS image sensors which are widely used for autonomous vehicles.

II. BACKGROUND

A. Sensing Logic of a Drone

All drones (multicopters) have multiple sensors, rotors, and a control unit (flight controller). Among them, the multi-sensor is important to enable the drone's controller to determine the correct rotor rotation. For a drone's operation, an accurate sensing of its surrounding environments is essential. Sensing refers to measuring the physical quantity required for the control unit to determine the appropriate actuation based on the drone's current state and surrounding environment. In general, sensing operates in the following sequences: First, the sensors measure a physical quantity and convert it into an analog signal. Then, the analog signal is amplified, filtered, and converted into a digital signal. Next, the digital signal is transmitted to the control unit through the communication channel using a predetermined protocol, such as I2C or SPI. The control unit then interprets the transmitted digital signal into a series of digitized values according to the protocol. Finally, the control unit retrieves a sensor value and then feeds it into the control algorithm of the drone to determine its subsequent action.

B. IMU: Essential for Attitude Control

An IMU is essential for the flight and attitude control of drones [73], [80], [81]. It is a single integrated chip comprising four sensors: a gyroscope, an accelerometer, a magnetometer,

and a barometer (optional). Each sensor measures a target physical quantity, such as an angular rate, linear acceleration, magnetic field, and atmospheric pressure, respectively. The measured quantities are then processed, transferred, and interpreted as digitized values for the drone's attitude control. Using these retrieved values, the control unit calculates the difference between the current and desired attitude for a stable flight and then determines appropriate commands to be sent to the rotors. During this process, the values of various sensors can be combined in a complementary way to reduce calculation errors. This is often referred to as sensor fusion. For instance, the Extended Kalman Filter (EKF) is a well-known sensor fusion method. It is used to precisely estimate a drone's current attitude by combining the values of the IMU's sensors. By repeating these steps, the drone can maintain its posture, thereby resulting in a stable flight.

C. Communication in Sensing Logic

There are two types of communication protocols: synchronous and asynchronous. Unlike asynchronous protocols, synchronous protocols continuously synchronize the communication endpoints (*i.e.*, sensors and the control unit) based on a common clock signal. Consequently, synchronous protocols provide higher reliability and a faster data transfer rate than asynchronous protocols. Owing to these advantages, synchronous protocols are widely used in automobiles or drones.

Among the various synchronous protocols, I2C and SPI are dominantly used for sensor data transmission. In both protocols, the main device (usually a control unit) controls the peripheral devices (usually sensors) using clock signals. As the communication signals according to these protocols are our main target, we describe them in details below. Note that the top ten global drone manufacturers [27] employ SPI and I2C [7], [59].

I2C protocol. The I2C protocol is appropriate for IMU data transmission because of its simplicity and add-on capability. It comprises two channels: serial data (SDA) and serial clock (SCL). The SDA transfers data signals either from the control unit to the sensors or vice versa, while the SCL transfers clock signals from the control unit to the sensors. The clock signals enable the signals to be correctly interpreted. Particularly, when the SCL becomes low (*i.e.*, 0), a data signal starts to be transferred. When the SCL becomes high (*i.e.*, 1), the transferred data signal is interpreted as one (if the SDA is high) or zero (if the SDA is low).

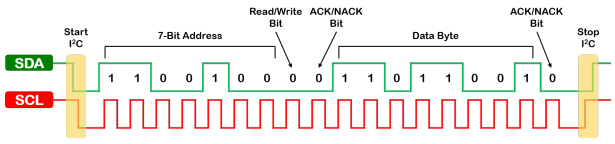

Fig. 2: Example of I2C communication logic.

Figure 2 shows an example of I2C communication and its interpretation. Before the communication initiates, both the SCL and SDA remain high, which represents the idle state. To initiate the communication, the control unit sends a start command by setting the SDA to low. Following that, it transmits a 7-bit address to determine the communication target, a 1-bit read/write flag, and a 1-bit ACK/NACK flag through the SDA. After receiving the start command, each sensor starts checking whether the address on the SDA matches its own address. The matched sensor determines whether to read/write data from/to the SDA by checking the read/write bit. Typically, it writes its sensed data on the SDA. Finally, after receiving the sensor data, the control unit ends the communication by setting the SDA to high and keeping the SCL high. After the communication is completed, the SDA and SCL remain high, waiting for the subsequent communication.

SPI protocol. The SPI protocol is mainly used in high-speed applications, such as images or video streams, since it provides a faster data transmission speed than I2C. For a high transmission speed, it leverages four channels, each of which has a specific communication direction: master out slave in (MOSI), master in slave out (MISO), chip select (SS), and serial clock (SCLK). On the one hand, MOSI and MISO transfer data signals from the control unit to the sensors and vice versa. On the other hand, both the SS and SCLK transfer signals from the control unit to the sensors. The SS designates a target sensor for communication, while the SCLK transmits the clock signals that serve as a time reference for interpreting the signals on MOSI and MISO.

Before the communication initiates, the SS remains high, which represents the idle state. To initiate the communication, the control unit alerts a target sensor by setting the corresponding SS signal to low. Next, the control unit and target sensor exchange data in full-duplex mode using MOSI and MISO. Upon completion of the data transmission, the control unit stops toggling the clock signal and deselects the sensor.

D. EM Coupling and EMI Injection

Signals on electronic circuits can be influenced by an EM field. This is referred to as *EM coupling* [11], [24], [45], [55], [70]. The EM field induces the voltage in the circuit's conductors, which consequently perturbs the circuit's electrical signals. Hence, by forcefully triggering strong EM coupling, an adversary can disrupt the electric signals of a target system [25], [32], [36], [40], referred to as an *EMI injection* attack. This attack exploits the fact that the wires and conductors of any electronic circuit could act as an unintentional antenna [55].

EM susceptibility refers to the amount of change in electrical signals in a circuit caused by EM waves. The EM susceptibility of a circuit could differ considerably, depending on the frequency of an injected EM wave. These frequencies are mainly determined by the circuit's design, particularly the resistor-inductor-capacitor (RLC) configuration. Hence, identifying a specific frequency for an EM wave that can strongly affect a target circuit is crucial for an efficient attack. Hereafter, we refer to the frequency that has had the most considerable impact on the circuit (experimentally) as the circuit's *susceptible frequency*. Injecting an EM wave using a susceptible frequency can be over two times more power-efficient than other frequencies [40]. To identify the susceptible frequency, it is often leveraged to sweep a range of frequencies during the EMI injection while monitoring the circuit's response [40], [67], [68].

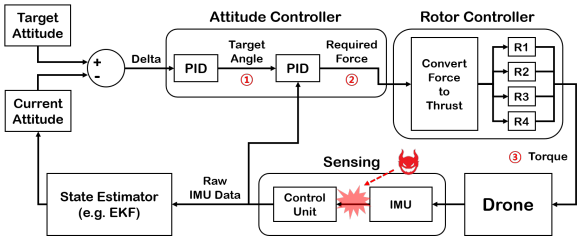

Fig. 3: Analysis of the influence of the communication channel distortion on the data flow of the attitude control algorithm.

III. ATTACK OVERVIEW

A. Threat Model

The attacker's goal is to remotely make a target drone crash down to the ground, regardless of the number and type of IMUs equipped. This can be achieved by leveraging EMI signals at the susceptible frequency of the target drone's control unit board, which we will detail in §V. When the attacker injects EMI signals into the communication channel between the IMU and control unit, all IMU sensor data are severely distorted. For this, the attacker should know the susceptible frequency of the target board. Here, we assume an attacker who can detect and identify the target drone as in previous studies [13], [87], [95]. Thus, the attacker is aware of the frequency required to attack the target drone. By acquiring a device of the same model as the target drone, the attacker can experimentally determine the susceptible frequency of it's control unit board and the appropriate power required to attack. Lastly, we assume that the target drone is secure against software vulnerabilities.

B. Attack Intuition

Distorting the communication channel between the IMU sensor and control unit could corrupt all sensor data simultaneously and consequently result in an immediate crash. This is because the corrupted sensor values are fed into the drone's attitude control algorithm directly. They are propagated from sensing to actuation, which inevitably leads to severe failures.

As described in §II-B, the main goal of the drone's attitude control is to reduce the difference between the current and desired attitudes for a stable flight. In particular, the drone's attitude is controlled by employing a nested proportional–integral–derivative (PID) feedback loop to minimize the difference (*i.e.*, "Delta") between the desired and current attitudes, which are derived from the IMU (Fig. 3). We derived the control flow diagram by analyzing the attitude control algorithms of the representative open source drones ArduCopter [6], PX4 [58], and MultiWii [49], as shown in Fig. 3.

According to the aforementioned, the external PID loop accepts the delta and derives the target rotation angle for the drone's x, y, and z-axis. Then, this angle is fed into the inner PID loop. The inner loop returns the required force to reach the target angle using the IMU raw data, which are the x, y, and z-axis angular velocities. The rotor controller converts this force into a thrust and later transmits the command to the rotors. Torque is then generated by the rotation of rotors, which causes a change in the drone's attitude. Subsequently, the sensor measures this change and feeds it into the attitude controller. By repeating these processes, the drone can adaptively control its attitude against external disturbances.

The control unit retrieves the IMU data based on the interpretation of the communication signals. If the communication between the sensor and control unit is disrupted, the control unit would not retrieve the correct IMU data. Then, incorrect IMU data causes the state estimator to return the current attitude away from the actual measurement, thereby resulting in an incorrect target angle (① in Fig. 3). Additionally, the internal PID loop yields the wrong force required to reach the target angle based on the distorted x, y, and z-axis angular velocities (② in Fig. 3). Consequently, the rotors generate torque, thereby causing the drone's attitude to deviate considerably from stable flight (③ in Fig. 3). Since the aforementioned problems are fed into the closed-feedback loop, creating an increasingly unstable attitude, the drone eventually crashes to the ground.

In summary, owing to the design, we showed that if the communication channels between the IMU and control unit are corrupted, distorted IMU values would be fed into the control algorithm, thereby severely impacting the drone's flight stability.

C. Roadmap

The main flow of this paper is organized as follows: First, the impact of distorted communication channels is investigated in §IV. In particular, we show how packets and retrieved sensor values were corrupted when communication signals were blocked or disturbed by fault injection. Further, we examine whether the communication errors caused by the direct communication channel distortion could also be induced remotely by EMI injection (§V). Particularly, we first show that the control unit board can act as an unintended antenna with point-of-entry (POE) evaluations. In addition, we demonstrate that 1) the susceptible frequency depends primarily depends on the board model and 2) the power requirement depends on both board model and sensor model. Experiments using real drones are presented in §VI. Here, we show that an adversary could instantly crash a drone through an appropriate EMI injection.

Additionally, practical considerations to apply our attack are investigated in §VII. Here, we present 1) the estimated power requirement for practical deployment and 2) the time requirement for corrupted IMU data to distort rotor commands by algorithmic analysis and data analysis using a real drone.

IV. CORRUPTING COMMUNICATION CHANNELS

Our ultimate goal is to make drones crash down to the ground by disrupting the communication channel that transfers the IMU sensor values to the control unit. The key intuition is that by distorting the communication channel, we can bypass the filtering and feed IMU errors directly into the drone's attitude control algorithm. By design, these errors propagate from sensing to actuation. In this section, we investigate the impact of corrupted communication channels using fault injection and identify signal-level conditions that could lead to severe communication failures. Note that "fault injection" refers to a well-known testing method for understanding how computing systems behave when stressed in unusual ways [31]. In particular, we employed target communication comprising an Arduino board and IMU sensor. Additionally, the MultiWii

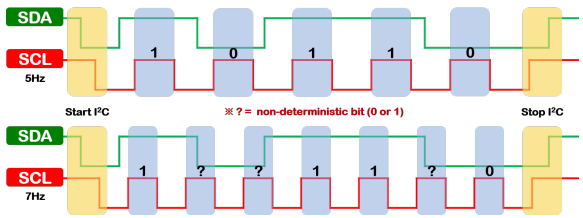

Fig. 4: I2C communication under stable SCL and SDA (top). The original message bits are inverted or irregularly deformed when the SCL is distorted (bottom).

firmware was used to measure the IMU data. Using these, we 1) physically blocked the benign communication signals and 2) injected additional noise directly into the benign communication signal to investigate the effect of distortion on communication as well as the interpretation of the IMU sensor values at the control unit board. Experimental results with I2C and SPI are presented in §IV-A and §IV-B.

A. Analysis of I2C Corruption

Owing to the principle of synchronous communication, it is essential to ensure the integrity of the SCL and SDA signals for reliable communication. Without the integrity of each signal, their interpretation could be considerably corrupted. Figure 4 shows an example of a case where the frequency of the SCL signals is distorted from 5 Hz to 7 Hz. Even when SDA signals are transmitted without error, the interpretation of the SDA bits considerably differs under distorted SCL signals. Corruption in the response and address bits, as well as start and stop commands, which are essential components of I2C communication, can greatly hinder the progress of I2C communication. To investigate this experimentally, we used an IMU sensor with a control unit board to artificially corrupt (block and distort) the signals.

Notably, we focused on analyzing the communication and retrieving data under distorted signals without considering the synchronization between the benign and injected signals.

Experimental setup. The connected sensor and control unit board communicated with I2C, and the communication signals and interpretation results were observed using a logic analyzer. We connected one of the IMU sensors (MPU 6050, 6500, 9150, 9250) and a control unit board (Arduino Uno) for our evaluations. The connected sensor and control unit board communicated through I2C, while a logic analyzer was used to observe the communication signal and interpretation results.

Blocking original signal. We analyzed the impact on communication and the retrieved IMU values when blocking the communication signal by forcing it to a high state. The resulting communication signals and retrieved values are shown in Fig. 5 and 7.

Blocked SDA channel: The garbage value was transferred to the control unit immediately, and communication was interrupted by maintaining the garbage values. This result is logically consistent with the following protocol characteristics: I2C communication with a change in the SDA from high to low and later requires other appropriate signals (*e.g.*, the ACK signal for address verification, command bit verification, and data transmission). Hence, communication could not progress with high-state SDA signals.

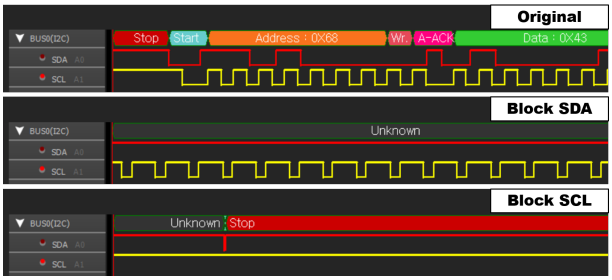

Fig. 5: I2C signals without blocking (first), blocking SDA (second), and SCL (third) channels as high. The communication cannot progress while any communication channel is blocked.

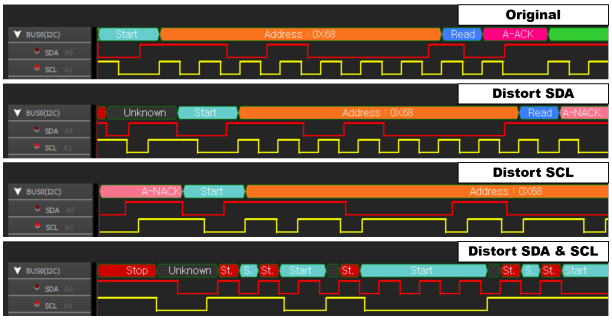

Fig. 6: I2C signals without disturbance (first), disturbed on SDA (second), SCL (third), and both channels (fourth). The communication suddenly stops its progress when the communication channels are disrupted.

Blocked SCL channel: I2C communication was interrupted immediately, while the control unit continuously received garbage values. The control unit and sensor sent and received SDA signals according to the change in the state of the SCL signals. However, if the forced high-state SCL persisted, unintended signal readings would occur, resulting in the interpretation of garbage values. Subsequently, the communication was suddenly terminated when SDA changed from low to high.

Distorting a benign signal. Furthermore, we analyzed the effect of channel distortion by injecting an external signal into the communication channel. By directly injecting an unsynchronized external signal that was generated by an additional Arduino-IMU I2C communication, we analyzed the effect of channel distortion. Thus, the injected signal had the same frequency and voltage level as the target SDA and SCL signals. Once the signal was injected, the communication signal was partially corrupted, thereby resulting in distortions in I2C communication. Figure 6 and 7 show the results of the retrieved IMU values and communication signals.

Disturbed SDA channel: The control unit received arbitrary data, and communication was disrupted. When uninterpretable or distorted address, read/write, and response bits occurred, communication was interrupted. This is illustrated by the sudden peak in Fig. 7. In addition, the control unit received unpredictable data values when data bit flips occurred during communication or garbage values were written to registers.

Disturbed SCL channel: During a temporary interruption in communication, the control unit received IMU data that fluctuated considerably. Additionally, we discovered data transmission distortion and abnormal communication. This is because I2C operation, SDA transmission, and reception depend on the state of the SCL signal.

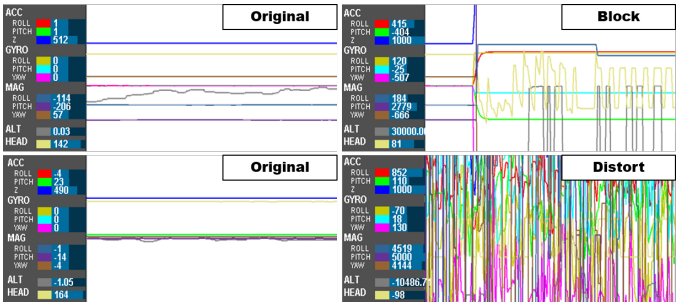

Fig. 7: Control unit receives corrupted IMU data when communication signals are blocked (top) and disturbed (bottom).

Disturbed both SDA and SCL channels: We observed a considerable abnormal data transfer and a temporary communication interruption while SCL and SDA signals were disturbed. In this case, abnormal communication occurred owing to the SDA and SCL distortion co-occurred, which resulted in more data transmission interruptions and bit errors than in the two previous cases. This caused a more substantial fluctuation in the IMU values (IMU-1 video [3]).

B. Analysis of SPI Corruption

We investigated the SPI protocol using fault injection approaches as in the I2C protocol evaluations. Here, we briefly share the overall experimental results since they are similar to those of the I2C protocol. Please refer to §A1 for more details.

We discovered that corruption in the four channels (*i.e.*, SS, MOSI, MISO, and SCLK) led to critical errors in the retrieved data. Specifically, distortions in the SS signals, which were used in selecting a communication endpoint, caused the sensor to misrecognize the transmitted signals from the control unit, although the communication signals of the other three channels were operating normally. Further, corruption in the MOSI and MISO signals, which provide data transmission between the sensor and the control unit, hindered the proceeding of communication signals. Additionally, the corrupted SLCK signals resulted in the incorrect interpretation of the MOSI and MISO signals. Consequently, distortions in the four channels (*i.e.*, SS, MOSI, MISO, and SCLK) led to critical misinterpretations.

In conclusion, we empirically discovered that corruption in I2C and SPI communication channels could trigger serious error propagations to the system, even with intentional partial distortions.

V. EMI Injection on Communication Channels

As shown in §III and §IV, the distortion in the communication channel between the sensor and control unit causes a serious failure in the drone's attitude control. In this section, we investigate whether remote EMI signal injection can effectively induce distortion in communication channels. In particular, we experimentally investigated the following: 1) We showed the feasibility of a remote attack by revealing that an EMI signal injection on a control unit corrupts every IMU sensor value from a distance. Additionally, we conducted physical shielding and near-field evaluations to show that the POE for the EMI injection is the control unit, and not the IMU or wire. The remaining investigations in this section focus on the details of this attack. 2) Particularly, to determine the effective EMI frequencies that could be employed in this attack, we examined the near-field of the control unit board and the induced voltage amplitude. This enabled us to identify the frequencies that are susceptible to EMI signal injection for each board. 3) For each control unit, we injected the EMI signal at the frequency selected in step 2). Further, we measured the voltage level to see if the injection caused bit flips in the communication channel. 4) We investigated how communication and retrieved sensor values got corrupted by an EMI signal injection.

A. Experimental Setup and Targets

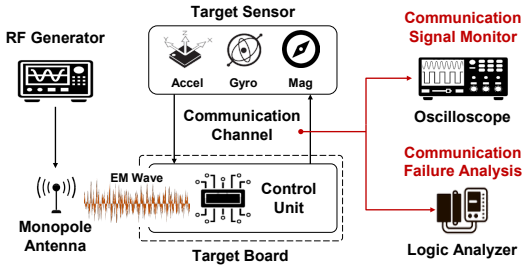

Fig. 8: Experimental setup of the EMI injection.

To determine the susceptible frequencies for effective EMI injections, we examined the control unit's EMI emissions at different frequencies and the degree of channel distortion between the control unit and IMU sensor during EMI injection. Note that we used five boards (Arduino Uno, Arduino Mega, Arduino Nano, Pixhawk4, and DJI Mavic Pro) and six IMUs (MPU6050, MPU6500, MPU9150, MPU9250, L3G4200D, and L3GD20) for evaluation. The IMU sensor used for the experiment is a commercial drone-typical IMU. Specifically, we measured the EMI emission of the control unit using a near-field EMC scanner [19] on five boards in a shielded chamber. The setup for near-field measurements is discussed in Fig. 26. This is a representative method for determining the EMI injection path and susceptible frequency, which includes measuring the intensity and frequency components of the EMI emission generated from the target board [23]. Additionally, we measured the communication signal voltage by varying the injected EMI frequency with six IMUs and five boards. Through this, we show that the EMI susceptible frequencies are board-dependent.

We conducted the majority of our experiments using Arduino boards for the following reasons: First, the high versatility of Arduino enables us to inject arbitrary signals into the communication channel, directly measure the channel's communication signal, decode it according to the protocol, and observe it at the packet level. Additionally, they support both I2C and SPI protocols with high connectivity and can be connected with various IMU sensors. Note that "Pixhawk4" and "DJI Mavic Pro", which are representative commercial drone control boards, do not allow any IMU sensor replacement. In the case of DJI, analyses and measurements were not possible without irreversible disassembling (Fig. 25).

For an EMI signal injection, we employed a monopole antenna and an RF generator that produced a 100 mW output. During the injection, we monitored the change in communication signals between the target IMU and control unit board using an oscilloscope and a logic analyzer (Fig. 8).

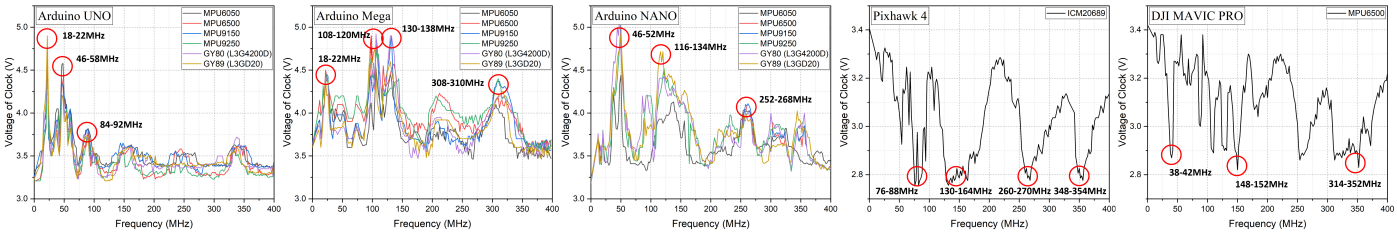

Fig. 9: Evaluation of the EMI susceptibility of the control unit board connected with multiple IMU sensors. Notably, the idle communication signal for the Pixhawk4 and DJI boards is low, while that for Arduino boards is high.

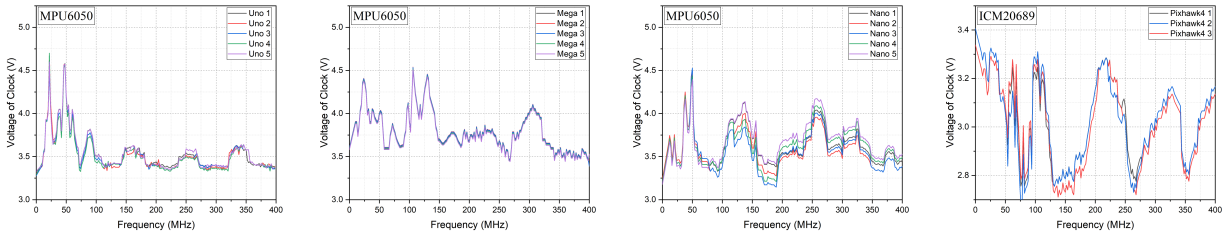

Fig. 10: Evaluation of the EMI susceptibility of the multiple control unit boards given a fixed IMU. The results show that manufacturing process errors have little impact on the susceptible frequency.

B. Attack Feasibility and Point of Entry

In this section, we investigate whether 1) the IMU sensor values could be corrupted by an EMI signal injection, and 2) the POE of this EMI signal injection is the control unit board. POE refers to a specific component of a circuit in which EM waves make EM coupling, which is described in §II-D along with the circuit. This investigation is a major challenge in electromagnetic research [79], which is used to identify the paths of EMI couplings to prevent and eliminate them.

First, we showed that the IMU value retrieved by the control unit could be significantly corrupted by remote EMI injection (IMU-2 video [3]) on the target communication comprising the IMU and Arduino board. Further, we validated the POE of the EMI signal injection via partial shielding with aluminum foil, which is a common method [34], [40]. Consequently, we discovered that the control unit board is POE through the following:

- Shielding on connecting wires and IMU sensors (IMU-2-2 video [3]): Despite the shielding, IMU values were still corrupted. This shows that the POE of EMI is not the IMU sensor or wire.
- Shielding only part of the control unit board (IMU-2-1 video [3]): Unlike the shielded connection wiring and sensors, EMI injection at a very short distance (3 cm) using the RF generator (100 mW) did not result in the interpretation's distortion of the IMU sensor values.

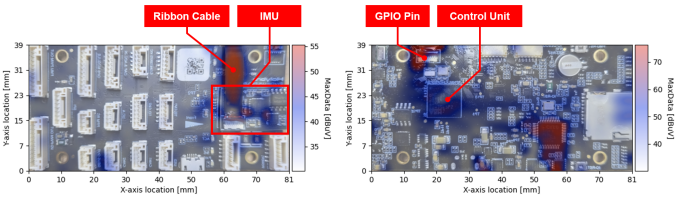

Fig. 11: EMC scanner measurement results of the front (left) and back (right) of the Pixhawk4 board. We confirmed that an EMI path exists between the control unit and the IMU.

In addition, EMC scanner measurements confirmed that the control unit board's processor and GPIO pins could serve as EMI paths. By utilizing this path, we could distort the communication channel between the control unit board and IMU (Fig. 11). These results indicate that the control unit can unintentionally act as an antenna for EMI injection.

C. Finding Susceptible Frequencies

In this section, to determine the effective frequency for the remote attack, we examined the EMI susceptibility of the control board at different frequencies.

In particular, we examined the intensity and frequency of EMI emitted from each control board using an EMC scanner. With this measurement, we confirmed that the control board's EMI is dominant at frequencies below 400 MHz, which means it can act as an antenna in this band. Next, we measured the susceptibility of the control unit board to the frequency of the injected EMI signal using various combinations of the control unit and IMU sensors. We used three sets of five Arduino boards, six IMU sensors, and three Pixhawk4 boards to evaluate the effects of manufacturing errors on EMI susceptibility at the same time.

The evaluation results are shown in Fig. 9 and 10. We found that EMI injection at susceptible frequencies of the control unit board causes distinct voltage level changes in the communication signal (Fig. 9). Even when different IMUs were connected, the tendency of voltage change according to the injected EMI frequency was maintained. This means that the susceptible frequency mainly depends on the control unit board model, while the amplitude of the induced voltage differs depending on the sensor model and board model. Additionally, the effect of manufacturing process errors on the determination of the susceptible frequency is negligible (Fig. 10).

D. Channel Distortions upon EMI Injection

We examined the voltage change of the communication signal to evaluate the influence of the EMI injection at susceptible frequency into the control unit board. Using the same experimental setup as §V-C, we analyzed the signal

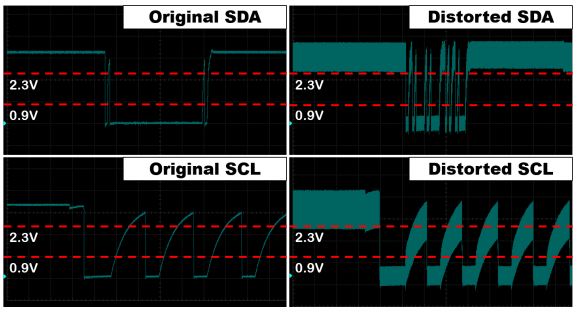

Fig. 12: Waveform of the SDA (top) and SCL (bottom) signals of I2C communication without (left) and with (right) an EMI injection.

distortion induced by EMI injection. This is because the retrieved IMU sensor values are a series of bits determined solely based on the communication signal's voltage. Voltages of benign I2C communication signals range between 0 and 3.3 V, while 0.9 and 2.3 V are transition thresholds. Hence, the bit interpretation changes from 1 to 0 when the voltage falls below 0.9 V. When the voltage level exceeds 2.3 V, its interpretation simultaneously changed from 0 to 1. Due to the protocol's design, voltage coupling in the communication signal causes unintended voltage transitions, which resulting in arbitrary bit flips.

The distorted shape of the communication signal when additional voltage signals were transmitted to the benign communication signals is shown in Fig. 12. Here, two problems can occur in interpreting the communication signals. First, the bit flips that occur unintentionally in the SDA signal might cause data distortion. Additionally, unintended bit flips in the SCL signal can distort the interpretation timing of the SDA signal.

Similar to I2C, the bit string in SPI communication is determined by the voltage of the communication channel. We also conducted a similar experiment on the control unit board of Pixhawk4 and DJI Mavic Pro, which are representative commercial drones that use SPI. We discovered that injecting EMI signals of 10 and 21 W into each of these two boards caused voltage distortion in the communication signal, resulting in the unintentional interruption of communication and distortion of data. Further evaluations are described in §V-E.

E. Retrieved IMU Values upon EMI Injection

In this section, we examine the aspects of the retrieved IMU sensor data by the control unit that communicates based on distorted signals due to the EMI injection.

Arduino. We discovered that communication signal distortions caused by EMI injection of 100 mW output power propagated without filtering and were interpreted as unintended packets on the Arduino Uno, Nano, and Mega (Fig. 14). We also revealed that these packets eventually caused considerable fluctuations in the sensor values, which were retrieved by the control unit (Fig. 13). These fluctuations are comparable to the distortion caused by fault injections (Fig. 7).

In particular, we discovered that the occurrence of A-NACK (address-NACK) and UNKNOWN packets, the unexpected occurrence of start and stop packets in the middle of regular packets, and temporary communication interruptions were induced by EMI injection. Additionally, read/write and the data packets were corrupted, causing the control unit to read or write garbage values to the sensor registers.

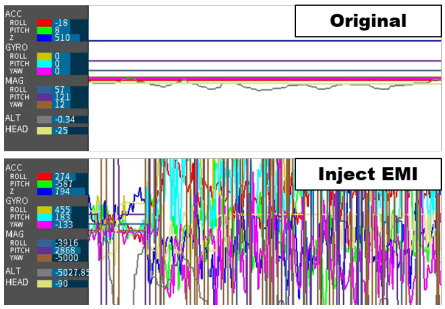

Fig. 13: Control unit retrieves extremely corrupted IMU data after EMI injection.

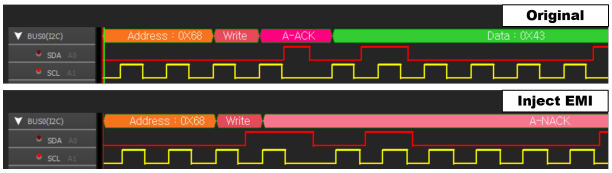

Fig. 14: I2C signals without (top) and with (bottom) EMI injection. Irregular intervals and glitches caused misinterpretations at the packet level.

Pixhawk4. Conversely, with the 100 mW output, the EMI injection could not sufficiently distort the communication signal in the control unit of Pixhawk4 and DJI drones. Hence, we evaluated the required voltage changes for an attack on the Pixhawk4 board and conducted additional experiments using a high-power experimental setup to determine the required attack power (Fig. 27).

- First, when a sufficient additional voltage was applied to the benign communication signal of the Pixhawk4 board using a connected ribbon cable, the interpretation of the IMU sensor value on the Pixhawk4 board was considerably corrupted (Fig. 15).
- Subsequently, we confirmed that an induced voltage of 0.1128 V was derived from the Pixhawk4 board's communication signal for every 3 dB EMI injection (approximately 2 mW). Based on the aforementioned, the estimated power required for an attack from a distance of 10 cm was 41 dBm (approximately 12.6 W).
- Based on the aforementioned estimation, we conducted a communication channel distortion experiment on the Pixhawk4 board at a distance of 10 cm using an amplifier. In this experiment, we increased the EMI output by 2 mW and confirmed that at 10 W output, an SPI communication error occurred due to the distortion of the SS signal of SPI (§IV-B). This error caused a sustained data link loss during the communication.

DJI. The DJI Mavic Pro drone comprises two boards, one for debugging and the other for flight control. To directly observe the communication signal between the IMU sensor and board, it is important to identify the communication signal pin on the flight control board (Fig. 25). Furthermore, both boards must be physically separated, which is irreversible, to accomplish this. Consequently, it is challenging to observe the interpretation

Fig. 15: IMU data from the Pixhawk4 board when a 1.44 V voltage is added to the benign clock signal.

of sensor values while measuring the communication signal. Due to the aforementioned, with the same basis (1.44 V) as the Pixhawk4 board, we estimated the power requirements that would cause considerable distortions in the retrieved IMU values on the DJI board at a distance of 10 cm.

- First, when applying a similar experiment as Pixhawk4, we measured the communication signal using the pin of the DJI board and confirmed that a voltage of 0.10152 V was induced for every 3 dBm of EMI injection.
- Based on the aforementioned, the estimated power required for an attack from a distance of 10 cm was 44.8 dBm (30.357 W).
- We conducted a further communication channel distortion experiment using an amplifier. In this experiment, we increased the EMI output by 2 mW and confirmed that the induced voltage level at 21 W of output was 1.44 V.

Difference in EMI susceptibility. We discovered through the aforementioned experiments that the required EMI power for communication channel distortion on commercial drone boards is greater than that on Arduino boards. Moreover, we experimentally confirmed that Arduino is more susceptible to EMI than commercial boards by observing the patterns and intensities of EMI emissions from each control board using a near-field EMC scanner [19]. The result shows that Arduino emits 19 dBuV more EMI on average than commercial boards, which means that Arduino is more vulnerable to EMI in that band. Concerning the EMI coupling path, we discovered that the commercial board had only a controller-IMU path, whereas the Arduino had more comprehensive paths, including a controller-GPIO-IMU path (Fig. 11 and 23).

This difference derives from the fact that commercial drone boards should adhere to the elcetromagnetic sensitivity (EMS) standard [78]. It is a mandatory standard applied to products used in industrial applications to prevent EMI from causing serious problems in the design and operation of electronic and electrical devices. However, academic devices, such as Arduino boards, are not required to follow the EMS standard, making them more susceptible to EMI than commercial boards [39].

In particular, the following three considerations are not sufficiently reflected on Arduino: 1) Electric circuits need to be isolated from EMI sources including power, transmitters, and oscillators, while the Arduino board has two or more VDD pins, and each pin shares the clock signals. 2) EM coupling paths should be blocked and minimized. However, Arduino utilizes fewer decoupling capacitors (which mitigate the influence of EM emission from the sources) than commercial boards. 3)

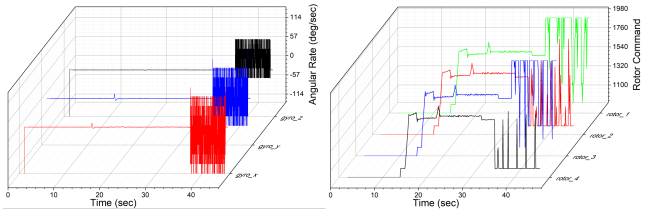

Fig. 16: Graph of PX4 SITL attack evaluation logs. When our attack corrupts the IMU data (left), it is fed into the PID control loop, resulting in corruption of the rotor command (right).

Connection noise between the emitter and circuits should be removed [43]. However, Arduino connects the control unit and the IMU sensor via wire which is more susceptible than a ribbon cable.

VI. Attacking Drones with EMI Injection

In §IV, we investigated if the communication signal distortion can cause considerable fluctuations in the retrieved IMU values. Further, in §V, we confirmed that the adversary could remotely distort the communication signal using an EMI injection at the susceptible frequency of the control unit board. In this section, we evaluate the practical implication of our attack on the control logic and behavior of a drone system. For this, we conducted both simulations as well as real-world experiments using physical drones. We confirmed that when the remote EMI was injected, the errors from distorted sensor data were effectively propagated to the drone's attitude control algorithm, resulting in the instantaneous crash of the drone.

A. Attack Simulation with PX4 SITL

We used PX4 software-in-the-loop (SITL) to investigate how a fluctuating IMU data stream propagates into the rotor operation and its effects to evaluate the impact of our attack. Particularly, we implemented the fluctuating IMU data, which was induced by communication distortion, using customized sensor drivers that periodically updated the sensor data to the drone's control algorithm. Additionally, to repeatedly simulate our attack by varying the degree and timing of the corruption in IMU values, we added attack events and parameters to the messaging modules that controlled the PX4 SITL events (such as error, speed, and mode change).

Propagation validation. When we simulated our attack during flight, we updated the highly fluctuating gyroscope (IMU) values at the sensor driver stage (Fig. 16). In this simulation, we discovered that there is no filtering on the IMU value itself, meaning that the fluctuating values were transmitted directly to the attitude control algorithm without bias correction and scaling. In addition, we confirmed that when estimating the attitude, the EKF-based attitude controller even amplifies the fluctuations in sensor values.

Impact of attack evaluation. The PID control loop determines the incorrect rotor commands for attitude control based on the crucial fluctuations of gyroscope data. The control loop is designed to stabilize the drone by issuing opposite rotor commands that minimize the change in attitude estimated by the gyroscope data. Consequently, rotors 1 and 3 make maximum rotations to create a rising torque, while rotors 2 and 4 stop at the lowest rotational command, resulting in the tumbling and

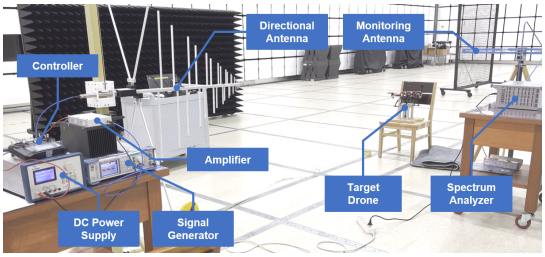

Fig. 17: Experimental setup of our attack using a hovering drone.

sudden fall of the drone (Fig. 16). Please see our attack demo (IMU-3 video: if our attack is launched on a drone hovering at 5.61 m, it crashes down to the ground within 1.07 sec [3]).

B. Attack Evaluation Using an Actual Drone

To demonstrate the impact of our attack on the sensing and actuation of drones without a gap between logic (emulation) and the actual world (e.g., the non-ideal condition of the hardware), we used an actual drone, which was built using the well-known open-source MultiWii flight control firmware and an MPU 6050. Additionally, we employed a hovering frame that enabled us to evaluate our attack without unwanted damages (e.g., broken arms) and allowed the hovering flight, which includes rotation in the x, y, and z-axis using a bearing ball structure. Our experimental setup for the actual drone evaluation is shown in Fig. 17.

Propagation evaluation. When the EM wave of a susceptible frequency was radiated to the real drone, the IMU data (gyroscope, accelerometer, magnetometer, and barometer) was corrupted immediately, as shown in Fig. 13. Since the drone's attitude control operates based on these values, the corrupted values made the rotors stop abruptly and rotate erratically. The following experiments determined whether the unintended rotor spin resulted from the EMI injection into the connecting wires or the propagation of the faulty IMU (PID control):

(i) **Rotor command evaluation.** In a stationary state (without starting rotors), an EMI injection caused the rotor command to fluctuate while the RC command remained unchanged. This indicates that EMI did not occur in the RC receiving wire, while the erratic rotor spin resulted from the command change, and not EMI (IMU-4 video: after 35 sec, the rotor commands (top right corner) fluctuated extremely [3]).

(ii) **Rotor spin evaluation.** We evaluated whether the rotation of the rotor corresponded to the rotor command. We confirmed that the rotors oscillated following the rotor command when the drone was fastened to the table, and EMI was injected during all rotor spins (IMU-5 video: this demo shows how rotors and their commands change upon an EM injection at 9 sec [3]).

Impact of attack evaluation. To demonstrate the impact of an attack on drones in less-than-ideal conditions, we used a hovering frame and injected EMI into a drone that was attached to our frame and hovering at distances of 0.44 and 2.4 m, respectively. When we injected EMI, the IMU value of the drone fluctuated instantly, as did the rotors, and some rotors even stopped temporarily. This erratic rotor rotation caused the drones to flip and neutralize their attitude control (IMU-6 and IMU-7 videos: as soon as the EM injection started, one of the rotors stopped, and hovering immediately stopped (the drone could have crashed) as well [3]). This rotor failure is a well-known hazard in drones (quadcopters and hexacopters), as a single rotor failure leads to catastrophic failures [28], [73]. In summary, through drone simulations, we discovered that our attacks corrupted IMU values without being filtered, leading to abnormal rotor behavior that eventually caused the drone to lose attitude control and fall. Further, we demonstrated that our attack remotely caused rotor failure on the actual drone, which is well-known as the root cause of the drone crash.

VII. Other Practical Considerations

In this section, we discuss some practical considerations required to expand our attack to the real-world environment. Specifically, we evaluated the power requirement at a practical attack distance based on real drones and simulation experiments and also suggested a potential attack scenario. Additionally, we carried out post-analysis of our attack propagation and response time.

A. Potential Attack Scenario

We validated the feasibility of EMI-based remote attacks on drones. In order to extend our attack to real-world environments, we present potential attack scenarios while maintaining the pre-defined attack assumptions (§III-A). First, the attacker detects and identifies the target drone using appropriate equipment such as radar or optical sensors. Then, the attacker obtains EMI susceptible frequencies and the required power for the identified target drone through a pre-built database. Lastly, the attacker aims a directional antenna at the target drone and, as soon as it enters the attack range, radiates malicious EMI to crash it.

For this attack, the attacker should satisfy the following requirements: 1) Signal-generating equipment including an RF signal generator [64], an amplifier [47] (about hundreds of kW), and directional antennas in the MHz band [66], 2) A module [13], [87], [95] that can detect and identify drones at a specified distance, and 3) A pre-built database that contains the required power based on the susceptible frequency and attack distance for each drone board by evaluating the drone boards in advance. Considering the aforementioned requirements, we suggest that one of the most promising applications would be a ground vehicle system with an EMI radiation module including a directional antenna and a radar module that can detect and identify drones (*e.g.*, THOR [41]).

B. Distance vs. Power

As aforementioned, our attack needs to know the power requirement for more practical applications, considering drones that are farther away than tens of meters. We used a real drone and ANSYS-HFSS [5], a well-known antenna simulation software, to determine the power requirements for a remote attack.

Actual drone experiments. To determine the required power over a distance, we measured the maximum distance at which the EMI could cause the retrieved IMU values to fluctuate considerably, along with varying the power of the RF generator (EMI). We discovered that a 100 mW EMI injection distorted the IMU sensor (MPU 6050) at 0.84 m on the target drone

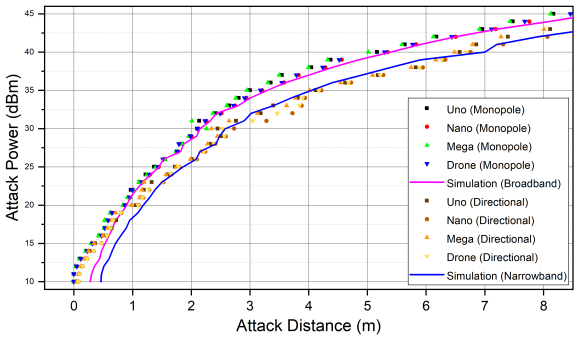

Fig. 18: Graph of the relationship between the power requirement and attack distance in our attack.

(IMU-7 video [3]). To evaluate the power requirements of a commercial drone's control unit board, a similar experiment was conducted in a shielded chamber using an EMI injection with 100 W (50 dBm) power and a directional antenna (Fig. 27). Particularly, we measured the attack distance (of the drone and control unit boards) according to the power with a monopole antenna and a directional antenna, while amplifying the output of the EMI injection from 10 dBm to 50 dBm by 1 dBm. In Fig. 18, we depict the measured power requirements to attack the drone and each board as a symbol. Based on the power-to-distance evaluation, we found that the smaller the area of an Arduino board, the more susceptible it was to EMI. This is because as the area of the board decreases, the EMI source and the GPIO pins on the board become closer, resulting in more EMI influence per area. Additionally, we found that the PX4 and DJI boards required 47 and 98 times more injection power compared to Arduino boards. In the case of the Pixhawk4, 100 W injection power was required at a distance of 0.5 m (IMU-8 video [3]).

Antenna simulation. In actual drone experiments, we measured the EMI power requirement using an EM field analyzer [50] which was able to induce IMU fluctuations. By using this power, we evaluated the minimum power required to induce severe fluctuations of the IMU values according to the change in the attack distance using ANSYS-HFSS simulation. For this estimation, we derived the relationship between the power requirements and attack distances. Particularly, the 7-430 MHz broadband monopole antenna model (a real-world experimental antenna specification) and narrowband monopole antenna were implemented. We estimated the required power based on the attack distance of 250 MHz. In Fig. 18, these are depicted by magenta and blue lines, respectively.

Our attack requires a lower attack power than the previous remote drone attacks, which distorted IMU data using a 3 W ultrasonic injection at 0.16 m [73]. Contrarily, we used a similar real drone to distort the IMU with approximately 22.19 mW power at this distance. Further, our attack is more critical to drones because it simultaneously distorts the gyroscope, accelerometer, and magnetometer, thereby making it hard to adopt a complementary sensor fusion that prevents drones from falling [14]. In addition, the EMI injection is more effective for long-distance attacks than ultrasound. The energy efficiency of the ultrasound over a longer distance is lower when the frequency of the waves grows higher [85].

For a more detailed investigation on the cost-effectiveness of our attack, we derived a relation between the power and distance and applied it to estimate the power requirements in long-range attack scenarios, such as military weapons[1]. Consequently, two relations were derived using farfield analysis and plot fitting of ANSYS HFSS: $y = 471x^2 - 702x + 324$ (Eq. 1) for a broadband antenna and $y = 320x^2 - 615x + 346$ (Eq. 2) for a narrowband antenna, where x is the attack distance in meters and y is the required power in milliwatts at distance x. Since our attack requires a narrow frequency band including the susceptible frequency, we estimated the power requirement for our attack at 100 m using Eq. 2.

Consequently, the power requirement to attack a drone using the Arduino Nano board at 100 m was estimated at 3.148 kW, whereas the power requirement to attack a drone using the Pixhwak4 and DJI boards was estimated at 147.756 and 310.70 kW, respectively. These results show that our attack is considerably more power-effective compared to the conventional anti-drone EMP weapons since they use 333 MW to 100 GW for similar distances [41], [46], [51], [63].

Algorithm 1: Simplified inner PID loop algorithm for drone attitude control.

Input: Target angle for 3 axes from the outer PID.
Input: Gyroscope data for 3 axes from the IMU raw data.
Input: Thrust command for 3 axes from the RC (remote controller).
Output: Rotor command.
Initialization;
KP, KI, and KD: pre-defined P (proportional), I (integral), and D (differential) gains for 3 axes;
dT = Sampling time;
while *True* **do**
  Read angular rate data from the gyroscope for 3 axes;
  Receive data from the transmitter for 4 channels (3 axes and throttle);
  for *axis* **do**
    $Error = Target_{angle}[axis] - gyro[axis]$;
    $P = Error \times KP[axis]$;
    $Error_{Integrated} = Error_{Integrated} + Error$;
    $I = Error_{Integrated} \times KI[axis] \times dT$;
    $delta = gyro[axis] - gyro_{prev}[axis]$;
    $gyro_{prev}[axis] = gyro[axis]$;
    $D = delta \times KD[axis] \backslash dT$;
    $PID_{ctrl}[axis] = P + I - D$;
  end
  for *rotor* **do**
    for *axis* **do**
      $Rotor_{ctrl}[axis] = Thrust_{ctrl}[throttle] + PID_{ctrl}[axis]$;
    end
  end
  return `Mixer`(*rotorCtrl[rotor], MIN, MAX*); Scaled rotor command within the $MIN(1,000)$ and $MAX(1,850)$ values;
  Actuate rotors;
end

C. Post Analysis of Our Attack

In this section, we present an algorithmic analysis to show that our attack affects rotor commands to be anomalous (within only one cycle). Rotor commands are determined through the inner PID, as explained in Fig. 3.

Algorithm 1 describes the detailed operation of the inner PID from the IMU values to rotor commands in representative open-source drone firmware [6], [49], [58]. Here, the inner PID takes a gyroscope value and target angle to calculate the rotor

[1]THOR dropping the hammer in drones (https://youtu.be/Ogi_o8dszrk?t=75).

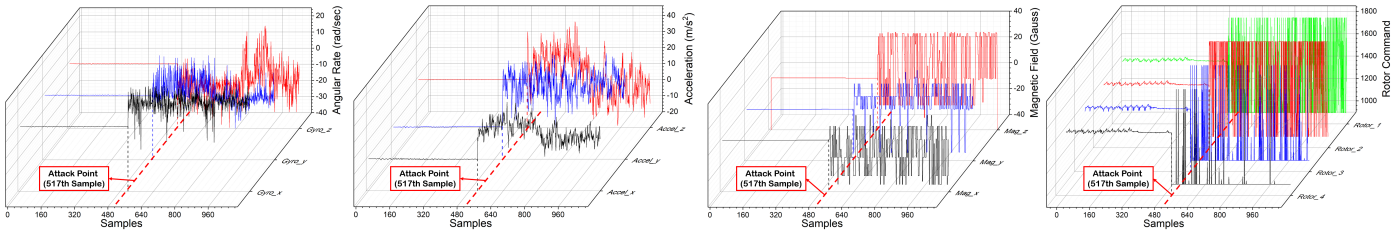

Fig. 19: Illustrations of the IMU sensor values and rotor commands when the EMI signal is injected. All IMU sensor values significantly fluctuate right after the attack (517th sample). Additionally, all rotor commands are significantly affected right after the corruption of the IMU sensor values (517th sample). For example, rotor 4's command immediately drops to 1100, lowering its speed to its minimum (stop). It indicates that our attack corrupted IMU values, affecting rotor commands immediately.

commands. The target angle is affected by the accelerometer, magnetometer, and barometer values. It has previously been presented that affecting the gyroscope values can directly influence the rotor commands [73]. However, since our attack fluctuates both the inputs of the inner PID and the estimated attitude by affecting all the IMU sensor values while the previous work did not, the propagated influences on the rotor commands are larger and more severe. Specifically, all the terms from lines 8–15 are affected by the corruption in the two inputs, target angle and gyroscope values. Moreover, the $Error$ term can be fluctuated more significantly by our attack than by distorting only gyroscope values by previous works. Additionally, our attack may need only a short period to affect the drone's rotor commands very quickly, as the error in the IMU values determines the rotor commands right inside the current loop.

To investigate it experimentally, we applied our attack to a real drone while it was hovering, and then compared the sensor values and the rotor commands simultaneously. The result that logs the sensor values and rotor commands with a 0.025 sec interval are shown in Fig. 19. Consequently, we discovered that our attack considerably caused the rotor commands to fluctuate within a single window (0.025 sec) after corrupting the sensor value. It is noteworthy that at least one rotor has almost stopped spinning. From a control point of view, the failure of one or more rotors of a multi-copter will lead to a drone crash [48], [74], [76], [77].

In summary, we analyzed how our attack effectively and rapidly corrupted the rotor commands at the algorithm level and discovered that the rotor commands were significantly affected within a very short time (0.025 sec) during real drone experiments.

VIII. COUNTERMEASURES

In this section, we present mitigations against our attack on drones. Since our attack corrupts the communication channels via which the sensor value is transmitted from the sensor to the control unit, existing mitigations using dummy sensor circuits [83] and EMI injection detection [94] at the analog circuit level are not effective against our attack.

Detection. Several studies presented attack detection methods for drones. Choi *et al*. suggested that GPS and gyroscope attacks could be detected using a control invariant-based detection, wherein invariant refers to a criterion for distinguishing abnormal changes from normal changes in the state of the drone in a standard control [15]. Additionally, Quinonez *et al*. presented a physical attack detection framework that detects attacks by monitoring the accumulative difference between predicted and measured values using non-linear prediction [60]. However, since the former requires an attack detection window of 80 samples and the latter needs an additional processing time of 0.2 sec for non-linear prediction, their time constraint makes it challenging to prevent our attacks.

Recovery. Several studies suggested that attacks on drones can be recovered or replaced to maintain a stable flight [4], [14], [22], [84], [92], [93]. Choi *et al*. proposed a detection and recovery framework that uses a system model that converts an attacked sensor into a software sensor upon detecting a sensor attack [14]. In addition, Fei *et al*. showed that through reinforcement learning, drones could hover even in bias attacks on a gyroscope using additional feedback control commands [22]. Zhang *et al*. proposed a detection and control algorithm that rolls back to the sensor value in the pre-attack state when a sensor attack is detected [93].

However, these methods could not recover drones from our attack since our attack requires a very short time of less than a single sampling time (0.025 sec) to crash the drone (Fig. 19). Choi's method requires 230 samples (0.575 sec) to detect attacks and an additional benign acceleration sensor is also necessary. Furthermore, Fei's and Zhang's techniques require additional computations of at least 0.2 and 1 sec for additional control algorithms.

Shielding. Finally, to protect the drone from our attack, we blocked the injection rather than the impact of EMI. Metal shielding, one of the traditional countermeasures, is well-known to be an effective mitigation against EMI signal injection attacks [34], [40], while most drones employ light carbon fiber cases. Shielding increases the power required for an effective EM injection by reducing the influence of EMI. As shown in §V-B (IMU-2-2 video [3]), shielding the control unit using aluminum foil is an effective countermeasure. However, although metal shielding can effectively reduce the impact of EMI injection, the following should be considered when using it in drones: First, metal shielding is more expensive than plastic shielding when applied to drones. Additionally, it can interrupt important wireless communication between drones and other systems, such as companion computers and remote controllers. Further, the control unit board cannot be entirely shielded since it can heat up and thus reduce the performance of circuit components, such as the clock, switching or flash memory, and power consumption [18]. Importantly, a magnetometer, which is one of the IMU's four sensors, is extremely sensitive to adjacent metals. Therefore, metal shielding on drones may interfere with the operation of the IMU sensor, thereby leading

to unstable attitude control.

IX. LIMITATIONS AND FUTURE WORK

Further EMI injection experiments. We discovered that a drone could be remotely crashed by distorting the communication channel of the drone's sensing system using the EMI signal injection. Although we have demonstrated the feasibility of the attack at an academic level, we have not implemented and conducted end-to-end long-range testing in the field, which requires EMI radiation of hundreds of kW or more and other evaluations that require government permission. Instead, we inductively revealed that PX4 and DJI drones could be remotely crashed through experiments on various popular boards and estimated the power requirement to do so. Further, EMI signal injection experiments to make the crash commercial drones over a long-range have been left as future work.

Consideration of unintended effects of EMI injection. Since our ultimate goal is to cause the drone to crash to the ground, we focused on the effect of the EMI signal injection on the communication channel. However, the control unit board performs various roles other than receiving IMU values, including post-processing, calculating the main control algorithms for the drone, and communicating with sensors other than the IMU. Hence, the EMI signal injection into the control unit board may affect components related to the drone control other than communication between the control unit and IMU sensor. This research is beyond the scope of our study because it requires detailed circuit-level analysis on the control unit board and verification in terms of electricity. This part is also left for future work.

Applying attacks on other sensors and applications. Since our attack distorts the communication channel with the sensor by using the EMI signal injection into the control unit board, it could be applied to other sensors and applications. We revealed the attack's feasibility for CMOS image sensors (§A). Further, evaluations on other sensors as well as their influence on applications are left for future work.

X. RELATED WORK

In this section, we comparatively explain the potential cyber-physical attack vectors that can be used for anti-drone purposes.

Since sensors are essential for drones, various physical-layer attacks could be considered for anti-drone purposes. On the one hand, several studies have suggested a sensor spoofing attack, one in which an attacker manipulates the physical stimulus that a sensor is designed to detect [38], [72], [88], [90]. The GPS spoofing attack has been proposed as one of the most promising anti-drone technologies [30], [35], [53]. However, it causes collateral damages because it also affects the surrounding receivers. When lidars, radars, or camera sensors are used for SLAM (Simultaneous Localization And Mapping), objects could be spoofed by injecting their target stimulus [12], [56], [71], [89], [90]. However, only a limited number of commercial drones rely on the SLAM. On the other hand, other studies have focused on a side-channel attack, which can manipulate the sensor output with a non-target physical stimulus [75], [88]. In particular, malicious acoustic wave injection corrupts the IMU sensor's measurements, resulting in the distortion of the drone's attitude control [73], [80], [81]. Owing to the use of acoustic waves, the attack distance is limited. Furthermore, a few studies have presented sensor attacks using malicious EMI injection. These EMI studies can be classified into attacks on the physical quantity measurement process, the signal processing mechanism of a sensor, and communication between the sensor and control units (Table I). Among them, the signal processing mechanism has been targeted more because even a weak attack signal could successfully corrupt the original analog signal. Particularly, Kune *et al*. injected EMI into the wiring between the analog filter and analog-to-digital converter (ADC) [40]. Kasmi *et al*. showed that EMI injection could induce sound signals into microphones and voice commands into the voice assistant system [20], [34]. Additionally, EMI injection studies on CCD image sensors [37], temperature sensors [82], LCD touch screens [33], [44], and hall sensors [9] were presented.

TABLE I: Comparison between our study and previous EMI injection studies on target sensor, and target processes.

Paper	Sensor	Injection Type	Target Process		
			Phy.	Sig.	Com.
[37]	CCD Image Sensor	EM wave	○	●	○
[40]	Cardiac medical devices, Microphone	EM wave	○	●	○
[20], [34]	Microphone	EM wave	○	●	○
[82]	Temperature sensor	EM wave	○	●	○
[33], [44]	LCD touch screen	EM wave	○	●	○
[9]	Hall sensor	EM wave	○	●	○
[89]	Radar	EM wave	●	○	○
Our work	MEMS IMU, CMOS image sensor	EM wave	○	○	●

* physical quantity measurement (Phy.), signal process of sensor (Sig.), sensor-control unit communication (Com.)

Recently, some EMI studies that focus on communication signals on boards have been suggested. They are difficult to mitigate because it directly distorts the original signal itself, making it difficult to adopt existing mitigations that separate the original signal from the attack signal [83], [94]. Some studies have pointed out that communication between control devices is vulnerable to electrical resonance on the communication channel (wire) [16], [67], [68], [86]. In addition, an attack that manipulates servo motor operation by overwriting the PWM command signal sent from the controller to the actuator in the same way has been proposed [17]. They demonstrated the feasibility of remote manipulation on servomotors through evaluations of fixed-wing drone.

However, the authors acknowledge that their attack is difficult to apply to brushless DC motors with electronic speed controllers (ESC) that prevent PWM signal distortion. Therefore, it cannot be applied to multi-copter and VTOL UAVs with BLDC motors. In terms of anti-drone solutions, our approach overcomes these limitations and is more power-efficient, effective, and difficult to mitigate than theirs. Specifically, our approach is more generalizable since our target is the digital circuits of IMU sensors and the control unit, which are necessary components in any drone. In addition, their power requirement is higher than that of our work. At the 2.4 m attack distance, their work needs more than 10 kW, while ours needs 12.6 W. Moreover, to implement their attack, the attacker should know the length of the wire between the ESC and controller, which might differ even in drones of the same model. However, our approach utilizes the susceptible frequency, which is mainly determined by the model of the control unit, which is varies less than the wire length.

Lastly, EM attacks, which utilize high-power ultra-wide-band signals to damage the victim's circuitry, have also be

considered [8], [10], [21], [26], [52], [54], [57], [61], [62], [69]. In contrast to our approach, these methods employ broad-band attack signals, resulting in collateral damage (direct impact on an ally's drone as well) while requiring significant energy (MW to GW scale).

XI. CONCLUSION

Herein, we presented an EMI injection attack on the communication channel between the IMU and control unit, that immediately causes a drone to crash to the ground. Compared to popular anti-drone technologies, our approach has several advantages: 1) The attack frequency depends on the control unit board, thereby allowing the attacker to target a particular type of drone while reducing the collateral damage from existing ones and 2) The attack immediately incapacitates the drone, thereby making it difficult to detect and mitigate. Detailed analyses of effectiveness, efficiency, and countermeasures suggest that the proposed attack could be used as a future anti-drone technology. Future research will focus on long-range experiments with advanced hardware and potential mitigation without side effects.

XII. ACKNOWLEDGEMENT

We sincerely appreciate the anonymous reviewers for their valuable comments and suggestions. This work was supported by the National Research Foundation of Korea (NRF; Grant No. 2020M3C1C1A0108452413, Anti-jamming and unauthorized unmanned vehicle detection and response technology development for unmanned vehicle security), Air Force Office of Scientific Research (Grant no. FA2386-20-1-4041). and Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT; Grant No. 2020-0-01202)

REFERENCES

[1] "Drone falling demonstration with our attack at 0.44m," https://youtu.be/8okgfRUSR5Q.

[2] "Drone falling demonstration with our attack at 2.4m," https://youtu.be/7LN8quYFThI.

[3] "Paralyzing Drones via EMI Website," https://sites.google.com/view/paralyzing-drones-via-emi.

[4] F. Akowuah, R. Prasad, C. O. Espinoza, and F. Kong, "Recovery-by-learning: Restoring autonomous cyber-physical systems from sensor attacks," in *2021 IEEE 27th International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA)*, 2021, pp. 61–66.

[5] "Ansys HFSS," https://www.ansys.com/products/electronics/ansys-hfss.

[6] "ArduCopter," https://ardupilot.org/copter.

[7] "Ardupilot codebase," https://ardupilot.org/dev/docs/code-overview-sensor-drivers.html.

[8] M. Bäckström, "HPM testing of a car: A representative example of the susceptibility of civil systems," in *13th International Zurich Symposium Supplement*, 1999, pp. 189–190.

[9] A. Barua and M. A. Al Faruque, "Hall spoofing: A non-invasive dos attack on grid-tied solar inverter," in *29th USENIX Security Symposium (USENIX Security 20)*, 2020, pp. 1273–1290.

[10] J. Bohl, R. Stark, and G. Wollman, "RF-weapons for non lethal interference and destruction of communication, information and electronic systems," in *Proceedings of the 3rd European Symposium on Non-Lethal Weapons, Ettlingen, Germany 10-12 May 2005*, 2005.

[11] I. Chahine, M. Kadi, E. Gaboriaud, A. Louis, and B. Mazari, "Characterization and modeling of the susceptibility of integrated circuits to conducted electromagnetic disturbances up to 1 GHz," *IEEE Transactions on Electromagnetic Compatibility*, vol. 50, no. 2, pp. 285–293, 2008.

[12] R. Chauhan, *A platform for false data injection in frequency modulated continuous wave radar*. Utah State University, 2014.

[13] Y. Chen, P. Aggarwal, J. Choi, and C.-C. J. Kuo, "A deep learning approach to drone monitoring," in *2017 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*. IEEE, 2017, pp. 686–691.

[14] H. Choi, S. Kate, Y. Aafer, X. Zhang, and D. Xu, "Software-based realtime recovery from sensor attacks on robotic vehicles," in *23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2020)*, 2020, pp. 349–364.

[15] H. Choi, W.-C. Lee, Y. Aafer, F. Fei, Z. Tu, X. Zhang, D. Xu, and X. Deng, "Detecting attacks against robotic vehicles: A control invariant approach," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018, pp. 801–816.

[16] G. Y. Dayanıklı, A. Z. Mohammed, R. Gerdes, and M. Mina, "Wireless manipulation of serial communication," in *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*, 2022, pp. 222–236.

[17] G. Y. Dayanıklı, S. Sinha, D. Muniraj, R. M. Gerdes, M. Farhood, and M. Mina, "Physical-layer attacks against pulse width modulation-controlled actuators," in *31st USENIX Security Symposium (USENIX Security 22)*, 2022.

[18] P. J. Doriol, Y. Villavicencio, C. Forzan, M. Rotigni, G. Graziosi, and D. Pandini, "EMC-aware design on a microcontroller for automotive applications," in *2009 Design, Automation & Test in Europe Conference & Exhibition*. IEEE, 2009, pp. 1208–1213.

[19] ERETEC, "RCE-40/25," http://www.eretec.com/bbs/content.php?co_id=5030.

[20] J. L. Esteves and C. Kasmi, "Remote and silent voice command injection on a smartphone through conducted IEMI: Threats of smart IEMI for information security," *Wireless Security Lab, French Network and Information Security Agency (ANSSI), Tech. Rep*, 2018.

[21] J. L. Esteves, E. Cottais, and C. Kasmi, "Unlocking the access to the effects induced by IEMI on a civilian UAV," in *2018 International Symposium on Electromagnetic Compatibility (EMC EUROPE)*. IEEE, 2018, pp. 48–52.

[22] F. Fei, Z. Tu, D. Xu, and X. Deng, "Learn-to-recover: Retrofitting uavs with reinforcement learning-assisted flight control under cyber-physical attacks," in *2020 IEEE International Conference on Robotics and Automation (ICRA)*. IEEE, 2020, pp. 7358–7364.

[23] R. Getz and B. Moeckel, "Understanding and eliminating emi in microcontroller applications. national semiconductor corporation," Application Note 1050, Tech. Rep., 1996.

[24] I. Gil and R. Fernández-García, "Characterization and modelling of EMI susceptibility in integrated circuits at high frequency," in *International Symposium on Electromagnetic Compatibility-EMC EUROPE*. IEEE, 2012, pp. 1–6.

[25] D. Giri and F. Tesche, "Classification of intentional electromagnetic environments (IEME)," *IEEE Transactions on Electromagnetic compatibility*, vol. 46, no. 3, pp. 322–328, 2004.

[26] D. Giri, F. 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.

[27] GLOBALBRANDS, "Top 10 drone companies in the world–2020," https://www.globalbrandsmagazine.com/top-10-drone-companies-in-the-world-2020.

[28] H. Hamadi, "Fault-tolerant control of a multirotor unmanned aerial vehicle under hardware and software failures," Ph.D. dissertation, Compiègne, 2020.

[29] Holybro, "Pixhawk4 Vision Kit," https://shop.holybro.com/px4-vision_p1225.html.

[30] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, P. M. Kintner *et al.*, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008)*, 2008, pp. 2314–2325.

[31] E. Jenn, J. Arlat, M. Rimen, J. Ohlsson, and J. Karlsson, "Fault injection into VHDL models: the MEFISTO tool," in *Predictably Dependable Computing Systems*. Springer, 1995, pp. 329–346.

[32] W. Jiang, G. Li, and T. Wang, "Research on Strong Electromagnetic Pulse Coupling of Radar Backdoor," in *2020 IEEE 9th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)*, vol. 9. IEEE, 2020, pp. 2171–2175.

[33] W. Jin, S. Murali, H. Zhu, and M. Li, "Periscope: A keystroke inference attack using human coupled electromagnetic emanations," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, 2021, pp. 700–714.

[34] C. Kasmi and J. L. 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.

[35] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *Journal of Field Robotics*, vol. 31, no. 4, pp. 617–636, 2014.

[36] S. Kim, J. Lee, J.-S. Choi, and J.-G. Yook, "Analysis of electromagnetic pulse coupling into electronic device considering wire and PCB resonance," in *Proc. Int. Symp. Antennas Propag.(ISAP)*, 2018, pp. 521–522.

[37] S. Köhler, R. Baker, and I. Martinovic, "Signal injection attacks against ccd image sensors," in *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*, 2022, pp. 294–308.

[38] S. Köhler, G. Lovisotto, S. Birnbach, R. Baker, and I. Martinovic, "They see me rollin': Inherent vulnerability of the rolling shutter in cmos image sensors," in *Annual Computer Security Applications Conference*, 2021, pp. 399–413.

[39] S. Kovář, V. Mach, J. Valouch, and M. Adámek, "Electromagnetic compatibility of arduino development platform in near and far-field," *International Journal of Applied Engineering Research*, 2017.

[40] 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 *2013 IEEE Symposium on Security and Privacy*. IEEE, 2013, pp. 145–159.

[41] U. A. F. R. Lab, "The tactical high power operational responder (thor)," https://www.airforce-technology.com/projects/tactical-high-power-operational-responder-thor-drone-killer-usa.

[42] S. Liu, X. Cheng, H. Yang, Y. Shu, X. Weng, P. Guo, K. C. Zeng, and Y. Yang, "Stars can tell: A robust method to defend against gps spoofing using off-the-shelf chipset," in *Proceedings of The 30th USENIX Security Symposium (USENIX Security)*, 2021.

[43] M. Mardiguian, *Interference control in computers and microprocessor-based equipment*. D. White Consultants, 1984.

[44] S. Maruyama, S. Wakabayashi, and T. Mori, "Tap'n ghost: A compilation of novel attack techniques against smartphone touchscreens," in *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2019, pp. 620–637.

[45] G. Masetti, S. Graffi, D. Golzio, and Z. M. Kovács-V, "Failures induced on analog integrated circuits by conveyed electromagnetic interferences: A review," *Microelectronics Reliability*, vol. 36, no. 7-8, pp. 955–972, 1996.

[46] S.-H. Min, H. Jung, O. Kwon, M. Sattorov, S. Kim, S.-H. Park, D. Hong, S. Kim, C. Park, B. H. Hong *et al.*, "Analysis of electromagnetic pulse effects under high-power microwave sources," *IEEE Access*, vol. 9, pp. 136 775–136 791, 2021.

[47] Mini-Circuits, "ZHL-5W-202-S+-Hig Power-Amplifier," https://www.minicircuits.com/WebStore/dashboard.html?model=ZHL-5W-202-S%2B%RFgenerator.

[48] M. W. Mueller and R. D'Andrea, "Relaxed hover solutions for multi-copters: Application to algorithmic redundancy and novel vehicles," *The International Journal of Robotics Research*, vol. 35, no. 8, pp. 873–889, 2016.

[49] "MultiWii," https://github.com/multiwii.

[50] NARDA, "ehp200-em-field-analyzer," https://www.narda-sts.com/en/selective-emf/ehp-200aac.

[51] G. Ni, B. Gao, and J. Lu, "Research on high power microwave weapons," in *2005 Asia-Pacific Microwave Conference Proceedings*, vol. 2. IEEE, 2005, pp. 4–pp.

[52] D. Nitsch, F. Sabath, H. Schmidt, and C. Braun, "Comparison of the high power microwave and ultra wide band susceptibility of modern microprocessor boards," in *Proc. 15th Int. Zürich Symp. EMC*, 2003, pp. 18–20.

[53] J. Noh, Y. Kwon, Y. Son, H. Shin, D. Kim, J. Choi, and Y. Kim, "Tractor beam: Safe-hijacking of consumer drones with adaptive GPS spoofing," *ACM Transactions on Privacy and Security (TOPS)*, vol. 22, no. 2, pp. 1–26, 2019.

[54] N. M. Parra, "Contribution to the study of the vulnerability of critical systems to intentional electromagnetic interference (iemi)," Ph.D. dissertation, Ecole Polytechnique Fédérale de Lausanne, 2016.

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

[56] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote attacks on automated vehicles sensors: Experiments on camera and lidar," *Black Hat Europe*, vol. 11, no. 2015, p. 995, 2015.

[57] W. D. Prather, C. E. Baum, R. J. Torres, F. Sabath, and D. Nitsch, "Survey of worldwide high-power wideband capabilities," *IEEE Transactions on Electromagnetic Compatibility*, vol. 46, no. 3, pp. 335–344, 2004.

[58] "PX4," https://github.com/PX4.

[59] "PX4 development guide," https://dev.px4.io/v1.10_noredirect/en/sensor_bus/i2c.html.

[60] R. Quinonez, J. Giraldo, L. Salazar, E. Bauman, A. Cardenas, and Z. Lin, "{SAVIOR}: Securing autonomous vehicles with robust physical invariants," in *29th USENIX Security Symposium (USENIX Security 20)*, 2020, pp. 895–912.

[61] W. A. Radasky and M. Bäckström, "Brief historical review and bibliography for Intentional Electromagnetic Interference (IEMI)," in *2014 XXXIth URSI General Assembly and Scientific Symposium (URSI GASS)*. IEEE, 2014, pp. 1–4.

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

[63] REPLEX, "T200-c," http://www.replex.co.kr/home/emp-gun/.

[64] Rohde & Schwarz, "SMB100A Microwave Signal Generator," https://www.rohde-schwarz.com/us/products/test-and-measurement/analog-signal-generators/rs-smb100a-microwave-signal-generator_63493-9379.html.

[65] H. Sathaye, G. LaMountain, P. Closas, and A. Ranganathan, "Semperfi: A spoofer eliminating gps receiver for uavs," in *Network and Distributed Systems Security (NDSS) Symposium 2022*, 2022.

[66] SCHWARZBECK, "570-vulb-9164-trilog-antenna," http://schwarzbeck.de/en/antennas/hybrid-ntenna/570-vulb-9164-trilog-broadband-antenna.html.

[67] J. Selvaraj, "Intentional electromagnetic interference attack on sensors and actuators," Ph.D. dissertation, Iowa State University, 2018.

[68] J. Selvaraj, G. Y. Dayanıklı, 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*, 2018, pp. 499–510.

[69] D. Serafin and D. Dupouy, "Potential IEMI threats against civilian air traffic," *Proceedings of the XXVIIIth URSI General Assembly*, 2005.

[70] G. Setti and N. Speciale, "Design of a low EMI susceptibility CMOS transimpedance operational amplifier," *Microelectronics Reliability*, vol. 38, no. 6-8, pp. 1143–1148, 1998.

[71] H. Shin, D. Kim, Y. Kwon, and Y. Kim, "Illusion and dazzle: Adversarial optical channel exploits against lidars for automotive applications," in *International Conference on Cryptographic Hardware and Embedded Systems*. Springer, 2017, pp. 445–467.

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

[73] 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)*, 2015, pp. 881–896.

[74] J. Stephan, L. Schmitt, and W. Fichter, "Linear parameter-varying control for quadrotors in case of complete actuator loss," *Journal of Guidance, Control, and Dynamics*, vol. 41, no. 10, pp. 2232–2246, 2018.

[75] T. Sugawara, B. Cyr, S. Rampazzi, D. Genkin, and K. Fu, "Light commands: laser-based audio injection attacks on voice-controllable

systems," in *29th USENIX Security Symposium (USENIX Security 20)*, 2020, pp. 2631–2648.

[76] S. Sun, G. Cioffi, C. De Visser, and D. Scaramuzza, "Autonomous quadrotor flight despite rotor failure with onboard vision sensors: Frames vs. events," *IEEE Robotics and Automation Letters*, vol. 6, no. 2, pp. 580–587, 2021.

[77] S. Sun, L. Sijbers, X. Wang, and C. de Visser, "High-speed flight of quadrotor despite loss of single rotor," *IEEE Robotics and Automation Letters*, vol. 3, no. 4, pp. 3201–3207, 2018.

[78] M. Tiegelkamp and K.-H. John, *IEC 61131-3: Programming industrial automation systems*. Springer, 2010, vol. 166.

[79] R. P. Tortorich, "A comprehensive study on printed circuit board backdoor coupling in high intensity radiated fields environments," Ph.D. dissertation, Louisiana State University and Agricultural & Mechanical College, 2021.

[80] 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)*. IEEE, 2017, pp. 3–18.

[81] Y. Tu, Z. Lin, I. Lee, and X. Hei, "Injected and delivered: Fabricating implicit control over actuation systems by spoofing inertial sensors," in *27th USENIX Security Symposium (USENIX Security 18)*, 2018, pp. 1545–1562.

[82] 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*, 2019, pp. 2301–2315.

[83] Y. Tu, V. S. Tida, Z. Pan, and X. Hei, "Transduction shield: A low-complexity method to detect and correct the effects of emi injection attacks on sensors," in *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, 2021, pp. 901–915.

[84] Z. Tu, F. Fei, M. Eagon, D. Xu, and X. Deng, "Flight recovery of mavs with compromised imu," in *2019 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*. IEEE, 2019, pp. 3638–3644.

[85] A. Vladišauskas and L. Jakevičius, "Absorption of ultrasonic waves in air," *Ultragarsas*, vol. 50, no. 1, pp. 46–49, 2004.

[86] D. A. Ware, "Effects of intentional electromagnetic interference on analog to digital converter measurements of sensor outputs and general purpose input output pins," Ph.D. dissertation, Utah State University, 2017.

[87] M. Wisniewski, Z. A. Rana, and I. Petrunin, "Drone model classification using convolutional neural network trained on synthetic data," *Journal of Imaging*, vol. 8, no. 8, p. 218, 2022.

[88] 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)*. IEEE, 2020, pp. 233–248.

[89] C. Yan, W. Xu, and J. Liu, "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle," *Def Con*, vol. 24, no. 8, p. 109, 2016.

[90] C. Yan, Z. Xu, Z. Yin, X. Ji, and W. Xu, "Rolling colors: Adversarial laser exploits against traffic light recognition," in *31st USENIX Security Symposium (USENIX Security 22)*, 2022.

[91] K. C. Zeng, S. Liu, Y. Shu, D. Wang, H. Li, Y. Dou, G. Wang, and Y. Yang, "All your GPS are belong to us: Towards stealthy manipulation of road navigation systems," in *27th USENIX security symposium (USENIX security 18)*, 2018, pp. 1527–1544.

[92] L. Zhang, X. Chen, F. Kong, and A. A. Cardenas, "Real-time attack-recovery for cyber-physical systems using linear approximations," in *2020 IEEE Real-Time Systems Symposium (RTSS)*. IEEE, 2020, pp. 205–217.

[93] L. Zhang, P. Lu, F. Kong, X. Chen, O. Sokolsky, and I. Lee, "Real-time attack-recovery for cyber-physical systems using linear-quadratic regulator," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 20, no. 5s, pp. 1–24, 2021.

[94] Y. Zhang and K. Rasmussen, "Detection of electromagnetic interference attacks on sensor systems," in *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2020, pp. 203–216.

[95] Y. Zheng, Z. Chen, D. Lv, Z. Li, Z. Lan, and S. Zhao, "Air-to-air visual detection of micro-uavs: An experimental evaluation of deep learning," *IEEE Robotics and Automation Letters*, vol. 6, no. 2, pp. 1020–1027, 2021.

APPENDIX

A. Attacking Other Sensors: CMOS Image sensor

To show that our attack works on other sensors, we conducted additional experiments on CMOS image sensors that are widely used for autonomous vehicles. Similar to §IV and §V, we analyzed the effects of corrupted communication channels and then evaluated whether remote EMI injection could corrupt the communication channels between the CMOS image sensor and control unit.

1) Analysis of SPI Corruption:

Experimental setup. For the experiments, we connected a CMOS image sensor (OV2640) and a control unit board (Arduino Uno). Both communicated using the SPI protocol. The communication signals and interpretation results were observed using a logic analyzer as in §IV-A.

Blocking original signal. We analyzed the communication signals when the benign signal of each SPI channel was physically blocked.

Blocked SS channel: The control unit did not update the image. Other communication signals, MOSI, MOSI, and SCLK signals, were observed; however, since the SS signal was blocked and the sensor requires appropriate active and inactive SS intervals to recognize any commands, the image sensor could not start image transmission.

Blocked MOSI channel: The control unit did not update the image. The SS and SCLK signals transmitted from the control unit to the sensor were observed normally. However, because control commands to the sensors included in MOSI signals such as starting data transmission were blocked, the data transmission could not begin.

Blocked MISO channel: The control unit did not update the image. MOSI and SCLK signals were observed. However, data transmission could not start because the response of capturing one frame to the control unit, which is necessary to start image data transmission, was unable to be transmitted.

Blocked SCLK channel: The control unit did not update the image. The sensor could not understand any transmitted MOSI commands as the interpretation of the MOSI and MISO signals depends on the SCLK signal. Therefore, image transmission could not occur when SLCK signals were blocked.

Distorting benign signal. Next, we analyzed the results when the benign signal of the SPI communication channels was distorted by noise signals. Injected signals are generated from a supplementary control unit board (Arduino Uno) without considering synchronization to distort the benign signals.

Disturbed SS channel: The control unit did not update the image. Because the SS signals were disturbed, the sensor could not recognize the MOSI signals as well. Therefore, the MISO transmission from the sensor was unstable. Consequently, the image data could not be transmitted to the control unit.

Disturbed MOSI channel: The control unit did not update the image. Data transmission did not start while the MOSI channel was disturbed because starting data transmission needs

an appropriate MOSI response for capturing the image data, which the disturbance in MOSI signals did not allow.

Disturbed MISO channel: The control unit did not update the image, and the corrupted image remained on the screen. The corruption of the image data was observed in the data transmission step while the control unit did not update the newer image (CMOS-1 video [3]).

Disturbed SCLK channel: The control unit did not update the image. Because all commands are interpreted based on the SCLK signals, the disturbed SLCK signals cannot translate the commands correctly, resulting in no image transmission.

In summary, we confirmed that if any channel is blocked or disturbed, it considerably affects the retrieved sensor value. In particular, the control unit did not receive any new image data when any of the four channels were blocked or disturbed. Moreover, when the MISO channel was disturbed during the image transmission step, we discovered that the image update was also stopped, and the stopped image was often corrupted (CMOS-1 video [3]).

2) EMI injection targeting CMOS image sensor: We connected a CMOS image sensor and a control unit board and then injected EMI signals to analyze changes in the communication signals between the sensor and the control unit as well as the retrieved sensor values.

Experimental setup. We used four CMOS sensors: OV2640, OV5642, OV9281, and an Occipital Structure Core depth camera. OV2640 and OV5642 communicated with the Arduino Uno board using the SPI protocol. OV9281 was connected to the Raspberry Pi board, and the I2C-MIPI protocol was used for communication. Finally, the Occipital Structure Core depth camera was connected to its custom control unit board.

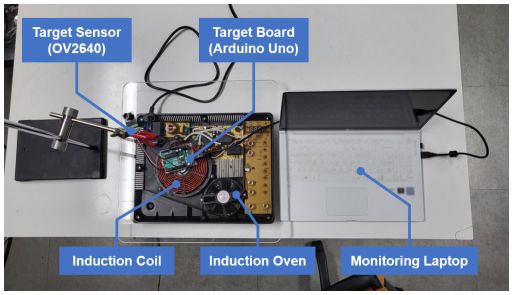

Fig. 20: Experimental setup of the CMOS image sensor.

As an EM source, we employed an induction oven (a coil antenna), a publicly available EMI injection source. The experimental setup for the CMOS image sensors is shown in Fig. 20. The coil antenna emitted an EM field at a frequency of 45 kHz and all experiments were conducted at a distance of approximately 3 cm between the sensor and the antenna (separated by an acrylic board).

Experimental results. Communication signals between the sensors and the control units were distorted through EMI signal injection. These disturbances made the sensor stop updating the image or caused corruption in image data.

The difference between the normal and EMI-injected communication signals with the OV2640 CMOS sensor is shown in Fig. 21. Consequently, the control unit interpreted the corrupted signals, resulting in image data corruption (Fig. 22).

We also observed the corruption of image data of OV5642 and OV9281 (CMOS-3 video [3]). Finally, the Occipital Structure Core depth camera stopped updating the image when the EMI signal was injected (CMOS-4 video [3]). Note that the Occipital Structure Core depth camera is mainly employed in commercial PX4 drones [29].

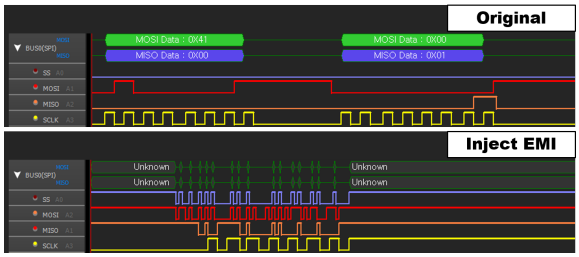

Fig. 21: SPI signals without (top) and with (bottom) EMI injection. Irregular intervals and glitches lead to misinterpretation at the packet level.

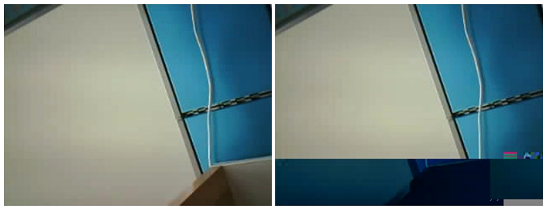

Fig. 22: Normal (left) and EM injected (right) results of the OV2640 CMOS image sensor.

B. Teardown of Commercial Drone Boards and EMI Injection

Commercial drone boards utilize a ribbon cable attached to the board to restrict access to the communication channel between the IMU sensor and control unit and reduce electromagnetic interference. Because of this, disassembling of the drone becomes necessary to access this channel properly. As shown in Fig. 25, we disassembled the commercial drone board irreversibly and determined the communication channel through hardware analysis. Then, we conducted the EMI injection experiment on a separate commercial drone board in the same way as described in §V earlier and measured the communication signal's voltage. As a result, we confirmed that the clock signal of the original communication channel was distorted when a certain frequency of EMI was injected.

C. Experimental Setup Used for Drone Evaluation

We determine the effective EMI frequency for the attack by analyzing the electrical characteristics of each board, and we evaluate the relationship between EMI power and attack distance. Fig. 26 and 27 show the near-field EMC scanner setup and high-power EMI injection equipment used in the experiment, respectively. Specifically, we performed an EMC scan on Arduino boards and commercial drone boards (PX4 and DJI) with a 10 kHz resolution from the 1 MHz to 1 GHz frequency range. As a result, we discovered that the boards had a susceptible frequency susceptible to EMI injection, and the susceptible frequencies were below 400 MHz.

Further, we conducted EMI injection experiments on drone boards with high power (up to 100 W). As a result, we showed the practicality of our remote EMI injection attack at a practical

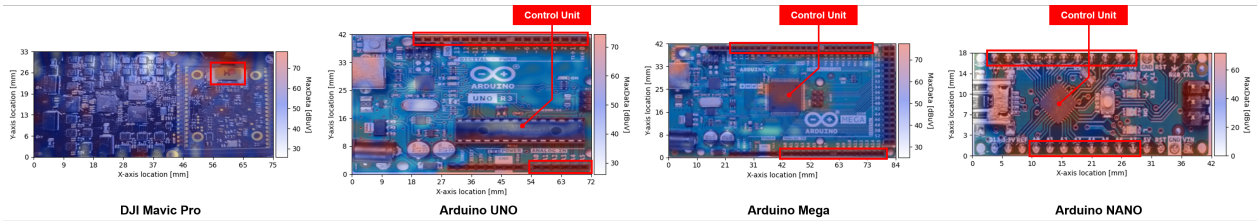

Fig. 23: Examination result of Arduino board's EMI coupling path through EMC scanner: The entire circuit of an Arduino board, including the control unit and the GPIO-IMU path, has an EMI path. This is particularly noticeable near the GPIO pins.

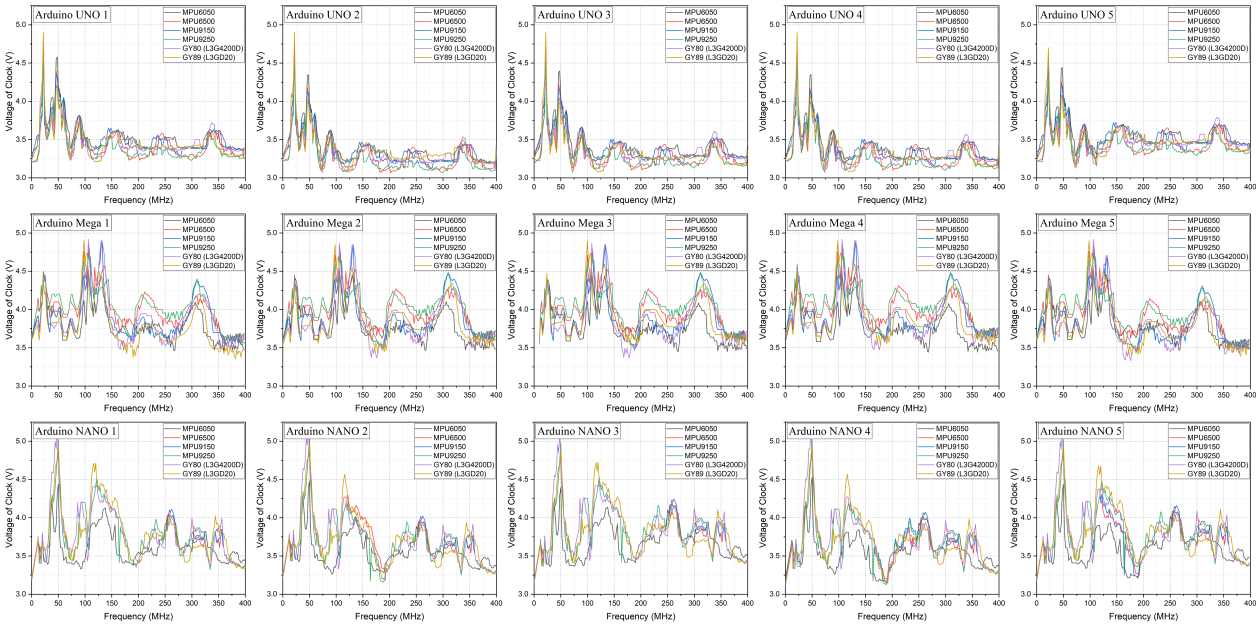

Fig. 24: Evaluation of the EMI susceptibility of the multiple control unit board: The EMI-susceptible frequency mainly depended on the control unit board model, while the amplitude of the induced voltage differed depending on the sensor model and board model.

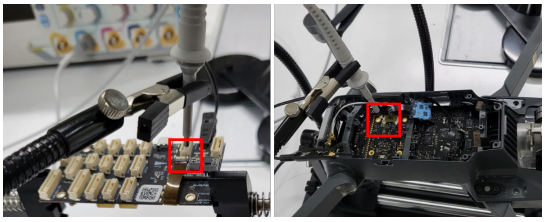

Fig. 25: Teardown of Pixhawk4 (left), DJI Mavic Pro (right) board. Pixhawk4 and DJI not only do not disclose circuit information but also have a control unit board and IMU attached. Further, DJI has a double board structure.

attack distance and derived the relationship between attack distance and power requirement. Fig. 18 shows the evaluation results of these experiments.

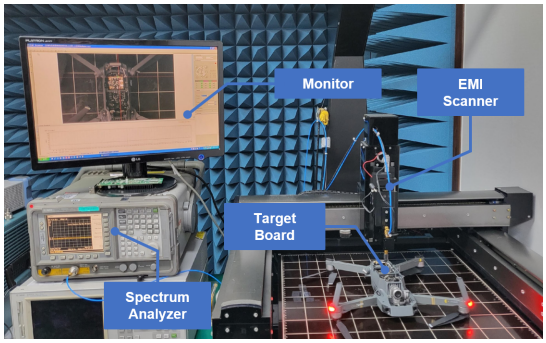

Fig. 26: Experimental setup for near-field EMC scanning.

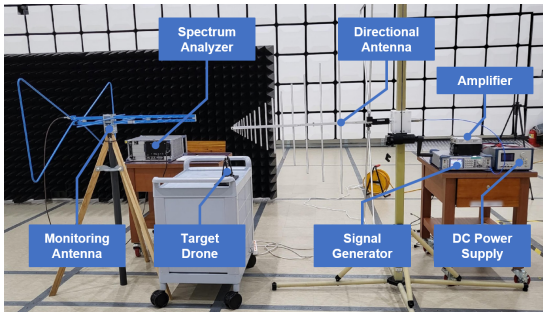

Fig. 27: Experimental setup for high power (up to 100 W) EMI injection.