SoK: Security of Cyber-physical Systems Under Intentional Electromagnetic Interference Attacks

Qinhong Jiang*[1], Yan Long*[2], Youqian Zhang*[1],
Chen Yan†[3], Xiaoyu Ji[3], Xiapu Luo[1], Kevin Fu[4], Jiannong Cao[1], Wenyuan Xu[3]
[1]*The Hong Kong Polytechnic University,* [2]*HKUST (GZ),* [3]*Zhejiang University,* [4]*Northeastern University*
{qinhong.jiang, you-qian.zhang, daniel.xiapu.luo, jiannong.cao}@polyu.edu.hk
yanlong@hkust-gz.edu.cn; {yanchen, xji, wyxu}@zju.edu.cn; k.fu@northeastern.edu

Abstract

Falsifying electrical signals in computer systems—the gateway between the physical and digital worlds—intentional electromagnetic interference (IEMI) attacks have become increasingly pervasive and damaging to cyber-physical systems due to their ability to disrupt or control a wide range of safety- and security-critical applications. Existing studies of IEMI attacks are often highly device-specific and exploit disparate, insufficiently compared attack vectors. The absence of a unified, model-based understanding of IEMI vulnerabilities hinders both transferable security assessments and effective cross-disciplinary collaboration toward deployable protections. To address this gap, this work analyzes over 80 instances of IEMI attacks and defenses to provide an analytical framework that models how adversaries achieve IEMI coupling and sample manipulation to inject malicious electromagnetic energy that alters hardware behavior and impacts software execution. The primary goal is to move the field beyond exhaustive empirical discovery of vulnerable instances and toward in-depth theoretical analysis and proactive defense strategies applicable to both existing and future cyber-physical systems. In addition to identifying gaps in current IEMI attack and defense research, this work outlines important directions for future work tailored to the needs and roles of different stakeholder communities. To foster future research on IEMI attacks, we are releasing and maintaining an open-source IEMI research database at https://iemi-research-database.github.io/.

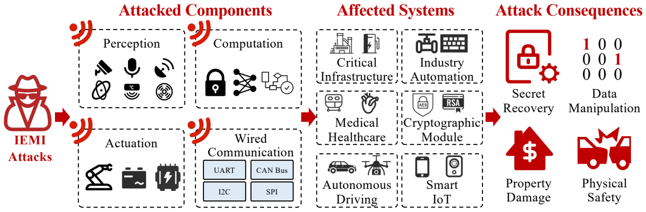

Figure 1: IEMI attacks affect cyber-physical systems by compromising the operation of perception, computation, actuation, and wired communication components, which are widely integrated into critical infrastructures, medical healthcare devices, smart IoT systems, etc, causing various consequences.

1 Introduction

In the era of cyber-physical systems (CPS) that are built from and depend upon the seamless integration of computation and physical components [1], trustworthy operations in the physical world are crucial to ensuring system security. A growing number of research works have highlighted the security vulnerabilities of CPS hardware to adversarial physical interference like acoustic [2–4], optical [5, 6], and electromagnetic signals [7–9], demonstrating how hardware flaws or errors could cascade to computation and software, ultimately compromising the services CPS provides.

Among these physical attack vectors, electromagnetic interference (EMI) has a universal impact since *the underlying electric circuits of modern system computer hardware are inherently susceptible to EMI.* Due to this phenomenon, even unintentional electromagnetic interference between electronic devices could easily cause fatal system failures [10–12]. Although electromagnetic compatibility (EMC) design and testing are mandated for most electronic devices, extensive research reveals that these devices are still vulnerable to intentionally designed EMI, allowing attackers to disrupt or control device functionalities despite the existing EMC protections. Notably, such adversarial interference has demonstrated profound security impacts in a wide range of CPS applications such as critical infrastructure and industrial automation [13–16], autonomous driving [9, 17–19], medical healthcare [7, 20, 21], IoT devices [22–31], cryptographic modules [32–36], etc., with consequences ranging from stealing connected Tesla cars [28] to injecting false electrocardiography signals that compromise the operations of implantable defibrillators [7]. This work investigates these attacks that intentionally inject malicious EM energy, introducing faults

[*] These authors contributed equally to this work.
[†] Corresponding author.

or false signals into electronic systems to disrupt, confuse, or damage these systems [37], which we collectively refer to as *Intentional Electromagnetic Interference Attacks* or *IEMI Attacks*.

Despite individual prior research investigating how to conduct and mitigate IEMI attacks on specific devices, it remains unknown how security researchers can effectively explain, predict, and defend against IEMI threats in a systematic way. Notably, the number of individually reported IEMI attacks has increased almost exponentially over the past 20 years significantly outnumbering the amount of defense analysis, while it is still unclear how we can scientifically analyze and compare different instances of attacks so that their practical impacts are understood and vulnerability causality may be utilized for designing deployable protections.

A fundamental challenge is that the vast number of potentially susceptible CPS devices have unique hardware and software, making the enumeration and manual experimental verification of all exploitable interfaces infeasible. Predicting and preventing possible IEMI attacks thus necessitate a model-based approach that synthesizes usable theoretical formulations from existing literature. Widening the gap is the misalignment among stakeholders—such as EM fault injection (EMFI) and EM signal injection (EMSI) researchers, device designers and manufacturers, and EMC researchers and regulators—largely due to the absence of a shared analytical framework. To close this gap, this work provides a systematization of IEMI attack and defense based on over 80 peer-reviewed publications.

In *IEMI attack systematization*, we introduce an analytical framework that decomposes IEMI attacks into two tightly integrated processes: *IEMI coupling*, which models how malicious electromagnetic energy is injected into circuits——a process primarily grounded in EMC theory and electrical engineering——and *sample manipulation*, which captures how the injected energy perturbs original circuit signals and propagates to affect software execution, drawing primarily on methodologies from security research. The framework enables in-depth understandings of existing IEMI attacks, based on which we dissect existing attack instances and make key observations, such as the often overlooked factors of real-world attack feasibility assessment, the possible convergence of EMFI and EMSI attack approaches, the emergence of new attack vectors, the missing development of crucial feedback methodologies for closed-loop injection control, etc.

In *IEMI defense systematization*, we start by providing a high-level interpretation of the myths observed in existing IEMI research, including the security communities' misperception about the protective power of EMC and the dangerous false sense of security with the proposed seemingly adequate mitigation, despite the lack of theoretical reasoning and assurance, experimental validations, and real-world deployments. We then analyze existing and other possible defense strategies based on the essential stages and requirements of the IEMI coupling and sample manipulation processes. Important identified gaps include the lack of automated coupling interface discovery strategies, proactive synchronization countermeasures, etc., highlighting the need for more theory-grounded and deployment-based defenses developments.

Based on the systematization, we further extract the remaining observed gaps and summarize important future works for IEMI attack researchers, defense researchers, and general security practitioners and designers respectively. In summary, our work offers the first comprehensive survey and systematization of knowledge on IEMI attacks and defenses and how they interact with and inform each other, making several unique contributions, as summarized below:

- **Extensive analysis of existing IEMI works:** We compile and categorize over 80 studies in IEMI security, providing a systematic overview for understanding the variations and trends in existing research.
- **Framework for modeling IEMI attacks and defenses:** We introduce a structured framework for dissecting IEMI attacks and defenses, facilitating deeper understanding, comparative analysis, and prediction of attack and defense methodologies.
- **Identified gaps and directions for future research:** We further summarize critical gaps and propose future research directions to assist the community in addressing significant, unexplored areas of IEMI security.

Systematization Scope and Roadmap: We provide a comprehensive review of over 80 peer-reviewed papers from the security and EMC communities from 2000 to August 2025 (see Appendix A for details). Section 2 examines the historical context and regulatory landscape that drive the need to address the IEMI security in the age of CPS. Section 3 introduces a model-based IEMI analysis framework with dedicated terminologies. Based on it, Section 4 systematizes attack research, providing a detailed analysis of key observations and open questions. Section 5 further analyzes representative defense methods and remaining challenges. Finally, Section 6 explores open problems in IEMI attacks, discusses current limitations, and identifies promising future directions.

2 Background & Motivation

This section provides a brief history of IEMI attacks, discusses its known threats and impacts, and examines current policies related to electromagnetic compatibility (EMC) in both government and industry sectors. We next underscore the critical motivations for addressing the security of IEMI threats in cyber-physical systems.

2.1 History of Electromagnetic Threats

Research into IEMI attacks began in the 1960s with investigations of high-altitude electromagnetic pulse as a tool to disrupt critical electrical infrastructures such as aircraft and communications systems [38], giving birth to the concept of electromagnetic warfare (EW) [39]. By the late 1990s, the focus shifted to investigating how high-power electromagnetic interference on the order of kilowatts could disrupt or destroy civilian systems and cause property loss or safety problems [40, 41]. Over the past two decades, the computer security community has explored the use of low-power, low-profile IEMI equipment (e.g., USRP [42] and PicoEMP [43]) to achieve much more fine-grained controls over the target systems' behaviors. This research has primarily followed two paths: electromagnetic fault injection (EMFI) and electromagnetic signal injection (EMSI) attacks.

Electromagnetic Fault Injection (EMFI) attacks induce faults in the hardware operation of a system using IEMI to retrieve encryption keys through differential fault analysis [32, 44] or to bypass/execute privileged program segments [45–48]. EMFI research began with theoretical works on fault injection attacks against cryptographic protocols. In 2002, Quisquater et al. [44] demonstrated the experimental feasibility of using EM disturbances to induce faults in processor chips for cryptanalysis, stimulating extensive research on the effectiveness of EMFI attacks for compromising cryptographic operations and privilege escalation attacks.

Electromagnetic Signal Injection (EMSI) attacks induce changes to the signals processed by the hardware of a system using IEMI to maliciously disrupt or control downstream software operations of the system. Unlike EMFI, which induces discrete faults to compromise security primitives, EMSI aims to continuously modify system behavior within a seemingly normal range. These attacks often target a broader range of components, such as sensors, that lack security primitives. This category of attacks is also referred to as EM/EMI injection attacks [7–9, 19] and electromagnetic induction attack [15] in the literature. Early research by Rasmussen et al. [49] in 2009 demonstrated that radio signals could induce currents in implanted medical devices. Kune et al. [7] further advanced this in 2013 by demonstrating the first systematic low-power (less than 10 W) IEMI attacks on cardiac implantable electric devices (CIEDs) and microphones. Since then, low-power IEMI has been established as an effective tool for achieving fine-grained manipulation on a wide range of target cyber-physical systems.

2.2 Motivation for SoK

Electromagnetic interference has long been a concern in system design, but the growing threat of IEMI attacks against interconnected cyber-physical systems has made this issue increasingly urgent. We identify several key gaps that motivate this systematization.

Inherent Vulnerability. Fundamental electromagnetic principles render modern electronic circuits inherently susceptible to EMI, making most cyber-physical systems theoretically vulnerable to IEMI attacks. However, the factors that determine why some targets are more easily exploitable than others remain poorly understood.

Energy-Security Trade-off. The push toward low-power and energy-efficient designs, central to mobile and IoT systems, increases susceptibility to IEMI by reducing operating voltages and noise margins. How to effectively protect future ultra-low-power and highly miniaturized electronics remains an open challenge.

Evolving Threat Landscape. Reported and suspected IEMI attacks have grown rapidly in recent years, driven by the widespread deployment of vulnerable devices and the availability of low-cost, portable IEMI equipment. This trend is especially concerning for critical cyber-physical infrastructure, such as autonomous vehicles, industrial automation, and medical systems. Moreover, attacks are shifting from coarse disruption to more precise EMFI and EMSI techniques, highlighting the need for systematic characterization of feasible targets and attack impacts.

Imbalanced Attack/Defense Efforts. IEMI attacks are often significantly easier and cheaper to execute than to defend against, particularly at the physical layer. Defenders must protect complex systems against a broad and evolving attack surface while preserving functionality, leading to a research landscape dominated by attack demonstrations. A key missing piece is effective modeling of IEMI attacks to enable systematic defense design and evaluation.

3 IEMI Problem Formulation

This section introduces the model underpinning our systematization of IEMI attacks and defenses. Fig. 2 overviews the IEMI attack process against a hardware *target sampler* and its surrounding system, modeling it as the combination of *IEMI coupling*, which establishes a physical channel for malicious signal delivery, and *sample manipulation*, which translates attacker intent and target behavior into adversarial IEMI waveform designs. The model is deliberately kept simple while preserving generality and precision and serves as the foundation for our subsequent literature analysis.

Target Sampler and System. A target sampler is a hardware entity that discretizes analog electrical signals. As the gateway between the physical world and the cyber world, samplers are essential to all modern computer systems. *The susceptibility of target samplers to electromagnetic interference is a fundamental cause of IEMI attacks.* A target sampler $\mathcal{S}[\cdot]$ converts an input signal $V(t)$ that the sampler intends to measure into discrete data samples. This process is orchestrated by a clock signal $C(t)$ which sets the sampling rate, and a reference signal $R(t)$ which provides a reference for the measurement. The acquired sample $Samp[n]$ at time t is (detailed in Appendix B):

$$Samp[n] = \mathcal{S}[V(t), C(t), R(t)] \tag{1}$$

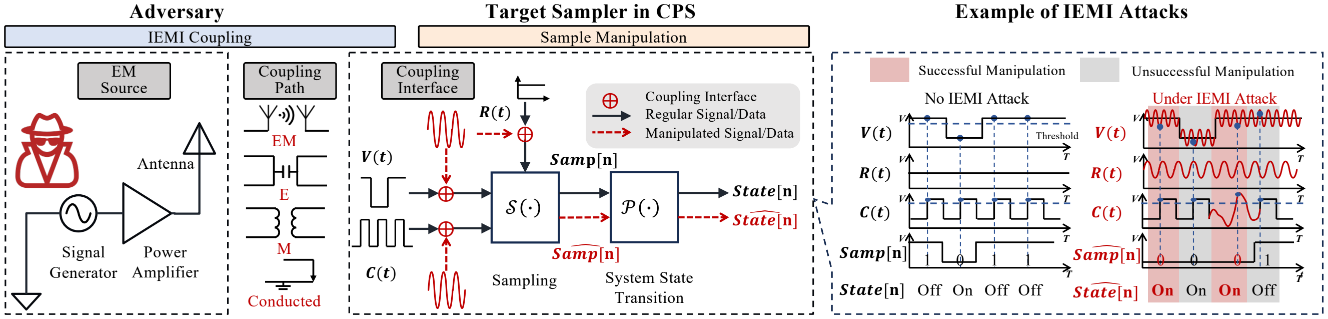

Figure 2: The proposed IEMI analysis framework consisting of IEMI coupling and sample manipulation processes, with an illustrative example of an attacker using IEMI to turn a smart glass on/off in [28] (distinguished paper of IEEE S&P 2024). The red area in the example under attack shows successful manipulation; the gray area showcases how the coupled IEMI signals could fail due to insufficient knowledge of the system's current state and/or lack of precise timing and amplitude control.

A target system is a software-hardware entity whose behavior depends on the output of the target sampler, modeled as a finite-state machine [50, 51]. A function $\mathcal{P}[\cdot]$ represents the state transitions, which maps the current input and the previous state to the next state. The current state can then be formulated recursively as:

$$State[n] = \mathcal{P}[State[n-1], Samp[n]]. \tag{2}$$

In an end-to-end IEMI attack, the adversary causes changes in at least one of $V(t)$, $C(t)$, or $R(t)$ to modify $Samp[n]$ to be an erroneous value, $\widehat{Samp}[n]$, forcing the state machine to enter an insecure state $\widehat{State}[n]$.

IEMI Coupling is the process of delivering electromagnetic energy generated on the adversary's end to targets to induce analog voltages that change target sampler inputs. The fundamental mechanisms for changing $V(t), C(t), R(t)$ are the same. Hence, we use the example of changing $V(t)$, where the input voltage signal under IEMI attacks is:

$$V(t) = V_{true}(t) + \mathcal{T}(V_{adv}(t)) \tag{3}$$

$V_{true}(t)$ is the authentic electrical voltage on the input without IEMI. The attacker-induced malicious voltage is modeled by $V_{adv}(t)$—the IEMI source signal sent from the adversary's antenna—subjected to the transfer function $\mathcal{T}(\cdot)$ of the IEMI coupling process. The function $\mathcal{T}(\cdot)$ is characterized by its frequency response to the EM energy generation by the adversary and embodies the impact of several target-specific factors, such as the distance and angle between the adversary and the target, the casing material of the target hardware, etc (detailed in Appendix B).

Sample Manipulation is the process of designing the IEMI's time-varying waveform based on the malicious voltages that the adversary wants the target samplers to receive, which would result in manipulated data in the software space. This consists of (1) reverse engineering the working principle of the target system to map desired state transitions to required samples, i.e., *state-sample mapping*, (2) applying *timing controls* to align the induced IEMI signals with internal timing of the target, and (3) applying *amplitude controls* to trick the target sampler into perceiving desired values.

Specifically, reverse engineering on Eqs. (1) and (2) enables the adversary to find a state-sample mapping function $\mathcal{R}(\cdot)$ that predicts a viable sequence of required samples:

$$[Samp[1], ..., Samp[n]] = \mathcal{R}(State[n], State[0]). \tag{4}$$

Furthermore, the IEMI signal that an adversary needs to generate in Eq. (3) can be modeled as a baseband signal $b(t)$ modulated onto a carrier signal, i.e.,

$$V_{adv}(t) = modul[b(t), \sum_{\{i\}} A_i(t) \cdot sin(2\pi f_i \cdot t + \varphi(t))], \tag{5}$$

where $modul[\cdot]$ performs modulation, $\varphi(t)$ and $A_i(t)$ are adjustable phases and amplitudes for timing and amplitude control, and f_i represents the frequency of a single sinusoidal component with $\{i\}$ indexing the set of all carrier frequency components. In practice, the IEMI signal's amplitude and frequency ranges are constrained by the maximum output power and frequency of the EM modulation and generation device, denoted as $V_{\lim}$ and $f_{\lim}$, respectively.

IEMI Threat Models. We note that factors of common IEMI threat models could be mapped to the parameters in $T(\cdot)$, $S[\cdot]$, and $\mathcal{P}[\cdot]$. Physical deployment conditions that affect coupling feasibility can be abstracted into the coupling channels characterized by $T(\cdot)$. For example, metal enclosures and better grounding generally result in lower transfer efficiencies compared to plastic devices without proper grounding, increasing attack difficulties. The target's operating state during injection maps to the clock and sampling process, where $C(t)$ determines the sampling edges, and implementation-specific decision thresholds can be represented by extending $S[\cdot]$ with additional threshold parameters when needed. Finally, an attacker's knowledge of target timing corresponds to what the attacker can infer about the target's internal sampling schedule and state transition schemes.

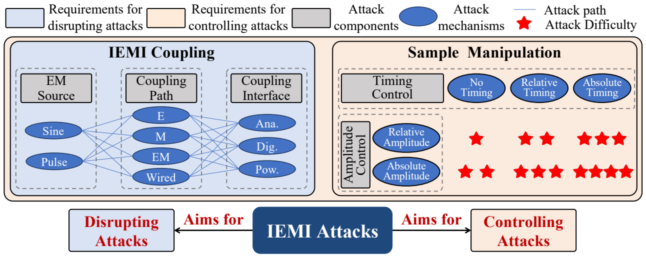

Figure 3: The essential components of IEMI disrupting and controlling attacks. By mapping attack objectives to the required knowledge and mechanisms, it's possible to compare the difficulty of executing different IEMI attacks.

4 Attack Systematization

This section provides a taxonomy and detailed analysis of existing IEMI attack research. Our attack systematization methodology dissects an IEMI attack into its adversary and target profiles, IEMI coupling methodologies, and sample manipulation methodologies (Fig. 3).

4.1 Adversary & Target Profiles

4.1.1 Adversary Profiles

IEMI adversaries are profiled by several key characteristics.

(i) *Attack objective & knowledge.* Attackers leverage IEMI to achieve either controlling or disrupting outcomes, where feasibility is strictly constrained by the attacker's knowledge of the target's internal state, specifically their ability to synchronize with sampling windows.

Controlling attacks (marked as ☠) aim to force the system into a specific, adversary-chosen state ($State[n] = State_{target}$). This objective necessitates *white-box* knowledge (e.g., exact sampling timing, target sampler's state), control over relative and/or absolute timing, and access to a similar target system for preliminary assessment. For instance, Yang et al. [13] assume the adversary acquires a replica device to profile these fine-grained timing parameters beforehand.

Disrupting attacks (marked as ⚠) aim to cause deviations ($State[n] \neq State_{true}$) without precise control. These attacks are feasible with significantly lower requirements. Attackers can operate under *gray-box* or *black-box* assumptions, knowing only the approximate operating frequency rather than the exact sampling instants. Furthermore, there are no timing or synchronization requirements, and methods using continuous single-frequency sinusoidal waves are sufficient to induce denial-of-service (DoS) without aligning with specific data bits.

(ii) *Attacker's capabilities & scenarios* define the factors the attacker can control. The capability (i.e., adjustable IEMI parameters) and size of the attack equipment, together with the achievable attack distances, collectively determine the attack scenarios and stealthiness, and thus influence an attack's feasibility as a real-world threat.

The capability of an IEMI attack depends on three essential pieces of equipment (shown in Fig. 2): a signal generator, a power amplifier, and an antenna. This equipment enables an adversary to precisely control the attack signal's frequency (f_i), amplitude (A_i), and modulation method ($modul[\cdot]$). The maximum attainable frequency (f_{lim}) and peak power (V_{lim}) are inherently constrained by the technical specifications of the available equipment. A sufficiently capable attacker can craft a fine-grained attack signal such that $V_{adv}(t)$ enables either controlling or disrupting attacks.

The physical distance between the adversary and the target system differentiates three typical attack scenarios. *Physical Access* (marked as ▭) scenarios assume the attacker has direct physical access to the target system, allowing for direct signal injection by tapping into wires [27, 54]. *Proximity* (marked as 🟨) scenarios assume the attacker operates from a nearby location, mostly by placing miniaturized or camouflaged IEMI generation equipment near the target [25, 26]. *Long-range* (marked as 🟥) scenarios assume the attacker operates from a more significant distance, typically several meters away.

Research Gap. Our analysis in Table 1 observes that indicate that a large portion of IEMI attacks still use large equipment as proof-of-concept demonstrations, and the number of proximity attacks using real miniaturized devices is very limited. In particular, there is a common assumption that the use of high-power amplifiers and high-gain antennas extend the attack distance [19, 26, 70]. A novel approach introduced by LightAntenna [93] aims to enhance attack stealthiness and practicality by turning non-antenna devices, such as fluorescent lamps, into unintentional IEMI injectors.

Key Observation 1

Most existing IEMI attacks still demonstrate physical access or proximity to targets. This constraint mostly arises from their proof-of-concept research scope.
Open Question: Despite the prevailing belief that employing advanced amplifiers and antennas can increase attack distance, how practical is this assumption, and how can researchers and manufacturers validate it?

4.1.2 Target Profiles

Prior IEMI attack research has already shown the feasibility of affecting a wide range of target systems and samplers.

(i) *Target system.* The documented target systems span multiple domains. The most prevalent targets are household, consumer-grade devices, such as Internet of Things (IoT) smart devices.

This phenomenon could be largely attributed to their easy accessibility and thus a higher degree of adversary knowledge through extensive reverse engineering. Critical infrastructure and industrial automation systems are also common targets primarily due to their static nature and the potential for sub-

Table 1: Systematization of IEMI Attacks with IEMI coupling- Sample manipulation Model.

Adversary Profiles							IEMI Coupling			Sample Manipulation				
Application	**Target System**	**Target Sampler**		**Paper**	**Attack Objective**	**Adversary Proximity**	**EM Source**	**Coupling Interface**	**Coupling Path**	**Sampler Number**	**Timing Control**		**Amplitude Control**	
											Relative	**Absolute**	**Relative**	**Absolute**
Smart IoT	Smartphone	Microphone	ADC	[7, 22, 23, 52–54]	☠	▭ 🟨 🟥	Sine	Ⓐ Ⓟ	M,EM,Wired	🗎	●	○	○	●
		Touchscreen	ADC	[24–27, 55–58]	☠	▭ 🟨	Sine	Ⓐ Ⓟ	E,EM,Wired	🗐	●	●	●	○
		Camera	ADC,GPIO	[8, 54, 59–64]	☠	▭ 🟨 🟥	Sine&Pulse	Ⓐ Ⓓ Ⓟ	M,EM,Wired	🗐	●	●	●	○
	Tablet	Touchscreen	ADC	[55, 56]	☠	🟨	Sine	Ⓐ	E	🗎	●	●	●	○
	Smart Glass	Touch sensor	GPIO	[28]	☠	🟨	Sine&Pulse	Ⓐ	EM	🗎	●	○	●	○
	Smart Lock	Motor	GPIO	[29]	☠	🟨	Sine	Ⓓ	M	🗎	●	●	●	○
	Smart Speaker	Microphone	ADC	[30]	☠	🟥	Sine	Ⓐ	EM	🗐	●	○	○	●
		Speaker	ADC	[31]	☠	🟨	Sine	Ⓐ	M	🗐	●	○	○	●
Autonomous Driving	Vehicle	Camera*	GPIO	[8]	☠	🟥	Sine&Pulse	Ⓓ	EM	🗎	●	●	●	○
		LiDAR*	ADC,GPIO	[9, 18, 65]	☠	🟥	Sine	Ⓐ Ⓓ	EM	🗐	●	●	○	●
		ABS	ADC	[66]	⚠	🟨	Sine	Ⓐ	M	🗎	○	○	●	○
	UAV	Camera	ADC,GPIO	[19, 67]	⚠	🟥	Sine	Ⓐ Ⓓ	EM	🗎	○	○	●	○
		IMU*	GPIO	[19, 67–69]	⚠	🟥	Sine	Ⓓ	EM	🗎	●	○	●	○
		Servo motor	GPIO	[70, 71]	☠	🟨	Sine	Ⓓ	EM	🗎	●	●	○	●
Medical Healthcare	Cardiac Device	Lead	ADC	[7]	⚠	🟨	Sine	Ⓐ	EM	🗎	●	○	●	○
	BCI System	Electrode	ADC,GPIO	[20, 21]	⚠	🟥	Sine	Ⓐ Ⓓ	EM	🗎	●	○	○	●
	Infant Incubator	Thermometer	ADC	[14, 72]	⚠	🟥	Sine	Ⓐ	EM	🗎	●	○	○	●
Critical Infrastructure & Industrial Automation	Power Grid	Inverter	ADC	[13, 73]	☠	🟥	Sine	Ⓐ	M,EM	🗎	●	○	○	●
		Converter	ADC	[74]	⚠	🟥	Sine	Ⓐ	EM	🗎	●	○	●	○
	Industrial Automation	Camera	ADC	[75]	☠	🟨	Sine	Ⓐ	EM	🗐	●	●	○	●
		IR Sensor	ADC	[15, 76]	⚠	🟨	Sine	Ⓐ	M	🗎	●	○	●	○
		Valve	ADC	[77]	⚠	▭	Sine	Ⓐ	Wired	🗎	●	○	●	○
	EV Charger	Converter	GPIO	[16, 78–80]	⚠	🟨	Sine	Ⓓ Ⓟ	EM	🗎	●	●	●	○
	HCI Devices	Keyboard	GPIO	[81]	☠	🟥	Sine	Ⓐ	EM	🗐	●	●	●	○
		Mouse	ADC	[82]	☠	🟨	Sine	Ⓐ	EM	🗎	●	●	○	●
General	Cryptographic Module & Microcontroller	AES	FF	[32–34, 83–85]	☠	▭ 🟨 🟥	Sine&Pulse	Ⓐ Ⓟ	EM	🗐	●	●	●	○
		RSA	FF	[35, 45]	☠	🟨	Pulse	Ⓟ	EM	🗐	○	●	●	○
		DSA	FF	[86]	☠	🟨	Pulse	Ⓟ	EM	🗐	○	●	●	○
		Instruction	FF	[36, 45–48]	☠	🟨	Pulse	Ⓐ Ⓟ	EM	🗐	○	●	●	○
	Wired Serial Communication	UART	GPIO	[15, 76, 87, 88]	☠	🟨	Sine	Ⓓ	M	🗎	●	●	●	●
		I2C, SPI	GPIO	[19, 88–90]	⚠	🟥	Sine	Ⓓ	EM	🗎	●	●	●	○
		CAN Bus	GPIO	[91, 92]	⚠	🟥	Sine	Ⓓ	M, EM	🗎	●	●	●	○

FF: Flip-flop. ADC: Analog-to-digital converter. GPIO: General-purpose inputs/outputs. ☠: Controlling attack. ⚠: Disrupting attack. *: Attacks on sensor's serial buses. EM: Electromagnetic coupling. E: Capacitive coupling. M: Inductive coupling. Wired: Conducted coupling. 🗎: Single-sampler attack. 🗐: Multi-sampler attack. ▭: Physical Access. 🟨: Proximity. 🟥: Long-range. Ⓐ: Analog signal traces. Ⓓ: Digital data lines. Ⓟ: Power cables. ●: Required. ○: w/o Requirement.

stantial operational security impact. In contrast, while medical systems and autonomous driving systems have attracted offensive research attention owing to their severe safety consequences, they are generally more challenging systems to target due to the lack of accessibility and the challenge of injecting coherent signals into moving targets. A common characteristic across most existing targets is their susceptibility to IEMI attacks at relatively short distances. Long-distance targets, particularly distributed critical infrastructure (e.g., smart grid sensors [13], inverters [13, 73], and converters [74]), have been investigated and experimentally verified via proof-of-concept demonstration. These systems are typically exposed in open environments yet remain difficult to access, making them realistic long-range targets.

(ii) *Target sampler.* Existing attacks have targeted three main categories of sampler structures.

Flip-flops (FFs) and other similar logic gate structures between two registers are target samplers of EMFI attacks against hardware in computation and cryptographic units [33, 83, 84].

Analog-to-digital converters (ADCs) are the most attacked type of samplers in EMSI attacks, as they widely exist in sensors and currently have no security primitives for authentication. Almost all common sensors, including cameras, microphones, IMUs, temperature sensors, etc., have been shown to be vulnerable to IEMI attacks.

General-purpose inputs/outputs (GPIOs) in digital communication interfaces, such as UART, I2C, SPI, and MIPI CSI-2 [8], are another common type of targets in sensors and actuators. GPIOs could be viewed as a special form of ADC that determines 0 or 1 from an input voltage.

Although FFs are more fundamental and thus more ubiquitous in modern computer systems, Table 1 shows attacks against ADCs and GPIOs are, counterintuitively, outnumbering attacks against FFs. This is most likely due to the significantly higher clock rate ($C(t)$) of FFs (GHz-range) compared to GPIOs and ADCs (MHz/kHz-range), posing significantly more challenges of timing control (Section 4.3).

Research Gap. It is observed that most previous EMSI attacks aim to change the inputs $V(t)$ of ADCs and GPIOs, while EMFI attacks focus more on affecting the clock signals $C(t)$. There are only a few recent works [27, 77] that have explored how to affect reference signals $R(t)$ to change sampler output, which suggests a possible direction for future offensive research.

Key Observation 2

A wide variety of sampler structures, each deployable on different CPS devices, have been targeted. The main factors influencing the choice of targets include their accessibility, whether they are mobile or stationary, and the magnitude of their safety impact.
Open Question: How can target sampler susceptibility observed in easy-to-access systems be extrapolated to hard-to-access or even unseen systems for IEMI threat prediction?

4.2 IEMI Coupling

The IEMI coupling process builds upon essential components: EM source, coupling path, and coupling interface.

4.2.1 EM Source

An EM source could be characterized mainly by the frequency and amplitude of the carrier signal it generates, as shown by Eq. (5). The baseband information $b(t)$ and modulation type $modul[\cdot]$, which are primarily controlled for sample manipulation, will be further discussed in Section 4.3. Two types of carrier signals are mostly used in IEMI attacks.

(i) *Continuous single-frequency sinusoidal waves* are well suited for long-range EM propagation and are therefore commonly used in EMSI attacks at *longer attack distances* (🟨/🟥) [8, 9, 14, 19, 23]. The carrier frequency (f_i in Eq. (3)) critically affects the coupling efficiency of the transfer function $\mathcal{T}(\cdot)$, motivating prior work to identify EM resonant frequencies of the target sampler's circuitry based on impedance and geometry. Such resonances are identified via either *theoretical analysis* [15, 25, 76] or, more commonly due to modeling complexity, *empirical testing* [8, 15, 26, 81].

(ii) *Pulse waves* are effective for transient disturbances but less efficient for long-distance attacks. Most EMFI attacks exploit high-energy pulses (e.g., around 100 Volts for A_i) to introduce sudden disturbances in the target systems' hardware operations. These attacks require *close proximity* (▭/🟨) to the target devices. A pulse wave consists of a single-frequency sinusoidal wave and a near-infinite series of its harmonics, covering a very large band of frequencies. Adversaries using pulse waves thus often do not need to find target resonance frequencies.

Research Gap. *Although most prior EMSI attacks used single-frequency sinusoidal waves targeting longer-distance attacks while most EMFI attacks used pulses targeting physical-proximity attacks, there is a potential trend and opportunity of integrating the advantages of these two types of waveforms.* For example, a recent work by Nishiyama et al. [34] exploited sine waves for remote fault injection, and Zhang et al. [28] used commercial EM pulse generators to inject false signals into smart glasses' touch sensors.

Key Observation 3

Empirical device-dependent testing of the effectiveness of different electromagnetic waveforms and frequencies dominates the current research landscape.
Open Question: How challenging and beneficial would it be to pursue more rigorous quantitative characterization that builds upon modeling and simulation of the target system's electrical resonance characteristics?

4.2.2 Coupling Interface

The coupling interface of an IEMI attack is a wire component within the target system that acts as an unintentional antenna to receive EM energy that affects the target sampler's $V(t)$, $C(t)$, or $R(t)$. Different coupling interfaces are often associated with different types of affected sampler inputs.

(i) *Power cables* (marked as Ⓟ): Examples include charging cables of smartphones [27, 58] and the power supply modules of sensors (e.g., accelerator, microphone, camera) [54, 77] and actuators (e.g., servos and valves) [77]. Power cables are uniquely positioned to modify the clock signal $C(t)$ of FFs for clock glitching attacks [32, 33, 83, 84], but can also affect the voltage inputs $V(t)$ and reference signals $R(t)$ of ADCs and GPIOs when connected to sensors and actuators.

(ii) *Analog signal traces* (marked as Ⓐ): IEMI attacks frequently exploit sensor electrodes [9, 24, 26, 31, 55, 56] and analog conductive pathways on printed circuit boards (PCB) [7, 14, 16] to receive IEMI signals. Analog signal traces predominantly connected to and thus influence the voltage inputs ($V(t)$) of analog-to-digital converters (ADCs), making them a direct pathway for manipulating sensor readings.

(iii) *Digital data lines* (marked as Ⓓ): These include sensor-to-controller data buses [8, 9, 19, 90], the controller-to-actuator data buses [16, 29], and inter-controller communication buses [88, 91]. Digital data lines mainly affect the voltage inputs ($V(t)$) of GPIO [8, 88] flip-flops structures [51]. While the majority of existing works exploited the analog signal traces of sensors, a few works explicitly targeted sensors' specific serial buses [8, 9, 19], highlighting a promising direction for broader future investigation.

Beyond specific sensors, studies have investigated general serial buses including I^{2}C [19, 88–90], SPI [19, 88], UART [15, 76, 87, 88] and CAN buses [91, 92]. It is worth noting that attacking different digital bus types implies different attacker capabilities because each bus defines a distinct sampling mechanism, timing structure, and tolerance to transient perturbations, which directly constrain the attacker's feasible timing and amplitude control. For example, *synchronous* buses such as I^{2}C and SPI expose explicit sampling edges through a clock, so an IEMI attacker can affect their operation either by driving the data line or perturbing the clock. In contrast, *asynchronous* buses (e.g., UART) do not provide an explicit clock line; therefore, repeatable IEMI controls generally require stronger timing knowledge or synchronization to the receiver sampling schedule. The *wire structure* also matters: single-ended, single-wire signaling offers fewer coupling degrees of freedom, while multi-wire buses give attackers additional opportunities as well as constraints because different subsets of lines may be perturbed to cause qualitatively different effects. *Physical bus constructions* further affect capabilities: shielding, twisting, and differential signaling can reduce susceptibility to common coupling modes, pushing attackers toward higher field strength, closer proximity, or common-mode injection strategies. Finally, *transmission speed* sets the timing granularity required for control, with higher-speed buses (e.g., MIPI buses in cameras [8]) generally posing more IEMI attack challenges than lower-speed buses (e.g., SPI buses in accelerometers).

Research Gap. As shown in Table 1, many potential coupling interfaces remain entirely unexplored in even common targets. Existing research on IEMI attacks primarily exploits analog signal traces (Ⓐ) as the coupling interface, likely due to a prevailing belief that digital signals are inherently more robust and thus harder to attack. However, this has led to a significant research gap, as there is a lack of systematic study into the full range of possible coupling interfaces for a given target, making it difficult to definitively determine a new device's true susceptibility to IEMI attacks.

4.2.3 Coupling Path

The choice of coupling paths depends on specific target characteristics, which also result in distinct behaviors of effective signal frequencies and achievable attack distances.

(i) *Capacitive coupling (E)* exploits mutual capacitance between the target and IEMI emitters, which primarily targets devices sensitive to electric fields or capacitance changes, such as capacitive touchscreens. Effective frequencies f_i of capacitive coupling in reported attacks range from 90 kHz [24] to 140-980 kHz [25], with a documented maximum attack distance of 7 cm (physical proximity: 🟨) in [24].

(ii) *Inductive coupling (M)* exploits mutual inductance, typically targeting devices that are sensitive to magnetic fields, such as Hall effect sensors in vehicle anti-lock braking system (ABS) systems, smartphone microphones and speakers, and motors in smart locks or drones. Inductive coupling utilizes effective frequencies f_i that can range from as low as 100 kHz [22, 31] to tens or even hundreds of MHz [70, 71]. Inductive coupling also necessitates physical proximity (🟨), though with a slightly greater reported maximum attack distance of 15 cm [70, 71].

(iii) *Electromagnetic coupling (EM)* leverages the interaction of varying electric fields and magnetic fields to deliver EM energy. It is highly flexible, enabling attacks on diverse interfaces across a wide frequency range (from tens of MHz to GHz). As shown in Table 1, most documented IEMI attacks adopt this approach. Notably, EM coupling theoretically supports greater attack distances (🟨/🟥) compared to inductive or capacitive methods, with some cases reported to exceed 6 meters [9, 52]. However, current practical attacks are largely limited to close proximity due to the constraints of laboratory equipment in proof-of-concept scenarios. While advanced hardware is often hypothesized to extend this range, such claims remain largely unverified in existing literature.

(iv) *Conducted coupling (Wired)* delivers EM energy to the target through a physical connection, typically the power cables connecting targets to power outlets. By its nature, conducted coupling requires direct physical access (▭) and consequently exhibits the most limited attack range among all methods, which has been exploited to affect smart IoT and industrial automation devices [23, 27, 57, 58, 77].

4.3 Sample Manipulation

In **state-sample mapping**, an IEMI attack objective is mapped to required system state transitions, and further to a sequence of samples at a specific set of target samplers. The choice of samplers presents an important decision that affects attack impact and consequence.

Single-sampler attack (marked as 🗎) is the most common in existing attacks since its timing and amplitude controls do not need to coordinate across multiple samplers. Examples include attacks against GPIO communications and a single ADC in low-dimension sensors such as single-channel temperature sensors [14] and microphones [7].

Multi-sampler attack (marked as 🗐), in contrast, could be found in those targeting the analog sensing of high-dimensional sensors, such as inducing touch or keystroke events at specific locations on touch screens [25] and keyboards [81], which employ an array of ADCs.

It is possible to achieve the same state transitions by affecting different samplers. For instance, modifying the photon-induced voltages input into each of the thousands of ADCs on a CMOS imaging sensor array (multi-sampler attack) could have similar impacts as changing voltages input into the GPIOs of the MIPI CSI interfaces (single-sampler attack) that transmit the digitized pixel values [8, 94].

Research Gap. Different state-sample mapping strategies will result in different levels of timing and amplitude control difficulty. Adversaries thus need to thoughtfully design $\mathcal{R}(\cdot)$. However, research exploring and comparing these alternative approaches is missing in the literature. In addition, the literature body has seen an increasing portion of multi-sampler attacks in recent years, suggesting that adversaries' capabilities keep improving.

4.3.1 Timing Control

Depending on their attack objectives, there are three typical types of timing control requirements. (1) *No timing/synchronization requirements*: Simple disrupting attacks often do not require timing control. (2) *Relative timing requirements*: Certain controlling attacks only require the adversary to change a consecutive sequence of $[Samp[n_0], \dots, Samp[n_0+m]]$ but the selection of n is flexible. For example, in [7] an adversary can inject a segment of speech audio into the microphone at any time. (3) *Absolute timing requirement*: Other controlling attacks could require changing the sample sequence also at a specific n. Certain attacks fall under both the relative and absolute timing requirement categories in Table 1, depending on their specific attack objective. For example, GhostTouch [26] only requires relative timing controls for random touches but necessitates absolute timing controls for targeted key injection on touch screens. It is also important to note that absolute timing control inherently satisfies relative timing requirements since it is more demanding.

(i) *Relative timing control*: The key technical challenge relative timing control needs to address is the mismatch between the carrier $c(t)$'s frequency and the sampling rate of the target sampler. Effective IEMI coupling frequencies (e.g., often on the order of MHz) often far exceed the target system's sampling rate (e.g., often on the order of kHz for sensors), making it difficult to change sample values precisely at consecutive timestamps $[n_0, ..., n_0 + m]$. Existing solutions primarily employ pulse modulation (e.g., [26, 81]), or leverage inherent non-ideal characteristics of sampler hardware for down-sampling, such as exploiting nonlinearity of amplifiers [7, 20, 30], rectification/clipping effects of ADCs and electrostatic discharge (ESD) diodes [15, 16, 88], and aliasing effects of ADCs [9, 18, 60].

(ii) *Absolute timing control*: The key challenge is that an external IEMI adversary needs to know the system's internal states at time n. There are two approaches:

Passive eavesdropping is a side-channel technique that uses additional receiving antennas and low-noise amplifiers to capture unintentional EM emanations from the target system for operation timing synchronization. While commonly used in existing attacks, it faces limitations: the requirement of additional hardware increases the attack cost and complexity, and the weak EM leakage of the target system often requires physical proximity to the target [8, 26].

Proactive control could leverage a system's special mechanisms, such as energy-efficient designs, to trigger a specific operation that internally synchronizes with external IEMI injections. For example, Jiang et al. [81] exploited the energy-efficient designs of keyboards to inject an activation signal to trigger the keyboard re-scanning to inject targeted keystrokes. However, this requires in-depth knowledge of about target system and is system-dependent. Alternatively, EMFI attacks against cryptographic units typically assume that the adversary can pause and even control program execution to precisely align fault injections with target operations, presenting a more intrusive approach that requires physical access or prior instrumentation.

Key Observation 4

Achieving absolute timing control that accurately aligns IEMI with system internal timing to achieve controlling attacks is challenging and relatively rare in existing works.
Open question: How can IEMI attacks be more integrated with EM side-channel attack methodologies to design advanced feedback control loops for precise timing control?

4.3.2 Amplitude Control

The impact of an IEMI attack could be measured by quantifying the amplitude of deviation from the hypothetical authentic sample without IEMI (Eq. (8)). Accordingly, the adversary's amplitude control requirements can also be classified into two categories. (1) *Relative amplitude control*: This only requires the adversary to successfully induce a change in $Samp[n]$, and is most common in disrupting attacks. (2) *Absolute amplitude control*: This requires $Samp[n]$ to be changed to specific values, and is required for conducting precise controlling attacks, e.g., changing a temperature reading of a thermometer from 70 to 80 degrees [14].

(i) *Relative amplitude control*: A relative amplitude change is easy to induce by manually increasing the amplitude of the IEMI signals, i.e., the output power of the IEMI source. In binary-output samplers such as flip-flops in EMFI attacks and GPIOs lines [8, 26] in EMSI attacks, it is often possible to achieve successful attacks by increasing $|V_{adv}(t)|$ to enforce $|\delta_{samp}| \geq 1$ in Eq. (8).

(ii) *Absolute amplitude control*: This requires more delicate controls that make $|V_{adv}(t)|$ reside between an upper and a lower threshold to achieve a specific δ_{samp} in Eq. (8). Existing attacks achieve precise control of $V_{adv}(t)$'s amplitude often by using amplitude modulation (AM) [7, 17, 60, 75], pulse-width modulation (PWM) [22, 31], or phase shift keying (PSK) [87] for the $modul[\cdot]$ function in Eq. (5).

Similarly to absolute timing control, the challenge of absolute amplitude control is for the adversary to estimate the target sampler's output. However, *almost all IEMI controlling attacks so far rely on an active control approach to achieve this*, where the adversary is assumed to be able to directly observe the sampler output while the adversary tries to adjust $V_{adv}(t)$ [8, 14]. Passive eavesdropping methods, such as using electromagnetic side channel leakage to estimate $Samp[n]$, have not yet been explored. Another challenge for precise controlling attacks is the high sensitivity of the coupling channel function $\mathcal{T}(\cdot)$ with regard to variations in adversary-target distances, angles, and positions. This dependence often makes attacks effective only against stationary targets and requires prior knowledge of the location or orientation of the target system [7, 26], significantly limiting their practicality.

Key Observation 5

Little work demonstrated how to use IEMI to precisely change voltages in non-physical access threat models due to the lack of voltage information feedback channels.
Open question: What strategies could exist to non-invasively probe the internal voltages of target sampler inputs, especially against moving targets?

5 Defense Systematization

Despite growing awareness of threats posed by IEMI attacks, the development of defenses has lagged behind. Since Kune's paper [7] in 2013 specifically detailing primary attack methods, more than 70 attack papers have appeared by 2025. Most attack papers (shown in Table 2) briefly cite Electromagnetic Compatibility (EMC) practices as defenses, such as layout optimization [16, 21, 22, 30, 52, 53, 95, 96], differential signaling [7, 8, 73, 87, 91], twisted-pair cabling [78, 88, 90], shielding [7, 8, 22, 25, 31, 34, 75, 81, 87], and filtering [7, 14, 15, 23, 24, 55, 74, 76, 87], while arguing that existing EMC implementations in CPS devices are inadequate. This presents the first prevalent myth: **Myth 1:** *IEMI attacks succeed because the devices exhibit substandard EMC.*

Furthermore, many of these attack papers conclude with high-level overview of defensive solutions, creating the false impression that the attacks are easy to defend against: **Myth 2:** *Cursory, end-of-paper defenses in attack-focused studies imply that existing solutions are adequate.*

To examine these prevailing myths, we establish a taxonomy for defenses grounded in our dissection of the essential stages and requirements for successful IEMI attacks in Section 4. By comparing existing defenses across three key dimensions, including objective, overhead, and robustness (defined below), we analyze their strengths and limitations. Furthermore, we identify directions of defense strategies that are currently underexplored. A structured summary of this information is presented in Table 2.

Defense comparison dimensions. The following three key dimensions characterize different defense strategies.

(i) *Defense objective.* We classify defense objectives into three categories: *prevent* –completely stop the attack (marked as ⊘). *downgrade* –downgrade the impact of attacks from a more severe controlling attack to a less severe disrupting attacks (marked as ↓). *detect* –identify the presence of an IEMI attack to activate pre-defined countermeasures or post-attack responses (marked as 🔍).

(ii) *Deployment overhead.* A defense's real-world feasibility can be gauged by three factors. *Expertise* represents the technical knowledge and skill required for defense implementation, including hardware (📳), software (💻), or hardware-software co-design (⚙). *Deployment cost* refers to the demands of financial and time resources: medium (🛢) and high (🪙). *Applicability* refers to the ability to be applied to legacy (↺) or emerging (⏩) systems.

(iii) *Defense robustness.* We categorize the robustness of countermeasures into three levels: *low*–The attacker can defeat countermeasures simply by employing more capable IEMI sources with higher power, better directionality, etc. *moderate*–The attacker is required to have more knowledge about the targets and more sophisticated signal controls to achieve the same objective. *high*–The countermeasures eliminate the attack surface.

5.1 IEMI Coupling-Stage Defense

This category of defenses work by reducing the IEMI energy delivered to the circuitry of a target sampler by disrupting the adversary's EM source, coupling interface, or coupling path.

5.1.1 Eliminate Coupling Interface

Eliminating circuitry components that could unintentionally act as receiving antennas can fundamentally *prevent* a system from IEMI attacks. Existing techniques primarily achieve this through hardware (📳) methods with a high cost (🪙) such as redesigning circuits or replacing cables.

(i) *Layout optimization* is proposed to minimize a system's susceptibility to IEMI by reducing exposed traces [16, 21] or optimizing electric component structures [22, 30]. Despite their *high* robustness hypothesized in previous papers, these methods *lack sufficient validation in real-world settings.*

(ii) *Canceling common-mode interference* leverages techniques such as differential signaling [7, 91] or balanced twisted cables [78, 88, 90] to make external EM interference affect two signal lines identically, allowing the receiver to effectively cancel common-mode noise. However, these methods offer only *moderate* robustness, as they have already been demonstrated to be ineffective by attackers that exploit differential-mode injection [8, 27].

(iii) *EM isolation* completely eliminates the electrical coupling interface by replacing all electrical cables with optical fibers, as these fibers transmit data through photons that are inherently immune to external EM interference [70, 97]. Although demonstrating *high* robustness even under intense IEMI [97], this approach involves significant redesign costs and may not be feasible in all contexts.

Research Gap. Coupling interface eliminations have been discussed in prior research. However, there is no proactive methodology for systematically discovering potential coupling interfaces in complex systems. Most defenses remain reactive: interfaces are identified post hoc after an attack and then patched. This attack–patch scheme leaves uncharted interfaces exploitable and fails to provide coverage guarantees.

5.1.2 Block Coupling Path

This strategy aims to attenuate the EM energy ($\mathcal{T}(V_{adv}(t))$) along the coupling path to *prevent* successful attack. Existing techniques achieve this through the following hardware (📳) methods with a medium cost (🛢) that are based on established Electromagnetic Compatibility (EMC) practices.

(i) *EM shielding* offers high effectiveness by reflecting or absorbing EM energy [7, 25]. However, this approach introduces significant trade-offs in terms of weight, cost, and usability. Moreover, this method offers *low* robustness, as attackers can render it ineffective simply by increasing the power of attack signals. For example, even though shielding may attenuate EM energy by 40 dB, a well-resourced attacker can transmit 10^4 times more power to overcome this defense and achieve the same attack effect [7].

(ii) *Low-pass filter* attenuates high-frequency EM signals outside the system's functional spectrum by introducing hardware filters at vulnerable circuit nodes [7, 74, 76, 76]. Similarly, this method only offers *low* robustness. Even with a prohibitively expensive filter designed to be effective over a wide frequency range, a small section of the connecting wire or parasitics can still result in vulnerability [74].

Table 2: Systematization of IEMI Defenses.

Strategies	Technologies and Methods		Paper Source		Experimental Validation	Defense Objective	Deployment Overhead			Defense Robustness
			Attacks	Defenses			Expertise	Cost	Applicability	
IEMI Coupling Stage	Eliminate Coupling Interface	Layout optimization	[16, 21, 22, 30, 31, 34, 52, 53, 96]	[95]	◔	⊘	▮	⛁	⏩	*high*
		Canceling CM interference	[7, 70, 73, 78, 87, 88, 90]	[97]	◔	⊘	▮	⛁	⏩	*moderate*
		EM isolation	[70]	[97]	◔	⊘	▮	⛁	⏩	*high*
	Blocking Coupling Path	EM shielding	[7, 22, 30, 31, 34, 53], etc.	[97]	◔	⊘	▮	☰	⟲⏩	low
		Low-pass filter	[7, 14, 15, 23, 24, 27, 55, 56, 74, 76, 87, 89]	?	◔	🔍	▮	☰	⏩	low
	Detect EM Source	Monitor environmental disturbances	[98, 99]	?	○	🔍	⚙	☰	⟲⏩	*moderate*
		Detect signal contamination	[7, 14, 30, 53, 55, 56, 73]	?	○	⊘	⚙	☰	⏩	*moderate*
Sample Manipulation Stage	Detect System State Deviations	Authentication & verification	[7, 21–23, 53, 55, 56, 74, 75]	[100–104]	◕	🔍	💻	☰	⏩	*high*
		Anomaly detection	[8, 14, 18, 22, 26, 27, 74, 75]	[100, 105–108]	◕	🔍	⚙	☰	⟲⏩	*high*
	Neutralize Timing Control	Vary sampling timing	[15, 21, 26, 81]	?	◔	↓	⚙	☰	⏩	*moderate*
		Obscure application timing	[8, 78, 81]	?	○	↓	⚙	☰	⏩	*moderate*
	Neutralize Amplitude Control	Increase operating voltage	[26, 55, 56, 78]	?	◔	↓	▮	⛁	⏩	low
		Relocate the target	?	[109]	◑	↓	▮	☰	⟲⏩	*moderate*
		Signal processing technique	[7, 24, 27, 110]	[18, 95]	◑	↓	💻	☰	⟲⏩	*moderate*

The defense technique is Red–Under-explored, Red–Widespread attention, and Red–Well-established. ?: Lack of evidence and potential future research direction.
○ : Unvalidated validation. ◔ : Limited validation. ◑ : Adequate validation. ◕ : Extensive validation. ☰: Middle deployment cost. ⛁: High deployment cose.
⊘: Prevent IEMI attacks. ↓: Downgrade attack's impact. 🔍: Detect IEMI attacks. low: Low robustness. *moderate*: Moderate robustness. *high*: High robustness.
▮: Hardware modification. 💻: Software design. ⚙: Hardware-software co-design. ⟲: Applicable for legacy systems. ⏩: Applicable for emerging systems.

Response to Myth 1. EMC design is an engineering discipline based on pragmatic trade-offs (e.g., cost, size, performance, and regulatory compliance), rather than a quest for perfect security protection. This goal inevitably leaves certain circuit areas less protected, which most existing IEMI attacks exploit. The issue is not that EMC is inadequate, but that its practical application is shaped by intentionally adversarial scenarios, economic considerations, and regulatory realities.

5.1.3 Detect EM Source

This strategy aims to *detect* the presence of IEMI attackers by monitoring a system's EM environment. Existing techniques require additional specialized additional hardware and detection software (⚙) to serve as a detector for IEMI coupling with a medium cost (☰).

(i) *Monitor environmental disturbances* is a proactive technique that uses antennas to continuously monitor the EM environment around target systems to provide early warning of anomalous EM activity indicative of an ongoing or impending attack [98, 99].

(ii) *Detect signal contamination* leverages knowledge of the system's normal electrical behavior to identify deviations caused by EM sources. By incorporating a reference conductor or redundant circuit or components, defenders can directly observe unexpected high-frequency components (f_i) or voltage anomalies in $V(t)$ that betray the presence of malicious EM source [7, 30, 56]. This method provides *moderate* robustness, as a sophisticated adversary may craft a stealthy attack that remains within the system's expected operating range.

Research Gap. The primary limitation of existing methods is their inability to reliably distinguish malicious signals from benign environmental noise or normal system fluctuations, a research gap highlights the need for more comprehensive profiling of IEMI's characteristics.

Key Observation 6

Hardware-based defenses, while extensively discussed, face significant engineering trade-offs. This results in a lack of experimental validation for most proposed defenses due to the challenges of hardware manufacturing.
Open question: How can security researchers quantitatively evaluate the trade-offs and possibly validate the strategies on potential simulation platforms?

5.2 Sample Manipulation-Stage Defense

This category of defenses aims to prevent or detect flaws in precise sample manipulation.

5.2.1 Detect System State Deviations

The majority of existing research focuses on hardware-software co-design (⚙) to *detect* deviations caused by imperfect state-sample mapping designs and implementations.

(i) *Authentication and verification* introduces explicit checks or leverages inherent system characteristics to validate the authenticity of captured signals or events. This strategy provides *moderate* robustness by forcing attackers to imitate normal system behavior while inducing critical state deviations only at a few key moments. Existing techniques include challenge-response authentication and fingerprinting. For example, Zhang et al. [101] embedded secret patterns in ADC sampler's on/off control signals.

(ii) *Anomaly detection* leverages statistical and temporal analysis to detect deviations from expected system behavior, making it particularly useful against unknown or evolving attack strategies. Existing techniques include sensor fusion [9, 106], time series forecasting [100] and abnormal activities detection [25, 26]. However, *the effectiveness of this technology relies on deep domain knowledge and can be challenged by benign but unmodeled system variability.*

Research Gap. This strategy naturally calls for integration with formal-method analysis of secure system behavior. However, such research is absent in the context of IEMI defenses.

5.2.2 Neutralize Timing Control

This strategy works by preventing attackers from determining the relative or absolute timing of target samplers to *downgrade* the impact from a more severe controlling attack to a less severe disrupting attack with a medium (⛁) cost.

(i) *Varying sampling timing* often requires hardware-software co-redesign (⚙). It undermines the attacker's ability to synchronize IEMI signals with the target's relative timing by introducing unpredictability, either through frequency jitter in clock $C(t)$ [15, 21] or randomized scanning sequences [81]. While traditionally deemed to have *high* robustness, the actual level of robustness depends on the implementation of randomization. For instance, recent works have shown how sophisticated attackers may leverage phase-coherent signal design techniques [111] to achieve synchronization with pseudo-random data permutations, suggesting only *moderate* robustness.

(ii) *Obscuring application timing* prevents attackers from determining the absolute timing of target systems by obscuring or shielding side-channel emissions, which adversaries often rely on to infer or predict the system's absolute timing, thereby making it significantly harder for attacks [8, 17, 26] to realize passive eavesdropping.

Research Gap. There is little research on countermeasures against proactive absolute timing controls. Possible methods may include authentications against malicious device wake-up triggers and tamper-resistant hardware against physical access-based fault injections.

5.2.3 Neutralize Amplitude Control

This strategy also *downgrade* the impact of attacks by disrupting IEMI amplitude controls.

(i) *Increase operating voltage* addresses threat scenarios where attackers attempt to overwhelm legitimate signals by sheer power. By increasing the system's operating voltage, i.e., reference $R(t)$ on the hardware-level (🔲), defenders can make attacks expensive [21, 26, 55, 56, 78]. This leverages fundamental physical constraints to tip the balance in favor of the defender, but apparently has *low* robustness.

(ii) *Relocating the target* leverages $\mathcal{T}(V_{adv}(t))$'s sensitivity to adversary-target relative positions. By moving the target system, this method provides *moderate* robustness by making fine-grained amplitude control significantly more challenging [109]. It could require hardware (🔲) or administrative-level changes.

(iii) *Signal processing technique* uses software-domain processing (💻) with both physical measurements and machine learning models [18, 27] to perform denoising and canceling [7, 27, 95, 110], identifying or suppressing anomalous inputs. These approaches offer updating flexibility but often have unclear robustness as their performance largely depends on the quality of signal characteristics modeling.

Response to Myth 2. The majority of proposed defenses are insufficiently robust against determined adversaries. The prevailing practice of mentioning unevaluated defenses briefly in attack papers risks causing more harm than benefit. A more constructive path forward is to acknowledge the unknowns and motivate in-depth research.

Key Observation 7

Existing defenses often focus on system-specific countermeasures that detect or to downgrade attacks. There is a need for proactive strategies that can prevent sample manipulation from occurring in the first place.
Open question: How can we design proactive strategies for preventing sample manipulation and make the defenses applicable across different devices and applications?

6 Discussion and Outlook

This summarizes our new insights, the remaining gaps, and possible future research directions.

6.1 Advice For IEMI Attack Researchers

Real-world Impact Motivating Defenses. Current attack research does not translate well into defense development. This is largely because many studies only present proof-of-concept attacks that are limited to physical proximity, and their scalability to practical, long-range scenarios is often speculative. This insufficient demonstration of real-world impact provides limited motivation for the design of effective IEMI defenses.

Future Direction. To better motivate defense research, IEMI attack studies should move beyond proof-of-concept demonstrations. From a practical impact standpoint, more research is needed to investigate how these attacks could be implemented in real-world settings, mapping out realistic adversary capabilities and system-level security consequences.

Path Towards an IEMI Attack Benchmarking Methodology. The research community needs a standardized benchmark for evaluating IEMI attacks. At present, it is nearly impossible to compare reported attack distances across different studies because of variations in IEMI generation equipment and experimental setups. This lack of comparability makes it difficult to assess which threats are most prevalent and therefore should be prioritized for defense.

Future Direction. We argue that a key step toward an IEMI benchmark is to systematically document core attack parameters from prior work and establish a protocol for quantitatively evaluating and reporting future attacks. Our parameter tables provide a practical starting point. Such a benchmark should standardize (i) measurement setups, (ii) outcome documentation, and (iii) reporting formats.

Setup specifications should include the minimum information needed for reproducibility, such as signal generation hardware, modulation settings, frequency/power limits, and target-side conditions (e.g., distance, orientation, enclosure, and operating state). We further recommend reporting low-level measurements (e.g., probe-based voltage or SNR at a fixed location) to enable fair comparisons beyond distance-only claims. Outcome documentation should define a clear attack objective and report quantitative success rates over repeated trials within a specified time window. When claiming a maximum attack distance, the success criterion and corresponding constraints should be stated. Finally, a unified template aligned with our systematization dimensions can ensure consistent reporting of setups, outcomes, and attacker assumptions. We release and maintain an open-source IEMI research database (https://iemi-research-database.github.io/) and welcome community use and contributions.

Device Susceptibility Prediction. The ability to predict device susceptibility through simulation could save researchers from the sheer amount of manual laboratory work and is the ultimate scientific goal of IEMI attack research. However, most attacks focus on measuring the impact of known attack techniques on new target devices, rather than investigating the more fundamental aspects of causality, methodologies, and models that could inform predictions of new threats.

Future Direction. While the systematization in this work lays out a modeling framework, achieving such quantitative predictions requires extensive future work in device and vulnerability modeling. We encourage researchers to incorporate more theoretical analysis. The community can also use our IEMI attack database and contribute to its continued maintenance and updates, enabling complementary data-driven predictions of potential threats.

6.2 Advice For IEMI Defense Researchers

Applicability Across Systems. Most existing defenses lack generality because they are highly tailored to individual system-specific attributes, such as the frequency response of coupling channels and the data formats of samplers.

Future Direction. It is important to develop reusable detection and prevention frameworks that can adapt to different application contexts and hardware. It may benefit from leveraging ML/AI techniques that are capable of cross-domain learning, or creating modular defense frameworks that are built upon individual hardware components and can be parameterized and assembled.

Implementation and Deployment. Most prior defense analysis consists of only theoretical discussion and hypotheses, without actual implementation and evaluation. It is thus hard to measure their effectiveness and cost, potentially preventing manufacturers from adopting the proposed defenses. This challenge is further compounded by common academic incentives, where engineering-focused deployments and assessments are often viewed as mere technical improvements rather than innovative scientific research.

Future Direction. We believe more experimental evaluations on prototypes and COTS devices, as well as input from manufacturers, are essential. It is also important to understand whether the lack of effective defenses is due to perceived impracticality, limited reproducibility, or a community bias toward novel attacks over practical defenses.

6.3 Advice For General Security Practitioners

Threat Modeling IEMI. It has been shown that the threat of IEMI is ubiquitous against computer-based systems. IEMI problems will always exist in future systems as long as they have electrical components.

Future Direction. We recommend security practitioners and even hardware and software system designers be aware of the attack surface of IEMI in threat modeling.

Critical Systems and Emerging Techniques. Researchers need to pay attention to safety-critical infrastructures interfacing with physical environments, particularly systems that directly interact with human physiological systems, and emerging techniques like quantum computers, AI sensors, etc.

Future Direction. Emerging low-cost consumer-grade healthcare devices that possess and transmit protected health information should be protected against IEMI attacks. For example, brain-computer interfaces [20, 21] and portable DNA sequencers [112] have become increasingly popular, but their sensing and communication circuits can be easily manipulated by nearby IEMI. Similarly, IEMI could even pose threats to quantum computers, as there will always be electrical components in the implementation of post-quantum cryptography schemes [113]. Finally, the increasing integration, miniaturization, and AI-empowered functionalities [114] of modern electronic devices amplify the potential impact of IEMI attacks on autonomous driving, embodied AI, and robotics.

7 Conclusions

This SoK analyzed over 80 peer-reviewed papers spanning more than two decades of IEMI security research. Based on this analysis, we present a unified framework to help both academia and industry better understand and mitigate IEMI attacks. We further argue that future work should move beyond exhaustive vulnerability discovery and toward deeper theoretical analysis to enable more effective defenses.

8 Acknowledgment

We sincerely thank all anonymous reviewers and shepherds for their constructive feedback. This work was supported in part by the HK RGC Theme-based Research Scheme (No. T43-513/23-N), HK RGC General Research Fund (No. PolyU-15235424), China NSFC Grant (No. 62201503 and No. U25B2001), Guangdong Provincial Key Lab of Integrated Communication, Sensing, and Computation for Ubiquitous Internet of Things (No. 2023B1212010007), and Research Institute for Artificial Intelligence of Things, The Hong Kong Polytechnic University. Fu's participation reflects only academic collaboration on this manuscript; no funds, materials, equipment, or non-public scientific or technical information were provided to or received from any co-author's institution in connection with this work. The opinions, findings, and conclusions expressed in this paper are those of the authors and do not necessarily reflect those of the supporting organizations.

Ethical Considerations

This work systematizes existing research on IEMI attacks. Although it introduces no new vulnerabilities and involves no human subjects, consolidating offensive knowledge carries inherent ethical risks. We therefore structure our ethical reasoning as follows.

Stakeholders and Ethical Context. This research concerns multiple stakeholders, including academic researchers, system vendors and operators, manufacturers, regulators and standards bodies, and end users of safety-critical cyber-physical systems (CPS). Our ethical approach emphasizes harm minimization and the promotion of defensive security knowledge. This systematization aims to clarify open problems, support practical threat modeling, and ultimately improve the security and reliability of CPS deployments.

Nature of the Contribution and Responsible Scope. As an SoK paper, this work synthesizes prior research and does not experimentally demonstrate new vulnerabilities or attacks on commercial systems. This scope reflects a deliberate effort to balance research transparency with misuse risk. All discussed attack vectors were previously disclosed by their original authors, and no personally identifiable information is involved.

Dual-Use Risks and Potential Impacts. We acknowledge the dual-use nature of IEMI research: improved understanding may lower barriers to misuse, yet fragmented knowledge disproportionately disadvantages defenders. We observe a defensive asymmetry in which attackers can exploit unavoidable physical effects, while defenders lack a unified threat model to assess practical risks.

Risk Mitigation Measures. To mitigate misuse, we present attack-related information at a controlled level of abstraction. While our IEMI research database and benchmarking table (Table 3 in our artifact) summarize reported parameters and setups, the data are aggregated, comparative, and non-operational. We avoid procedural guidance and exploit-ready configurations, focusing on threat models and system-level effects, complemented by a defense-oriented systematization (Section 5).

Decision to Publish and Anticipated Benefits. Despite residual dual-use risks, we believe publication is ethically justified because the defensive benefits outweigh potential misuse. By providing a unified threat model and a structured view of IEMI risks, this work supports proactive system hardening, informed design and regulation, and safer CPS deployments.

Open Science

This work fully supports the principles of Open Science. To facilitate transparency, reproducibility, and community engagement, we have created and will actively maintain a GitHub repository that provides a comprehensive collection of research literature related to IEMI attacks and defenses surveyed in this work (https://github.com/Jackjiang313/Awesome-EMI-Attacks-and-Defenses). The artifacts can be downloaded on Zenodo (https://zenodo.org/records/18019022). To foster future research on IEMI research, we also convert the surveyed literature into a researchable and open-source IEMI research database (https://iemi-research-database.github.io/), and we welcome the community to use this resource and contribute to its continued development and expansion.

References

[1] U.S National Science Fundation. Cyber-physical systems (cps). https://new.nsf.gov/funding/opportunities/cps-cyber-physical-systems, 2024.

[2] Xiaoyu Ji, Yushi Cheng, Yuepeng Zhang, Kai Wang, Chen Yan, Wenyuan Xu, and Kevin Fu. Poltergeist: Acoustic adversarial machine learning against cameras and computer vision. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 160–175. IEEE, 2021.

[3] Guoming Zhang, Chen Yan, Xiaoyu Ji, Tianchen Zhang, Taimin Zhang, and Wenyuan Xu. Dolphinattack: Inaudible voice commands. In *2017 ACM CCS*.

[4] Xiaoyu Ji, Qinhong Jiang, Chaohao Li, Zhuoyang Shi, and Wenyuan Xu. Watch your speed: Injecting malicious voice commands via time-scale modification. *IEEE TIFS*, 19:3366–3379, 2024.

[5] Zizhi Jin, Xiaoyu Ji, Yushi Cheng, Bo Yang, Chen Yan, and Wenyuan Xu. Pla-lidar: Physical laser attacks against lidar-based 3d object detection in autonomous vehicle. In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 1822–1839. IEEE, 2023.

[6] Chen Yan, Zhijian Xu, Zhanyuan Yin, Xiaoyu Ji, and Wenyuan Xu. Rolling colors: Adversarial laser exploits against traffic light recognition. In *31st USENIX Security Symposium (USENIX Security 22)*, 2022.

[7] Denis Foo Kune, John Backes, Shane S Clark, Daniel Kramer, Matthew Reynolds, Kevin Fu, Yongdae Kim, and Wenyuan Xu. Ghost talk: Mitigating emi signal injection attacks against analog sensors. In *2013 IEEE symposium on security and privacy*. IEEE, 2013.

[8] Qinhong Jiang, Xiaoyu Ji, Chen Yan, Zhixin Xie, Haina Lou, and Wenyuan Xu. {GlitchHiker}: Uncovering vulnerabilities of image signal transmission with {IEMI}. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 7249–7266, 2023.

[9] Zizhi Jin, Qinhong Jiang, Xuancun Lu, Chen Yan, Xiaoyu Ji, and Wenyuan Xu. Phantomlidar: Cross-modality signal injection attacks against lidar. In *NDSS Symposium*. Internet Society, 2025.

[10] Donald Witters. Facing the challenges of electromagnetic interference with medical devices in the wireless world. In *27th General Assembly of the International Union of Radio Science, Maastricht, The Netherlands*. Citeseer, 2002.

[11] Richard Leach. Failures and anomalies attributed to electromagnetic interference. In *Space Programs and Technologies Conference*, page 3654, 1995.

[12] Carolyn Ritchie. Potential liability from electromagnetic interference with aircraft systems caused by passengers' on-board use of portable electronic devices. *J. Air L. & Com.*, 61:683, 1995.

[13] Fengchen Yang, Zihao Dan, Kaikai Pan, Chen Yan, Xiaoyu Ji, and Wenyuan Xu. Rethink: Reveal the threat of electromagnetic interference on power inverters. In *NDSS Symposium*. Internet Society, 2025.

[14] Yazhou Tu, Sara Rampazzi, Bin Hao, Angel Rodriguez, Kevin Fu, and Xiali Hei. Trick or heat?: Manipulating critical temperature-based control systems using rectification attacks. In *2019 ACM SIGSAC Conference on Computer and Communications Security*.

[15] Jayaprakash Selvaraj, Gökçen Yılmaz Dayanıklı, Neelam Prabhu Gaunkar, David Ware, Ryan M. Gerdes, and Mani Mina. Electromagnetic induction attacks against embedded systems. In *2018 ACM Asia Conference on Computer and Communications Security*.

[16] Gökçen Yilmaz Dayanikli, Rees R Hatch, Ryan M Gerdes, Hongjie Wang, and Regan Zane. Electromagnetic sensor and actuator attacks on power converters for electric vehicles. In *2020 IEEE Security and Privacy Workshops (SPW)*.

[17] Yanze Ren, Qinhong Jiang, Chen Yan, Xiaoyu Ji, and Wenyuan Xu. Ghostshot: Manipulating the image of ccd cameras with electromagnetic interference. In *NDSS Symposium*. Internet Society, 2025.

[18] Sri Hrushikesh Varma Bhupathiraju, Jennifer Sheldon, Luke A Bauer, Vincent Bindschaedler, Takeshi Sugawara, and Sara Rampazzi. Emi-lidar: Uncovering vulnerabilities of lidar sensors in autonomous driving setting using electromagnetic interference. In *16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2023.

[19] Joon-Ha Jang, Mangi Cho, Jaehoon Kim, Dongkwan Kim, and Yongdae Kim. Paralyzing drones via emi signal injection on sensory communication channels. In *NDSS Symposium*. Internet Society, 2023.

[20] Md Imran Hossen, Yazhou Tu, and Xiali Hei. A first look at the security of eeg-based systems and intelligent algorithms under physical signal injections. In *2023 Secure and Trustworthy Deep Learning Systems Workshop*. ACM.

[21] Alexandre Armengol-Urpi, Reid Kovacs, and Sanjay E Sarma. Brain-hack: Remotely injecting false brainwaves with rf to take control of a brain-computer interface. In *5th Workshop on CPS&IoT Security and Privacy*, pages 53–66, 2023.

[22] Donghui Dai, Zhenlin An, and Lei Yang. Inducing wireless chargers to voice out for inaudible command attacks. In *2023 IEEE symposium on security and privacy (SP)*, pages 1789–1806. IEEE, 2023.

[23] José Lopes Esteves and Chaouki Kasmi. Remote and silent voice command injection on a smartphone through conducted iemi. *Wireless Security Lab, French Network and Information Security Agency (ANSSI), Tech. Rep*, 2018.

[24] Seita Maruyama, Satohiro Wakabayashi, and Tatsuya Mori. Tap'n ghost: A compilation of novel attack techniques against smartphone touchscreens. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 620–637. IEEE, 2019.

[25] Haoqi Shan, Boyi Zhang, Zihao Zhan, Dean Sullivan, Shuo Wang, and Yier Jin. Invisible finger: Practical electromagnetic interference attack on touchscreen-based electronic devices. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2022.

[26] Kai Wang, Richard Mitev, Chen Yan, Xiaoyu Ji, Ahmad-Reza Sadeghi, and Wenyuan Xu. {GhostTouch}: Targeted attacks on touchscreens without physical touch. In *31st USENIX Security Symposium (USENIX Security 22)*, 2022.

[27] Yan Jiang, Xiaoyu Ji, Kai Wang, Chen Yan, Richard Mitev, Ahmad-Reza Sadeghi, and Wenyuan Xu. Wight: Wired ghost touch attack on capacitive touchscreens. In *IEEE Symposium on Security and Privacy (SP)*, pages 984–1001. IEEE, 2022.

[28] Xingli Zhang, Yazhou Tu, Yan Long, Liqun Shan, Mohamed A Elsaadani, Kevin Fu, Zhiqiang Lin, and Xiali Hei. From virtual touch to tesla command: Unlocking unauthenticated control chains from smart glasses for vehicle takeover. In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 201–201. IEEE, 2024.

[29] Abdullah Z Mohammed, Alok Singh, Gökçen Y Dayanıklı, Ryan Gerdes, Mani Mina, and Ming Li. Towards wireless spiking of smart locks. In *2022 IEEE Security and Privacy Workshops (SPW)*.

[30] Zhifei Xu, Runbing Hua, Jack Juang, Shengxuan Xia, Jun Fan, and Chulsoon Hwang. Inaudible attack on smart speakers with intentional electromagnetic interference. *IEEE Transactions on Microwave Theory and Techniques*, 69(5):2642–2650, 2021.

[31] Tiantian Liu, Feng Lin, Zhangsen Wang, Chao Wang, Zhongjie Ba, Li Lu, Wenyao Xu, and Kui Ren. Magbackdoor: Beware of your loudspeaker as a backdoor for magnetic injection attacks. In *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2023.

[32] Yu-ichi Hayashi, Naofumi Homma, Takaaki Mizuki, Takafumi Aoki, and Hideaki Sone. Transient iemi threats for cryptographic devices. *IEEE transactions on Electromagnetic Compatibility*, 55(1):140–148, 2012.

[33] Yu-ichi Hayashi, Naofumi Homma, Takaaki Mizuki, Takafumi Aoki, and Hideaki Sone. Precisely timed iemi fault injection synchronized with em information leakage. In *2014 IEEE International Symposium on Electromagnetic Compatibility (EMC)*, pages 738–742. IEEE, 2014.

[34] Hikaru Nishiyama, Daisuke Fujimoto, and Yuichi Hayashi. Remote fault injection attack against cryptographic modules via intentional electromagnetic interference from an antenna. In *2023 Workshop on Attacks and Solutions in Hardware Security*, 2023.

[35] Jörn-Marc Schmidt and Michael Hutter. *Optical and em fault-attacks on crt-based rsa: Concrete results*. na, 2007.

[36] Alexandre Menu, Jean-Max Dutertre, Olivier Potin, Jean-Baptiste Rigaud, and Jean-Luc Danger. Experimental analysis of the electromagnetic instruction skip fault model. In *15th Design & Technology of Integrated Systems in Nanoscale Era (DTIS)*, pages 1–7. IEEE, 2020.

[37] William Radasky and Edward Savage. Intentional electromagnetic interference (iemi) and its impact on the us power grid. *Meta*, 1:1–3, 2010.

[38] GPS World Staff. Massive gps jamming attack by north korea. https://www.gpsworld.com/massive-gps-jamming-attack-by-north-korea/, 2012.

[39] D Curtis Schleher. *Electronic warfare in the information age*. Artech House, Inc., 1999.

[40] RL Gardner. Electromagnetic terrorism: A real danger. In *Electromagnetic compatibility 1998 (Wrocław, 23-25 June 1998)*, pages 10–14, 1998.

[41] William A Radasky, Carl E Baum, and Manuem W Wik. Introduction to the special issue on high-power electromagnetics (hpem) and intentional electromagnetic interference (iemi). *IEEE Transactions on Electromagnetic Compatibility*, 46(3):314–321, 2004.

[42] USRP Software Defined Radio (SDR). Chipshouter-picoemp kit. https://store.newae.com/chipshouter-picoemp, 2024.

[43] NewAE Tech. Chipshouter-picoemp kit. https://www.ettus.com/products/, 2024.

[44] Jean-Jacques Quisquater and D. Samyde. Eddy current for magnetic analysis with active sensor. 01 2002.

[45] Alessandro Barenghi, Luca Breveglieri, Israel Koren, and David Naccache. Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures. *Proceedings of the IEEE*, 100(11):3056–3076, 2012.

[46] Ang Cui and Rick Housley. Badfet: Defeating modern secure boot using second-order pulsed electromagnetic fault injection. In *11th USENIX WOOT 17*, 2017.

[47] Nicolas Moro, Amine Dehbaoui, Karine Heydemann, Bruno Robisson, and Emmanuelle Encrenaz. Electromagnetic fault injection: towards a fault model on a 32-bit microcontroller. In *2013 Workshop on Fault Diagnosis and Tolerance in Cryptography*, pages 77–88. Ieee, 2013.

[48] Jean-Max Dutertre, Alexandre Menu, Olivier Potin, Jean-Baptiste Rigaud, and Jean-Luc Danger. Experimental analysis of the electromagnetic instruction skip

fault model and consequences for software countermeasures. *Microelectronics Reliability*, 121:114133, 2021.

[49] Kasper Bonne Rasmussen, Claude Castelluccia, Thomas S Heydt-Benjamin, and Srdjan Capkun. Proximity-based access control for implantable medical devices. In *16th ACM conference on Computer and communications security*, pages 410–419, 2009.

[50] Thomas Dullien. Weird machines, exploitability, and provable unexploitability. *IEEE Transactions on Emerging Topics in Computing*, 8(2):391–403, 2017.

[51] Zhenyuan Liu, Dillibabu Shanmugam, and Patrick Schaumont. Faultdetective: Explainable to a fault, from the design layout to the software. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2024(4):610–632, 2024.

[52] Tanner Fokkens. *Prediction and Root-Cause Analysis for Smart Speaker Intentional Electromagnetic Interference Attacks*. PhD thesis, Missouri University of Science and Technology, 2023.

[53] Chaouki Kasmi and Jose Lopes Esteves. Iemi threats for information security: Remote command injection on modern smartphones. *IEEE Transactions on Electromagnetic Compatibility*, 57(6):1752–1755, 2015.

[54] Yan Jiang, Xiaoyu Ji, Yancheng Jiang, Kai Wang, Chenren Xu, and Wenyuan Xu. Powerradio: Manipulate sensor measurement via power gnd radiation. In *NDSS Symposium*. Internet Society, 2025.

[55] Ming Gao, Fu Xiao, Weiran Liu, Wentao Guo, Yangtao Huang, Yajie Liu, and Jinsong Han. Expelliarmus: Command cancellation attacks on smartphones using electromagnetic interference. In *IEEE INFOCOM 2023-IEEE Conference on Computer Communications*, pages 1–10. IEEE, 2023.

[56] Ming Gao, Fu Xiao, Wentao Guo, Zixin Lin, Weiran Liu, and Jinsong Han. Practical emi attacks on smartphones with users' commands cancelled. *IEEE Transactions on Dependable and Secure Computing*, 2023.

[57] Yan Jiang, Xiaoyu Ji, Kai Wang, Chen Yan, Richard Mitev, Ahmad-Reza Sadeghi, and Wenyuan Xu. Marionette: Manipulate your touchscreen via a charging cable. *IEEE Transactions on Dependable and Secure Computing*, 2023.

[58] Huifeng Zhu, Zhiyuan Yu, Weidong Cao, Ning Zhang, and Xuan Zhang. Powertouch: A security objective-guided automation framework for generating wired ghost touch attacks on touchscreens. In *Proceedings of the 41st IEEE/ACM International Conference on Computer-Aided Design*, pages 1–9, 2022.

[59] Ariel Schwarz, Yosef Sanhedrai, and Zeev Zalevsky. Digital camera detection and image disruption using controlled intentional electromagnetic interference. *IEEE Transactions on Electromagnetic Compatibility*, 54(5):1048–1054, 2012.

[60] Donghui Dai, Zhenlin An, Qingrui Pan, and Lei Yang. Magcode: Nfc-enabled barcodes for nfc-disabled smartphones. In *Proceedings of the 29th Annual International Conference on Mobile Computing and Networking*, pages 1–14, 2023.

[61] Ziwei Liu, Feng Lin, Zhongjie Ba, Li Lu, and Kui Ren. Magshadow: Physical adversarial example attacks via electromagnetic injection. *IEEE Transactions on Dependable and Secure Computing*, 2025.

[62] Hui Zhuang, Yan Long, and Kevin Fu. Rf-eye-d: Probing feasibility of cmos camera watermarking with radio-frequency injection. In *the 28th RAID*, 2025.

[63] Haoxiang Zhang, Qinhong Jiang, Yushi Cheng, Xiaoyu Ji, and Wenyuan Xu. Intentional electromagnetic interference attack against infrared thermal imaging sensor. In *2022 IEEE EI2*, pages 1748–1753. IEEE, 2022.

[64] Youqian Zhang, Zhihao Wang, Xinyu Ji, and Qinhong Jiang. Rainbow artifacts from electromagnetic signal injection attacks on image sensors. In *2025 IEEE SiPS*, pages 1–5. IEEE, 2025.

[65] Ziwei Liu, Feng Lin, Teshi Meng, Benaouda Chouaib Baha-eddine, Li Lu, Qiang Xue, and Kui Ren. Emtrig: Physical adversarial examples triggered by electromagnetic injection towards lidar perception. In *22nd ACM Conference on Embedded Networked Sensor Systems*, pages 351–364, 2024.

[66] Yasser Shoukry, Paul Martin, Paulo Tabuada, and Mani Srivastava. Non-invasive spoofing attacks for anti-lock braking systems. In *15th Cryptographic Hardware and Embedded Systemsc(CHES)*. Springer, 2013.

[67] Sung-Geon Kim, Euibum Lee, Ic-Pyo Hong, and Jong-Gwan Yook. Review of intentional electromagnetic interference on uav sensor modules and experimental study. *Sensors*, 22(6):2384, 2022.

[68] Minki Lee, Gangmin Kim, Jonghyun Kang, Hyunwoo Kim, Jangwon Lee, and Hongjun Choi. Demo: One shot all kill: Building optimal attack on swarm drones. In *2024 VehicleSec*, 2024.

[69] Alessandro Erba, John H Castellanos, Sahil Sihag, Saman Zonouz, and Nils Ole Tippenhauer. {ConfuSense}: Sensor reconfiguration attacks for stealthy {UAV} manipulation. In *3rd USENIX Symposium on Vehicle Security and Privacy*, 2025.

[70] Gökçen Yılmaz Dayanıklı, Sourav Sinha, Devaprakash Muniraj, Ryan M Gerdes, Mazen Farhood, and Mani Mina. Physical-layer attacks against pulse width modulation-controlled actuators. In *31st USENIX Security Symposium (USENIX Security 22)*, 2022.

[71] Gökçen Yılmaz Dayanıklı. *Electromagnetic Interference Attacks on Cyber-Physical Systems: Theory, Demonstration, and Defense*. PhD thesis, Virginia Tech, 2021.

[72] Yan Long, Sara Rampazzi, Takeshi Sugawara, and Kevin Fu. Protecting covid-19 vaccine transportation and storage from analog cybersecurity threats. *Biomedical Instrumentation & Technology*, 55(3):112–117, 2021.

[73] Anomadarshi Barua and Mohammad Abdullah Al Faruque. Hall spoofing: A non-invasive dos attack on grid-tied solar inverter. In *29th USENIX Security Symposium (USENIX Security 20)*, 2020.

[74] Marcell Szakály, Sebastian Köhler, Martin Strohmeier, and Ivan Martinovic. Assault and battery: Evaluating the security of power conversion systems against electromagnetic injection attacks. In *2024 Annual Computer Security Applications Conference (ACSAC)*.

[75] Sebastian Köhler, Richard Baker, and Ivan Martinovic. Signal injection attacks against ccd image sensors. In *2022 ACM Asia Conference on Computer and Communications Security*.

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

[77] Kai Wang, Shilin Xiao, Xiaoyu Ji, Chen Yan, Chaohao Li, and Wenyuan Xu. Volttack: Control iot devices by manipulating power supply voltage. In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 1771–1788. IEEE, 2023.

[78] Sebastian Köhler, Richard Baker, Martin Strohmeier, and Ivan Martinovic. Brokenwire: Wireless disruption of ccs electric vehicle charging. In *NDSS Symposium*. Internet Society, 2023.

[79] Soyeon Son, Kyungho Joo, Wonsuk Choi, and Dong Hoon Lee. Securing ev charging system against physical-layer signal injection attack. In *2024 Symposium on Vehicles Security and Privacy (VehicleSec)*, pages 1–11, 2024.

[80] Ce Zhou, Qiben Yan, Zhiyuan Yu, Eshan Dixit, Ning Zhang, Huacheng Zeng, and Alireza Safdari Ghanhdari. Short: Breaking the charge: Exploiting state manipulation in ev charging. In *3rd USENIX Symposium on Vehicle Security and Privacy*, 2025.

[81] Qinhong Jiang, Yanze Ren, Yan Long, Chen Yan, Yumai Sun, Xiaoyu Ji, Kevin Fu, and Wenyuan Xu. Ghosttype: The limits of using contactless electromagnetic interference to inject phantom keys into analog circuits of keyboards. In *NDSS Symposium*. Internet Society, 2024.

[82] Wenfan Song, Jianwei Liu, and Jinsong Han. Puppetmouse: Practical and contactless mouse manipulation attack via intentional electromagnetic interference injection. *ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 8(3):1–30, 2024.

[83] Amine Dehbaoui, Jean-Max Dutertre, Bruno Robisson, and Assia Tria. Electromagnetic transient faults injection on a hardware and a software implementations of aes. In *2012 Workshop on Fault Diagnosis and Tolerance in Cryptography*, pages 7–15. IEEE, 2012.

[84] Sébastien Ordas, Ludovic Guillaume-Sage, and Philippe Maurine. Electromagnetic fault injection: the curse of flip-flops. *Journal of Cryptographic Engineering*, 7, 2017.

[85] Hikaru Nishiyama, Daisuke Fujimoto, Hideaki Sone, and Yuichi Hayashi. Efficient noninvasive fault injection method utilizing intentional electromagnetic interference. *IEEE Transactions on Electromagnetic Compatibility*, 2023.

[86] Niels Samwel and Lejla Batina. Practical fault injection on deterministic signatures: the case of eddsa. In *10th International Conference on Cryptology in Africa,*, pages 306–321. Springer, 2018.

[87] Zhixin Xie, Chen Yan, Xiaoyu Ji, and Wenyuan Xu. Bitdance: Manipulating uart serial communication with iemi. In *the 26th RAID*, pages 63–76, 2023.

[88] Gökçen Yılmaz Dayanıklı, Abdullah Zubair Mohammed, Ryan Gerdes, and Mani Mina. Wireless manipulation of serial communication. In *2022 ACM Asia Conference on Computer and Communications Security*.

[89] Arne Pahl and Stefan Dickmann. Analysis of sensor disturbances caused by iemi. *https://doi.org/10.15488/12553*, pages 159–165, 2022.

[90] Arne Pahl, Kai-Uwe Rathjen, and Stefan Dickmann. Intended electromagnetic interference with motion detectors. In *2021 IEEE International Joint EMC/SI/PI and EMC Europe Symposium*, 2021.

[91] Youqian Zhang and Kasper Rasmussen. Electromagnetic signal injection attacks on differential signaling. In *2023 ACM Asia CCS*, 2023.

[92] Hiroto Ogura, Ryunosuke Isshiki, Kengo Iokibe, Yuta Kodera, Takuya Kusaka, and Yasuyuki Nogami. Electrical falsification of can data by magnetic coupling. In *2020 35th ITC-CSCC*, pages 348–353. IEEE, 2020.

[93] Fengchen Yang, Wenze Cui, Xinfeng Li, Chen Yan, Xiaoyu Ji, and Wenyuan Xu. Lightantenna: Characterizing the limits of fluorescent lamp-induced electromagnetic interference. In *NDSS Symposium*. Internet Society, 2025.

[94] Yan Long, Qinhong Jiang, Chen Yan, Tobias Alam, Xiaoyu Ji, Wenyuan Xu, and Kevin Fu. Em eye: Characterizing electromagnetic side-channel eavesdropping on embedded cameras. In *NDSS Symposium*. Internet Society, 2024.

[95] Paolo Crovetti and Francesco Musolino. Digital suppression of emi-induced errors in a baseband acquisition front-end including off-the-shelf, emi-sensitive operational amplifiers. *Electronics*, 10(17):2096, 2021.

[96] Andrea Lavarda, Luca Petruzzi, Nejc Radež, and Bernd Deutschmann. On the Robustness of CMOS-chopped Operational Amplifiers to Conducted Electromagnetic Interferences. *IEEE TEMC*, 60(2):478–486, 2017.

[97] Abdullah Z Mohammed, Louis Jenkins, Rees Hatch, Gökçen Y Dayanıklı, Craig Simpson, Ryan Gerdes, and Hongjie Wang. The iemi effect: On the efficacy of pcb-level countermeasures in adversarial environments. In *2024 IEEE 9th European Symposium on Security and Privacy (EuroS&P)*, pages 361–380. IEEE, 2024.

[98] Christian Adami, Christian Braun, Peter Clemens, Michael Suhrke, HU Schmidt, and Achim Taenzer. Hpm detection system for mobile and stationary use. In *10th International Symposium on Electromagnetic Compatibility*, pages 1–6. IEEE, 2011.

[99] Ch. Adami and Ch. Braun. Hpm detector system with frequency identification. In *2014 International Symposium on Electromagnetic Compatibility*, pages 140–145. IEEE, 2014.

[100] Devaprakash Muniraj and Mazen Farhood. Detection and mitigation of actuator attacks on small unmanned aircraft systems. *Control Engineering Practice*, 83:188–202, 2019.

[101] Youqian Zhang and Kasper Rasmussen. Detection of electromagnetic interference attacks on sensor systems. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 203–216. IEEE, 2020.

[102] Kai Fang, Tingting Wang, Xiaochen Yuan, Chunyu Miao, Yuanyuan Pan, and Jianqing Li. Detection of weak electromagnetic interference attacks based on fingerprint in iiot systems. *Future Generation Computer Systems*, 126:295–304, 2022.

[103] Tingting Wang, Jianqing Li, Wei Wei, Wei Wang, and Kai Fang. Deep-learning-based weak electromagnetic intrusion detection method for zero touch networks on industrial iot. *IEEE Network*, 36(6):236–242, 2022.

[104] Hongjun Choi, Sayali Kate, Yousra Aafer, Xiangyu Zhang, and Dongyan Xu. Software-based realtime recovery from sensor attacks on robotic vehicles. In *23rd International Symposium on Research in Attacks, Intrusions and Defenses*, pages 349–364, 2020.

[105] Youqian Zhang and Kasper Rasmussen. Detection of electromagnetic signal injection attacks on actuator systems. In *25th International Symposium on Research in Attacks, Intrusions and Defenses*, 2022.

[106] Yazhou Tu, Vijay Srinivas Tida, Zhongqi Pan, and Xiali Hei. Transduction shield: A low-complexity method to detect and correct the effects of emi injection attacks on sensors. In *2021 ACM Asia CCS*, pages 901–915, 2021.

[107] Hang Cai and Krishna K Venkatasubramanian. Detecting signal injection attack-based morphological alterations of ecg measurements. In *2016 IEEE DCOSS*, pages 127–135, 2016.

[108] Kevin Sam Tharayil, Benyamin Farshteindiker, Shaked Eyal, Roy Hershkovitz, Shani Houri, Ilia Yoffe, Michal Oren, and Yossi Oren. Sensor defense in-software (sdi): Practical software based detection of spoofing attacks on position sensors. *Engineering Applications of Artificial Intelligence*, 95:103904, 2020.

[109] Milad Rezaee, Sebastian Köhler, and Kasper Rasmussen. Ripple: Software-only detection of signal injection attacks in drone temperature sensors. In *18th ACM WiSec*, pages 147–159, 2025.

[110] Anomadarshi Barua and Mohammad Abdullah Al Faruque. Premsat: Preventing magnetic saturation attack on hall sensors. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 438–462, 2022.

[111] Dimitrije Erdeljan. *Eavesdropping risks of the displayport video interface*. PhD thesis, University of Cambridge (United Kingdom), 2023.

[112] Michele Menegon, Chiara Cantaloni, Ana Rodriguez-Prieto, Cesare Centomo, Ahmed Abdelfattah, Marzia Rossato, Massimo Bernardi, Luciano Xumerle, Simon Loader, and Massimo Delledonne. On site dna barcoding by nanopore sequencing. *PLoS One*, 12(10):e0184741, 2017.

[113] Ferhat Erata, Chuanqi Xu, Ruzica Piskac, and Jakub Szefer. Quantum circuit reconstruction from power side-channel attacks on quantum computer controllers. *ACR Transactions on Cryptographic Hardware and Embedded Systems*, 2025.

[114] Raspberry Pi. Ai camera. https://www.raspberrypi.com/documentation/accessories/ai-camera.html, 2024.

[115] Ariel Schwarz, Zeev Zalevsky, and Yosef Sanhedrai. Digital camera sensing and its image disruption with controlled radio-frequency reception/transmission. In *2011 IEEE COMCAS*.

[116] Hikaru Nishiyama, Daisuke Fujimoto, Youngwoo Kim, Hideaki Sone, and Yu-Ichi Hayashi. Iemi fault injection method using continuous sinusoidal wave with controlled frequency, amplitude, and phase. In *2021 EMC Compo Workshops*, pages 97–101, 2022.

[117] Arthur Beckers, Josep Balasch, Benedikt Gierlichs, Ingrid Verbauwhede, Saki Osuka, Masahiro Kinugawa, Daisuke Fujimoto, and Yuichi Hayashi. Characterization of em faults on atmega328p. In *2019 IEEE EMC Sapporo/APEMC*, pages 1–4. IEEE, 2019.

[118] M. J. Basford, C. Smartt, D. W. P. Thomas, and S. Greedy. On the disruption of wired serial communication links by time domain interference. In *2018 IEEE EMC/APEMC*.

A Surveyed Works

This SoK surveys over 80 IEMI attack and defense papers spanning major security venues (e.g., USENIX Security, IEEE S&P, ACM CCS, NDSS, ACSAC, AsiaCCS, RAID, WiSec, CHES,VehichleSec), related systems and networking venues (e.g., IMWUT, MobiCom, INFOCOM, ICCAD, SenSys, Sensors), theses, and the EMC community (e.g., IEEE T-EMC, T-MTT, EMC+SIPI, and major EMC symposia). Over the past two decades, reported IEMI attacks have increased almost exponentially, significantly outpacing defense-oriented studies. Yet, a systematic methodology for analyzing and comparing these attacks remains lacking, hindering accurate assessment of practical impact and the design of effective, deployable defenses. Accordingly, our systematization aims to enable in-depth comparison across prior work to highlight commonalities and key differences.

B Modeling Details

Target Sampler. A target sampler can be modeled as a sample function $\mathcal{S}[\cdot]$ that takes in three analog voltage signals, including an input $V(t)$ that the sampler intends to measure, a clock $C(t)$, and a reference signal R(t), and outputs a discrete data sample, i.e.,

$$\begin{aligned} Samp[n] &= \mathcal{S}[V(t), C(t), R(t)] \\ &= \left\lfloor (2^{N_{bit}} - 1) \cdot Clip\left(\frac{V(LocEdge(n,C))}{R(LocEdge(n,C))}\right) \right\rceil, \end{aligned} \quad (6)$$

where N_{bit} denotes the bit resolution of the sampler's output with $n \in \mathbb{N}$ representing a natural number index of the current operation cycle. $Clip(x) = min(max(x,0),1)$ limits saturated signals. $\lfloor \cdot \rceil$ rounds up to the nearest integer. As shown in Fig. 2, the target sampler updates its output at the rising (or falling) clock edge and holds it until the next cycle. The mapping from t to n follows

$$CntEdge(C(t)) = n \Rightarrow t = LocEdge(n,C), \quad (7)$$

where $CntEdge$ reports the current cycle of the processor and $LocateEdge$ finds the physical time t corresponding to the clock's cycle-advancing edge. This produces an instantaneous sampling rate of the target sampler as: $f_s(n) = 1/(LocEdge(n,C) - LocEdge(n-1,C))$.

IEMI Coupling. The transfer function $\mathcal{T}(\cdot)$ models EM energy delivery from the adversary to the target via an IEMI propagation channel T_P^{in} and a coupling channel $T_C^{in}(\cdot)$. $T_P^{in}(\cdot)$ characterizes signal transmission from the attacker to the target surface and is constrained by factors such as injection distance d_{inj}, angle θ_{inj}, casing and board materials (M_{case}, M_{board}), and the coupling interface location L_C.

Amplitude Control Causing Deviations. Eqs. (3) and (6) show that on the target sampler level, the impact of an IEMI attack could be measured by quantifying the deviation from the hypothetical authentic $\widehat{Samp}[n]$ with no IEMI attacks:

$$\delta_{samp} = Samp[n] - \widehat{Samp}[n] = \left\lfloor (2^{N_{bit}} - 1) \cdot Clip\left(\frac{V_{adv}(t)}{R(t)}\right) \right\rceil. \quad (8)$$