Sensor Security: Current Progress, Research Challenges, and Future Roadmap (Invited Paper)

Anomadarshi Barua and Mohammad Abdullah Al Faruque
Department of Electrical Engineering and Computer Science
University of California, Irvine, California, USA.
Email: *{anomadab, alfaruqu}@uci.edu*

ABSTRACT

Sensors are one of the most pervasive and integral components of today's safety-critical systems. Sensors serve as a bridge between physical quantities and connected systems. The connected systems with sensors blindly believe the sensor as there is no way to authenticate the signal coming from a sensor. This could be an entry point for an attacker. An attacker can inject a fake input signal along with the legitimate signal by using a suitable spoofing technique. As the sensor's transducer is not smart enough to differentiate between a fake and legitimate signal, the injected fake signal eventually can collapse the connected system. This type of attack is known as the transduction attack. Over the last decade, several works have been published to provide a defense against the transduction attack. However, the defenses are proposed on an ad-hoc basis; hence, they are not well-structured. Our work begins to fill this gap by providing a checklist that a defense technique should always follow to be considered as an ideal defense against the transduction attack. We name this checklist as the *Golden reference* of sensor defense. We provide insights on how this Golden reference can be achieved and argue that sensors should be redesigned from the transducer level to the sensor electronics level. We point out that only hardware or software modification is not enough; instead, a hardware/software (HW/SW) co-design approach is required to ride on this future roadmap to the robust and resilient sensor.

CCS CONCEPTS

• **Security and privacy → Embedded systems security**.

KEYWORDS

transduction attack, golden reference for sensor defense

1 INTRODUCTION

Sensors work as the eyes and ears of any embedded system. Therefore, any decision taken by a system depends upon the data coming from a sensor. Though sensors are technically developed nowadays compared to their earlier generation, from a security point of view, almost all sensors are still unsafe and prone to intelligent attacks by an attacker. The reason behind this is that the signals that a sensor measures in the surrounding environment are analog signals, which are not encrypted in the environment. Therefore, sensors cannot differentiate between a legitimate analog input and a fake analog input provided by an attacker. As a result, the transducer of a sensor converts any fake analog signal given as the input into a usable signal (e.g., an electrical signal), which is then propagated to downstream of the signal path and eventually arrives at the system controller. As the system controller does not have any way to authenticate the signal coming from a sensor, it has to blindly believe the sensor and then make decision based upon the sensor data. As there is no hardware/software firewall present between the sensor and the system interface, this could be an entry point for an attacker. An attacker can *noninvasively* inject fake signals into sensors by using a suitable spoofing technique [3, 30, 33, 35] and may compromise the system availability and integrity, causing a system failure and denial-of-service (DoS) attacks on systems.

As the attack at hand fools the sensor's transducer, this type of attack is named as the *transduction attack* [13]. There has been ongoing research on the transduction attack for the last two decades. However, this paper shows that defenses against this transduction attack are still not well-structured, and little to no work is done in the sensor defense domain. We point out that almost all defenses against the transduction attack are proposed on an ad-hoc basis. Therefore, there is no systematic approach present in the literature for defense. Our work begins to fill this gap by providing a checklist of reference points that an ideal defense should always follow to be considered as a successful defense against the transduction attack. We name this checklist as the *Golden reference* for sensor defense.

This Golden reference is the roadmap to a secured sensor that every designer should follow in the future before finally adopting a technique as a sensor defense. We also provide insights on how to achieve the Golden reference. We point out that the Golden reference for sensor defense can not be achieved alone by only hardware or only software modification; instead, a hardware/software (HW/SW) co-design approach is required in the sensor domain. The sensors should be redesigned from the transducer level to the sensor electronics level with the integration of smart hardware and software. We believe that the defenses highlighted in this paper will be relevant soon when sensors will pervade our lives.

2 BACKGROUND

2.1 Sensor physics

A sensor is an instrument that senses physical input signals from the environment and converts the measured physical quantities into understandable data that can be interpreted by either a human or a machine. For example, a simple glass thermometer presents visual data, which can be interpreted by a human, and an electronic pressure sensor can provide electronic data, which can be interpreted by machines. There are a multitude of types of sensors and the physics behind the conversion of physical input signals to understandable data varies from one sensor to another. However, all sensors have a common physics that is systematized below.

Sensing structure and transducer: The most common sensor physics is that all the sensors use a sensing structure, which typically senses the physical input signals and uses a *transducer* to convert the sensed physical input signals into understandable

ICCAD '22, October 30-November 3, 2022, San Diego, CA, USA

ACM ISBN 978-1-4503-9217-4/22/10.
https://doi.org/10.1145/3508352.3561100

data (see Fig. 1). For example, a pressure sensor has a diaphragm as the sensing structure and uses a capacitor plate as the transducer to convert the displacement of the diaphragm into an electrical signal. The converted understandable data is ideally proportional to physical input signals. Mathematically, if the sensed physical input signal is S_{in} and the corresponding converted data from the transducer is S_{con}, we can write S_{con} as follows:

$$S_{con} = k \times f\{S_{in}\} \tag{1}$$

where k is a proportionality constant and $f\{S_{in}\}$ is a function of the S_{in}. It is important to note that $f\{S_{in}\}$ can be a function of any type. For example, for a Hall sensor, $f\{S_{in}\}$ is a linear function of input magnetic fields and for a p-n junction temperature sensor, $f\{S_{in}\}$ is an exponential function of input temperature T (i.e., e^T).

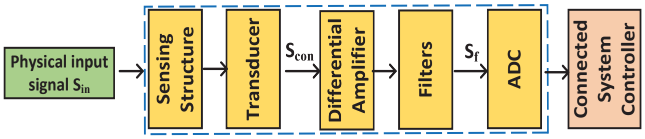

Figure 1: A basic overview of the sensor physics.

2.2 Sensor electronics

Though sensing structure and transducer are common in all sensors, most sensors have other additional electronics to improve the sensed signal quality (see Fig. 1). The converted understandable data S_{con} is typically an analog signal, which is given as an input to a differential amplifier to remove the common mode noise. A single or multiple stages of signal conditioning filters are applied afterward, which is followed by an analog-to-digital converter (ADC) for the data digitization. Filters are typically LPF used to remove high-frequency noise signals from the measurement. Typically, analog sensors output the analog signals from the differential amplifier or filters directly, while digital sensors contain the LPF and ADC.

2.3 Operating region and saturation region

As mentioned in Sections 2.1 and 2.2, the shape of the data S_{con} from the transducer can be linear, exponential or any other types and is given as an input to different filtration blocks (see Fig. 1). As these filters are powered by a finite power supply, the maximum value of S_{con} the filters can handle is limited by the power supply. In fact, the output S_f from the filtration block will begin to flatten when the S_{con} is too large and the power supply limits are reached. The region, where the output S_f is not flattened, is known as the operating region of the sensor (see Fig. 2). This region is typically linear between the signal S_{con} and S_f. In contrast, the region, where the output S_f is flattened, is known as the saturation region of the sensor. Please note that the exact value of the input S_{con} cannot be recovered while the filter output S_f is in the saturation region.

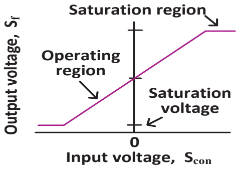

Figure 2: Operating and saturation region of a sensor.

2.4 Sensor physics from security perspective

Entry point for an attacker: Over the last three decades, transducers and sensing structures have been technically improved in terms of stability, accuracy, and sensitivity; however, to the best of our knowledge, designers still do not consider security as one of the fundamental requirements while designing transducers and sensing structures of sensors. As a result, it is noteworthy that *all* the transducers and sensing structures are naive, and they cannot differentiate between legitimate input signals and malicious fake input signals. As a consequence, if an adversary injects malicious fake input signals into the sensing structure, the injected fake input signals are converted into understandable data by transducers and then propagate up to the system controller. The system controller blindly trusts signals coming from sensors. Therefore, this can be an entry point for an attacker. An attacker can noninvasively inject fake input signals to the transducers or sensing structures and can fool the system controller, resulting in a catastrophic failure, system shutdown, or disruption of the system's normal behavior.

Systematization of the attack signal: We need to emphasize again that the *only* reason that facilitates this attack is that the sensor structure and the transducer cannot differentiate between the legitimate input signals and the malicious fake input signals. Therefore, this type of attack is denoted by the *transduction attack* [13, 32]. Let's denote malicious fake input signals by S^f_{in}. Therefore, the output S_{con} from the transducer in Eqn. 1 can be written as:

$$S^f_{con} = k \times f\{S_{in} + S^f_{in}\} \tag{2}$$

where S^f_{con} is the output from the transducer after the injection of the malicious fake input signals S^f_{in}. The term S^f_{con} can propagate from the transducer to the upper level as the existing sensor electronics blindly believe what is coming from the transducer.

Scope of our work: We consider only those attacks that originate from the fake signal injection into the sensing structures and transducers. Let us give an example to clarify the scope of our work. A pressure sensor can measure room pressure. If an attacker changes the room pressure by switching on/off the heating, ventilation, and air conditioning (HVAC) unit of the room, the room pressure changes. As a result, the pressure sensor measures a corrupted room pressure. We are not considering this type of attack on the pressure sensor. Instead, we are considering that type of attack, where the attacker directly injects fake signals into the sensing structure (i.e., diaphragm) and transducer of the pressure sensor.

3 SENSOR ATTACK MODEL

The basic components of the sensor attack model is explained below and also shown in Fig. 3.

i. Attacker's capability: The attacker may not get a long time to modify the sensor like a lunch-time attack [14]. Instead, the attacker may get a brief access near the sensor to inject the fake input signal S^f_{in} from a *close* distance. The fake input signal S^f_{in} is a physical signal coming from the physical domain in different forms, such as acoustics, ultrasound, infrared, visible light, magnetic field, and electric field, and impacting the cyber domain [11] of the sensor and connected systems.

ii. Noninvasive and stealthy attack: The attacker is not allowed to invasively access and modify any hardware and software

Table 1: Summary of the notable published work on sensor attack. (In-band = fake and legitimate signal share same frequency band; Out-band = fake and legitimate signal share different frequency band)

Sl.	Paper	Year	Sensor type	Sensor	Injected signal	Injected signal pattern	Industry
1	[3]	2020	Magnetic	Hall	Magnetic field	In-band, out-band	Power grid
2	[21]	2013	Magnetic	Hall	Magnetic field	In-band	Automotive
3	[30]	2017	Inertial	Accelerometer & Gyroscope	Ultrasound	Out-band resonant frequency	AR/VR
4	[25]	2015	Inertial	Gyroscope	Sound wave	Out-band resonant frequency	Drone
5	[26]	2017	Inertial	Accelerometer	Ultrasound	Out-band resonant frequency	Smart device
6	[27]	2018	Inertial	Accelerometer & Gyroscope	Sound wave	Out-band resonant frequency	Smart device
7	[10]	2018	Inertial	Shock sensor	Sound wave	Out-band	Hard disk
8	[5]	2022	Pressure	Pressure sensor	Sound wave	Out-band resonant frequency	NPR
9	[28]	2021	Pressure	Pressure sensor	EMI	Out-band	Inflation pump
10	[17]	2016	Optical	Optical sensor	Infrared	Out-band	Infusion pump
11	[12]	2016	Optical	Camera & Lidar	Light	In-band	UAV
12	[19]	2017	Optical	Lidar	Light	In-band	Automotive
13	[35]	2017	Acoustic	Microphone	Ultrasound	Out-band	Smart device
14	[33]	2016	Acoustic	Ultrasound	Ultrasound	In-band	Automotive
15	[16]	2013	Analog	Defibrillator	EMI	In-band	Medical device

of the sensor using physical tempering. This type of physical invasive attack is out of the scope of our study. Instead, our attack considers a scenario where the attacker injects a fake input signal to noninvasively perturb the sensor's transducer in a stealthy manner.

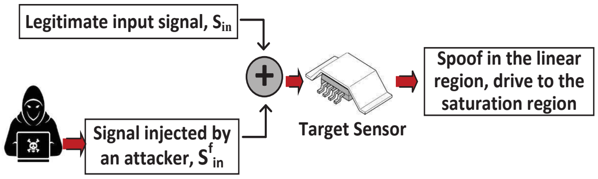
Legitimate input signal, S_{in}
Signal injected by an attacker, S^{f}_{in}
Target Sensor
Spoof in the linear region, drive to the saturation region

Figure 3: Basic components of the sensor attack model.

iii. Attack's outcome: As mentioned in Section 2.3, a sensor has a linear operating region and a flattened saturation region. The attacker can inject a fake input signal S^{f}_{in} to spoof the sensor output in its linear region or drive the sensor output to its saturation region.

In the linear region, the attacker can force the sensor to work at a particular operating point and can cause an adversarial control. For example, an attacker can use magnetic fields to spoof a Hall sensor in its linear region located in a solar inverter and can intentionally change the power of the solar inverter [2–4].

In the saturation region, the input-output linear relationship of sensors gets flattened, and sensors go completely blind to any variation of the input. This may cause catastrophic failure in the normal operation of the connected systems resulting in a DoS attack. Typically, the attacker requires a stronger fake input signal to drive the sensor output to its saturation region [7].

4 CURRENT PROGRESS

Sensor security is comparatively a new domain in the security community that has ongoing research for the last two decades. However, over the last decades, the research on sensor security has been accelerated due to the advent of the smart sensing systems in autonomous vehicles (AV), internet-of-things (IoT), and smart automation systems. Our paper broadly classifies the ongoing research on sensor security into two categories: (i) current progress on sensor attack and (ii) current progress on sensor defense.

4.1 Current progress on sensor attack

We discuss sensor attacks in the following broad categories. A summary of the most notable published work on sensor attack is given in Table 1 with their publication years.

Attack on magnetic sensors: Barua et al. [3] demonstrated a noninvasive attack on Hall sensors located in a solar inverter using a magnetic field from a close distance, resulting in a shutdown of a weak micro-grid. Shoukry et al. [21] showed a disruptive magnetic spoofing attack on a Hall sensor located in an anti-lock braking system (ABS) of a vehicle, resulting in a possible brake failure.

Attack on inertial sensors: Wang et al. [30] used an ultrasonic gun to spoof different inertial sensors, such as MEMS accelerometers and gyroscopes, at their resonant frequencies to create havoc in the connected systems. Son et al. [25] used a powerful sound wave to spoof the gyroscope of a drone at its resonance frequency, making the drone uncontrollable. Trippel et al. [26], and Tu et al. [27] showed an adversarial control over MEMS accelerometers and gyroscopes using acoustic signals at their resonant frequencies. Bolton et al. [10] showed how acoustic signal can compromise the MEMS shock sensor located in a hard disk drive.

Attack on pressure sensors: Barua et al. [5] demonstrated a spoofing attack on pressure sensors located in a negative pressure room (NPR), using acoustic signal at the sensor's resonant frequency. Tu et al. [28] showed a deliberate electromagnetic interference (EMI) attack on an inflation pump's pressure sensor while impacting the system's actuation.

Attack on optical sensors: Park et al. [17] used infrared to spoof optical sensors of an infusion pump to deliver overdose to patients. Davidson et al. [12] reported how spoofing optical sensors of an unmanned aerial vehicle (UAV) can compromise its complete control. Shin et al. [19] showed a spoofing attack on Lidar to create illusions of objects appearing closer in automotive systems.

Attack on acoustic sensors: Zhang et al. [35] injected inaudible commands into a microphone using ultrasonic carriers. Yan et al. [33] showed an attack on ultrasonic sensors of a vehicle using acoustic waves to impair vehicle safety.

Attack on other analog sensors: Kune et al. [16] spoofed sensors by EMI to induce defibrillation shocks on cardiac devices.

It is just a matter of time before more attacks on sensors will emerge from different attack surfaces as sensors are getting complex and sophisticated nowadays without improving their security.

4.2 Current progress on sensor defense

We discuss sensor defense in the following broad categories. A summary of the most notable sensor defenses is given in Table 2.

Table 2: Summary of the notable published work on sensor defense. (In-band = fake and legitimate signal share same frequency band; Out-band = fake and legitimate signal share different frequency band)

Sl.	Paper	Year	Sensor type	Sensor	Defense technique	Research challenge
1	[3]	2020	Magnetic	Hall	Shielding	Not scalable, bulky
2	[21]	2013	Magnetic	Hall	PyCRA	Can be bypassed
3	[30]	2017	Inertial	Accelerometer & Gyroscope	Noise cancellation	Not for in-band signal, not for saturation
4	[25]	2015	Inertial	Gyroscope	Sound wave	Not for in-band signal, not for saturation
5	[26]	2017	Inertial	Accelerometer	Randomized and 180^0 out-of-phase sampling	Not for in-band signal, DC attack signal
6	[27]	2018	Inertial	Accelerometer & Gyroscope	LPF and dampening	Not for in-band signal, not for saturation
7	[10]	2018	Inertial	Shock sensor	Sensor fusion	Costly, redundant, not for saturation
8	[5]	2022	Pressure	Pressure sensor	LPF	Not for in-band signal
9	[28]	2021	Pressure	Pressure sensor	Transduction shield	Finite physical distance, not for saturation
10	[17]	2016	Optical	Optical sensor	PyCRA	Can be bypassed
11	[12]	2016	Optical	Camera & Lidar	Modified optical flow algorithm	Not applicable
12	[19]	2017	Optical	Lidar	Sensor fusion, redundancy	Costly, not for saturation
13	[35]	2017	Acoustic	Microphone	Noise cancellation	Not for in-band signal
14	[33]	2016	Acoustic	Ultrasound	Acoustic noise reduction (ANR)	For acoustic only, Not for out-band signal
15	[16]	2013	Analog	Defibrillator	Adaptive filter, LPF	Not for saturation

Defense for magnetic sensors: Barua et al. [3] proposed strong magnetic shielding with a secure surrounding to prevent the magnetic spoofing attack on Hall sensors. Shoukry et al. [21] proposed PyCRA to randomize the transmission and reception of signals to prevent magnetic spoofing attacks on ABS sensors of automotive. However, PyCRA only works for active sensors [21].

Defense for inertial sensors: Trippel et al. [26] proposed randomized and 180^0 out-of-phase sampling to nullify acoustic spoofing signals injected into MEMS accelerometers. Son et al. [25] proposed resonance tuning using a feedback capacitor to prevent the out-band resonant frequency. Wang et al. [30] proposed to use an external microphone to detect the resonating sound and perform noise cancellation. Tu et al. [27] proposed low-pass filtering (LPF) along with the dampening of the injected ultrasound.

Defense for pressure sensors: Barua et al. [5] used an LPF to filter out the sound wave from pressure sensors to prevent acoustic spoofing on pressure sensors. Tu et al. [28] used a transduction shield to measure the fake signal first and then subtract it from the corrupted signal to recover the legitimate signal.

Defense for optical sensors: Park et al. [17] measured the light intensity to detect the attack and used PyCRA to prevent it. Shin et al. [19] propose sensor fusion and redundancy to prevent the optical attack on a lidar.

Defense for acoustic sensors: Zhang et al. [35] used a modulation - demodulation based noise canceling technique to cancel out the injected ultrasound. Yan et al. [33] proposed shielding and acoustic noise reduction (ANR) by emitting a sound with minor phase and amplitude adjustment.

Defense for other analog sensors: Kune et al. [16] proposed adaptive filtering to estimate the spoofing attack signal first and then subtract the estimated attack signal from the original signal to clean up the original signal.

5 RESEARCH CHALLENGES

The defense techniques described in Section 4.2 have research challenges. A summary of research challenges is given in Table 2.

Shielding and dampening: Barua et al. [3] and Tu et al. [27] proposed shielding to dampen the injected fake magnetic field and fake ultrasound, respectively. Though shielding is a cheap and quick countermeasure for a few of the fake injected signals, such as sound wave, ultrasound, and infrared, shielding might fail for other signals, such as magnetic fields. For example, a strong shield again may fail to a stronger magnetic field injected by an attacker. To increase the shielding property of a shield so that it can work for a stronger attack signal, the designer may need to increase the thickness of the shield. As even a thick shield can be penetrated by a stronger magnetic field, there is no *sweet spot* for shielding to claim that it can prevent a magnetic field of any strength. Therefore, only shielding cannot be considered as a *sole* defense for sensors.

Randomization of transmission (PyCRA): Shoukry et al [22] proposed PyCRA; however, PyCRA only works for active sensors, not for passive sensors. Moreover, Shin et al. [20] showed that the implemented authentication mechanism of PyCRA can be successfully bypassed with a low-cost circuit. This proves that there is currently no effective, robust and generalizable defense scheme against active sensor spoofing attacks.

Randomized and 180^0 out-of-phase sampling: These two techniques from [26] only work for out-band resonant frequency attack signals. However, they do not work other than a specific resonant frequency, for example, any attack frequency. Moreover, they do not work against a DC forged signal because randomized sampling cannot filter out a DC signal. In addition, they do not work when the sensor output is flattened in the saturation region.

Adaptive filter and transduction shield: Both of these defense techniques from [16, 28] work similarly by estimating the spoofing attack signal first and then subtracting the estimated attack signal from the original signal to clean up the original signal. These techniques will fail in the following two scenarios: (i) Because of the finite physical distance between the adaptive filter or transduction shield and the compromised sensor, the adaptive filter or transduction shield cannot measure the exact amplitude of the external attack signals. This is why we can not simply subtract the estimated attack signals from the original signals to recover the original signal. (ii) They do not work when the sensor output is flattened in the saturation region.

LPF and other filtering techniques: LPF and other filtering techniques in [5, 16] only work as a successful defense when the fake attack signal has a predicable frequency spectrum and is an out-band signal. If the injected fake signal shares the same frequency band as the legitimate signal, LPF or other filtering techniques cannot accurately filter out the fake attack signals. The reason behind this is that while filtering the attack signals, they also filter out the same band of legitimate signals.

Machine learning (ML) techniques: Machine learning (ML) techniques require complex computations to converge for attack detection and recovery, requiring powerful hardware resources. Therefore, they are not suitable for low-power real-time sensor systems with constrained resources. In addition, they may not work against a time-varying magnetic spoofing as a time-varying signal may create oscillations between two safe states of the controller, and they are incapable of handling these oscillations in real-time.

5.1 Area of focus

If we analyze all the notable defenses from Table 2 published throughout the last decade, we can conclude the following points:

■ The defenses were proposed on an ad-hoc basis. For example, the researchers first find a security issue with the sensor and then try to come up with a defense to overcome it. Researchers only focus on a specific security issue rather than focusing on all the corner cases from all the attack surfaces. Therefore, a proposed defense for a particular type of sensor is not applicable to other types. For example, the randomized and 180^0 out-of-phase sampling [26], which are applicable for MEMS inertial sensors to nullify out-band resonant attack frequency, is not applicable for magnetic Hall sensors because Hall sensors can have in-band attack frequency other than a specific out-band resonant frequency [3].

■ There is no defense technique exists in the literature that can prevent sensors from going into the saturation region or recover information from the sensor's saturation region.

■ There is no defense, which can contain a fake injected signal having the same frequency as the legitimate signal.

■ As PyCRA [22] can be bypassed, there is no defense in the literature for active sensors till to date.

Therefore, sensor security is still a *malnourished* domain, which requires more attention from security researchers.

6 FUTURE ROADMAP

Sensor heterogeneity: The fundamental challenge of designing and modeling a robust and secured sensor is the heterogeneity of sensor types. The heterogeneity of sensors exists because of the sensor's signal modality, which differs from the sensor to sensor. For example, a Hall sensor handles magnetic fields and a pressure sensor handles pressure waves as the signal modality. As sensors differ from each other in terms of signal modality, the proper selection of transducers and sensor electronics also differ from sensor to sensor depending on the signal modality. Therefore, a single generalized defense technique that is applicable to all sensors will be quite complicated. However, it is still worth giving it a try from a sensor security research point of view because the future days will be the days for smart sensors, and security will be a big concern for them.

6.1 Golden reference for sensor defense

The next generation of research on sensor security should have to consider the security from designing the transducer to the implementation of the sensor electronics. Instead of implementing an ad-hoc defense, researchers must ensure a checklist before finally adopting a technique as a sensor defense. We name this checklist by the *Golden reference* for a sensor defense against a transduction attack. This golden reference has the following points.

(i) The defense should simultaneously work for in-band and out-band fake injected input signals.
(ii) The defense should prevent a sensor from going into the saturation region because of the injection of fake input signals.
(iii) The defense should contain a fake injected signal even it has the same frequency as the legitimate input signal.
(iv) The defense should work for active and passive sensors. If a single defense does not simultaneously work for both sensors, there should be a defense targeting an active sensor and another separate defense targeting a passive sensor.
(v) The defense should be hard real-time.
(vi) The defense should not hamper the existing data processing speed or bandwidth of the sensor.

6.2 Roadmap to achieve the Golden reference

The Golden reference for sensor defense can not be achieved *alone* by only hardware or only software modification; instead, a hardware/software (HW/SW) co-design approach is required in the sensor domain. The sensors should be redesigned from the transducer level to the sensor electronics level. A smart transducer should be built instead of a naive one, and an intelligent and low-complexity algorithm should be adopted in the sensor electronics. We explain the roadmap to achieve the Golden reference below.

6.2.1 *Encrypted analog signal:*

The main reason for sensor vulnerability is that the legitimate analog signal S_{in}, which is going to be measured by the sensor, is not encrypted before going into the transducer. Therefore, the attacker can use a fake signal S_{in}^f to corrupt the legitimate signal S_{in}. This problem can be solved by encrypting the legitimate analog signal with a key in the *analog domain* and decrypting the legitimate signal in the transducer side or in the sensor electronics using the same key. The analog domain encryption can be achieved using the following ways:

■ **First**, an orthogonal noise can be padded with the legitimate signal S_{in} to hide the information from the attack surface. This method is known as analog scrambling [18].

■ **Second**, the legitimate signal S_{in} can be mapped into the broad spectrum. This technique is known as frequency hopping spread spectrum [15] and can be adopted in the sensor domain.

■ **Third**, the legitimate signal S_{in} can be encrypted in the analog domain using a pseudo-noise, which is the original key. More keys can be generated using the original key to decrypt the signal [24].

Please note that encryption of the legitimate analog signal is the *ultimate* solution for a robust sensor. This defense technique would achieve the points i-iv of the Golden reference in Section 6.1; however, it may or may not hamper the data processing speed (point v) and real-time requirement (point vi) of the sensor depending upon the encryption complexity.

6.2.2 *Modifying the transducer:*

The transducer must be resilient enough to reject the injected fake signal S_{in}^f. As a transducer is an entry point to the sensor, if a transducer can reject the fake signal, this approach would diminish the burden of using a complex encryption algorithm in the sensor hardware. Industry is adopting this scheme nowadays where ever it is feasible. For example, Hall current sensors use a Hall element as a transducer. Two Hall elements (see Fig. 4) are placed inside of a Hall current sensor in a differential manner to reject common-mode noise [1]. As the injected fake signal S_{in}^{f} is common to the differential Hall element, the injected fake signal S_{in}^{f} can be considered as common-mode noise and can be eliminated from the sensor at the transducer level. Though this strategy is quite novel, it has its own implementation challenge for all types of sensors. Research along this direction would be *influential* in future for a secured sensor.

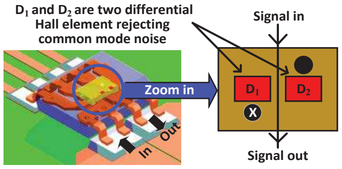
D_1 and D_2 are two differential Hall element rejecting common mode noise
Signal in
Zoom in
D_1
D_2
Signal out
In
Out

Figure 4: A basic overview of the differential sensing.

6.2.3 ***Preventing sensor saturation:*** As mentioned in Section 3, if an attacker can drive the sensor to its saturation region, the output gets flattened, and no information can be retrieved, resulting in a DoS attack on sensors. This attack is known as saturation attack [7]. The core idea behind preventing a saturation attack is to generate an internal signal, which has the *same* strength but in *opposite polarity* to the injected fake signal, so that the internal signal can nullify the injected fake signal. Barua et al. [7] conceptualized and implemented this idea in the context of Hall magnetic sensors by providing a defense named *PreMSat*. The idea of *PreMSat* can be extended to other sensor types as well.

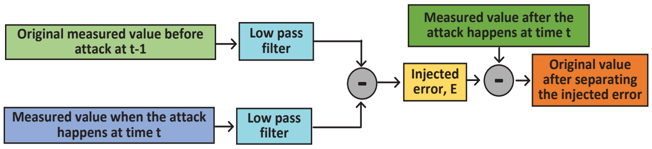
Original measured value before attack at t-1
Low pass filter
Measured value when the attack happens at time t
Low pass filter
-
Injected error, E
Measured value after the attack happens at time t
-
Original value after separating the injected error

Figure 5: A basic overview of the improved algorithm [6].

6.2.4 ***Improving the adaptive filter and transduction shield:*** The main bottleneck of using the adaptive filter and transduction shield is the introduced error in the estimated attack signals for the physical distance present between the sensor and the shield (see Section 5). This problem can be solved by using an improved defense algorithm proposed by Barua et al. [6]. The main idea of this algorithm is that the difference between the measured signal during the attack and before the attack gives the amount of injected error after the attack. This algorithm tracks this difference all the time and generates a feedback signal to nullify the injected error by the attacker. The idea is illustrated in Fig. 5.

6.2.5 ***Context-aware anomaly detection:*** An injected fake signal can be considered as an anomaly. Traditional anomaly detection algorithms are not low-power and hence, they are not suitable for sensor hardware. Therefore, a low-power and low- complexity algorithm may be another feasible option to run on the sensor hardware to detect injected fake signals. A low-power anomaly detection algorithm named as Hierarchical Temporal Memory (HTM) can be evaluated to detect *context aware* anomaly detection on the sensor data [8, 9]. Moreover, the context-aware sensor association method [34] can be evaluated further as a defense technique for sensors.

6.2.6 ***Control-theoretic approach:*** State estimation and state recovery based control-theoretic defense approaches can be another option to recover a system controller after the transduction attack. Shoukry et al. [23] proposed reconstructing the sensor state to recover from a sensor spoofing attack using the satisfiability modulo theory (SMT). Wang et al. [29] demonstrated a graph-based technique to track states in the system controller to detect an intrusion. However, the correct direction will be to incorporate the sensor's physics and physical knowledge of the system with the control-theoretic approach for accurate estimation of the states.

6.2.7 ***Sensor fusion based context aware:*** Sensor fusion and redundancy [10, 19, 30, 31] based approaches can be merged with ML algorithm to create an appropriate context and abstraction of the sensor data. Therefore, during an attack, the sensor data can be recovered from a proper context using abstracted sensor data. The data abstraction can be made intelligent and adaptive to tackle the continuous change of the sensor environment. However, sensor fusion adds extra price and complexity to the system; therefore, designers try to avoid this unless it is arguably required.

7 CONCLUSION

In this paper, we present a notion of sensor security, whereby, we focus on the importance of security measures that needs to be taken while designing a sensor. We discuss that sensors are vulnerable to external fake signals and give a summary of existing defenses in the sensor domain. We point out the limitations of existing defense techniques and emphasize that very little to no work exists in the sensor security domain. Therefore, we emphasize that the next generation of research on sensor security should have to ensure a Golden reference before finally adopting a technique as a sensor defense. We also provide a roadmap on how to achieve the Golden reference checklist while designing a robust and resilient sensor.

ACKNOWLEDGMENTS

This work was partially supported by the National Science Foundation (NSF) under awards CMMI-1739503 and ECCS-2028269. Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of the funding agencies.

REFERENCES

[1] Latham Alexander. 2019. *Common Mode Field Rejection in Coreless Hall-Effect Current Sensor ICs*. https://www.allegromicro.com/-/media/files/application-notes/an269123-common-mode-field-rejection-in-coreless-current-sensor-ics.pdf. (Accessed: 03-22-2022).

[2] Anomadarshi Barua and Mohammad Abdullah Al Faruque. 2019. *The Hall Sensor Security*. Springer Berlin Heidelberg, Berlin, Heidelberg, 1–4. https://doi.org/10.1007/978-3-642-27739-9_1652-1

[3] Anomadarshi Barua and Mohammad Abdullah Al Faruque. 2020. Hall Spoofing: A Non-Invasive DoS Attack on Grid-Tied Solar Inverter. In *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, 1273–1290. https://www.usenix.org/conference/usenixsecurity20/presentation/barua

[4] Anomadarshi Barua and Mohammad Abdullah Al Faruque. 2020. Special session: Noninvasive sensor-spoofing attacks on embedded and cyber-physical systems. In *2020 IEEE 38th International Conference on Computer Design (ICCD)*. IEEE, 45–48.

[5] Anomadarshi Barua and Mohammad Abdullah Al Faruque. 2022. A Wolf in Sheep's Clothing: Spreading Deadly Pathogens Under the Disguise of Popular Music. In *29th ACM Conference on Computer and Communications Security (CCS)*.

[6] Anomadarshi Barua and Mohammad Abdullah Al Faruque. 2022. HALC: A Real-time In-sensor Defense against the Magnetic Spoofing Attack on Hall Sensors. In *25th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2022)*.

[7] Anomadarshi Barua and Mohammad Abdullah Al Faruque. 2022. PreMSat: Preventing Magnetic Saturation Attack on Hall Sensors. In *International Conference on Cryptographic Hardware and Embedded Systems (TCHES 2022)*.

[8] Anomadarshi Barua, Deepan Muthirayan, Pramod P Khargonekar, and Mohammad Abdullah Al Faruque. 2020. Hierarchical temporal memory based machine learning for real-time, unsupervised anomaly detection in smart grid: WiP abstract. In *2020 ACM/IEEE 11th International Conference on Cyber-Physical Systems (ICCPS)*. IEEE, 188–189.

[9] Anomadarshi Barua, Deepan Muthirayan, Pramod P Khargonekar, and Mohammad Abdullah Al Faruque. 2020. Hierarchical temporal memory based one-pass learning for real-time anomaly detection and simultaneous data prediction in smart grids. *IEEE Transactions on Dependable and Secure Computing* (2020).

[10] Connor Bolton, Sara Rampazzi, Chaohao Li, Andrew Kwong, Wenyuan Xu, and Kevin Fu. 2018. Blue note: How intentional acoustic interference damages availability and integrity in hard disk drives and operating systems. In *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1048–1062.

[11] Sujit Rokka Chhetri, Jiang Wan, and Mohammad Abdullah Al Faruque. 2017. Cross-domain security of cyber-physical systems. In *2017 22nd Asia and South Pacific design automation conference (ASP-DAC)*. IEEE, 200–205.

[12] Drew Davidson, Hao Wu, Rob Jellinek, Vikas Singh, and Thomas Ristenpart. 2016. Controlling UAVs with sensor input spoofing attacks. In *10th {USENIX} Workshop on Offensive Technologies ({WOOT} 16)*.

[13] Kevin Fu and Wenyuan Xu. 2018. Risks of trusting the physics of sensors. *Commun. ACM* 61, 2 (2018), 20–23.

[14] Christina Garman, Matthew Green, Gabriel Kaptchuk, Ian Miers, and Michael Rushanan. 2016. Dancing on the lip of the volcano: Chosen ciphertext attacks on apple imessage. In *25th {USENIX} Security Symposium ({USENIX} Security 16)*. 655–672.

[15] Valeri P Ipatov. 2005. *Spread spectrum and CDMA: principles and applications*. John Wiley & Sons.

[16] Denis Foo Kune, John Backes, Shane S Clark, Daniel Kramer, Matthew Reynolds, Kevin Fu, Yongdae Kim, and Wenyuan Xu. 2013. Ghost talk: Mitigating EMI signal injection attacks against analog sensors. In *2013 IEEE Symposium on Security and Privacy*. IEEE, 145–159.

[17] Youngseok Park, Yunmok Son, Hocheol Shin, Dohyun Kim, and Yongdae Kim. 2016. This ain't your dose: Sensor spoofing attack on medical infusion pump. In *10th {USENIX} Workshop on Offensive Technologies ({WOOT} 16)*.

[18] Franz Pichler. 1982. Analog scrambling by the general fast Fourier transform. In *Workshop on Cryptography*. Springer, 173–178.

[19] Hocheol Shin, Dohyun Kim, Yujin Kwon, and Yongdae Kim. 2017. Illusion and dazzle: Adversarial optical channel exploits against lidars for automotive applications. In *International Conference on Cryptographic Hardware and Embedded Systems*. Springer, 445–467.

[20] Hocheol Shin, Yunmok Son, Youngseok Park, Yujin Kwon, and Yongdae Kim. 2016. Sampling Race: Bypassing {Timing-Based} Analog Active Sensor Spoofing Detection on {Analog-Digital} Systems. In *10th USENIX Workshop on Offensive Technologies (WOOT 16)*.

[21] Yasser Shoukry, Paul Martin, Paulo Tabuada, and Mani Srivastava. 2013. Non-invasive spoofing attacks for anti-lock braking systems. In *International Conference on Cryptographic Hardware and Embedded Systems*. Springer, 55–72.

[22] Yasser Shoukry, Paul Martin, Yair Yona, Suhas Diggavi, and Mani Srivastava. 2015. Pycra: Physical challenge-response authentication for active sensors under spoofing attacks. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. 1004–1015.

[23] Yasser Shoukry, Pierluigi Nuzzo, Nicola Bezzo, Alberto L Sangiovanni-Vincentelli, Sanjit A Seshia, and Paulo Tabuada. 2015. Secure state reconstruction in differentially flat systems under sensor attacks using satisfiability modulo theory solving. In *2015 54th IEEE Conference on Decision and Control (CDC)*. IEEE, 3804–3809.

[24] Dalila Slimani and Fatiha Merazka. 2018. Encryption of speech signal with multiple secret keys. *Procedia computer science* 128 (2018), 79–88.

[25] Yunmok Son, Hocheol Shin, Dongkwan Kim, Youngseok Park, Juhwan Noh, Kibum Choi, Jungwoo Choi, and Yongdae Kim. 2015. Rocking drones with intentional sound noise on gyroscopic sensors. In *24th USENIX Security Symposium (USENIX Security 15)*. 881–896.

[26] Timothy Trippel, Ofir Weisse, Wenyuan Xu, Peter Honeyman, and Kevin Fu. 2017. WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks. In *2017 IEEE European symposium on security and privacy (EuroS&P)*. IEEE, 3–18.

[27] Yazhou Tu, Zhiqiang Lin, Insup Lee, and Xiali Hei. 2018. Injected and delivered: Fabricating implicit control over actuation systems by spoofing inertial sensors. In *27th USENIX Security Symposium (USENIX Security 18)*. 1545–1562.

[28] Yazhou Tu, Vijay Srinivas Tida, Zhongqi Pan, and Xiali Hei. 2021. 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*. 901–915.

[29] Yong Wang, Zhaoyan Xu, Jialong Zhang, Lei Xu, Haopei Wang, and Guofei Gu. 2014. Srid: State relation based intrusion detection for false data injection attacks in scada. In *European Symposium on Research in Computer Security*. Springer, 401–418.

[30] Zhengbo Wang, Kang Wang, Bo Yang, Shangyuan Li, and Aimin Pan. 2017. Sonic gun to smart devices: Your devices lose control under ultrasound/sound. *Black Hat USA* (2017), 1–50.

[31] Wenyuan Xu, Chen Yan, Weibin Jia, Xiaoyu Ji, and Jianhao Liu. 2018. Analyzing and enhancing the security of ultrasonic sensors for autonomous vehicles. *IEEE Internet of Things Journal* 5, 6 (2018), 5015–5029.

[32] Chen Yan, Hocheol Shin, Connor Bolton, Wenyuan Xu, Yongdae Kim, and Kevin Fu. 2020. Sok: A minimalist approach to formalizing analog sensor security. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 233–248.

[33] Chen Yan, Wenyuan Xu, and Jianhao Liu. 2016. Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle. *DEF CON* 24, 8 (2016), 109.

[34] Rozhin Yasaei, Felix Hernandez, and Mohammad Abdullah Al Faruque. 2020. Iot-cad: context-aware adaptive anomaly detection in iot systems through sensor association. In *2020 IEEE/ACM International Conference On Computer Aided Design (ICCAD)*. IEEE, 1–9.

[35] Guoming Zhang, Chen Yan, Xiaoyu Ji, Tianchen Zhang, Taimin Zhang, and Wenyuan Xu. 2017. Dolphinattack: Inaudible voice commands. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. 103–117.