SoK: Understanding the Fundamentals and Implications of Sensor Out-of-band Vulnerabilities

Shilin Xiao, Wenjun Zhu, Yan Jiang, Kai Wang, Peiwang Wang, Chen Yan, Xiaoyu Ji[*], Wenyuan Xu
Zhejiang University
{xshilin, zwj_, yj98, eekaiwang, wangpw, yanchen, xji, wyxu}@zju.edu.cn

***Abstract*—Sensors are fundamental to cyber-physical systems (CPS), enabling perception and control by transducing physical stimuli into digital measurements. However, despite growing research on physical attacks on sensors, our understanding of sensor hardware vulnerabilities remains fragmented due to the ad-hoc nature of this field. Moreover, the infinite attack signal space further complicates threat abstraction and defense. To address this gap, we propose a systematization framework, termed sensor *out-of-band* (OOB) vulnerabilities, that for the first time provides a comprehensive abstraction for sensor attack surfaces based on underlying physical principles. We adopt a bottom-up systematization methodology that analyzes OOB vulnerabilities across three levels. At the component level, we identify the physical principles and limitations that contribute to OOB vulnerabilities. At the sensor level, we categorize known attacks and evaluate their practicality. At the system level, we analyze how CPS features such as sensor fusion, closed-loop control, and intelligent perception impact the exposure and mitigation of OOB threats. Our findings offer a foundational understanding of sensor hardware security and provide guidance and future directions for sensor designers, security researchers, and system developers aiming to build more secure sensors and CPS.**

I. Introduction

Sensors serve as the essential bridge between the physical and cyber worlds by transducing physical stimuli into digital signals. They are widely deployed in cyber-physical systems (CPS), ranging from industrial robots to critical infrastructure, and are crucial in providing correct measurements for decision-making in safety-sensitive CPS. Incorrect sensor measurements have been linked to major safety incidents, including factory explosions [1], airplane crashes [2], and fatalities caused by industrial robots [3]. These events highlight the importance of ensuring sensor reliability as a fundamental requirement for CPS security.

Unfortunately, sensors are vulnerable to physical-world attacks, such as signal injection attacks and side-channel attacks. In signal injection attacks, sensor measurements can be manipulated by various physical signals [4–7]. For instance, ultrasound or lasers modulated with voices can inject malicious commands into microphones, while carefully-crafted electromagnetic signals can induce fake touchpoints on touchscreens. In side-channel attacks, sensors can unintentionally leak sensitive information through TEMPEST-like side channels [8–10], where electromagnetic radiation can be exploited to extract biometric data such as fingerprints or iris patterns. These works reveal that sensors exhibit non-negligible hardware vulnerabilities that have become severe threat vectors in CPS.

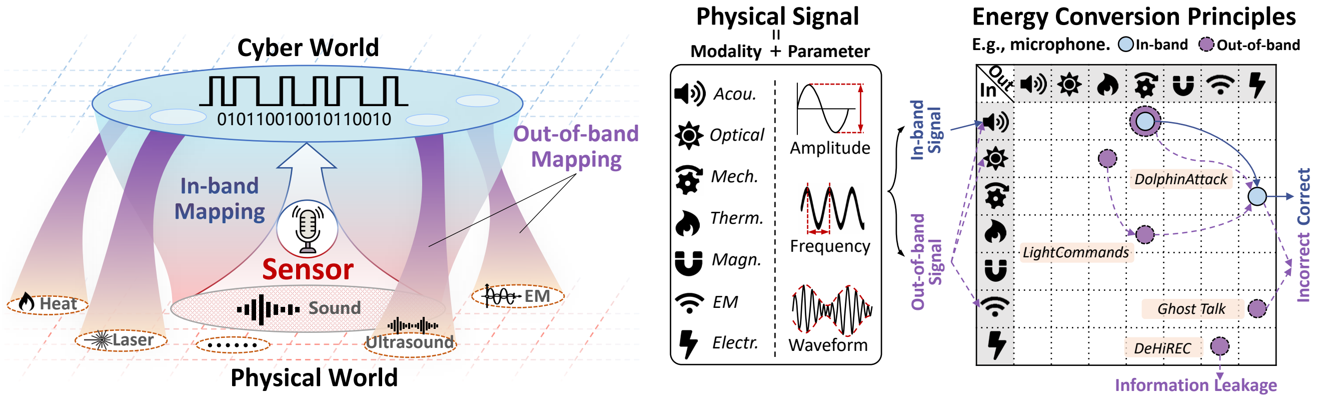
However, despite extensive research uncovering various threat vectors, our understanding of sensor vulnerabilities remains limited, due to the standalone and ad-hoc nature of this research area. Furthermore, the virtually infinite combinations of physical signals that can compromise sensor security make it difficult to abstract these threats comprehensively. As a result, a unified and effective framework that captures both known and potential vulnerabilities is urgent for improving sensor security but has yet to be fully established. While several SoK papers and surveys have examined sensor security, they mainly focus on unifying attack methodologies [11, 12] or analyzing specific scenarios [13–15], without providing a profound understanding of sensor vulnerabilities themselves. This lack of systematic understanding continues to hinder the effective detection and defense strategies.

To bridge this gap, this paper integrates previous research and domain knowledge with physical principles to develop a systematic framework for categorizing and analyzing threat vectors. We begin by examining the fundamental operation of sensors. Each sensor establishes a *mapping* between physical stimuli and digital measurements, which we refer to as *in-band mapping*. For example, the in-band mapping of a microphone converts audible sounds into voice recordings. However, studies have shown that lasers or ultrasound can also produce voice recordings, as illustrated in Fig. 1a. These interactions fall outside the sensor's intended operational scope and are referred to as *out-of-band* (OOB) mappings. OOB mappings stem from the inherent limitations of sensor components, such as material, mechanical, electrical non-idealities. Accordingly, we define sensor *out-of-band* vulnerability as the security risk caused by OOB mappings.

To abstract OOB threat vectors, we model attack signals in terms of their modality and physical parameters, as illustrated in Fig. 1b. From a physical perspective, measurand modalities can be classified into seven categories: acoustic, optical, mechanical, thermal, magnetic, electromagnetic, and electrical [16]. Each modality can be further characterized

[*] Xiaoyu Ji is the corresponding author.

Network and Distributed System Security (NDSS) Symposium 2026
23-27 February 2026, San Diego, CA, USA
ISBN 979-8-9919276-8-0
https://dx.doi.org/10.14722/ndss.2026.230450
www.ndss-symposium.org



(a) In-band mapping v.s. Out-of-band mapping

(b) Energy conversion principles

Fig. 1. Illustration of sensor *in-band* and *out-of-band* mappings. *In-band* reflects a sensor's intended functionality, while out-of-band refers to unintended functionality between physical and cyber worlds.

by its amplitude, frequency, and waveform. The fundamental interactions between attack signals and sensor OOB vulnerabilities can be captured using a 7 × 7 matrix, where each cell represents a specific energy conversion pathway, e.g., mechanical-to-electrical transduction. A vulnerability exists if there is a viable path through this matrix that starts with an injected signal modality and ends in the electrical column, ultimately producing a measurable digital output. For instance, the LightCommands attack [17] exploits a chain of conversions: optical-to-thermal, thermal-to-mechanical, and mechanical-to-electrical. Similarly, EM side-channel leakage, as demonstrated by DeHiREC [18], leverages an electrical-to-electromagnetic conversion pathway, as shown in Fig. 1b. Building on this abstraction, we further analyze the underlying mechanisms of OOB vulnerabilities across key sensor components (e.g., amplifiers, filters, transducers), and identify threat vectors that may emerge during different stages of sensor design, thereby providing guidance for secure sensor design practices.

Based on the modeled energy conversion pathways, we classify OOB vulnerabilities into two types: *out-of-range* and *cross-field*. *Out-of-range* vulnerabilities arise when the attack signal shares the same physical modality as the intended signal but exceeds the sensor's design limits in amplitude or frequency. In contrast, *cross-field* vulnerabilities involve signals from unintended physical modalities that exploit unintended energy conversions to manipulate sensor measurements or induce electrical signals through side channels.

While many attacks have been demonstrated in laboratory settings, some studies suggest their practicality may be limited in real-world environments [14], or that they pose minimal threat to specific CPS applications [19]. To assess real-world impact, we evaluate each attack across multiple dimensions: attacker prior knowledge required, effective attack distance, attack cost that includes device cost, size. This evaluation gain insights to guide future directions for improving exploitation efficiency and uncovering new attack surfaces. Furthermore, we systematically show that none of the key CPS characteristics, such as closed-loop control, multi-sensor fusion, and intelligent perception, can completely defend against OOB vulnerabilities, and highlight their respective strengths and limitations against sensor attacks. This analysis helps system developers prioritize and tailor their defense strategies.

We summarize our contributions as follows.

- To the best of our knowledge, we proposed the first systematic framework that provides a comprehensive abstraction for sensor threats at the signal level, which essentially models sensor out-of-band (OOB) vulnerabilities and elucidate their core mechanisms, providing a theoretical framework for efficient vulnerability detection.
- We model and analyze existing OOB exploitation methods to evaluate their feasibility in practical settings and identify critical research gaps, utilizing the proposed systematic framework and validating its generalizability.
- We explore the system-level implications of OOB vulnerabilities, revealing how different CPS architectures react to sensor attacks, thus offering enhanced security guidance for system designers.

II. Background and Threat Model

In this section, we introduce the background of sensor hardware composition, identify the threat model of sensor OOB vulnerability, and clarify our research scope.

A. Sensor Background

A sensor is designed to respond to a physical stimulus and generate electrical measurements. Sensors can be classified into over 350 categories based on their measurand types [20] and vary widely in function and operational principles. Nevertheless, a modern sensor comprises four main components: transducer, signal conditioning circuits, communication interface, and power supply [21], as shown in Fig. 2.

- *Transducer.* Transducers respond to physical stimuli and consist of sensitive and conversion elements [22]. The former detects a physical stimulus, and the latter transforms the physical stimulus into an analog electrical signal.

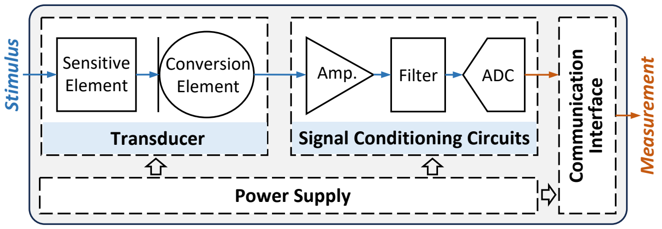


Fig. 2. The hardware composition of a modern sensor.

- *Signal conditioning circuits.* Since the analog signal from the transducing process is noisy and weak, the signal conditioning circuits have to amplify it, reduce noise, digitize it, and even perform additional digital signal processing before measurement can be utilized. These are typically accomplished by amplifiers, filters, ADCs, etc.
- *Communication interface.* The communication interface enables sensor measurements to be transferred for calculation or decision-making and contains interface circuits with a chosen protocol, e.g., I2C or SPI.
- *Power supply.* Typically, a DC power supply is adopted to provide energy to ensure the continuous operation of other sensor components, and may include a transformer, rectifier, filter, and regulator that are designed to control and modulate the power supply.

Each component may introduce sensor vulnerabilities, and we will analyze their root cause and implications at the system level in the following section. Note that Fig. 2 represents a typical composition of most sensors, but special sensors may include extra components, e.g., an active sensor such as LiDARs may incorporate signal transmitters.

B. Threat Model

We identify a common threat model from existing work.

- *Attacker capabilities.* **a) Knowledge.** A conservative assumption is that attackers have no prior knowledge of the target sensors and their associated systems. In practice, most studies assume attackers can gain partial knowledge by prestudying identical devices or reading related documentation. **b) Accessibility to victim sensors.** Most studies assume that attackers have no physical access to victim's sensors to avoid raising the victim's awareness. Instead, attackers can determine whether an attack succeeds by indirect feedback from the system, such as changes in LED indicators or system behavior. In some scenarios, attackers can also implant malware on the victim's device to access sensor readings. **c) Attack devices.** Attackers can use commonly available devices such as signal generators, amplifiers, speakers, laser emitters, and antennas to inject signals or capture side-channel emissions. Moreover, they can customize attack devices to meet requirements for portability and stealth.
- *Attack goals.* The attack goals can be classified into three types: **a) Denial-of-Service (DoS).** The attacker aims to make the measurement unavailable by overwhelming it with high-intensity noise, such as emitting ultrasound to jam ultrasonic sensors [23]. **b) Measurement spoofing.** The attacker spoofs the sensor to produce seemingly legitimate but erroneous measurements, such as creating fake touchpoints on touchscreens by injecting EMI signals into the power cable [24]. **c) Privacy Snooping.** The attacker can exploit the side-channel leakage of a sensor to recover private information, such as inferring the victim's keystrokes by recognizing the touchscreen's electromagnetic emanations [25].
- *Defense goals.* We adapt the well-known CIA (Confidentiality, Integrity, and Availability) triad specifically to the context of sensor security. While achieving a perfect CIA triad is nearly impossible, these goals provide general guidelines to help designers understand and prioritize the defenses against sensor attacks. **a) Availability.** A sensor's functionality shall be available to the system in spite of disturbances from the outside world. **b) Integrity.** A sensor's sensitive measurement shall correctly reflect the physical quantity being measured according to its design function. **c) Confidentiality.** A sensor's measurement shall not be divulged to the outside world in the form of any physical signals. Note that the three defense goals align with the aforementioned three attack goals: (1) *availability* $\leftrightarrow$ *denial-of-service*, (2) *integrity* $\leftrightarrow$ *spoofing*, and (3) *confidentiality* $\leftrightarrow$ *snooping*.

C. Scope of the Study

To provide a more focused systematization and clarify our research scope, the following topics are excluded. **a) Sensors for security purpose and atypical sensors.** This excludes sensors that are specifically used to detect tampering or signal injection attacks in CPS, and atypical sensors without transducers, such as time-to-digital converters and ring oscillators. **b) Cyber-domain security on sensor-involved systems.** This excludes sensor network security research [26] and physical adversarial example attacks [27], which do not exploit sensor vulnerabilities. **c) Privacy snooping using sensor's intended functionality.** This excludes attacks such as eavesdropping via radar [28, 29], keystroke inference via motion sensors [30–34] or microphones [35–40], and identity inference via motion sensors [10].

III. Component-level Vulnerability Analysis

In this section, we present a component-level analysis of sensor OOB vulnerabilities. Specifically, we formalize an OOB model that categorizes OOB vulnerabilities into two types: *out-of-range* and *cross-field*, and thoroughly analyze their underlying principles. Based on this, we summarize the exploited and potential OOB vulnerabilities across different sensor components, which can further guide the secure sensor design and help prioritize testing strategies.

A. Out-of-band Vulnerability Model

Sensor *out-of-band* (OOB) vulnerabilities refer to security flaws resulting from unintended mappings between physical-world signals and cyber-world measurements, which is beyond

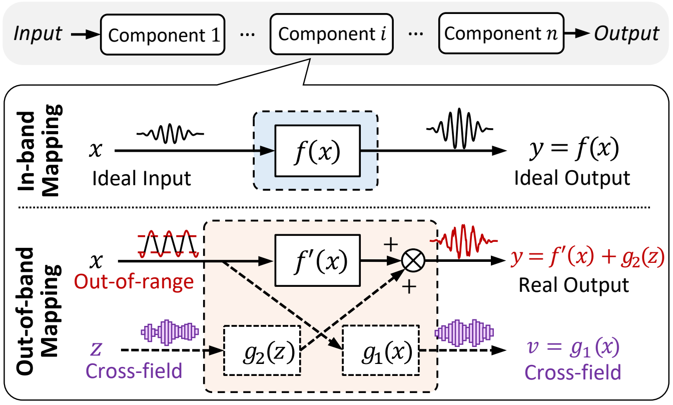


Fig. 3. Sensor OOB vulnerability model. We use the input-output mapping functions to formalize the intended and unintended behaviors of sensors.

the sensor's intended functionality. The OOB vulnerability model is presented in Fig. 3. The intended functionality of each sensor component is formalized as an input-output mapping function $y = f(x)$, i.e., *in-band mapping*. However, due to non-ideal factors such as material limitations and electrical properties, sensor components may exhibit unintended behaviors, namely *out-of-band mapping*. Specifically, these unintended mappings can be categorized into *out-of-range* mappings and *cross-field* mappings, described as follows:

- *Out-of-range mapping $f'(x)$* represents the response to an input signal x that lies within the intended physical field, but falls outside the intended operational range, including amplitude and frequency. For instance, the acoustic transducer of a microphone is intended to receive audible sounds, ranging from 20 Hz to 20 kHz, but it can also respond to ultrasonic signals (>20 kHz) that are out of the intended frequency range, which enables malicious inaudible voice command injection [4].
- *Cross-field mapping $g(\cdot)$* refers to the unintended signal interactions across different physical fields and consists of two directions: **a) cross-field output** $g_1(x)$ describes the case where an internal signal x unintentionally radiates or leaks signals v into another physical field (e.g., optical, acoustic, thermal, or electromagnetic). For example, circuit wires may inadvertently act as antennas, emitting electromagnetic interference (EMI) that leaks information about internal signals [41]. **b) cross-field input** $g_2(z)$ models the reverse situation, where the system receives an input z from a non-intended physical field, leading to unintended outputs $g_2(z)$ that superimpose with or distort the intended output y. For example, MEMS microphones designed to pick up sound can also be stimulated by modulated laser light, leading to injected signals or commands [17].

B. Fundamentals of Out-of-band Vulnerability

To further investigate the fundamentals of sensor OOB vulnerabilities, we systematize the vulnerabilities of various sensor components and their mechanisms, as summarized in Table I. Specifically, we identify which components contribute to either *out-of-range* vulnerability or *cross-field* vulnerability.

1) Out-of-range Vulnerability: We consider *out-of-range* vulnerabilities from two aspects: amplitude and frequency.

- *Amplitude out-of-range* (**OR.A**). An amplitude *out-of-range* signal impacts the output by the **saturation effect**. Transducers and signal conditioning circuits operate well within a predefined amplitude range. When the input signal exceeds this range, saturation occurs, resulting in signal clipping, i.e., $f'(x) = c \ (x \geq x_{max})$. For transducers, saturation is mainly due to the physical constraints of the transducer materials, e.g., the number of electron-hole pairs that can be generated in photovoltaic materials is limited [42]. Thus, a high-intensity light can saturate an optical sensor [43], leading to the maximum output. In signal conditioning circuits, saturation is generally caused by supply voltage limitations in active circuit elements. When the input is an alternating current (AC) signal, symmetric saturation introduces harmonic distortion, while asymmetric saturation also introduces a direct current (DC) bias. This mechanism has been exploited in amplifiers [5], and we posit it likely exists in filters and ADCs as well.
- *Frequency out-of-range* (**OR.F**). A frequency *out-of-range* signal can affect the output by nonlinearity, non-ideal cutoff, and aliasing effect. **Nonlinearity** is common in both transducers and signal processing circuits, and can be formulated as $f'(x) = a_0 + a_1 x + a_2 x^2 + \cdots$. In exploited cases, acoustic transducers and amplifiers have been shown to convert modulated high-frequency signals into low-frequency outputs via inter-modulation distortion (IMD) [4]. Similarly, nonlinear rectification in amplifiers can convert AC signals into DC offsets [44]. **Non-ideal cutoff** refers to the imperfect frequency response of transducers and filters, which fails to effectively suppress high-intensity signals in the stop-band. As a result, we have $|F'(\omega)| > 0 \ (\omega \geq \omega_c)$, where F' is the Fourier transform of f' and ω_c is the cutoff frequency. Exploited cases include microphone transducers responding to ultrasound [4], ultraviolet sensors reacting to visible lasers [45], and low-pass filters failing to eliminate stop-band frequencies [7]. The **aliasing effect** occurs when ADCs receive input signals containing frequency components above the Nyquist frequency (i.e., $\omega > \omega_s/2$), where ω_s is the sampling rate. Then, the spectrum of $F'(\omega)$ contains aliasing frequencies $\omega_a = |\omega - k\omega_s|$ where $k = \text{round}(\omega/\omega_s)$. As a result, high-frequency signals can be incorrectly interpreted as low-frequency components during sampling, effectively demodulating them into the output [46].

2) Cross-field Vulnerability: We consider *cross-field* vulnerabilities in terms of signal modalities, i.e., acoustic, optical, electromagnetic, mechanical, and thermal. While optical, EM, and thermal signals all belong to the EM spectrum in the physical sense, we discuss them separately due to their fundamental differences in energy conversion mechanisms and propagation behaviors. Besides, since electric, magnetic, and EM signals

TABLE I. Taxonomy and mechanisms of sensor OOB vulnerability

Taxonomy			Transducer					Signal Cond.			Com.	Pwr.	Unsecure Phase			
Type	Subtype	Label	🔊	☀	📶	⚙	🔥	Amp.	Fil.	ADC			TS	ECD	P&A	T&C
Out-of-range	Amplitude *out-of-range*	OR.A	◐	●	◐	◐	◐	●	◐	◐	○	○	✔	✔		✔
	Frequency *out-of-range*	OR.F	●	◐	◐	◐	×	●	●	●	×	●	✔	✔		✔
Cross-field	Acoustic signal *cross-field*	CF.🔊	×	○	○	●	○	○	○	○	○	○	✔		✔	✔
	Optical signal *cross-field*	CF.☀	●	×	●	◐	◐	◐	◐	◐	○	○	✔		✔	✔
	EM signal *cross-field*	CF.📶	◐	◐	×	◐	◐	●	●	●	●	●	✔	✔	✔	✔
	Mechanical signal *cross-field*	CF.⚙	●	○	○	×	○	○	○	○	○	○	✔		✔	✔
	Thermal signal *cross-field*	CF.🔥	◐	○	○	○	×	◐	◐	◐	○	○	✔	✔	✔	✔

🔊 Acoustic ☀ Optical 📶 Electromagnetic (also includes electrical and magnetic) ⚙ Mechanical 🔥 Thermal
● Exploited ◐ Potential to be exploited ○ Not exploitable × Not applicable
TS Transducer selection **ECD** Electronic circuit design **P&A** Packaging and assembling **T&C** Testing and calibration

are inherently coupled, we unify them under the term EM to simplify the taxonomy.

- *Acoustic signal cross-field* (CF.🔊). Acoustic *cross-field* signals can affect transducers by **resonance effect**. MEMS transducers used in motion sensors, such as accelerometers and gyroscopes, exhibit inherent resonant frequencies, making them sensitive to acoustic noise [47]. As a result, sound or ultrasound waves near the resonant frequency can induce high-intensity interference signals within the transducer [5], i.e., we have $g_2(z) = A\cos(\omega_a t + \phi)$ where ω_a is the acoustic signal frequency.
- *Optical signal cross-field* (CF.☀). Optical *cross-field* signals can affect transducers by **photoacoustic effect** and **photoelectric effect**. The photoacoustic effect converts light energy into mechanical vibrations, which can disturb sensors with diaphragm structures designed to detect such vibrations, such as MEMS microphones. These microphones have been shown to respond to amplitude-modulated light [17], producing outputs like $g_2(z) = A[1 + \cos(\omega_o + \phi)]$, where ω_o is the modulation frequency. The photoelectric effect, on the other hand, occurs when light liberates electrons from a material's surface, generating electric currents. Sensors with exposed conductive parts, such as MEMS barometers [48], are vulnerable to this effect, allowing the attacks to induce output bias under illumination, i.e., $g_2(z) = b$.
- *Electromagnetic signal cross-field* (CF.📶). Electromagnetic (EM) *cross-field* signals can affect signal conditioning circuits by **antenna effect**, where conductive elements (especially wires) act as unintended antennas, receiving ($g_2(z)$) or transmitting ($g_1(x)$) electromagnetic radiation. This effect is especially pronounced when the conductor length approaches a quarter of the EM signal's wavelength, forming a resonant structure that efficiently couples EM energy into the circuit. This mechanism has been exploited by attackers in transducers [8], amplifier input wires [44], ADCs [18], and communication cables [49].
- *Mechanical signal cross-field* (CF.⚙). Just as acoustic signals can affect mechanical transducers, mechanical *cross-field* signals can influence acoustic transducers also by **resonance effect**. A notable example is the injection of vibration signals directly into the diaphragm of an acoustic transducer [50]. However, mechanical signals must propagate through rigid media to reach the sensor, so their practicality for inducing OOB vulnerabilities is limited. Consequently, mechanical signals are not commonly exploited in this field.
- *Thermal signal cross-field* (CF.🔥). Thermal *cross-field* signals have not yet been directly exploited in attacks due to the difficulty of transmitting thermal energy over long distances and inducing swift temperature changes. Nevertheless, many sensor components are known to exhibit temperature sensitivity, such as **temperature drift** in amplifiers and other analog circuits [51]. Thus, we consider thermal *cross-field* signals a potential but underexplored vector for inducing OOB vulnerabilities, which represents a notable gap in current research.

Note that the above analysis is grounded in the energy conversion principles that have been exploited in existing attacks. In fact, other physical principles remain unexplored, which can be promising directions for future research. For instance, the optical-pressure effect in mechanical transducers and thermal laser stimulation in thermal transducers may introduce new attack vectors, which are marked as potential in Table I. Our taxonomy of OOB vulnerability thus can serve as a reference for identifying such research gaps.

C. Implications for Sensor Design and Vulnerability Testing

Despite the inherent presence of OOB vulnerabilities in sensors, it is impractical to eliminate all non-idealities during the design phase due to the broad interdisciplinary nature of sensor engineering and the physical limitations of materials and components. Instead, it is essential to identify and prioritize non-idealities that may lead to exploitable vulnerabilities. To this end, our proposed vulnerability model and mechanism analysis can serve as a practical guide for designers to anticipate and mitigate security-critical issues throughout the sensor development lifecycle.

1) Sensor Design: Sensor design typically consists of three major stages: transducer selection, electronic circuit design, and packaging and assembling [21, 52]. Non-ideal behaviors can arise at each of these stages and, while often treated as tolerable deviations in conventional performance metrics, they may be leveraged by attackers as vectors for OOB exploitation. **a) Transducer Selection.** This phase is a critical source of potential OOB vulnerabilities. Designers often overlook unintended energy conversion pathways that arise from the inherent physical properties of selected materials or structural designs. For example, choosing MEMS-diaphragm-based transducers can expose even non-optical sensors to optical *cross-field* signals due to the diaphragm's susceptibility to light-induced vibrations [17, 48]. These *cross-field* responses are typically undocumented in datasheets, yet they can pose significant security risks. **b) Electronic Circuit Design.** This phase introduces OOB vulnerabilities associated with signal conditioning circuits, power supplies, and communication interfaces. Non-idealities, such as saturation and nonlinearity, are inherent properties of electronic circuits. Designers typically define valid input ranges to mitigate their impact. However, in practice, it is infeasible to physically restrict the injection of OOB signals. As a result, sensor design alone is insufficient to fully eliminate OOB vulnerabilities in this phase, necessitating complementary system-level defense strategies, as discussed in Sec. VI. **c) Packaging and Assembly.** This phase can introduce additional *cross-field* vulnerabilities due to insufficient shielding and structural alterations. Assembly may modify the mechanical structure and electrical characteristics of the sensor, potentially introducing new mechanical resonance or electromagnetic coupling frequencies. For instance, through consulting with system developers, we found that MEMS vibration sensors mounted at certain locations on a motherboard can be affected by system-level resonance frequencies, leading to inaccurate measurements.

2) Vulnerability Testing: Existing sensor testing is insufficient since it primarily focuses on the sensor's accuracy. Key characteristics such as functionality, sensitivity, and linearity are typically evaluated using *in-band* signals, while the potential effects of OOB vulnerabilities are largely overlooked. Although some tests, such as electromagnetic compatibility (EMC) testing, consider EM *cross-field* signals, they are limited to specific frequency ranges and cannot effectively cover the broader spectrum of potential attack signals [7]. Consequently, such tests are inadequate for detecting OOB vulnerabilities, which also remain undocumented in sensor datasheets. That said, not all OOB signals warrant mitigation. Whether an OOB signal should be considered a threat depends on whether the sensor's transduction principle allows it to respond to that signal, and whether the transduction process is efficient enough to be exploited. For example, although MEMS sensors contain conductive components in both the transducer and internal circuitry, typical EMI signals rarely succeed in attacking them. We suppose this is due to the highly integrated, micrometer-scale internal structure of MEMS devices, which would require electromagnetic waves with micrometer-scale wavelengths, i.e., in the terahertz (THz) or near-infrared range, to interact effectively. Since such frequencies border on or fall within the optical spectrum, conventional EMC testing for these bands is neither practical nor necessary for MEMS transducers and their associated conditioning circuits.

In conclusion, we argue that *security-aware sensor design* must evolve beyond traditional performance-centric paradigms. By incorporating OOB vulnerability taxonomy early in the design process, engineers can better anticipate potential attack vectors and adopt mitigation strategies such as shielding, filtering, redundancy, or cross-domain isolation, which will be further discussed in Sec. VI. Rather than attempting to eliminate all nonidealities, designers should focus on identifying and mitigating those most likely to be adversarially exploitable. Our formalization provides the foundation for this security-aware approach to sensor security.

IV. Sensor-level Attack Systematization

In this section, we systematically analyze how OOB sensor vulnerabilities enable *sensor-level* attacks. While numerous attacks exist, they remain fragmented as isolated cases with disparate attack scenarios and threat models of varying severity, which hinders the generalization of the attack methods across different sensors. Moreover, attackers tend to adopt favorable threat models for attack success that may exaggerate the real-world practicality of attacks [14]. Thus, in this section, we conduct a comprehensive analysis of existing literature, identify common mechanisms among different studies, and evaluate the practicality of each attack.

A. Systematization Methodology

We systematize sensor-level attacks in terms of *attack signal*, *target sensor*, *attack path*, *attack goal*, and *attack practicality*, as shown in Table II.

1) Attack Signal: We classify the attack signals into four modalities. **a) Sound/Ultrasound**, **b) Laser**, **c) Radiated EMI**, and **d) Conducted EMI**. Note that in our context, the term *attack signal* refers to both malicious signals actively emitted by attackers and passive side-channel leakage from sensors. This helps to unify the commonality of various attack vectors that exploit OOB vulnerabilities.

2) Attack Goal: We identify three attack goals in existing work. **a) Denial-of-Service (DoS):** The attacker aims to make the measurement unavailable by overwhelming it with powerful noise. **b) Spoofing:** The attacker spoofs the sensors to produce seemingly legitimate but erroneous measurements. **c) Snooping:** The attacker exploits the side-channel leakage of a sensor to recover private information.

3) Attack Path: The attack path includes three stages. **a) Signal parameter:** describes how attack signals are modulated. This includes constant signals (Const.), single-frequency wave (Sine), amplitude modulation (AM), frequency modulation (FM), phase modulation (PM), and pulse width modulation (PWM). **b) Signal transduction:** describes how attack signals are either injected into or emitted from the target sensor. **c) Signal processing:** describes how these signals are manipulated by the sensor's internal circuitry. For each stage, we identify the underlying OOB vulnerability mechanisms (OR.A OR.F CF.🔊 CF.☀ CF.📶) and the associated sensor components (Sec. III-B). The **Pre-** prefix denotes that the signal is injected into the front-end wires of the components.

TABLE II. Systematization of sensor-level attacks

Attack Signal	Target Sensor	Attack Goal			Attack Path			Attack Practicality				Paper
		DoS	Spoof	Snoop	Parameter	Transduction	Process	Knowl.	Range	Cost	Size	
Sound/ Ultrasound	🎙	✓	✓		AM/PWM/FM	Trans. OR.F	Amp. OR.F	■	1~5	2~5	1~5	[4, 50, 53–63]
	✣	✓	✓		Sine	Trans. CF.🔊	Amp. OR.A/Fil. OR.F/ADC OR.F	□	4	3~5	1~3	[5, 64–67]
				✓	/	Trans. CF.🔊	/	■	2	5	5	[6, 10, 68–74]
	⚲		✓		Sine	Trans. CF.🔊	/	□	1	4	5	[75]
Laser	🎙		✓		AM/PWM	Trans. CF.☀	/	■	3~5	3	5	[17, 76–78]
	⚲		✓		AM	Trans. CF.☀	/	■	N/A	1	1	[48]
	📷 📡 IR	✓			Const.	Trans. OR.A	/	■	3~5	2~5	1~5	[43, 79, 80]
Radiated EMI	🎙	✓	✓		AM	Pre-Amp. CF.📶	Amp. OR.F	■	1~3	4	1~5	[46, 81, 82]
	📷		✓		AM/PM	Pre-ADC CF.📶	/	□	2	1~2	1~3	[83, 84]
				✓	/	Comm. CF.📶	/	■	2	3	1	[85]
	📡		✓		AM	Pre-Amp. CF.📶	Amp. OR.F/ADC OR.F	□	4	1	1	[86]
	👆	✓	✓	✓	Sine	Trans. CF.📶	/	■/□	1~2	1~5	1~5	[25, 87–91]
	🫆			✓	/	Trans. CF.📶	/	■	1	4	5	[8]
	V/A		✓		Sine	Pre-ADC CF.📶	ADC OR.F	□	1	3	3	[92]
			✓		AM	Pre-Amp. CF.📶	Amp. OR.F	□	3	1	1	[93]
	🌡		✓		Sine	Pre-Amp. CF.📶	Amp. OR.F	□	5	1	1	[44]
	IR			✓	/	Comm. CF.📶	/	■	1	1	3	[94]
Conducted EMI	🌡 💧 ✣ ⚲	✓	✓		Sine	Pwr. OR.F	Amp. OR.F/ADC OR.F	□	N/A	1~2	5	[7]
	🎙		✓		AM	Pwr. OR.F	Amp. OR.F	□	5	3	3	[41]
			✓		Const./Sine/AM	Pwr. OR.F	Amp. OR.F/ADC OR.F	□	5	2	1	[95]
	📷		✓		Sine	Pwr. OR.F	Amp. OR.F	□	N/A	4	3	[96]
	👆	✓	✓		Sine/AM	Pwr. OR.F	Trans. CF.📶	□	3	3~4	1~3	[24, 97, 98]
				✓	/	Pwr. CF.📶	/	■	N/A	5	5	[9]

🎙 Microphone ✣ Motion sensor ⚲ Force/pressure sensor 📷 Image sensor 📡 Lidar IR Infrared sensor 👆 Touchscreen 🫆 Fingerprint sensor V/A Voltage/current sensor 🌡 Thermometer 💧 Humidity sensor OR.A OR.F CF.🔊 CF.☀ CF.📶 Exploited OOB vulnerability mechanisms
■ Black-box □ White-box 1 2 3 4 5 Higher level indicates higher practicality N/A Not available

4) Attack Practicality: We evaluate attack practicality through four dimensions. **a) Prior knowledge:** black-box (■) indicates the attack requires no sensor-specific knowledge, while white-box (□) indicates the need for detailed sensor parameters such as sensor model, sensitive frequencies, or hardware characteristics. Note that the knowledge here is sensor-level rather than system-level. **b) Attack range:** we classify the maximum demonstrated attack range into five intervals: 1: ≤0.1m, 2: (0.1, 1m], 3: (1, 5m], 4: (5, 10m], and 5:>10m. **c) Attack device cost:** the price to set up the attack device is divided into 1: >10,000\$, 2: (5,000\$, 10,000\$], 3: (1,000\$, 5,000\$], 4: (100\$, 1,000\$], and 5: <100\$. **d) Attack device size:** indicates the ease and stealth to perform an attack [15], and we classify it into 1: fixed installation, 3: backpack-portable, and 5: hand-held device based on their size. In summary, a higher score indicates a higher practicality, which corresponds to a higher attack threat level.

B. Review of Existing Work

1) Attacks by Sound/Ultrasound: **a) Acoustic sensors (🎙).** Attackers can conduct DoS and spoofing attack by exploiting the sensor's response to ultrasonic signals (OR.F) through the injection of frequency *out-of-range* ultrasounds [4, 50, 53–63]. By applying amplitude modulation, ultrasounds can be demodulated into *in-band* audible commands or noises via the nonlinear IMD (OR.F) of the amplifier. Such attacks are considered black-box (■) since nonlinearities are common in microphones and cannot be eliminated. The longest attack range is around 20m (5), as demonstrated in [58]. Most of these attacks have low device costs (4 [4, 53, 54, 58], 5 [55, 56]) and good portability (3 [50, 57], 5 [4, 53–56, 60]). However, there remains a trade-off between attack range and device portability. **b) Non-acoustic sensors (✣ ⚲).** Attackers can launch DoS and spoofing attacks via *cross-field* injections of sound or ultrasound, which induce mechanical resonance in the sensor structure (CF.🔊) [5, 64–67, 75]. These induced signals can be further exploited through mechanisms such as amplifier saturation (OR.A), imperfect filter cutoff (OR.F), and ADC aliasing (OR.F). Since effective attacks require knowledge of the target sensor's resonant frequency, they are categorized as white-box attacks (□). The maximum demonstrated attack range is 7.7m (4 [64]). However, such attacks typically require an audio amplifier to improve the attack signal strength, limiting their portability (1 [5, 64]). In addition, attackers can perform snooping attacks by using motion sensors to capture subtle mechanical vibrations induced by sound waves [6, 10, 68–74], enabling the reconstruction of private speech information. Although such attacks require no extra devices, they suffer from limited attack range (3 [68], 2 [69, 73, 74]) due to the low power of human voice signals.

2) Attacks by Laser: **a) Optical sensors (📷 📡 IR).** Attackers can launch DoS attacks by exploiting the saturation effect (OR.A) of optical transducers through the injection of amplitude *out-of-range* laser signals [43, 79, 80]. These attacks are classified as black-box (■), as saturation is a common and predictable characteristic of optical sensors, requiring no sensor-level knowledge. Thanks to the strong directivity and low divergence of laser beams, signal attenuation over distance is minimal, enabling long-range attacks exceeding 10 meters (5 [43, 80]) to be carried out using low-cost (5 [43, 79]) and highly portable laser devices (5 [43, 79]). However, in real-world scenarios, maintaining a stable laser focus on the target sensor over a long distance often requires fixed setups, which can reduce the practical portability of the attack. Note that here we do not consider lidar spoofing attacks [99–105] since the signals are *in-band*. **b) Non-optical sensors (🎙 ⏲).** Spoofing attacks have also been demonstrated against non-optical sensors such as MEMS microphones [17, 76–78] and pressure sensors [48], by leveraging the photoacoustic (CF.☀) and photoelectric (CF.☀) effects, respectively. For microphones, attackers amplitude-modulate acoustic signals onto laser beams to induce signal injection, achieving ranges of up to 25 meters (5 [17]). The necessary attack devices, including laser drivers, signal repeaters, etc, can be obtained at moderate cost (3 [17, 77, 78]). However, similar to optical DoS attacks, long-range attacks typically require stable and fixed installations, such as tripods [17], limiting portability.

3) Attacks by Radiated EMI: Attackers can utilize signal generators, software radios, power amplifiers, and antennas to emit malicious signals that couple into vulnerable components, such as transducers [87–91], amplifier front-end wiring [44, 46, 81, 82, 86, 93], and ADC front-end wiring [83, 84, 92], leading to DoS or spoofing behaviors. The injected signals can be further manipulated by the nonlinearity of amplifiers (OR.F) [44, 46, 81, 82, 86, 93] or the aliasing effect of ADCs (OR.F) [86, 92]. In addition to active injection, attackers can also employ antennas and spectrum analyzers to passively receive side-channel EM emissions from transducers [8, 25] and communication wires [85, 94] to launch snooping attacks. These attacks share a common mechanism, i.e., all conductors in sensors exhibit the antenna effect (CF.📶). However, effective EMI injection requires knowledge of the coupling frequencies of the target conductors, which are typically obtained by preliminary frequency sweeping tests. Thus, EMI injection attacks are classified as white-box (□). Despite their broad applicability, the practical implementation of these attacks is limited. On the one hand, the attack range is generally short (1 [8, 81, 87–92, 94], 2 [25]) due to the need for precise alignment with vulnerable components or the inherently weak power of emitted side-channel signals. On the other hand, the devices required, including high-end RF gear and precision antennas, are generally expensive (1 [44, 84, 91, 93, 94], 2 [83, 90]) and bulky (1 [44, 46, 82, 84–91, 93]), reducing the portability and stealth of such attacks.

4) Attacks by Conducted EMI: Conducted EMI propagates along transmission lines such as power or ground cables, enabling attackers to induce false measurements in connected sensors (🌡 🌡💧 ✥ ⏲ 🎙 👆 📷). The primary mechanism that facilitates the injection is the non-ideal filtering (OR.F) of the power supply noise. Furthermore, these attacks can exploit other mechanisms, such as the nonlinearity of amplifiers (OR.F) [7, 41, 95], the non-ideal cutoff of filters (OR.F) [7], and aliasing effect of ADCs (OR.F) [7, 41, 95]. Because the attack signal can propagate stably along cables, these attacks are effective in relatively long ranges (5 [41, 95], 3 [24, 97, 98]). One representative approach involves manipulating sensor outputs by injecting fluctuations into the power supply [7, 41, 96], exploiting the sensitivity of internal sensor components to voltage variations. Another technique targets the ground line, where attackers inject malicious signals by exploiting circuit asymmetries [24, 95, 97, 98]. However, similar to radiated EMI attacks, conducted EMI attacks typically require prior knowledge of the vulnerable coupling frequency. As a result, they are classified as white-box attacks (□).

C. Research Gaps and Future Directions

1) Enhancing the attack practicality: Attack practicality is critical to assessing real-world threats, but often overlooked. Our analysis above reveals that acoustic/ultrasonic and radiated EMI attacks typically suffer from limited attack ranges and bulky, expensive attack devices. Thus, we highlight two directions for improving practicality as follows.

- *Extending attack range.* While increasing signal power may improve range, it always introduces trade-offs: higher device cost, larger device size, and safety risks to attackers. Moreover, for acoustic signals, higher power may cause audible leakage due to nonlinearities in speakers and air propagation [60, 106] and compromise attack stealthiness. Instead, attackers can improve signal directionality to boost received power at the target. Promising techniques include using phased arrays, acoustic metamaterials [60] and metasurfaces [107], and metasurface antennas [108] to enhance the signal directionality.
- *Optimizing attack devices.* Many attacks still rely on laboratory-grade signal generators and power amplifiers, despite their functionalities often exceeding the actual needs of signal injection. For example, attacks that use single-frequency signals (denoted as Sine in Table II) do not require full-featured signal generators. In such cases, smartphones can serve as substitutes for generating acoustic signals, while phone-sized USRPs can be used for EM signal generation. Similarly, power amplifiers can be tailored to the signal's frequency band. For example, attackers can employ dedicated audio amplifiers and RF-specific amplifiers instead of bulky and general-purpose amplifiers.

2) New Attack Surfaces: Based on the analysis in Table I and II, we find some potential attack surfaces that have not yet been explored, which are summarized below.

- *Acoustic-based attacks on MEMS components.* Acoustic attacks have largely targeted MEMS-based transducers (e.g., accelerometers), due to their ultrasonic resonance. Other MEMS sensors (e.g., magnetometers, thermometers) and MEMS-based components such as clock oscillators [109] may also be susceptible to acoustic injection, especially in smart sensors with integrated timing circuits. Thus, it's also possible to determine the presence of resonance frequencies by sweeping test and to further investigate their effect on sensor measurements.

- *Laser-based attacks on signal conditioning circuits.* Laser-based attacks mainly target transducers, overlooking signal conditioning components. Yet, prior studies show that lasers can disrupt digital ICs [110, 111] via photoelectric effects. Given that amplifiers, filters, and ADCs also use transistors, these circuits may similarly be vulnerable. Researchers can inject lasers into circuits and analyze their effect on sensor measurements.
- *EM-based snooping attacks on signal conditioning circuits.* Existing EM-based snooping attacks focus on transducers and communication wires. However, studies have also shown that EM side-channel emissions from ADCs [18] and clock circuitry [112] can also leak sensor activity. These findings suggest that signal conditioning circuits could expose additional side-channel attack surfaces. Future work could investigate how to capture these emissions using antennas and reconstruct sensitive measurement data using AI-based inference techniques, such as generative adversarial networks (GANs) [71].
- *Attacks on membrane-structured sensors.* Sensors with exposed membrane structures are always vulnerable, such as microphones [4] and barometers [48]. Flexible sensors used in wearables and biomedical applications such as photoacoustic spectroscopy IR detectors and thermal-film sensors also feature exposed membranes. Due to lightweight design constraints, these sensors often lack proper shielding, making them likely susceptible to optical and EM interference. Thus, researchers can also study the effect of lasers and EM signals on these sensors.
- *Self-attack paradigm.* For scenarios where attack signals are hard to reach and focus, such as high speed drones, we envision a new attack paradigm called *self-attack*, where attackers can exploit a device's own components to compromise its sensors. This idea is inspired by previous studies showing that onboard speakers can emit malicious audio targeting local microphones [113], and capacitors can generate ultrasonic signals via the inverse piezoelectric effect [55]. Therefore, it is an interesting research direction to study, for example, how to make motors generate acoustic signals and thus interfere with motion sensors.

V. System-level Implications

In this section, we expand the implications of attacks from individual sensors to CPS. While sensors are critical components of CPS, the intuition that *sensor-level failures lead to system-level consequences* may not always be true. To understand *why* sensor-level failures *can/cannot* lead to system-level consequences, we identify three key characteristics of modern CPS: **a) closed-loop control**, **b) multi-sensor fusion**, and **c) intelligent perception**, as shown in Fig. 4. These characteristics complicate the relationship between sensor failures and system behavior. In contrast, a naive CPS, defined by open-loop control, single-sensor input, and no intelligent processing, reacts directly to sensor data, such as a light switch based on ambient brightness. Although CPSs are diverse and encompass many other characteristics, we focus on these three because they are the most prevalent and influential when it comes to the system-level impact of sensor attacks. More importantly, this section does not delve into specific attack methods, as discussed in Sec. IV. Instead, we take sensor failures as a basic assumption for analyzing their implications at the system level.

A. Implications on Closed-loop Control

For CPS requiring accurate control and robustness to external disturbances or internal variations, it is pervasive to adopt a closed-loop (CL) architecture, as shown in Fig. 4, where the sensor acts as the feedback for continuous control adjustments [114]. Compared to open-loop systems, the sensor feedback mechanism in CL systems complicates the relationship between sensor failures and system consequences.

1) System's Strength: Since CL systems are less sensitive to noise and disturbances in the environment than open-loop systems [114], they can, to some extent, resist noisy sensor readings that are equivalent to environmental disturbances. For example, CL flight control systems are immune to most sinusoidal perturbations (e.g., >5 Hz [115]) induced by resonant acoustic signal injection on MEMS gyroscopes [65].

Moreover, CL systems use sensors to measure states that are largely affected by previous actions, making the sensor measurements somewhat predictable. This characteristic benefits anomaly detection mechanisms, e.g., monitoring the discrepancy between the expected state and sensor feedback. A substantial discrepancy may trigger alarming [44] or fail-safe logic [19]. A line of research develops more advanced anomaly detection methods. Choi et al. [116] proposed to detect malicious sensor readings by monitoring control invariants obtained from a linear model of the victim system. Quinonez et al. [117] further improved this method by introducing non-linear control invariants and employing an efficient algorithm for detection.

2) System's Weakness: The fundamental principle of CL systems is to compensate for the errors calculated by the sensor feedback [114]. By exploiting the compensation mechanism, compromised sensor feedback can lead to severe system consequences [44, 118]. For example, a stabilizer uses feedback from inertial sensors to correct its orientation. If this feedback is faulty, the stabilizer may overcompensate, effectively turning into a destabilizer or shaker [64, 66, 67]. This weakness is particularly critical when the sensor measures first-order or even multiple-order derivatives of the system's state, e.g., the gyroscope measures angular velocity, which is the first-order derivative of heading angle. In such cases, the errors induced by compromised sensors accumulate over time, causing system-level errors to grow exponentially [117, 119].

B. Implications on Multi-Sensor Fusion

For advanced, especially safety-critical applications, CPS equips multiple sensors, which can be either homogeneous or heterogeneous, to perceive the same target comprehensively [120]. The measurements from different sensors are collected by fusion algorithms, e.g., a Kalman filter [121], to

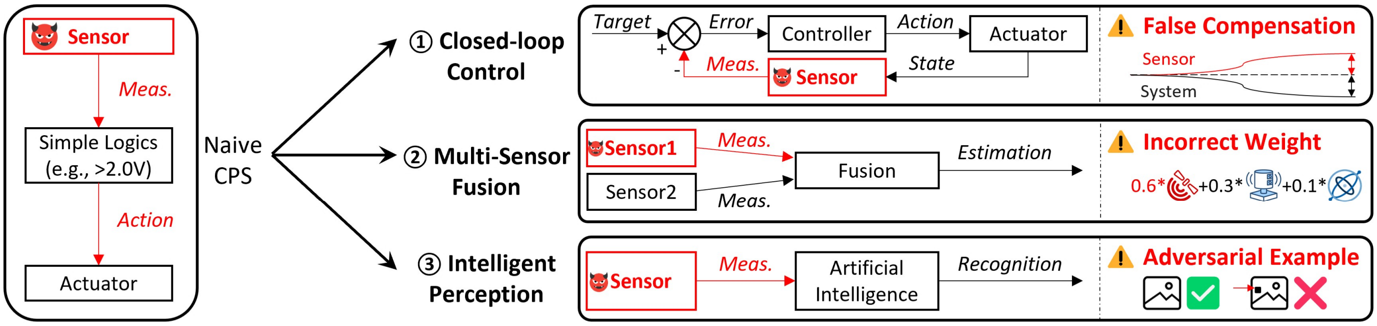


Fig. 4. Implications of sensor failures on naive CPS and three typical advanced CPS. The red color indicates the compromised elements. While naive CPS behavior is directly affected, advanced CPS remain resilient unless a specific vulnerability is exploited.

achieve a refined estimate, as illustrated in Fig. 4. Since most sensor security studies focus on single sensors, it is crucial to understand their implications on multi-sensor fusion (MSF) systems.

1) System's Strength: The redundancy of sensors in MSF systems enables cross-verification, which is commonly believed to be a reliable countermeasure in sensor attack papers [17, 44, 66, 80, 83, 122]. The ability for sensor data cross-verification is supported by the assumption that a portion of sensors are not compromised, and their data is trustworthy. It is challenging to simultaneously attack multiple sensors even if they are homogeneous, e.g., different types of IMUs usually have different resonant frequencies [5, 65]. To achieve cross-verification, outlier detection and filtering based on statistics is the main technique [123].

2) System's Weakness: While it is widely accepted that MSF increases the robustness of sensor measurements, a few studies [119, 124] have shown that it is not effective against well-designed sensor spoofing. The basic idea of compromising MSF is to attack the most critical sensor that determines the fusion result. Nashimoto et al. [124] studied attitude-heading reference systems, which estimate the inclination based on the fusion of gyroscope, accelerometer, and magnetometer. It is found that single-sensor spoofing can tamper with the fused results by exploiting the dominant sensor mechanism [124]. Shen et al. [119] found a similar mechanism existed in another fusion algorithm of GPS, LiDAR, and IMU for autonomous driving. They demonstrated that in certain cases where the uncertainties of both IMU and LiDAR measurements are high, the GPS becomes dominant, and then GPS spoofing can take over the fusion algorithm [119].

C. Implications on Intelligent Perception

Artificial intelligence (AI) is crucial to extract useful information from those sensors, e.g., cameras, microphones, and LiDARs, whose raw data is highly unstructured [125]. As shown in Fig. 4, a typical intelligent perception system involves an AI algorithm, usually a deep neural network (DNN), which recognizes sensor measurements to obtain high-level information, such as classification, detection, and segmentation.

1) System's Strength: Conventional sensor attacks [4, 23, 46, 79, 80] may not affect the intelligent perception results effectively, due to the complex and opaque relationship between sensor data and AI recognition. For example, the replaying commands injected by ultrasonic sound injection [4] cannot easily pass intelligent speaker verification [61]. Furthermore, AI algorithms are resistant to noisy or limited corruption since they can selectively perceive useful information [126–128], making it difficult to achieve the required level of arbitrary manipulation via signal attacks.

2) System's Weakness: For intelligent perception systems, it is crucial to involve the guidance of AI vulnerability for successful sensor attacks. Manual analysis can reveal explicit weaknesses, like in [99], where tiny point clouds were misclassified by object detection models and exploited via LiDAR spoofing. However, in practice, many systems are black-box and thus their weaknesses are implicit and harder to exploit. A popular methodology considers it as an end-to-end optimization problem, where the attack signals are the optimization variable [102, 126, 127, 129]. The optimization is accomplished by gradient descent, similar to adversarial example attacks [130, 131]. When the gradient information is unavailable, the optimization method is alternated by black-box methods like grid search [128] and Bayesian optimization [66]. Moreover, recent work explored the use of unique corruptions by sensor attacks to trigger neural network backdoors [61, 63] or adversarial patches [67].

VI. Defense Systematization

In this section, we provide a systematic analysis of defense strategies against sensor OOB vulnerabilities. Our study compares these strategies across several key dimensions, including attack vector coverage, defense effectiveness, deployment overhead. This framework facilitates a qualitative evaluation of defense mechanisms using normalized metrics. A structured overview of the results is summarized in Table III.

A. Systematization Methodology

We systematize existing countermeasures based on the system components they modify and categorize them into three levels: **a) Component-level defense:** This category focuses on hardening critical internal modules within sensors to eliminate

TABLE III. Systematization of defense methods

Defense Level		Defense Methods	Targeted Attack Type				Defense Goal			Overhead				Paper
			🔊	☀	📶	⚡	C	I	A	Exp.	Cost	Usab.	Maint.	
Component Level	Trans.	Transducer response limitation	●	●	●	○	🟥	🟩	🟩	🎖🎖	1	1	2	[4, 58]
	Signal Cond. Circuit	Filter stopband enhancement	●	●	●	●	🟥	🟩	🟩	🎖🎖🎖	2	2	3	[5, 44, 64–66]
		AMP nonlinearity reduction	●	●	●	●	🟥	🟩	🟨	🎖🎖🎖	2	1	2	[4, 5, 57, 58]
		ADC anti-aliasing	●	●	●	●	🟥	🟩	🟩	🎖🎖	1	1	1	[6]
		CMRR enhancement	○	○	●	●	🟥	🟨	🟨	🎖🎖🎖	2	1	3	[24, 95, 97, 132]
	Power	PSRR enhancement	○	○	●	●	🟥	🟨	🟨	🎖🎖	1	1	2	[7, 96]
	Comm.	Crosstalk noise isolation	○	○	●	●	🟥	🟨	🟨	🎖🎖🎖	3	2	3	[7, 9, 96]
Sensor Level	Input	OOB signal shielding	●	●	●	●	🟩	🟩	🟩	🎖🎖	2	2	2	[50, 66]
	Output	Randomization	●	●	●	●	🟨	🟩	🟥	🎖🎖	1	2	1	[5, 102, 128, 133, 134]
		Data encryption	●	●	●	●	🟩	🟥	🟥	🎖🎖	2	2	2	[135]
System Level	H.	Redundancy deployment	●	●	●	○	🟥	🟨	🟩	🎖🎖	3	3	3	[67, 80, 83, 102]
	H.&S.	Anomaly detection	●	●	●	●	🟥	🟩	🟨	🎖🎖🎖	2	2	3	[43, 44, 50, 58, 136]
	S.	Access authentication	○	●	○	●	🟩	🟨	🟨	🎖	1	2	1	[24, 97, 102]
		Model fusion	●	●	●	●	🟥	🟩	🟨	🎖🎖🎖	3	3	2	[103, 137, 138]
		Data recovery	●	●	●	●	🟥	🟨	🟩	🎖🎖🎖	2	1	2	[46, 66]

H. Hardware H.&S. Hardware or Software S. Software ●Applicable ○Not applicable **C** Confidentiality **I** Integrity **A** Availability
🟥 Less effective 🟨 Moderately effective 🟩 Highly effective 1 Low 2 Medium 3 High 🎖 Layman 🎖🎖 Proficient 🎖🎖🎖 Expert

exploitable vulnerabilities. Key measures include reinforcing the transducer's anti-interference capabilities, optimizing signal conditioning circuits and power supply modules, and mitigating crosstalk among communication interfaces. These enhancements aim to prevent attackers from reshaping signals or physically damaging components, thereby ensuring the intrinsic robustness of core subsystems. **b) Sensor-level defense:** These defenses secure the sensor as a whole, protecting both its input and output while maintaining its core functionality. For input protection, techniques like shielding can block out-of-band interference. For output protection, methods such as real-time signal randomization or data encryption can prevent spoofing and information leakage. **c) System-level defense:** These methods enhance sensor security from a broader system perspective by integrating cross-layer solutions across hardware, software, or both. Hardware-based approaches may include deploying redundant sensors to increase system resilience. In some cases, combined hardware and software solutions are necessary, such as integrating additional devices with detection algorithms to counter sophisticated attacks. Purely software-based methods often employ AI-driven techniques for tasks like access control, model fusion, or data recovery. This multi-dimensional framework strengthens security at the cyber-physical system level, enabling coordinated defense beyond the limitations of individual sensors.

To facilitate a comprehensive analysis of sensor defense methods, we compare each approach across three key dimensions: targeted attack types, defense goals, and deployment overhead.

1) Target Attack Types: We classify the targeted sensor attacks by their signal modality: attacks by sound/ultrasound (🔊), attacks by lasers (☀), attacks by radiated EMI (📶), and attacks by conducted EMI (⚡). Some defenses are broadly applicable, while others are modality-specific. For example, sensor redundancy is ineffective against conducted EMI attacks, as the injected signal can propagate to all redundant sensors.

2) Defense Goal: We use the classical CIA (Confidentiality, Integrity, Availability) security model to assess each defense's primary protection focus, and the effectiveness is categorized into three levels: low (🟥), moderate (🟨), and high (🟩). Confidentiality (**C**) means preventing unauthorized access or inference of sensitive sensor data. Integrity (**I**) indicates defenses can ensure sensor readings are not altered or spoofed. Availability (**A**) means maintaining reliable sensor operation despite external disruptions.

3) Overhead: We evaluate real-world feasibility based on four sub-factors: Expertise Knowledge represents the required technical skill level for defense implementation, and we divide it into three levels: layman (🎖), proficient (🎖🎖), expert(🎖🎖🎖)). 🎖 means the defense is easy to apply and only requires little or no technical background. 🎖🎖 means the defense needs basic technical skills, and is suitable for trained staff. 🎖🎖🎖 means the defense method requiring deep technical knowledge of both the hardware and software of sensors. We rate the remaining three overhead factors as Low(1), Medium(2), and High (3). Deployment Cost refers to financial and hardware resource demands. Usability indicates the impact on user experience or system functionality. Maintenance assesses ease of upkeep and adaptability to evolving threats.

B. Review of Existing Work

1) Component-level Defense: **a) Transducer.** Limiting the transducer's response range can reduce its susceptibility to abnormal stimuli, thereby mitigating the risk of malicious signal injection. For example, prior studies [4, 58] suggest that microphones should be designed to be insensitive to ultrasonic waves. **b) Signal Conditioning Circuit.** Enhancing the performance of signal conditioning circuits is an effective defense strategy. Key methods include improving the filter's stopband to suppress unwanted frequencies [5, 44, 64–66], increasing the amplifier's linearity to minimize distortion and the generation of new frequency components [4, 5, 57, 58], applying anti-aliasing techniques at the analog-to-digital converter to prevent signal misinterpretation [6], and enhancing the common-mode rejection ratio (CMRR) to resist differential noise [24, 95, 97, 132]. **c) Power Supply.** Enhancing the power supply rejection ratio (PSRR) helps shield internal circuits from adversarial power fluctuations. Wang et al. [7] demonstrate that PSRR can be improved by modifying the architecture of the low-dropout regulator. **d) Communication Interface.** Isolating crosstalk noise preserves data integrity and prevents unintended signal propagation between channels, as shown in recent work [7, 9, 96].

2) Sensor-level Defense: At the sensor level, defense mechanisms aim to protect the sensor as a unified entity by securing its **input** and **output** pathways. **a) Input protection.** Implementing *out-of-band (OOB) signal shielding* is an effective strategy. This approach involves using physical or electromagnetic shielding materials to block unintended or malicious signals such as ultrasound [50, 66], light [17] or electromagnetic waves [90, 92] from reaching the sensor's input interface or being leaked from the sensors [85], thereby preserving signal integrity and confidentiality. **b) Output protection.** On the output side, two key techniques are commonly employed. *Randomization* involves introducing controlled variability into the sensor output, such as frequency hopping [133], randomized sampling [5], rolling shutter sequence [128], pulse [102] or pixel noises [134], to make it more difficult for attackers to infer or replicate true measurements. This method can disrupt attempts at sensor spoofing or replay attacks. Meanwhile, *data encryption* secures the sensor's output during transmission by encoding the data, ensuring that even if intercepted, it cannot be easily interpreted or altered [135]. These output-level methods are especially crucial in networked or distributed sensor systems, where data confidentiality and authenticity are paramount. Together, these input and output protections strengthen the end-to-end security of the sensor against a wide range of physical-layer and signal-based attacks.

3) System-level Defense: System-level defense mechanisms aim to improve overall system resilience using both hardware and software rather than protecting individual sensor elements alone. **a) Hardware-based defenses.** One widely used strategy is the deployment of redundant sensors, where multiple sensors of the same or different types are used to measure multiple physical quantities that are related to the same task, such as combining lidars and cameras in automotive systems [67, 80, 83, 102], enabling error correction or failover mechanisms. **b) Hardware&Software-based defenses.** Hybrid methods like anomaly detection [4, 43, 44, 50, 57, 58, 67, 81, 136, 139] are commonly applied to identify unexpected behaviors or outputs that may indicate tampering or spoofing. For instance, study [136] suggests using a matched dummy sensor circuit that shares the sensor's vulnerabilities to EMI but is insensitive to legitimate signals that the sensor is intended to measure to detect sensor attacks. **c) Software-based defenses.** Access authentication ensures that only authorized entities [24, 97] can read or write sensor data, or only verified signals [102] can be received and processed, preventing unauthorized control or data leakage; Model fusion [103, 137, 138] integrates data from multiple models or sensor sources to validate and reinforce output correctness, improving robustness against targeted attacks; And data recovery techniques [46, 66] attempt to restore accurate sensor outputs from corrupted or missing data, using interpolation, signal reconstruction, or AI-based methods. Together, these system-level methods provide layered protection and enable coordinated threat response across the entire sensor ecosystem.

C. Research Gaps and Future Directions

Based on the above analysis, we identify key limitations and provide future research directions.

- *Cross-component interactions.* Most component-level defenses are designed for isolated modules (e.g., transducers, amplifiers), overlooking cross-component interactions that can lead to OOB vulnerabilities. To mitigate this issue, a promising direction is to incorporate safety simulations during the sensor design phase. For instance, researchers can conduct multiphysics simulations [140] to capture field coupling effects in MEMS transducers and proactively identify resonant acoustic frequencies that may compromise sensor integrity. Similarly, combining electromagnetic field simulations with circuit-level modeling of signal conditioning stages can help reveal electrical characteristics that contribute to OOB vulnerabilities. These approach can inform design decisions early in the development cycle, reducing the risk of post-deployment security issues.
- *Lack of defenses for snooping attacks.* We find that there are few methods specifically aimed at protecting the confidentiality of sensor measurements. We believe a viable direction is to leverage internal hardware components within the sensor itself for encryption, rather than relying on software-based encryption. For example, prior work has demonstrated that the physical unclonable function (PUF) properties of image sensor phototransistors can be used to encrypt captured signals, enabling verification of authenticity and originality [141]. This in-sensor encryption paradigm can offer a novel approach for protecting privacy-sensitive measurements at the hardware level.
- *High integration complexity of redundancy methods.* Redundancy-based defenses (e.g., sensor fusion) often increase system-level complexity and cost, limiting their practicality in cost-sensitive applications. For example, adding redundant IMUs to a drone requires changes to both PCB layout and flight control algorithms. Inspired by paper [142], which uses redundant ADCs for attack detection, a more lightweight alternative is to embed redundancy components within a single sensor. For example, multiple transducers with distinct resonant frequencies can be integrated into a single accelerometer to ensure at least one remains unaffected during an attack.

VII. Discussion

A. Comparison with Previous Work

Compared with previous SoK papers and surveys in this field, our paper differs in the following aspects.

Terminology. The term out-of-band has been used inconsistently across prior works. SoK [12] and paper [143] interpret band as the frequency range of the signal, while paper [11] adopt definitions from network communication, referring to signals injected through covert communication channels. This inconsistency may lead to confusion and hinder a unified understanding of the field. In this work, we offer a formal and structured definition of OOB vulnerabilities based on physical energy conversion principles. This not only clarifies the boundary between in-band and out-of-band but also lays a conceptual foundation for future research.

Scope. Our SoK centers on the concept of sensor OOB vulnerabilities. In contrast, SoK [12] focuses on transduction attacks and signal injection techniques, without identifying the underlying commonalities in sensor vulnerabilities and covering side-channel and privacy snooping attacks. SoK [14, 15] focus on specific attack scenarios, i.e., eavesdropping via mobile sensors and sensor spoofing against robotic vehicles.

Systematization Methodology. We for the first time adopt a bottom-up methodology that examines vulnerabilities at the component, sensor, and system levels. In particular, our sensor-level analysis provides a dedicated analysis of the practicality of sensor attacks, which is overlooked in SoK [12]. Our system-level analysis provides new insights into how CPS architecture influence vulnerability exposure and mitigation trade-offs, which is not covered in previous work.

B. Sensor Design Trade-offs

Sensor design inherently involves trade-offs between performance, cost, and resilience to attack signals. Enhancing sensitivity improves signal detection in low-power applications, but also lowers the threshold for OOB interference. Filtering and shielding can block malicious input, but risk degrading legitimate functionality or increasing size and cost. Software-based defenses (e.g., anomaly detection, sensor fusion) offer flexibility but strain the limited compute and power budgets of embedded CPS. Designing sensors that balance utility with OOB robustness remains an open challenge, especially as sensors become more intelligent and integrated. Nonetheless, we encourage sensor designers to explicitly consider OOB vulnerabilities during the design process. For legacy sensors where redesign is impractical, these vulnerabilities should at least be acknowledged in the datasheet, which can provide a primary reference for system developers to raise awareness and guide secure integration.

C. OOB Vulnerabilities for Good

In this paper, we assume by default that sensors are used for benign purposes. However, sensors can be used for malicious purposes, such as hidden cameras and eavesdropping voice recorders that invade privacy. In such cases, the sensor OOB vulnerabilities can be leveraged to implement proactive defenses. For instance, defenders can detect malicious devices by sensors' EM radiation [18, 112, 144, 145]. Ramesh et al. [112] proposed a system to detect microphone status by probing EM emanations from laptop circuitry carrying mic clock signals, which only appear during recording. Similarly, Chaman et al. [144] introduced Ghostbuster, which detects hidden eavesdroppers like cameras by probing RF clock leakage without modifying current transmitters and receivers. Additionally, Liu et al. [145] presented a method to detect hidden cameras by observing changes in EM emanations caused by the camera's clock modulation.

D. Security Outlook for Smart Sensors

Sensors are increasingly armed with intelligent technologies. In the Internet of Things (IoT) applications, transmitting large volumes of raw sensory data consumes significant communication and computational resources. To alleviate the issue, computational tasks start to be integrated into the sensors, leading to the rise of smart sensors [146, 147]. Nowadays, sensor manufacturers are embarking on the smart sensor market, e.g., voice-wakeup microphones [148], glass-break sensors [149], and fitness-tracking motion sensors [150]. These smart sensors offer advantages like reducing device power consumption and processing sensitive data within the device [151], thus minimizing the risk of privacy leakage [152].

However, smart sensors are increasingly susceptible to attacks due to their reliance on intelligent algorithms and sophisticated hardware. As discussed in Sec. V, intelligent perception is vulnerable to targeted attacks that exploit these algorithmic weaknesses [131]. In addition, the computing hardware within smart sensors is exposed to physical side-channel attacks. Besides sensor readings, these attacks can extract sensitive information, such as model architecture and parameters, by analyzing EM emissions [153, 154].

VIII. Conclusion

In this SoK, we systematically analyze sensor OOB vulnerabilities from the perspective of energy conversion. By classifying attack signals into *out-of-range* and *cross-field* types and analyzing their propagation paths, we build a unified framework to better understand and formalize sensor attacks. This helps in creating effective detecting and defenses on sensor OOB vulnerability and offers guidance for designing more secure sensors in the future. The study also highlights the wider impact of sensor security on CPSs, calling attention to both the growing range of sensor attacks and the core physical principles behind sensor function.

Acknowledgment

We thank the anonymous reviewers for their valuable comments. This work is supported by the National Science Foundation of China (NSFC) Grant 62222114 and 62201503.

References

[1] AIChE, "Process safety beacon: Excess cooling can cause a runaway reaction," https://www.aiche.org/resources/publications/cep/2018/july/process-safety-beacon-excess-cooling-can-cause-runaway-reaction/, 2018.

[2] CNN, "Boeing relied on single sensor for 737 max that had been flagged 216 times to faa," https://www.cnn.com/2019/04/30/politics/boeing-sensor-737-max-faa, 2019.

[3] CBS NEWS, "Process safety beacon: Excess cooling can cause a runaway reaction," https://www.cbsnews.com/news/industrial-robot-crushes-worker-dead-south-korea/, 2023.

[4] G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang, and W. Xu, "Dolphinattack: Inaudible voice commands," in *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security*, 2017, pp. 103–117.

[5] T. Trippel, O. Weisse, W. Xu, P. Honeyman, and K. Fu, "Walnut: Waging doubt on the integrity of mems accelerometers with acoustic injection attacks," in *Proceedings of the 2017 IEEE European symposium on security and privacy (EuroS&P)*. IEEE, 2017, pp. 3–18.

[6] Y. Michalevsky, D. Boneh, and G. Nakibly, "Gyrophone: Recognizing speech from gyroscope signals," in *Proceedings of the 23rd USENIX Security Symposium (USENIX Security 14)*, 2014, pp. 1053–1067.

[7] K. Wang, S. Xiao, X. Ji, C. Yan, C. Li, and W. Xu, "Volttack: Control iot devices by manipulating power supply voltage," in *Proceedings of the 2023 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, 2023, pp. 1771–1788.

[8] T. Ni, X. Zhang, and Q. Zhao, "Recovering fingerprints from in-display fingerprint sensors via electromagnetic side channel," in *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, 2023, pp. 253–267.

[9] P. Cronin, X. Gao, C. Yang, and H. Wang, "Charger-surfing: Exploiting a power line side-channel for smartphone information leakage," in *Proceedings of the 30th USENIX Security Symposium (USENIX Security 21)*, 2021, pp. 681–698.

[10] C. Shi, X. Xu, T. Zhang, P. Walker, Y. Wu, J. Liu, N. Saxena, Y. Chen, and J. Yu, "Face-mic: inferring live speech and speaker identity via subtle facial dynamics captured by ar/vr motion sensors," in *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*, 2021, pp. 478–490.

[11] I. Giechaskiel and K. Rasmussen, "Taxonomy and challenges of out-of-band signal injection attacks and defenses," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 645–670, 2019.

[12] C. Yan, H. Shin, C. Bolton, W. Xu, Y. Kim, and K. Fu, "Sok: A minimalist approach to formalizing analog sensor security," in *Proceedings of the 2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2020, pp. 233–248.

[13] A. K. Sikder, G. Petracca, H. Aksu, T. Jaeger, and A. S. Uluagac, "A survey on sensor-based threats and attacks to smart devices and applications," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 1125–1159, 2021.

[14] P. Walker and N. Saxena, "Sok: assessing the threat potential of vibration-based attacks against live speech using mobile sensors," in *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2021, pp. 273–287.

[15] Y. Xu, X. Han, G. Deng, J. Li, Y. Liu, and T. Zhang, "Sok: Rethinking sensor spoofing attacks against robotic vehicles from a systematic view," in *Proceedings of the 2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*. IEEE, 2023, pp. 1082–1100.

[16] J. Fraden and J. King, *Handbook of modern sensors: physics, designs, and applications*. Springer, 2004, vol. 3.

[17] T. Sugawara, B. Cyr, S. Rampazzi, D. Genkin, and K. Fu, "Light commands:laser-based audio injection attacks on voice-controllable systems," in *Proceedings of the 29th USENIX Security Symposium (USENIX Security 20)*, 2020, pp. 2631–2648.

[18] R. Zhou, X. Ji, C. Yan, Y.-C. Chen, W. Xu, and C. Li, "Dehirec: Detecting hidden voice recorders via adc electromagnetic radiation," in *Proceedings of the 2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2023, pp. 3113–3128.

[19] H. Kim, R. Bandyopadhyay, M. O. Ozmen, Z. B. Celik, A. Bianchi, Y. Kim, and D. Xu, "A systematic study of physical sensor attack hardness," in *Proceedings of the 2024 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, 2024, pp. 143–143.

[20] Wikipedia, "List of sensors," 2023, https://en.wikipedia.org/wiki/List_of_sensors.

[21] J. G. Webster and H. Eren, *Measurement, Instrumentation, and Sensors Handbook: Two-Volume Set*. CRC press, 2018.

[22] J. Yu, "9 different types of sensor transmitters," 2021, https://www.electronicdesign.com/technologies/test-measurement/article/21166704/okmarts-9-different-types-of-sensor-transmitters.

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

[24] Y. Jiang, X. Ji, K. Wang, C. Yan, R. Mitev, A.-R. Sadeghi, and W. Xu, "Wight: Wired ghost touch attack on capacitive touchscreens," in *Proceedings of the 2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2022, pp. 984–1001.

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

[26] D. G. Padmavathi, M. Shanmugapriya *et al.*, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," *arXiv preprint arXiv:0909.0576*, 2009.

[27] A. Kurakin, I. J. Goodfellow, and S. Bengio, "Adversarial examples in the physical world," in *Artificial intelligence safety and security*. Chapman and Hall/CRC, 2018, pp. 99–112.

[28] S. Sami, S. R. X. Tan, Y. Dai, N. Roy, and J. Han, "Lidarphone: acoustic eavesdropping using a lidar sensor," in *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*, 2020, pp. 701–702.

[29] P. Hu, W. Li, R. Spolaor, and X. Cheng, "mmecho: A mmwave-based acoustic eavesdropping method," in *Proceedings of the 2023 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, 2023, pp. 1840–1856.

[30] Z. Xu, K. Bai, and S. Zhu, "Taplogger: Inferring user inputs on smartphone touchscreens using on-board motion sensors," in *Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*, 2012, pp. 113–124.

[31] X. Liu, Z. Zhou, W. Diao, Z. Li, and K. Zhang, "When good becomes evil: Keystroke inference with smartwatch," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015, pp. 1273–1285.

[32] A. Maiti, O. Armbruster, M. Jadliwala, and J. He, "Smartwatch-based keystroke inference attacks and context-aware protection mechanisms," in *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, 2016, pp. 795–806.

[33] E. Miluzzo, A. Varshavsky, S. Balakrishnan, and R. R. Choudhury, "Tapprints: your finger taps have fingerprints," in *Proceedings of the 10th international conference on Mobile systems, applications, and services*, 2012, pp. 323–336.

[34] E. Owusu, J. Han, S. Das, A. Perrig, and J. Zhang, "Accessory: password inference using accelerometers on smartphones," in

Proceedings of the twelfth workshop on mobile computing systems & applications, 2012, pp. 1–6.

[35] Y. Berger, A. Wool, and A. Yeredor, “Dictionary attacks using keyboard acoustic emanations,” in *Proceedings of the 13th ACM conference on Computer and communications security*, 2006, pp. 245–254.

[36] D. Foo Kune and Y. Kim, “Timing attacks on pin input devices,” in *Proceedings of the 17th ACM conference on Computer and communications security*, 2010, pp. 678–680.

[37] J. Liu, Y. Wang, G. Kar, Y. Chen, J. Yang, and M. Gruteser, “Snooping keystrokes with mm-level audio ranging on a single phone,” in *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*, 2015, pp. 142–154.

[38] L. Lu, J. Yu, Y. Chen, Y. Zhu, X. Xu, G. Xue, and M. Li, “Keylistener: Inferring keystrokes on qwerty keyboard of touch screen through acoustic signals,” in *Proceedings of the IEEE INFOCOM 2019-IEEE Conference on Computer Communications*. IEEE, 2019, pp. 775–783.

[39] I. Shumailov, L. Simon, J. Yan, and R. Anderson, “Hearing your touch: A new acoustic side channel on smartphones,” *arXiv preprint arXiv:1903.11137*, 2019.

[40] T. Zhu, Q. Ma, S. Zhang, and Y. Liu, “Context-free attacks using keyboard acoustic emanations,” in *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*, 2014, pp. 453–464.

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

[42] P. Agostini and G. Petite, “Photoelectric effect under strong irradiation,” *Contemporary physics*, vol. 29, no. 1, pp. 57–77, 1988.

[43] Y. Park, Y. Son, H. Shin, D. Kim, and Y. Kim, “This ain’t your dose: Sensor spoofing attack on medical infusion pump,” in *Proceedings of the 10th USENIX workshop on offensive technologies (WOOT 16)*, 2016.

[44] Y. Tu, S. Rampazzi, B. Hao, A. Rodriguez, K. Fu, and X. Hei, “Trick or heat? manipulating critical temperature-based control systems using rectification attacks,” in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp. 2301–2315.

[45] L. Shi and S. Nihtianov, “Comparative study of silicon-based ultraviolet photodetectors,” *IEEE Sensors Journal*, vol. 12, no. 7, pp. 2453–2459, 2012.

[46] D. F. Kune, J. Backes, S. S. Clark, D. Kramer, M. Reynolds, K. Fu, Y. Kim, and W. Xu, “Ghost talk: Mitigating emi signal injection attacks against analog sensors,” in *Proceedings of the 2013 IEEE Symposium on Security and Privacy*. IEEE, 2013, pp. 145–159.

[47] R. N. Dean, S. T. Castro, G. T. Flowers, G. Roth, A. Ahmed, A. S. Hodel, B. E. Grantham, D. A. Bittle, and J. P. Brunsch, “A characterization of the performance of a mems gyroscope in acoustically harsh environments,” *IEEE Transactions on Industrial Electronics*, vol. 58, no. 7, pp. 2591–2596, 2010.

[48] T. Tanaka and T. Sugawara, “Laser-based signal-injection attack on piezoresistive mems pressure sensors,” in *2022 IEEE Sensors*. IEEE, 2022, pp. 1–4.

[49] Q. Jiang, X. Ji, C. Yan, Z. Xie, H. Lou, and W. Xu, “Glitchhiker: Uncovering vulnerabilities of image signal transmission with iemi,” in *Proceedings of the 32nd USENIX Security Symposium (USENIX Security 23)*, 2023, pp. 7249–7266.

[50] Q. Yan, K. Liu, Q. Zhou, H. Guo, and N. Zhang, “Surfingattack: Interactive hidden attack on voice assistants using ultrasonic guided waves,” in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2020.

[51] J. A. Svoboda and R. C. Dorf, *Introduction to electric circuits*. John Wiley & Sons, 2013.

[52] M. Tartagni, *Electronic sensor design principles*. Cambridge University Press, 2022.

[53] N. Roy, H. Hassanieh, and R. Roy Choudhury, “Backdoor: Making microphones hear inaudible sounds,” in *Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services*, 2017, pp. 2–14.

[54] H. Shen, W. Zhang, H. Fang, Z. Ma, and N. Yu, “Jamsys: Coverage optimization of a microphone jamming system based on ultrasounds,” *IEEE Access*, vol. 7, pp. 67 483–67 496, 2019.

[55] X. Ji, J. Zhang, S. Jiang, J. Li, and W. Xu, “Capspeaker: Injecting voices to microphones via capacitors,” in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, 2021, pp. 1915–1929.

[56] Y. Jiang, X. Ji, J. Zhang, Y. Jiang, S. Jiang, and W. Xu, “Capspeaker: Injecting commands to voice assistants via capacitors,” *IEEE Transactions on Dependable and Secure Computing*, 2023.

[57] N. Roy, S. Shen, H. Hassanieh, and R. R. Choudhury, “Inaudible voice commands: The long-range attack and defense,” in *Proceedings of the 15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18)*, 2018, pp. 547–560.

[58] C. Yan, G. Zhang, X. Ji, T. Zhang, T. Zhang, and W. Xu, “The feasibility of injecting inaudible voice commands to voice assistants,” *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 3, pp. 1108–1124, 2019.

[59] G. Li, Z. Cao, and T. Li, “Echoattack: Practical inaudible attacks to smart earbuds,” in *Proceedings of the 21st Annual International Conference on Mobile Systems, Applications and Services*, 2023, pp. 383–396.

[60] Z. Ning, J. He, Z. Tang, W. Hu, and X. Chen, “A portable and stealthy inaudible voice attack based on acoustic metamaterials,” *arXiv preprint arXiv:2501.15031*, 2025.

[61] X. Li, J. Ze, C. Yan, Y. Cheng, X. Ji, and W. Xu, “Enrollment-stage backdoor attacks on speaker recognition systems via adversarial ultrasound,” *IEEE Internet of Things Journal*, 2023.

[62] X. Li, C. Yan, X. Lu, Z. Zeng, X. Ji, and W. Xu, “Inaudible adversarial perturbation: Manipulating the recognition of user speech in real time,” in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2024.

[63] Z. Zheng, X. Li, C. Yan, X. Ji, and W. Xu, “The silent manipulator: A practical and inaudible backdoor attack against speech recognition systems,” in *Proceedings of the 31st ACM International Conference on Multimedia*, 2023, pp. 7849–7858.

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

[65] Y. Son, H. Shin, D. Kim, Y. Park, J. Noh, K. Choi, J. Choi, and Y. Kim, “Rocking drones with intentional sound noise on gyroscopic sensors,” in *Proceedings of the 24th USENIX Security Symposium (USENIX Security 15)*, 2015, pp. 881–896.

[66] X. Ji, Y. Cheng, Y. Zhang, K. Wang, C. Yan, W. Xu, and K. Fu, “Poltergeist: Acoustic adversarial machine learning against cameras and computer vision,” in *Proceedings of the 2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2021, pp. 160–175.

[67] W. Zhu, X. Ji, Y. Cheng, S. Zhang, and W. Xu, “Tpatch: A triggered physical adversarial patch,” in *Proceedings of the 30th USENIX Security Symposium (USENIX Security 21)*, 2023.

[68] S. A. Anand and N. Saxena, “Speechless: Analyzing the threat to speech privacy from smartphone motion sensors,” in

Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP). IEEE, 2018, pp. 1000–1017.

[69] J. Han, A. J. Chung, and P. Tague, "Pitchln: eavesdropping via intelligible speech reconstruction using non-acoustic sensor fusion," in *Proceedings of the 16th ACM/IEEE International Conference on Information Processing in Sensor Networks*, 2017, pp. 181–192.

[70] Z. Ba, T. Zheng, X. Zhang, Z. Qin, B. Li, X. Liu, and K. Ren, "Learning-based practical smartphone eavesdropping with built-in accelerometer." in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2020.

[71] P. Hu, H. Zhuang, P. S. Santhalingam, R. Spolaor, P. Pathak, G. Zhang, and X. Cheng, "Accear: Accelerometer acoustic eavesdropping with unconstrained vocabulary," in *Proceedings of the 2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2022, pp. 1757–1773.

[72] R. Matovu, I. Griswold-Steiner, and A. Serwadda, "Kinetic song comprehension: Deciphering personal listening habits via phone vibrations," *arXiv preprint arXiv:1909.09123*, 2019.

[73] L. Zhang, P. H. Pathak, M. Wu, Y. Zhao, and P. Mohapatra, "Accelword: Energy efficient hotword detection through accelerometer," in *Proceedings of the 13th Annual International Conference on Mobile Systems, Applications, and Services*, 2015, pp. 301–315.

[74] A. Kwong, W. Xu, and K. Fu, "Hard drive of hearing: Disks that eavesdrop with a synthesized microphone," in *Proceedings of the 2019 IEEE symposium on security and privacy (SP)*. IEEE, 2019, pp. 905–919.

[75] A. Barua, Y. G. Achamyeleh, and M. A. A. Faruque, "A wolf in sheep's clothing: spreading deadly pathogens under the disguise of popular music," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, 2022, pp. 277–291.

[76] B. Cyr, T. Sugawara, and K. Fu, "Why lasers inject perceived sound into mems microphones: Indications and contraindications of photoacoustic and photoelectric effects," in *2021 IEEE Sensors*. IEEE, 2021, pp. 1–4.

[77] H. Shi, Y. He, Q. Wang, J. Zhuge, Q. Li, and X. Liu, "Laser-based command injection attacks on voice-controlled microphone arrays," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2024, no. 2, pp. 654–676, 2024.

[78] G. Zhang, X. Ma, H. Zhang, Z. Xiang, X. Ji, Y. Yang, X. Cheng, and P. Hu, "Laseradv: Laser adversarial attacks on speech recognition systems," in *Proceedings of the 33rd USENIX Security Symposium (USENIX Security 24)*, 2024, pp. 3945–3961.

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

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

[81] D. Dai, Z. An, and L. Yang, "Inducing wireless chargers to voice out for inaudible command attacks," in *Proceedings of the 2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2023, pp. 1789–1806.

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

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

[84] Y. Ren, Q. Jiang, C. Yan, X. Ji, and W. Xu, "Ghostshot: Manipulating the image of ccd cameras with electromagnetic interference," *Proceedings of the Network and Distributed System Security Symposium*, 2025. [Online]. Available: https://api.semanticscholar.org/CorpusID:276862924

[85] Y. Long, Q. Jiang, C. Yan, T. Alam, X. Ji, W. Xu, and K. Fu, "Em eye: Characterizing electromagnetic side-channel eavesdropping on embedded cameras," in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2024.

[86] Z. Jin, Q. Jiang, X. Lu, C. Yan, X. Ji, and W. Xu, "Phantom-lidar: Cross-modality signal injection attacks against lidar," in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2025.

[87] S. Maruyama, S. Wakabayashi, and T. Mori, "Poster: Touch-flood: A novel class of attacks against capacitive touchscreens," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 2551–2553.

[88] ——, "Tap'n ghost: A compilation of novel attack techniques against smartphone touchscreens," in *Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2019, pp. 620–637.

[89] H. Shan, B. Zhang, Z. Zhan, D. Sullivan, S. Wang, and Y. Jin, "Invisible finger: Practical electromagnetic interference attack on touchscreen-based electronic devices," in *Proceedings of the 2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2022, pp. 1246–1262.

[90] K. Wang, R. Mitev, C. Yan, X. Ji, A.-R. Sadeghi, and W. Xu, "Ghosttouch: Targeted attacks on touchscreens without physical touch," in *Proceedings of the 31st USENIX Security Symposium (USENIX Security 22)*, 2022, pp. 1543–1559.

[91] ——, "Analyzing and defending ghosttouch attack against capacitive touchscreens," *IEEE Transactions on Dependable and Secure Computing*, 2024.

[92] G. Y. Dayanikli, R. R. Hatch, R. M. Gerdes, H. Wang, and R. Zane, "Electromagnetic sensor and actuator attacks on power converters for electric vehicles," in *Proceedings of the 2020 IEEE Security and Privacy Workshops (SPW)*. IEEE, 2020, pp. 98–103.

[93] F. Yang, Z. Dan, K. Pan, C. Yan, X. Ji, and W. Xu, "Rethink: Reveal the threat of electromagnetic interference on power inverters," in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2025.

[94] W. Li, J. Wang, G. Zhang, Y. Yang, R. Spolaor, X. Cheng, and P. Hu, "Emiris: Eavesdropping on iris information via electromagnetic side channel," in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2025.

[95] Y. Jiang, X. Ji, Y. Jiang, K. Wang, C. Xu, and W. Xu, "Powerradio: Manipulate sensor measurementvia power gnd radiation," in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2025.

[96] Y. Jiang, R. Li, Y. Cheng, X. Ji, and W. Xu, "V-phanton: Voltage-based physically-triggered backdoor attack against facial recognition," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2025, pp. 1–5.

[97] Y. Jiang, X. Ji, K. Wang, C. Yan, R. Mitev, A.-R. Sadeghi, and W. Xu, "Marionette: Manipulate your touchscreen via a charging cable," *IEEE Transactions on Dependable and Secure Computing*, 2023.

[98] H. Zhu, Z. Yu, W. Cao, N. Zhang, and X. 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*, 2022, pp. 1–9.

[99] J. Sun, Y. Cao, Q. A. Chen, and Z. M. Mao, "Towards robust lidar-based perception in autonomous driving: General black-

box adversarial sensor attack and countermeasures," in *Proceedings of the 29th USENIX Security Symposium (USENIX Security 20)*, 2020, pp. 877–894.

[100] Y. Cao, N. Wang, C. Xiao, D. Yang, J. Fang, R. Yang, Q. A. Chen, M. Liu, and B. Li, "Invisible for both camera and lidar: Security of multi-sensor fusion based perception in autonomous driving under physical-world attacks," in *Proceedings of the 2021 IEEE symposium on security and privacy (SP)*. IEEE, 2021, pp. 176–194.

[101] R. S. Hallyburton, Y. Liu, Y. Cao, Z. M. Mao, and M. Pajic, "Security analysis of camera-lidar fusion against black-box attacks on autonomous vehicles," in *Proceedings of 31st USENIX Security Symposium (USENIX Security 22)*, 2022, pp. 1903–1920.

[102] Z. Jin, X. Ji, Y. Cheng, B. Yang, C. Yan, and W. Xu, "Pla-lidar: Physical laser attacks against lidar-based 3d object detection in autonomous vehicle," in *Proceedings of the 2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2023, pp. 1822–1839.

[103] Y. Cao, S. H. Bhupathiraju, P. Naghavi, T. Sugawara, Z. M. Mao, and S. Rampazzi, "You can't see me: Physical removal attacks on lidar-based autonomous vehicles driving frameworks," in *Proceedings of 32nd USENIX security symposium (USENIX Security 23)*, 2023, pp. 2993–3010.

[104] T. Sato, Y. Hayakawa, R. Suzuki, Y. Shiiki, K. Yoshioka, and Q. A. Chen, "Lidar spoofing meets the new-gen: Capability improvements, broken assumptions, and new attack strategies," in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2024.

[105] T. Sato, R. Suzuki, Y. Hayakawa, K. Ikeda, O. Sako, R. Nagata, R. Yoshida, Q. A. Chen, and K. Yoshioka, "On the realism of lidar spoofing attacks against autonomous driving vehicle at high speed and long distance," in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2025.

[106] K. Naugolnykh and L. Ostrovsky, *Nonlinear wave processes in acoustics*. Cambridge University Press, 1998.

[107] B. Assouar, B. Liang, Y. Wu, Y. Li, J.-C. Cheng, and Y. Jing, "Acoustic metasurfaces," *Nature Reviews Materials*, vol. 3, no. 12, pp. 460–472, 2018.

[108] M. E. Badawe, T. S. Almoneef, and O. M. Ramahi, "A true metasurface antenna," *Scientific reports*, vol. 6, no. 1, p. 19268, 2016.

[109] J. Liu, H. Li, H. Wang, M. Sun, H. Wen, J. Wang, and L. Sun, "Timetravel: Real-time timing drift attack on system time using acoustic waves," pp. 3885–3902, 2025.

[110] S. P. Skorobogatov and R. J. Anderson, "Optical fault induction attacks," in *Proceedings of the Cryptographic Hardware and Embedded Systems-CHES 2002: 4th International Workshop Redwood Shores, CA, USA, August 13–15, 2002 Revised Papers 4*. Springer, 2003, pp. 2–12.

[111] M. Nagata, T. Miki, and N. Miura, "Physical attack protection techniques for ic chip level hardware security," *IEEE transactions on very large scale integration (VLSI) systems*, vol. 30, no. 1, pp. 5–14, 2021.

[112] S. Ramesh, G. S. Hadi, S. Yang, M. C. Chan, and J. Han, "Ticktock: detecting microphone status in laptops leveraging electromagnetic leakage of clock signals," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, 2022, pp. 2475–2489.

[113] Q. Xia, Q. Chen, and S. Xu, "Near-ultrasound inaudible trojan (nuit): Exploiting your speaker to attack your microphone," in *Proceedings of the 32nd USENIX Security Symposium (USENIX Security 23)*, 2023, pp. 4589–4606.

[114] N. S. Nise, *Control systems engineering*. John Wiley & Sons, 2020.

[115] J. Jeong, D. Kim, J.-H. Jang, J. Noh, C. Song, and Y. Kim, "Un-rocking drones: Foundations of acoustic injection attacks and recovery thereof." in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2023.

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

[117] R. Quinonez, J. Giraldo, L. Salazar, E. Bauman, A. Cardenas, and Z. Lin, "Savior: Securing autonomous vehicles with robust physical invariants," in *Proceedings of the 29th USENIX security symposium (USENIX Security 20)*, 2020, pp. 895–912.

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

[119] J. Shen, J. Y. Won, Z. Chen, and Q. A. Chen, "Drift with devil: Security of multi-sensor fusion based localization in high-level autonomous driving under gps spoofing," in *Proceedings of the 29th USENIX security symposium (USENIX Security 20)*, 2020, pp. 931–948.

[120] Z. Wang, Y. Wu, and Q. Niu, "Multi-sensor fusion in automated driving: A survey," *Ieee Access*, vol. 8, pp. 2847–2868, 2019.

[121] R. E. Kalman, "A new approach to linear filtering and prediction problems," 1960.

[122] W. Xu, C. Yan, W. Jia, X. Ji, and J. Liu, "Analyzing and enhancing the security of ultrasonic sensors for autonomous vehicles," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 5015–5029, 2018.

[123] J.-A. Ting, E. Theodorou, and S. Schaal, "A kalman filter for robust outlier detection," in *Proceedings of the 2007 IEEE/RSJ International Conference on Intelligent Robots and Systems*. IEEE, 2007, pp. 1514–1519.

[124] S. Nashimoto, D. Suzuki, T. Sugawara, and K. Sakiyama, "Sensor con-fusion: Defeating kalman filter in signal injection attack," in *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, 2018, pp. 511–524.

[125] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," *Advances in neural information processing systems*, vol. 25, 2012.

[126] Y. Cao, C. Xiao, B. Cyr, Y. Zhou, W. Park, S. Rampazzi, Q. A. Chen, K. Fu, and Z. M. Mao, "Adversarial sensor attack on lidar-based perception in autonomous driving," in *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*, 2019, pp. 2267–2281.

[127] Y. Man, M. Li, and R. Gerdes, "Ghostimage: Remote perception attacks against camera-based image classification systems," in *Proceedings of the 23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2020)*, 2020, pp. 317–332.

[128] C. Yan, Z. Xu, Z. Yin, S. Mangard, X. Ji, W. Xu, K. Zhao, Y. Zhou, T. Wang, G. Gu *et al.*, "Rolling colors: Adversarial laser exploits against traffic light recognition," in *Proceedings of the 31st USENIX Security Symposium (USENIX Security 22)*, 2022, pp. 1957–1974.

[129] A. Sayles, A. Hooda, M. Gupta, R. Chatterjee, and E. Fernandes, "Invisible perturbations: Physical adversarial examples exploiting the rolling shutter effect," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2021, pp. 14 666–14 675.

[130] A. Madry, A. Makelov, L. Schmidt, D. Tsipras, and A. Vladu, "Towards deep learning models resistant to adversarial attacks," *arXiv preprint arXiv:1706.06083*, 2017.

[131] N. Carlini and D. Wagner, "Towards evaluating the robustness of neural networks," in *Proceedings of the 2017 ieee symposium on security and privacy (sp)*. Ieee, 2017, pp. 39–57.

[132] Z. Xu, R. Hua, J. Juang, S. Xia, J. Fan, and C. Hwang, "Inaudi-

ble attack on smart speakers with intentional electromagnetic interference," *IEEE Transactions on Microwave Theory and Techniques*, 2021.

[133] T. Gluck, M. Kravchik, S. Chocron, Y. Elovici, and A. Shabtai, "Spoofing attack on ultrasonic distance sensors using a continuous signal," *Sensors*, 2020.

[134] S. Fernández, E. Martínez, J. Varela, P. Musé, and F. Larroca, "Deep-tempest: Using deep learning to eavesdrop on hdmi from its unintended electromagnetic emanations," in *Proceedings of the 13th Latin-American Symposium on Dependable and Secure Computing*, 2024, pp. 91–100.

[135] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, "Security and privacy in smart city applications: Challenges and solutions," *IEEE communications magazine*, vol. 55, no. 1, pp. 122–129, 2017.

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

[137] Z. Jin, X. Lu, B. Yang, Y. Cheng, C. Yan, X. Ji, and W. Xu, "Unity is strength? benchmarking the robustness of fusion-based 3d object detection against physical sensor attack," in *Proceedings of the ACM Web Conference 2024*, 2024, pp. 3031–3042.

[138] S. H. V. Bhupathiraju, J. Sheldon, L. A. Bauer, V. Bindschaedler, T. Sugawara, and S. Rampazzi, "Emi-lidar: Uncovering vulnerabilities of lidar sensors in autonomous driving setting using electromagnetic interference," in *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2023, pp. 329–340.

[139] D. Davidson, H. Wu, R. Jellinek, V. Singh, and T. Ristenpart, "Controlling uavs with sensor input spoofing attacks," in *Proceedings of the 10th USENIX workshop on offensive technologies (WOOT 16)*, 2016.

[140] A. Frangi *et al.*, *Advances in multiphysics simulation and experimental testing of MEMS*. Imperial College Press, 2008, vol. 2.

[141] B. Shao, T. Wan, F. Liao, B. J. Kim, J. Chen, J. Guo, S. Ma, J.-H. Ahn, and Y. Chai, "Highly trustworthy in-sensor cryptography for image encryption and authentication," *ACS nano*, vol. 17, no. 11, pp. 10 291–10 299, 2023.

[142] J. Zhang, Y. Wang, Y. Tu, S. Rampazzi, Z. Lin, I. Lee, and X. Hei, "Adc-bank: Detecting acoustic out-of-band signal injection on inertial sensors," in *International Conference on Security and Privacy in Cyber-Physical Systems and Smart Vehicles*. Springer, 2023, pp. 53–72.

[143] A. Barua and M. A. A. Faruque, "Sensor security: Current progress, research challenges, and future roadmap," in *Proceedings of the 41st IEEE/ACM International Conference on Computer-Aided Design*, 2022, pp. 1–7.

[144] A. Chaman, J. Wang, J. Sun, H. Hassanieh, and R. Roy Choudhury, "Ghostbuster: Detecting the presence of hidden eavesdroppers," in *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*, 2018, pp. 337–351.

[145] Z. Liu, F. Lin, C. Wang, Y. Shen, Z. Ba, L. Lu, W. Xu, and K. Ren, "Camradar: Hidden camera detection leveraging amplitude-modulated sensor images embedded in electromagnetic emanations," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 6, no. 4, pp. 1–25, 2023.

[146] F. Zhou and Y. Chai, "Near-sensor and in-sensor computing," *Nature Electronics*, vol. 3, no. 11, pp. 664–671, 2020.

[147] P. Warden, M. Stewart, B. Plancher, S. Katti, and V. J. Reddi, "Machine learning sensors," *Communications of the ACM*, vol. 66, no. 11, pp. 25–28, 2023.

[148] Knowles, "Knowles aisonic smartmics," https://www.knowles.com/products/smart-mics.

[149] Ring, "Ring alarm glass break sensor," https://ring.com/products/glass-break-sensor.

[150] BOSCH, "Smart sensor: Bhi260ap," https://www.bosch-sensortec.com/products/smart-sensor-systems/bhi260ap/, 2021.

[151] S. Sinha, "5 iot sensor technologies to watch," https://iot-analytics.com/5-iot-sensor-technologies.

[152] X. Ji, W. Zhu, S. Xiao, and W. Xu, "Sensor-based iot data privacy protection," *Nature Reviews Electrical Engineering*, vol. 1, no. 7, pp. 427–428, 2024.

[153] L. Batina, S. Bhasin, D. Jap, and S. Picek, "Csinn: Reverse engineering of neural network architectures through electromagnetic side channel," in *Proceedings of the 28th USENIX Security Symposium (USENIX Security 19)*, 2019, pp. 515–532.

[154] X. Hu, L. Liang, S. Li, L. Deng, P. Zuo, Y. Ji, X. Xie, Y. Ding, C. Liu, T. Sherwood *et al.*, "Deepsniffer: A dnn model extraction framework based on learning architectural hints," in *Proceedings of the Twenty-Fifth International Conference on Architectural Support for Programming Languages and Operating Systems*, 2020, pp. 385–399.