Electromagnetic Sensor and Actuator Attacks on Power Converters for Electric Vehicles

Gökçen Yılmaz Dayanıklı*
Virginia Tech
gyd@vt.edu

Rees R. Hatch*
Utah State University
rees.hatch@usu.edu

Ryan M. Gerdes
Virginia Tech
rgerdes@vt.edu

Hongjie Wang
Utah State University
hongjie.wang@usu.edu

Regan Zane
Utah State University
regan.zane@usu.edu

***Abstract*—Alleviating range anxiety for electric vehicles (i.e., whether such vehicles can be relied upon to travel long distances in a timely manner) is critical for sustainable transportation. Extremely fast charging (XFC), whereby electric vehicles (EV) can be quickly recharged in the time frame it takes to refuel an internal combustion engine, has been proposed to alleviate this concern. A critical component of these chargers is the efficient and proper operation of power converters that convert AC to DC power and otherwise regulate power delivery to vehicles. These converters rely on the integrity of sensor and actuation signals. In this work the operation of state-of-the art XFC converters is assessed in adversarial conditions, specifically against Intentional Electromagnetic Interference Attacks (IEMI). The targeted system is analyzed with the goal of determining possible weak points for IEMI, viz. voltage and current sensor outputs and gate control signals. This work demonstrates that, with relatively low power levels, an adversary is able to manipulate the voltage and current sensor outputs necessary to ensure the proper operation of the converters. Furthermore, in the first attack of its kind, it is shown that the gate signal that controls the converter switches can be manipulated, to catastrophic effect; i.e., it is possible for an attacker to control the switching state of individual transistors to cause irreparable damage to the converter and associated systems. Finally, a discussion of countermeasures for hardware designers to mitigate IEMI-based attacks is provided.**

***Index Terms*—cyber-physical system security, power converter security, intentional electromagnetic interference (IEMI) attacks**

I. Introduction

In order to increase the adoption of electric vehicles (EV) it is necessary that extremely fast chargers (XFC), along with the attendant battery management systems (BMS), be developed. These advances in charging technology will ensure that EVs can be charged in a time frame commensurate with that of refilling an internal combustion engine vehicle, and therefore alleviate concerns vehicle owners have regarding the feasibility of using EV for routine and long distance travel. The security of XFC chargers and BMS are of great importance since attacks on these systems could result in the overcharging of the EV battery (leading to, e.g., potential fire). Larger scale synchronized attacks on XFC chargers, since they connect the EV to the power grid, could cause instability in the grid leading to blackouts.

Until now the security of EV power converter systems has been largely ignored. In this work we seek to enhance the security of EVs by examining the potential vulnerabilities of XFC chargers and BMS. To this end we provide simulation and experimental results for attacks against critical components of the systems, namely their sensor and actuator (switching) capabilities. For the first time, we demonstrate electromagnetic-based, non-intrusive attacks on actual power converters (comprising AC-DC and BMS power converters) and discuss possible countermeasures.

A. Related Work

IEMI is known to be an important threat for analog sensor readings in the security literature. IEMI attacks have been reported on light sensors, temperature sensors, speed sensors, implantable cardiac devices and microphones [1]–[4]. Although each attack starts with injecting radiation at the resonance frequency of the targeted device, device-specific non-linearities, due to amplifiers [2], [4] and ADCs [1], can be exploited by attackers to manipulate the sensor data. The reader is referred to [5] for a comprehensive review of such attacks. Since amplifiers and ADCs are commonly used in power converters for sensing and feedback control, IEMI can be used to attack XFC power converters with both relatively low-cost and low-power.

B. Contributions

In this work we examine the vulnerability of state-of-the art XFC power converter designs to IEMI attacks. To the best of authors' knowledge, this is the first study that focuses on power converter security from the perspective of IEMI attacks. Specifically, we demonstrate three attacks to show that both the sensing and actuator signals of power converters can be manipulated via non-invasive means (i.e., no physical connection with the hardware are necessary, thereby allowing for proximate attacks). Our primary contributions are:

- Showing that the voltage and current sensor outputs of power converters, necessary to maintain the proper and safe control of the converters, can be manipulated with low-cost and low-power amplifiers and radiators.
- Demonstrating that, and proving an analytical model that explains how, drivers/switches can be controlled (i.e., open or closed) via difficult to shield IEMI. Such drivers/switches are ubiquitous in hardware and cyber-physical systems and we are the first to show and explain how their proximate manipulation may be effected.
- Proposing several widely applicable design changes to hardware level to mitigate IEMI attacks.

Attacks are experimentally validated and, for safety's sake, their affects demonstrated in simulation via Matlab Simulink.

*Dayanıklı and Hatch are co-first authors.

DOI 10.1109/SPW50608.2020.00032

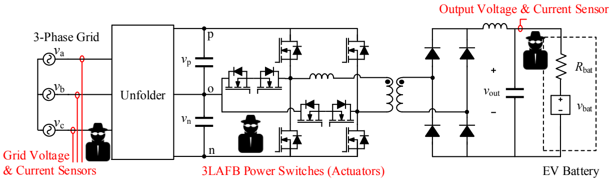


Fig. 1: Functional diagram of the 3-phase AC-DC converter with 3LAFB topology. The figure highlights attack points in red, viz. the output and grid voltage and current sensors as well as the gate signals to the power switches (actuators).

II. System Models

The targeted/victim system consists of an extreme fast charger (XFC) and battery management system (BMS). The XFC is a high-power (350 kW) converter designed to convert 3-phase AC power into DC voltage for EV charging; thus, it is known as an AC to DC (AC-DC) converter. As the power-level increases, the battery charging process poses potential safety risks to EV users in the event that an adversary gains control of the system, as described later. This section describes the AC-DC and BMS, their controls, and weak points from a theoretical perspective.

The specific AC-DC converter analyzed in this paper is the 3-Level Asymmetric Full Bridge (3LAFB) [6], which is an isolated converter topology intended for use in Unfolding based rectifiers. The functional diagram of the Unfolder and 3LAFB topology is shown in Fig. 1. Based upon a safety analysis, the diagram identifies the most sensitive points of attack to be the voltage and current sensors used to monitor the converter inputs and outputs, as well as the power switches. The control objective of the AC-DC converter is to regulate the charging of EV batteries. Battery charging is typically implemented in a constant current constant voltage (CC-CV) scheme. The EV battery is charged at a constant current until the max battery voltage is reached. The charger then switches to constant voltage (CV) control until the battery is fully charged. It is important to note that EV batteries subjected to charging currents or voltages greater than allowable values cause the cells to overheat which creates a fire hazard.

The control of the AC-DC is achieved by switching the 3LAFB to regulate average voltage and current. The feedback sensors are commonly implemented by low voltage analog hardware that is digitalized by an ADC. The controller updates the duty cycle for switches based on the sensed error. (The duty cycle determines the average amount of time the switches are turned on in one switching period.) In actuality, individual power transistors are turned on and off by gate drivers driven by pulse width modulation (PWM) signals.

The switches and their gate drivers can be thought of as the system actuators because they actuate the PWM gate signals from a micro-controller. The gating signals, being PWM signals, command the transistor to turn on (logic high) or off (logic low). The 3LAFB has 8 transistors and 8 gating signals while the unfolder requires 12 of each. Gate drivers operate similar to transistors in that they require the input signal to rise above a certain threshold voltage in order to change the devices switching state.

The system's weak points, with respect to IEMI, lie within the feedback sensors and low-voltage gating signals. The converter can only regulate the output correctly if the feedback voltage/current sensors are measuring accurately. Furthermore, the system can only be controlled if the correct gate signal from the controller is being acted upon by the switches. Thus, large enough disruptions in the gating signal (3.3 V logic) can cause the gate driver to actuate a false turn-on or turn-off of a power switch.

The BMS operates on the same principles as the AC-DC converter. The purpose of the BMS, comprised of multiple DC-DC converters, is to balance the individual cells that make up an EV battery-pack. Each DC-DC converter has its own voltage and current sensors that measure the flow of power for that cell. The BMS employs a current and/or voltage feedback loop for each DC-DC by controlling the duty cycle (or equivalent control signal).

III. Attack Simulations and Outcomes

To explore the effects of IEMI attacks on the battery charging operation of the AC-DC, the attack scenario is simulated in Matlab. The system is modeled on a switching level using PLEC's Blockset add-on for Simulink. The hardware parameters from a 2 kW prototype [6] were used for the simulation. The operating point for the simulation is given in Table I. The 3LAFB attack is implemented at a DC operating point where the input voltages of the 3LAFB are held constant at a particular grid phase angle rather than the time-varying input that occurs during normal AC operation. The AC input should be considered when the attackers target the grid voltage and current sensors which will affect the Unfolder operation and AC-DC power quality. Due to space constraints, only the CV regulator will be investigated; however, the presented analysis can be extended to other parts of the system.

Based on an efficiency and safety analysis of the system, we consider a scenario wherein an attacker is able to overcharge the battery by manipulation of the power converter's feedback voltage signal. Such over-voltage charging would lead to increased charging current at the maximum voltage. The extra power dissipated as heat by the resistive losses of the battery would cause cell heating. Repeated attacks of this nature would lead to decreased battery capacity and lifespan. In the extreme case, where the battery is subjected to sustained over-current charging, the increase in cell temperatures could lead to thermal runaway in which the battery pack would ignite and create a self-sustaining fire. To cause damage to the battery it is simply necessary to subvert CV control (specifically the

TABLE I: Operating Point for CV IEMI Simulations

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

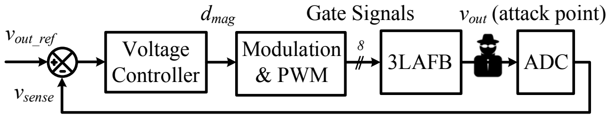


Fig. 2: Block diagram of the constant voltage controller for the 3LAFB. The attacker targets the analog circuitry before the sensing information is digitized by the ADC.

second phase of the CC-CV charging scheme). The CV control loop demonstrated in Fig. 2 uses feedback from the output voltage sensor to control the magnitude of applied duty cycles, d_{mag}. In this scenario, the attacker is targeting the v_{sense} which is the sensed feedback signal of v_{out}, the output voltage of the converter.

In the simulation shown in Fig. 3 an IEMI attack is initiated on the hardware at 10 ms. The attack is simulated by altering the feedback signal, v_{sense}, by subtracting 1 V from the actual output voltage; i.e., the attacker decreases the apparent output voltage which will cause the control system to compensate by increasing the output voltage. This alteration represents the average voltage distortion that is induced on an ADC sensor used to measure output voltage during an IEMI attack. The simulated attack is sustained for 30 ms.

As can be seen from the figure, the controller regulates the sensed voltage to the reference voltage of 502 V; however, the actual output voltage is 503 V. On the short time scale of the simulation, the battery voltage is approximately constant and 500 V. The extra 1 V on the output causes the battery current to increase from 4 to 6 A, a significant increase in current that would cause heating. The charging current is extremely sensitive to changes in v_{out} due to the small battery resistance (<1 Ω), which implies that small changes in sensed voltage result in geometrical increases in current (and thus heat).

IV. Theory of Attack

Our attacks are based on Faraday's law of induction, which states that a time varying magnetic field captured by a conducting loop results in a voltage on the loop [7]. By such means are we able to modify the voltages measured by sensors, and used to control switches, in power converters. To observe how a time varying current, i_a, supplied by an attacker, induces a voltage, v_i, on a victim loop, an infinitely long, z-axis directed current is assumed to be positioned at distance d_a from the victim circuit having dimensions w and l (Fig. 4a). By Faraday's law and Ampere's law the relationship between the attacker signal, i_a, and the induced voltage, v_i, is:

$$v_i(t) = -\mu \left[\frac{w}{2\pi} \ln \left(\frac{d_a + l}{d_a} \right) \right] \frac{d}{dt} i_a(t) \tag{1}$$

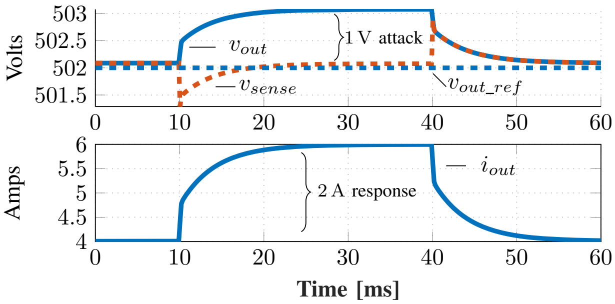


Fig. 3: Simulation of constant voltage controller attack. An attacker induces a 1 V offset into the v_{sense} signal causing the charging current to increase from 4 to 6 A, which indicates that a small change in sensed voltage can lead to a substantial increase in current (and thus heating of a battery).

where the permeability of the medium is μ.

The amplitude and shape (waveform) of v_i are determined by a geometry coefficient (square brackets) and the time derivative of i_a. In the following attack scenarios, the attacker uses a continuous sinusoidal i_a attack waveform, so the form of v_i is a sinusoidal with a phase shift due to transmitting hardware. We note that an increased victim loop size results in an increase induced v_i.

A. Threat Model

We assume an attacker aiming to manipulate the operation of an AC-DC converter and BMS through IEMI. It is assumed that the attacker can place EM radiators in proximity to the converters but there is no physical connection between the attacker hardware and victim circuitry. The attacker has access to commodity RF component devices and like components, e.g., waveform generators, RF amplifiers and EM radiators like toroids and antennas (Figure 4b). We consider an attacker who targets weak points of the victim system using a toroid with a focused magnetic field or a ZPSL antenna with a directive near field radiation pattern. The weak points discussed in detail in Section II are chosen as attack points (voltage sensor output,v_{out}, BMS current sensor output,i_{cell}, and the low voltage gate signals that control the AC-DC switches).

1) Attack Point I - Voltage Sensor Output: The attacker uses IEMI to manipulate the voltage sensor data v_{out} by inducing voltage v_i on the victim cable that connects the analog sensor output and the ADC input of the CV controller. The attack has two phases: the first phase is the efficient EM coupling to the victim cable through the use of cable resonant frequency as an attack frequency [4]. Before each attack, a frequency sweep is applied to detect the resonant frequency of the victim cable. The next phase is the manipulation of non-linearity of ADC. An ADC samples and digitizes an analog signal in the ADC input range (v_{min} to v_{max}). A very common practice is to average the digitized data to filter out high frequency noise. It is discussed in [1] how a generic ADC transfer function and electrostatic discharge (ESD) diodes result in a phenomenon called clipping. We assume the input voltage of the ADC is compromised and a time varying voltage v_{ADC} is fed into the ADC as follows:

$$v_{ADC}(t) = V_s + v_i(t) \tag{2}$$

where V_s is a relatively low frequency sensor output which is assumed as a DC offset and v_i is a purely sinusoidal induced

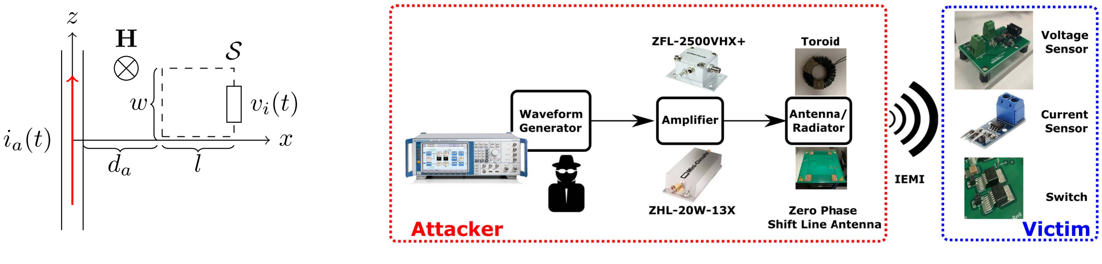


Fig. 4: (a) IEMI attack model [1] (b) Attacker hardware and attack points for power converters

signal by IEMI with frequency f and amplitude V_i. For small sensor output V_s close to v_{min} case, we assumed that $v_i = 0\,\mathrm{V}$. In that case, the measured voltage by the ADC has the form of a half wave rectified signal assuming $V_i < v_{max}$. The average value (DC) of a half wave rectified sinusoidal waveform with amplitude V_i and period $T = 1/f$ is:

$$V_{DC} = \frac{1}{T}\left(\int_0^{\frac{T}{2}} V_i sin(2\pi f t)\mathrm{d}t + \int_{\frac{T}{2}}^{T} 0\mathrm{d}t\right) = \frac{V_i}{\pi} \qquad (3)$$

Note that Equation 3 assumes an infinite sampling frequency and ignores the effects which is observed when the attack frequency is a perfect multiple of sampling frequency (i.e., relative phase becomes important). Other affects also render Equation 3 an approximation that works well in practice; the reader is referred to [1] for a detailed discussion of inducing DC voltages via AC signals.

2) Attack Point II - Current Sensor Output: This attack point consists of the PCB trace between the analog current sensor output and the input of controller ADC (Figure 2). It is assumed that the attacker can place the EM radiator (e.g., an air gap toroid) to induce a high magnetic field. The two phase attack mechanism that includes the efficient coupling and manipulation of the ADC discussed in the previous section is applicable in this attack as well. However, this attack has a fundamental difference: the attack point is a PCB trace which requires the manipulation of smaller victim loops than *Attack I* and necessitates higher attack powers.

3) Attack Point III-Gate Control Signal: The 3LAFB employs a high current gate driver [8] that controls an SiC switch [9] as shown in Figure 5. The attacker aims to change the input voltage V_{IN} of gate driver to control the switch. To turn on the gate driver and switch, the attacker should satisfy the condition in 4 which is also demonstrated in Figure 5:

$$v_i(t) = V_i sin(2\pi f t) > V_{th} \text{ Switch ON} \qquad (4)$$

where v_i is the voltage induced at the input of the gate driver and V_{th} is the minimum voltage to activate the gate.

V. Experimental Results

Three attack points are experimentally tested against IEMI.

A. Attack I: False Voltage Sensor Data Injection

The attacker locates the toroid around the victim cable as in Figure 6a. The toroid has an air-gap which can be filled with a ferrite piece which eliminates the need for the attacker to unplug any wire in the victim. The attacker system consists of a Mini-Circuits ZFL-2500VHX+ RF amplifier and a 30 coil toroid (Figure 4b). The attack power is fixed at $200\,\mathrm{mW}$ throughout Attack I.

Measurement Methodology: The voltage output of a DC supply is adjusted to $21\,\mathrm{V}$ and connected to the voltage sensor as reference voltage. The system is observed to function properly before the IEMI applied. To magnify the effect of IEMI attack (i.e. less power same data manipulation or same power more data manipulation), an attacker can use the resonant frequency of the victim system as attack frequency [4]. At resonance the imaginary component of the impedance is minimum, which results in higher induced voltages. To detect the resonant frequency of the victim cable, a frequency sweep between $100\,\mathrm{MHz}$ and $500\,\mathrm{MHz}$ is applied with $10\,\mathrm{MHz}$ increments and voltage sensor data manipulation is observed from a PC. Although all tested attack frequencies result in varying increases in the voltage readings, it is observed that between $380\,\mathrm{MHz}$ and $420\,\mathrm{MHz}$, the effect is more pronounced.

Results: Figure 6b shows the voltage reading manipulation under IEMI. Depending on the frequency, the voltage readings are manipulated up to the range between $28\,\mathrm{V}$ and $42\,\mathrm{V}$, while the reference voltage is $21\,\mathrm{V}$. Specifically, at $380\,\mathrm{MHz}$, the voltage reading is increased by % 100 to $42\,\mathrm{V}$. Another observation is that the IEMI injection results in an increase of voltage readings throughout the frequency range. This observation is parallel to the ADC nonlinearity discussion in Section IV, as the $21\,\mathrm{V}$ test voltage results in sensor voltages

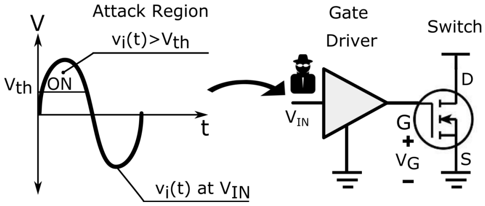
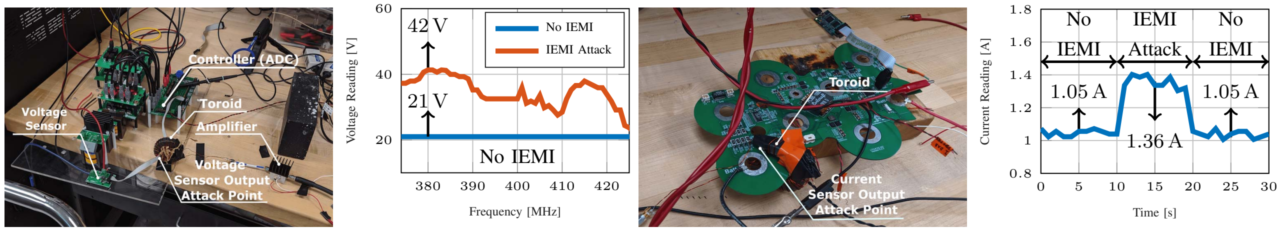


Fig. 5: The induced voltage $v_i(t)$ to V_{IN} should exceed the gate driver threshold voltage V_{th} to turn the switch on.



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

Fig. 6: False voltage and current sensor data injection attacks (a) Experimental setup for voltage sensor output manipulation (b)Voltage sensor output manipulation with regard to attack frequency: measured voltage increased by 21 V under IEMI (c) Experimental setup for current sensor output manipulation (d) Current readings with regard to time, when IEMI is applied between $t = 10$ s and $t = 20$ s, the average of current readings increased from 1.05 A to 1.36 A

on the lower half of ADC input range. The IEMI on voltage sensor output is a significant threat for a converter because of the low power nature of the attack. On the other side, Simulink analyze shows that even a 1 V data manipulation can increase the output current significantly (Figure 3).

B. Attack II: False Current Sensor Data Injection

The attacker aims to manipulate the current sensor data on the printed circuit board (PCB) of the BMS. The air gapped toroid is positioned on the PCB trace as shown in Figure 6c. The attacker hardware consists of a 20 W RF amplifier (Mini-Circuits ZHL-20W-13X) and the toroid. The amplifier output power is adjusted to 2.5 W to eliminate any mismatch problem due to dominantly imaginary impedance of the toroid.

Measurement Methodology: The current sensor is supplied with a 1 A test current and the system is tested before IEMI radiation. It is observed that the system is operating properly and correct current data is received by the controller. Then, a sinuosidal EMI with varying frequency between 10 MHz and 500 MHz with 10 MHz increments is applied and it is observed that in the vicinity of 100 MHz, the current data manipulation is much more pronounced.

Results: In Figure 6d, the current sensor outputs of the system is provided under a temporary IEMI attack between $t = 10$ s and $t = 20$ s. The attack frequency is 100 MHz. It is observed that when IEMI starts at $t = 10$ s, the mean value of current readings increase by % 30 from 1.05 A to 1.36 A. Note that the test current of 1 A is still applied during the attack. On the other side, it is observed that the attack results in an increase in the sensor data which is parallel with the discussion made in Section IV. This attack shows that the PCB traces can be direct targets for IEMI which means PCB level countermeasures are necessary for secure systems.

C. Attack III: False Gate Voltage Injection: Turning on Switches with IEMI

The attacker hardware includes a 20 W RF amplifier (Mini-Circuits ZHL-20W-13X) and a Zero-Phase-Shift Loop (ZPSL) antenna (Figure 4b). ZPSL antenna is a near field resonant antenna with a strong magnetic field at 72 MHz directed through z axis. The attacker positions the ZPSL antenna 10 cm above intertwined and shielded cables that carry V_{IN} and ground of the gate driver. We will use the terminology where V_{IN} is the gate driver input or voltage and V_G is switch gate voltage (Figure 5).

Measurement Methodology: Attack frequency is chosen as 72 MHz and the attack power is increased by 1 dB increments from 100 mW to 20 W, V_{IN} and V_G are observed with an oscilloscope. V_{IN} is set to low throughout the measurements which results V_G is held at -3 V to ensure the switch stays off. If the attack is successful (i.e., switch is turned on by gate drive), the gate voltage V_G is expected to increase to 18 V by the gate driver. To capture the turn on characteristic for V_G and V_{IN}, the oscilloscope is set to single trigger for a low to high transition at V_G.

Results: When the 20 W IEMI applied from an attack distance of 10 cm, it is observed that the IEMI is not sufficent to turn on the switch. This is an expected result, because the loop area between cables that carry ground and V_{IN} connection is small and differential voltage between V_{IN} and ground is not high enough to satisfy the condition in Equation 4. Although this shows that sending V_{IN} and ground cables through intertwined cables are relatively secure, in PCB based systems, the V_{IN} and ground traces/pads is not always close due to the minimum spacing requirements of manufacturing process. To observe this phenomenon, the green V_{IN} and the white ground cables are physically separated and a loop of $4\,\mathrm{cm}^2$ is exposed as demonstrated in Figure 7a. When the attack power is to 20 W, it is observed that the V_G increases and switch turns on as shown in yellow plot of Figure 7b. First of all, it is observed that the switch turns on and off until it stabilizes at turn on condition. As we trigger the oscilloscope for a time window of 100 µs, the power increase is not observable in the V_{IN} (blue). A possible reason for this phenomenon is the output power increase is smaller than 1 decibel as the amplifier operates in saturation.

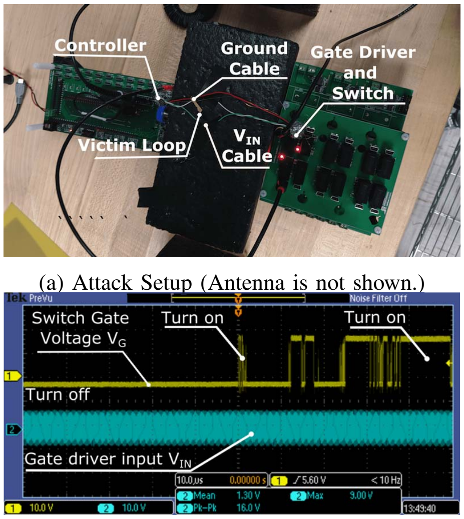
VI. Discussion of Attacks

IEMI attacks on the prototype (Section V) have exposed potentially catastrophic weaknesses in the AC-DC and BMS systems. The ability for the attackers to significantly alter the average ADC values of the power converter's feedback sensors poses a serious threat to the safety of XFC. The v_{out} voltage sensor with a range of 600 V had an induced error equivalent to 21 V of error. As was shown in Section III, an error of 1 V in the output voltage sensing was enough to significantly disrupt the operation of the CV controller.

Every voltage and current sensor used for control in the converter design is a potential weakness to be mitigated. The attacker's ability to control the switches through alteration of the gate signal is another attack point. The digital gate signals are not as sensitive to the IEMI as the sensed, analog signals; however as was shown, if the victim loop of the gate signal is large enough, the attackers are able to turn on switches that were intended to be closed. If this event occurs on live hardware, a short-circuit event is likely to occur. The incredible currents and heat generated in a short-circuit is highly likely to cause system wide device failure or at least system shutdown.

Countermeasures

Although RF shielding (e.g., conductive sheet or foam) is effectively used against relatively high frequency signals, the low frequency (< 100 MHz) and magnetic nature of the reported attack signal makes it very difficult to shield fast chargers [10]. Adding to that, none of the magnetic field shielding options (e.g., MuMetal and Faraday cage) are employed in commercial fast chargers. In order to protect PCB traces transmitting sensitive signals (e.g., analog sensor outputs and gate/switch control signals), hardware designers should be aware of IEMI threats from the first moment of layout generation and eliminate large loops between significant traces and ground pad/traces. However, due to minimum spacing restrictions of PCB manufacturing process and complex layout designs with many components, eliminating large loops may not always possible. In those situations, we suggest using via-fenced striplines for analog sensor outputs and gate driver signals. Although via-fenced stripline is for eliminating crosstalk between traces, it can also be used to eliminate high frequency IEMI from outside sources. We are also investigating alternative approaches that seek to randomize multiple sections of the pathway signals take from sensor to ADC, controller or actuator that would make the resonant frequency of traces unknown to the attacker and thus limit their ability to couple to circuits and affect signals.



(a) Attack Setup (Antenna is not shown.)

(b) Turn on increment of the transistor

Fig. 7: False V_{IN} injection: turning on switches with IEMI

VII. Conclusion

The AC-DC and Battery Management System (BMS) of the power converter is observed to be vulnerable to IEMI attacks. Both systems rely on feedback of the converter outputs to properly regulate the flow of power in the circuit. The system's low voltage current and voltage sensor outputs and gate control signals are susceptible to IEMI attacks which distort the converter's control by inducing a DC offset to the sensed value. The attackers can gain control of the system by manipulation of the feedback signal and can cause damage to the EV, XFC, and BMS systems with one or combination of attacks. Furthermore, the control signals from the micro-controller to the gate drivers can also be vulnerable given the victim loop and attacker power level is large enough to induce sufficient voltage. As a future work, we plan to investigate additional PCB level countermeasures and produce prototypes to test these ideas. Our end goal is to provide a design guideline for secure PCB layout design against IEMI.

Acknowledgment

This work was supported in part by the Department of Energy under grant No. DE-EE0008453.

References

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

[2] Y. Tu, S. Rampazzi, B. Hao, A. Rodriguez, K. Fu, and X. Hei, "Trick or heat? manipulating critical temperature-based control systems using rectification attacks," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, CCS '19, (New York, NY, USA), p. 2301–2315, Association for Computing Machinery, 2019.

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

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

[5] I. Giechaskiel and K. B. Rasmussen, "Sok: Taxonomy and challenges of out-of-band signal injection attacks and defenses," *arXiv preprint arXiv:1901.06935*, 2019.

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

[7] M. Clerk, *A treatise on electricity and magnetism*. 01 2010.

[8] IXYS, *IXD 609 9 Ampere Low Side Ultrafast MOSFET Drivers*, 10 2017.

[9] Cree, *C3M0120100J Silicon Carbide Power MOSFET*, 04 2017.

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