Transduction Shield: A Low-Complexity Method to Detect and Correct the Effects of EMI Injection Attacks on Sensors

Yazhou Tu
University of Louisiana at Lafayette
Lafayette, Louisiana, USA
yazhou.tu1@louisiana.edu

Vijay Srinivas Tida
University of Louisiana at Lafayette
Lafayette, Louisiana, USA
vijay-srinivas.tida1@louisiana.edu

Zhongqi Pan
University of Louisiana at Lafayette
Lafayette, Louisiana, USA
zhongqi.pan@louisiana.edu

Xiali Hei
University of Louisiana at Lafayette
Lafayette, Louisiana, USA
xiali.hei@louisiana.edu

ABSTRACT

The reliability of control systems often relies on the trustworthiness of sensors. As process automation and robotics keep evolving, sensing methods such as pressure sensing are extensively used in both conventional systems and rapidly emerging applications. The goal of this paper is to investigate the threats and design a low-complexity defense method against EMI injection attacks on sensors.

To ensure the security and usability of sensors and automated processes, we propose to leverage 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. Our method can detect and correct corrupted sensor measurements without introducing components or modules that are highly complex compared to an original low-end sensor circuit. We analyze and evaluate our method on sensors with EMI injection experiments using different attack parameters. We investigate several attack scenarios, including manipulating the DC voltage of the sensor output, injecting sinusoidal signals, white noises, and malicious voice signals. Our experimental results suggest that, with relatively low cost and computation overhead, the proposed method not only detects the attack but also can correct corrupted sensor data to help maintain the functioning of systems based on different kinds of sensors in the presence of attacks.

CCS CONCEPTS

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

KEYWORDS

Sensing Security, Countermeasure, EMI, Pressure Sensor, Microphone

ASIA CCS '21, June 7–11, 2021, Virtual Event, Hong Kong.

ACM ISBN 978-1-4503-8287-8/21/06…$15.00
https://doi.org/10.1145/3433210.3453097

ACM Reference Format:
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 (ASIA CCS '21), June 7–11, 2021, Virtual Event, Hong Kong.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3433210.3453097

1 INTRODUCTION

Sensors measure physical properties in the real world and provide feedback to guide automated processes in industrial and robotic applications. For instance, pressure sensors are widely utilized in monitoring and control processes in industrial applications, aircraft systems, critical facilities such as the nuclear power plant, and emerging applications such as the sensorization of humanoids to measure physical properties, including strain, weight, flow rate, air and fluid pressure [12, 15, 21, 43, 47, 49].

Ideally, sensors should only be sensitive to specific physical stimuli in the intended spatial and frequency ranges that it is designed to measure. However, in the real world, analog sensor components often exhibit susceptibility to the influence of signals that are out of the intended sensing channel, frequency band, or measuring range [23]. Adversaries can craft malicious sensor output by exploiting the transduction of such signals in sensor circuits [51]. Since sensors do not distinguish maliciously induced signals from the legitimate signal, the corrupted sensor data would be sent to the control system, resulting in malfunctioning or adversarial control of the system.

This paper presents a case study to reveal the threats of electromagnetic interference (EMI) attacks on pressure sensing and control processes, and proposes a general defense method to enhance the security and reliability of sensing systems in the presence of low-power intentional EMI attacks.

In our case study of pressure sensing security, we deploy inflation pumps to inflate a vehicle tire and observe the effects of EMI attacks on the actuation of the system during this control process. We show that, by manipulating the air pressure measurements, an adversary can intentionally deceive the pump into over/under-inflating the tire, leading to an undesired value of the property (*e.g.*, internal air pressure) that should be controlled by the process[1].

[1]A demo video of the proof-of-concept attack is available at https://youtu.be/WVwn4CspV1M.

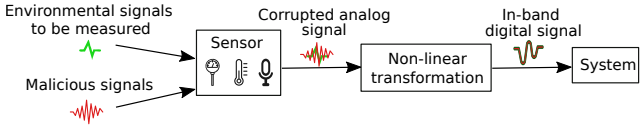


Figure 1: The effect of EMI attacks on sensors. Adversaries can exploit the non-linear analog sensor components to transform high-frequency EMI signals to manipulate the output. The attack effect can vary in different sensor circuits or with different attack parameters.

EMI attacks can be a general threat to different classes of sensing systems. For instance, as voice interfaces gain popularity, microphone circuits have become a target where adversaries can induce malicious audio signals to spoof voice-controllable systems using EMI [20, 27, 33]. Prior works also demonstrated potential security or safety issues related to maliciously inducing actuations of a system by EMI attacks on different kinds of sensors or circuits [33, 37, 46]. The potential integrity issue related to physical-level signal injections with EMI affects the security and usability of systems relying on sensors in the presence of attacks.

We investigate a low-complexity defense approach that can be applied to different kinds of sensors to detect and correct the corrupted sensor data under EMI signal injections. Under the effect of EMI, illegitimate signals can be induced in the analog circuits and imposed on the original signal. By exploiting non-linear effects, an adversary can transform EMI signals to in-band signals to manipulate the sensor output. From the perspective of the system, only the corrupted in-band signals will be observed. Figure 1 illustrates the attack effects of EMI on sensors. Since both the environmental signal source and the malicious signal source are not entirely predictable, it is challenging to detect or correct the corrupted signals. The signals can be transformed differently when the injection occurs in different sensor circuits. Also, to defend against intentional EMI attacks, it is necessary to consider that adversaries are able to use various attack parameters that result in different attack effects.

Sensor redundancy and sensor fusion based approaches could be used for anomaly detection. However, it can be challenging to maintain the functioning of the system if it cannot determine which sensor(s) to trust to make decisions when measurements from multiple sensors indicate conflicts. Multiple sensors can still be subject to the effects of both the legitimate and malicious signals simultaneously (Figure 2 a). Moreover, such approaches often require modeling and testing for specific systems, environments, or applications.

We propose *Transduction Shield* (TS) as a low-complexity defense method against signal injection attacks that exploit the malicious transduction of EMI in analog sensor circuits. The design principle is to enhance the security and usability of the system in the presence of intentional EMI attacks without introducing complex modules or functions to an original low-end sensing system.

Since complete elimination of EMI by shielding or filtering can be difficult and could lead to cost or design challenges for system designers, we do not attempt to eliminate the effects of EMI in our approach. Instead, we propose to integrate an EMI transduction attack-aware circuit to harness the vulnerabilities. In our design, the attack-aware circuit is simply a matched dummy sensor circuit that

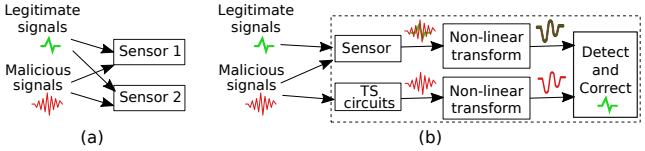


Figure 2: (a) In sensor redundancy based approaches, the multiple sensors can still be subject to the effects of both the legitimate and malicious signals. (b) The Transduction Shield (TS) circuit is a matched dummy sensor circuit with components that are usually no more complex than the original sensor circuit. It shares the same vulnerabilities with the sensor but is not sensing the legitimate signal. The system can detect and correct the corrupted signals leveraging the TS circuit output.

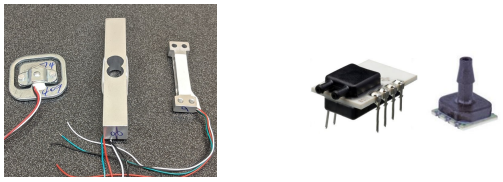
shares the same vulnerabilities as the sensor to be protected. The components of the matched dummy sensor circuit would usually not be more complex than the original sensor circuit.

Ideally, the matched dummy sensor circuit should be exactly the same as the sensor to be protected, but it does not have a sensor transducer in it for sensing purposes. The dummy sensor circuit should only generate an output with a predefined value if there is no EMI signal injection. Due to the similarity of the circuits, the malicious signals will be received and non-linearly transformed in the TS circuit in a similar way as the signals in the sensor circuit. Therefore, we can leverage the output of the TS circuit to detect the attack and correct the corrupted sensor data (Figure 2).

We study the defense approach on different kinds of sensors. We analyze and evaluate our defense method with EMI injection experiments on load cell pressure sensors and microphones using various attack parameters. We assume that the malicious EMI signal source is not completely predictable in intentional EMI attacks. Therefore, we use different EMI frequencies, transmitting power, and modulations to evaluate the performance of our method.

The proposed method not only detects the attack but also can correct corrupted sensor data. The defense method achieves a relatively high error reduction rate in intentional EMI attack scenarios that adversaries attempt to manipulate the DC voltage level of the sensor output or inject sine wave and white noise signals to the sensor data. Additionally, when malicious voice signals are injected to dominate the sensor output, our method can mitigate the malicious signal to a much lower level. Thus, the voice recognition system could correctly identify the legitimate voice command from the microphone signals. Our experimental results show that the proposed method can be applied to different sensors to improve the security and reliability of the system in the presence of EMI signal injection attacks.

Defense methods related to capturing the physical-level EMI signals or using a reference value were also explored in prior studies [33, 46, 54]. The methods proposed in prior studies improve the security of sensor systems and can be used for effective EMI attack detection. However, existing approaches often need to introduce components or functionalities (*e.g.*, RF processing) that can be relatively complex compared to a low-end sensor system. In comparison, our defense method leverages a simple matched dummy sensor design with components that are usually no more complex than an original sensor circuit. Thus, our method is different from



(a) (b)

Figure 3: (a) Load cell sensors that measure forces and weights. More examples in different applications can be accessed at online resources [8, 9]. (b) Examples of pressure sensors integrated with IC. They can measure air/fluid pressure and flow rate in applications such as combustion airflow control and medical devices [4, 5].

the mitigation method that utilized RF monitoring and processing modules to determine the EMI contamination level [33]. Furthermore, the goal of our study is not only the detection but also the correction of corrupted sensor data in the presence of EMI signal injections, which is different from existing studies that primarily focused on the detection of attacks [46, 54].

We list the main contributions of this paper as follows:

- We investigate EMI attacks on inflation pumps and show how a control system can misapply actuations in an automated process guided by spoofed air pressure measurements. Consequently, the process variable (*e.g.*, internal air pressure) being controlled can be subject to manipulation.
- We propose a low-complexity defense method to ensure the security and reliability of sensor-based systems in the presence of intentional low-power EMI attacks. The defense method can detect and correct the corrupted sensor data to help maintain the functioning of sensor-based systems.
- We analyze and evaluate the defense method with attack experiments using various attack parameters on different kinds of sensors. Our experimental results show that the proposed method can effectively detect and correct the attack effects to help maintain the functioning of sensor-based systems under EMI signal injection attacks.

2 BACKGROUND

2.1 Sensors and Applications

Sensors are used to measure the physical properties related to a specific environment. Monitoring and control systems often rely on the feedback of sensors to determine the status of the environment and make decisions. For example, sensors such as pressure sensors and temperature sensors are key components in industry process control systems [32], medical devices [3], aircraft systems [49, 50], and critical facilities such as nuclear power plants [25]. Rapidly emerging applications such as the sensorization of robots [42], telepresence control and robotic surgery [29, 31] also employ abundant sensors.

Pressure sensing. Generally, the principle of pressure sensing is to convert the force applied to an object or a sensing element of constant area (such as a diaphragm) into an analog electrical signal.

There are various designs of pressure sensors. To simplify the discussion, we will focus on two common types of them (Figure 3): *1) Force measuring sensors based on strain gauges.* The force causes a distortion of the material. The resistance changes as the sensing element extends or contracts. Based on the application, the design and size of the sensing element can vary. There are larger ones, such as load cells used in machines and platforms to pressure and weight. There are also load cells that come with smaller sizes, such as those used in scales. The sensing element can also be used in the form of thin films, which allow them to be fitted into various applications. The physical property to be measured is the force. The unit of the measured property is usually represented in Newton (N), kg, or lbs. *2) Air or fluid pressure measuring and flow rate measuring sensors.* The sensing elements are usually very small and can be built into IC sensor chips used in various application scenarios [10, 18, 26]. The pressure sensor has a thin membrane covering a reference cavity, which is typically sealed at a low vacuum pressure [7, 11]. When there is a change in the external pressure, the membrane will stretch or deform, and an electric signal would be induced in the sensor circuit correspondingly. The measurement that depicts air or fluid pressure is usually in units of Pascal (Pa) and pound-force per square inch (psi).

Microphones and voice controllable systems. Recently, voice interfaces have gained popularity in smart devices, representing a trend utilizing sensors to improve the usability of human-computer interfaces. With voice-controllable systems, a digital system can be controlled with commands from a microphone that receives acoustic signals in the real world. For instance, the voice interface can be utilized to make phone calls, perform transactions in online shopping and banking, or control smart home devices. There is also a growing interest in using voice interfaces to control vehicles' functions, manipulate surgical robots [55], and give orders to robotic systems in military applications [2].

2.2 Intentional EMI on Sensing Components

While the increasing usage of sensors greatly improves the usability of various applications, the trustworthiness of sensing interfaces remains to be a concern [22]. With intentional EMI, adversaries could affect analog circuits to gain adversarial control over sensing and control systems.

Depending on the application, the sensor circuit, and parameters of EMI attack signals, there can be different kinds of induced attack effects [23, 51]. From the perspective of adversaries, we will mainly discuss two common kinds of attack effects with a low-power attack setting: 1) amplitude-modulated attacks to inject specific waveform signals by demodulating out-of-band EMI signals with the generation of intermodulation and harmonics. For instance, adversaries could inject noise, intelligible speech, and malicious voice commands to a voice interface [20, 27, 33]. By modulating the adversarial audio signal with a high-frequency carrier to which the sensor circuit responds (*e.g.*, resonant frequency), the attack usually requires a relatively low transmission power. 2) EMI attacks to change the value of the measured property by manipulating an injected DC voltage offset. For instance, adversaries can leverage the unintended rectification effect of operational and instrumentation amplifiers to control the measurements of different kinds of sensors such as thermocouples, thermistors, and resistance temperature detectors (RTDs) [46].

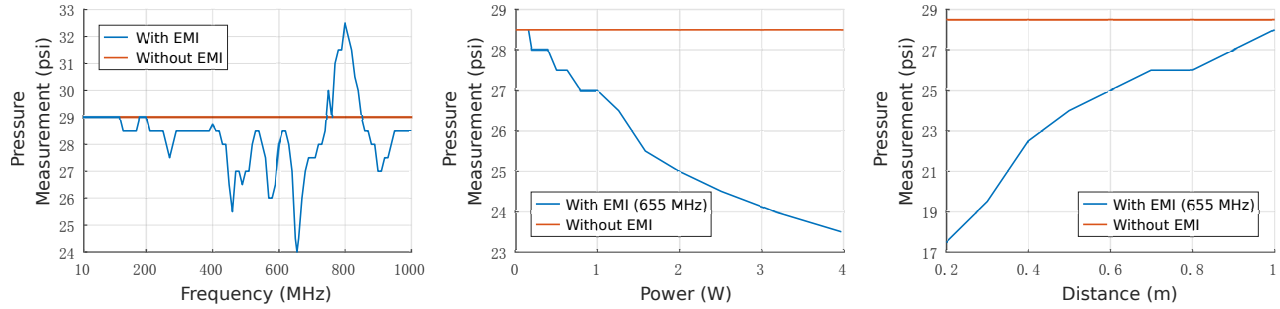


Figure 4: Left: The attack effect with different frequencies of EMI on inflation pump #1 at an attack distance of 0.5 m and a transmitting power of 4 W. Middle: The attack effect with varying transmitting power at an attack distance of 0.4 m. Right: The effect of the EMI attack in at different distances with a frequency of 655 MHz and a 4-W transmitting power. In the experiments, there could be a measurement error within ±0.5 psi.

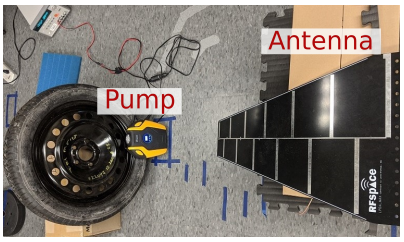


Figure 5: An illustration of the setting of EMI attack experiments on the tire inflation pump.

The above attack effects can be induced in different classes of sensors [28, 30] with similarly vulnerable components. To defend against EMI attacks leveraging these effects, we will analyze and evaluate our defense method with EMI attack experiments in several different attack scenarios in Section 5.

3 CASE STUDY ON PRESSURE SENSING AND CONTROL PROCESS

To identify the threats related to intentional EMI attacks on pressure sensors, we conduct a case study on digital inflation pumps that utilize the pressure sensor feedback in a control process. Digital inflation pumps measure the internal air pressure of the tire during the inflation. In this process, the air compressor of the system keeps pumping air into the connected tire until the setpoint is reached.

In our case study, we first investigate the effect of intentional EMI attacks on the pressure sensor measurements of inflation pumps. Then we deploy them to inflate a vehicle tire and observe the attack effects on the actuation of the system in this control process.

3.1 Experiment Setup

Figure 5 illustrates the experimental setting. We use a directional antenna [1] to emit EMI signals. The maximum transmitting power we use is 36 dBm (4 W). The signal source is an Agilent N5172B vector signal generator. The signal is amplified with a Mini Circuits ZHL-4240 amplifier. We test two pumps with different models: pump #1: Breezz SG-J3012 portable auto tire pump, and pump #2: JOYROOM CZK-3631 portable tire pump. The pump is connected to a vehicle tire during the experiments.

3.2 Attack and Process Manipulation

We sweep the EMI attacking frequency from 10 MHz to 1 GHz with an interval of 10 MHz and observe the air pressure measurement of the pump #1. We then adjust the frequency with a step such as 5 MHz or 1 MHz to find the optimal attack frequency. As shown in Figure 4 (left), signals with frequencies close to the peaks at around 655 Mhz and 800 MHz can be employed to decrease and increase the tire pressure measurement, respectively. We also test the attack effect at different attack distances (Figure 4, right). At a distance of 0.2 m, the adversary can decrease the pressure measurement from 28.5 psi to 17.5 psi. The attack effect attenuates as the distance increases.

Next, we use an attack frequency of 655 MHz and observe the attack effect with different power. As shown in Figure 4 (middle), by adjusting the transmitting power, adversaries can manipulate the induced offset to control the pressure measurement.

In the tire inflation process, the inflation pump monitors the air pressure of the tire and keeps pumping air into the tire until the setpoint is reached. Therefore, by increasing the pressure measurement with EMI, the actual tire pressure at the end of the process would be lower than the setpoint, resulting in underinflated tires. Similarly, by intentionally decreasing the pressure with EMI, the air compressor would pump more air into the tire than necessary, leading to overinflation.

In our experiments, we notice that it may not be easy to manipulate the pump to reach a specific value accurately. However, it is still possible to gain targeted adversarial control over this process. The adversary can manipulate the process to intentionally over/under-inflate the tire, causing an undesired actual tire pressure that should be controlled by the process. For instance, we try to inflate the vehicle tire from a low tire air pressure to 29.5 psi. However, by EMI signal injections (655 MHz) that maliciously decrease the pressure measurement, the adversary can trick the control system into overinflating the tire, leading to an actual tire pressure of 36 psi by the end of the process (at a 0.3-m attack distance). Similarly, under EMI attacks (800 MHz) to maliciously increase the pressure measurement to cause underinflation, the actual tire pressure only reaches 25 psi at the end of the process.

We also test the attack effect on pump #2. The experimental results on pump #2 are in the Appendix.

4 THREAT MODEL

We discuss the threat model from a perspective to defend against low-to-medium power intentional EMI attacks on sensing systems. An adversary's objective could range from sensor data corruption, denial-of-service (DoS) attacks, to achieving adversarial control of the target sensor-based control system.

We assume that adversaries cannot tamper with the victim system. They cannot directly alter any hardware or software component of the target system. The adversary cannot manipulate the setpoint of the system. Moreover, the adversary cannot directly modify the actual physical property.

The adversary could use directional antennas to launch the attack from a certain distance (*e.g.*, several meters) away. We assume that adversaries can emit low or medium power EMI, which is typically in several Watts. Adversaries might use a higher transmitting power to launch the attack from a further distance, but we do not consider near-field high-power EMI attacks.

The adversary could use portable EMI emitting devices. For instance, the operating frequency of handheld transceivers (*e.g.*, walkie-talkies) can cover certain frequency ranges in VHF (Very High Frequency) and UHF (Ultra High Frequency) channels, which could overlap with vulnerable frequencies of many of the devices. An adversary might leverage such devices to conduct a portable, low-cost attack. Alternatively, adversaries could use off-the-shelf software-defined radio (SDR) devices (*e.g.*, HackRF One [6]), an amplifier, and a battery to make a portable attack device that can be easily carried with a backpack.

It may also be possible for the adversary to leverage a remote-controlled EMI emitter. The adversary could attach the attack device to places that are close to the victim device. Since EMI attacks do not require line-of-sight transmission, adversaries might put the device in inconspicuous places that are not directly visible to users. For instance, the adversary could hide it behind/under/inside a wall/table/box or other objects.

In scenarios of intentional EMI attacks, adversaries can try to use different frequencies, modulation methods to affect the target system. Therefore, we assume that the behavior or frequency of the EMI source is unknown to the victim system, and the defense method will be designed and tested accordingly. The proposed defense method is designed to protect different kinds of sensors instead of one specific device.

Since the adversaries' objective is to corrupt or intentionally manipulate the sensor data to affect the system, we assume that the EMI signals would not be strong enough to crash the system or damage the components. The voltage level of signals in the circuits could be affected by EMI but is usually inside the operating or tolerable range of the components.

5 DEFENSE

In this section, we explain the design of the Transduction Shield method to defend against intentional EMI injection attacks on sensors. We analyze and evaluate our method on two sensors, including load cell pressure sensors and microphones. We implement the experimental Transduction Shield (TS) circuit on pressure sensors and microphones using simple common components in low-end sensing systems.

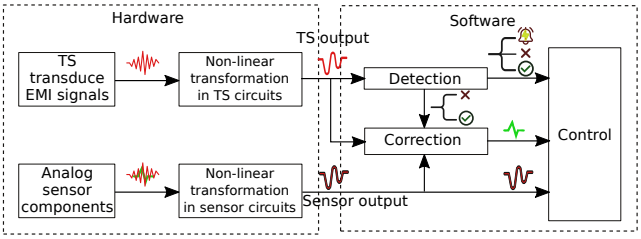


Figure 6: An illustration of basic modules with the Transduction Shield method. Based on the TS output, the detection module detects the attack. It sends the detection results to the correction module. If an attack is detected, the correction module will correct the corrupted sensor output leveraging the TS output. The control system can still function with the corrected sensor data.

We then inject EMI signals to manipulate the sensor measurements. In intentional EMI attacks, the malicious EMI signal is not entirely predictable. Therefore, we try different attack parameters and modulated signals to evaluate the performance of our method. We investigate several attack scenarios when adversaries attempt to manipulate the DC voltage level of the sensor output, inject sine wave, white noise, or malicious voice commands to the microphone data.

Our experimental results show that the proposed method can detect the attack with high accuracy. Moreover, it can correct corrupted sensor data with a relatively high error reduction rate, improving the reliability and usability of sensor-based systems under EMI attacks.

5.1 Overview

The basic principles to design and implement our defense method are: 1) the TS circuit shares the same vulnerabilities as the sensor circuit, and 2) the TS circuit is not sensitive to the legitimate signal that the sensor is intended to measure. Using the same circuit components and the same topology, sharing power lines, we can make the TS circuit have similar responses to EMI to meet the first design principle. By modifying an off-the-shelf sensor component or using non-sensor components (*e.g.*, resistors), we can make the TS circuit insensitive to the legitimate signal that the sensor is intended to measure.

The purpose of the design is to distinguish the effects of EMI injections to protect different kinds of sensors. The malicious signals will be induced and transformed in the TS circuit in a similar way as in the sensor circuit. The output of the TS circuit can be leveraged to detect the attack and correct the corrupted sensor data with light-weight computations based on in-band signals.

As illustrated in Figure 6, based on the TS output, the detection module detects the attack and sends the detection result to the correction module. If an attack is detected, the correction module will correct the corrupted sensor data leveraging the in-band TS output. The correction module can be implemented in the software layer using simple, light-weight computations to correct the sensor data corruption in real-time. The correction module can also be implemented in the hardware layer with a differential amplifier circuit.

The control system can make more appropriate decisions based on the detection and correction results in the presence of attacks. When necessary, the control system could still keep functioning by using the corrected sensor measurements. However, the detection module will send an alarm signal to the system if it detects severe data corruptions in cases such as when strong EMI signals saturate the circuit elements.

In practice, it is not trivial to eliminate the susceptibilities of analog sensor circuits to EMI in many scenarios. Therefore, our focus in this study is not preventing EMI injection. Instead, we propose a defense method to harness the vulnerabilities to help maintain the functioning of the system in the presence of EMI attacks. Also, the functionality of low-end sensor systems is usually designed to be simple. Our method keeps the design and functionality of sensors simple and enhances the security of sensors in the presence of EMI.

5.2 TS Circuit Design

First, we explain the design of the hardware part of the defense method.

TS circuit. The TS circuit is based on a matched dummy sensor design. Ideally, the dummy sensor circuit should be exactly the same as the sensor to be protected, but it does not have a sensor transducer for sensing purposes. The dummy sensor circuit should only generate an output with a default value (such as zero) if there is no EMI signal injection.

Due to the similarity of the circuits, the malicious signals will be received and non-linearly transformed in the TS circuit in a similar way as the signals in the sensor circuit (Figure 2).

Therefore, the output of the TS circuit can be leveraged to detect the attack and correct the corrupted sensor data.

We make a few design considerations based on observations on how sensor circuits are affected by EMI. The purpose of fulfilling these requirements is to make both the spatial features and electrical properties of the TS circuit highly similar to the sensor circuit. In this way, the TS circuit would share the same vulnerabilities to EMI injections as the sensor to be protected. We list the design considerations as follows:

(1) We implement the TS circuit in the same topology as the sensor circuit.
(2) The TS circuit is in close proximity to the sensor circuit. Optimally, the closest proximity can be achieved in manufacturing.
(3) The TS circuit shares the same power and ground lines with the sensor circuit. It is preferred to make their connections to power and ground lines to be as close as possible.
(4) In the TS circuit, we use the same or similar components (the same length of wires, the same type of amplifiers, etc.) as in the sensor circuit.
(5) We make the TS circuit insensitive to the environmental signal that the sensor is intended to measure. This can be achieved by modifying an off-the-shelf sensor transducer or using non-sensor components (*e.g.*, resistors) to replace the transducer of the matched dummy sensor circuit. We will explain how to meet this requirement in the TS transducer configuration in the following.

TS Transducer Configuration. In the TS circuit, we refer to the counterpart to the sensor transducer as the TS transducer. We note that this term is selected to simplify the discussion. The TS transducer does not work as a real sensor transducer commonly used for sensing purposes. The TS transducer can be a non-sensor component (*e.g.*, resistor) and would not transduce legitimate signals that the sensor is intended to measure.

In practice, there are several ways to make the TS circuit insensitive to the legitimate signals so that it should only generate an output close to a default value (such as zero) if there is no EMI signal injection:

(1) Configuring or positioning the TS transducer so that it would not be subject to the effect of the legitimate signal. For instance, the load cell in the TS circuit can be positioned so that it will not be subject to force.
(2) Modifying the TS transducer so that it does not respond to the legitimate signal (*e.g.*, applying glue on a MEMS microphone to block acoustic signals).
(3) Using non-sensor components with matching electrical properties (*e.g.*, resistance and capacitance). For instance, to protect resistive sensors like thermistors, RTDs, and strain gauges, resistors can be used as the TS transducer. To protect thermocouples, we could construct the TS transducer by a conducting wire with the same length as the thermocouple. To protect microphones, we will use a resistor and a capacitor as the TS transducer.

In our proof-of-concept experiments, we build the circuit manually using off-the-shelf components and apply simple modifications to configure the TS transducer. In practice, the manufacturer can integrate the sensor and the TS circuit into one package to reduce mismatch. Also, the TS transducer can be easily replaced with elements (*e.g.*, resistors) that have matching resistance and capacitance during manufacturing.

5.3 Detection and Correction

Next, we explain the software modules of the defense method to detect and correct the corrupted sensor data leveraging the TS circuit output.

The adversary tries to inject malicious signals into the sensor data by intentional EMI signal injection attacks without directly modifying the actual physical phenomenon being sensed. We assume that the emitted EMI signal is $e(t)$. After being received by the victim circuit and non-linearly transformed, it would become $m(t)$, which is the malicious signal that the adversary injects into the sensor data. This non-linear transformation could be incurred by different effects, such as the demodulation of high-frequency waveform signals or the generation of a DC voltage offset.

We assume that $s(t)$ represents the original sensor data when there is no EMI signal injection. Under the injection, the sensor data is $s'(t)$, and we have $s'(t) = s(t) + m(t)$.

The output of the TS circuit is denoted as $d(t)$, which should be close or equal to a default value b if there is no EMI signal injection. When adversaries inject EMI signals to the sensor, the TS circuit would also capture and transform the EMI signals. Therefore, the TS output $d(t)$ can be utilized to detect the attack. Since we use a matched dummy sensor design, the EMI signals would be induced

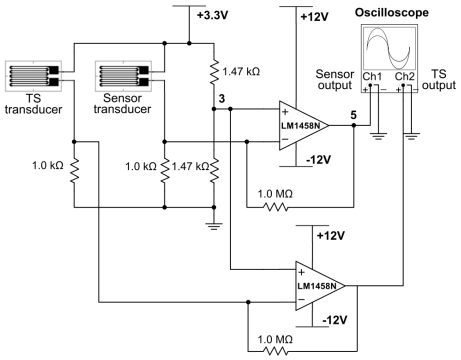


Figure 7: The diagram of the experimental circuit we build to evaluate our defense against EMI signal injections on load cell pressure sensors. The TS circuit has the same topology as the sensor circuit.

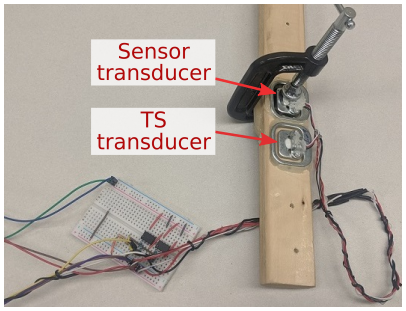


Figure 8: The experimental circuitry of Transduction Shield to defend a load cell pressure sensor against EMI signal injection. In the experiment, we use two sensors: one for real pressure measurement (sensor transducer); one is used in the matched dummy sensor for attack detection and correction (TS transducer). Manufacturers can integrate a real sensor and a paired dummy sensor into one package.

and non-linearly similarly transformed in the TS circuit as the sensor circuit. Ideally, we would have $d(t) - b \approx m(t)$. Therefore, the corrupted sensor signal $s'(t)$ can be corrected by subtracting the TS output $d(t)$.

Detection Module. The detection module detects EMI signal injections by analyzing the TS output. The detection module will send detection results to the correction module and to the system.

Since the TS circuit is not sensitive to legitimate signals being sensed, when there is no EMI signal injection, the TS output $d(t)$ should always be a predefined constant value such as zero. If we consider a small amount of benign circuit noise, $d(t)$ could be slightly fluctuating around the default value. If an adversary is trying to manipulate the sensor output via EMI injection, the TS circuit will capture and transform the malicious signals. Thus, the induced changes in the TS output signal can indicate the presence of an attack.

To detect attacks that induce a DC voltage offset (such as EMI attacks on temperature and pressure sensors), we can compare the value of $|d(t) - b|$ (the absolute value of the TS output deviation from the default value) with a threshold H. The threshold H can be set based on the level of benign circuit noises. We can consider that with benign circuit noises, the TS output $d(t)$ would fluctuate around the default value b within a range of $[-h, h]$. With the benign circuit noise, we have $|d(t) - b| \leq h$. The value of h can be set based on the measured noise range or an estimated small value (such as 50 mV) to bound the range of common circuit noise. The threshold H can be set based on h and a sensitivity adjusting parameter a ($a \geq 1$). We have $H = a \cdot h$. When $|d(t) - b| > H$, the EMI signal injection attack is detected at time t.

The module can be adjusted and configured based on the sensor application. To detect attacks that inject waveform signals (such as EMI attacks on microphone circuits to inject audio signals), we can compare the root-mean-square (RMS) deviations of the TS output with the threshold H. The RMS deviations of the TS output in a window of n samples would be

$$TS_{RMS}(t) = \sqrt{\frac{\sum_{i=0}^{n-1}\left(d(t - \frac{i}{F_S}) - b\right)^2}{n}}$$

F_S is the sample rate of the sensor. We consider that with benign circuit noises, the RMS deviation would fluctuate within a range of $[0, h]$. With the benign circuit noise, we have $TS_{RMS}(t) \leq h$. h can be set to an estimated small value or a value based on the measured noise range. The H can be set based on h and a sensitivity parameter a ($a \geq 1$). We have $H = a \cdot h$. When $TS_{RMS}(t) > H$, the EMI signal injection attack is detected at time t.

In cases that severe data corruptions are detected, an alarm signal would be sent to the system. For instance, when the TS output reaches the maximum range of the circuit, it is likely that the circuit components might have been saturated by strong EMI signals. For instance, in pressure sensors, we can compare the TS output deviation $|d(t) - b|$ with a threshold H_a that has a value close to the maximum output of the circuit. If $|d(t) - b| > H_a$ holds for several sample points in a time window (such as 1 second), a severe sensor data corruption would be detected and the module would send an alarm signal to the system. In such cases, the correction module could still mitigate the attack to a certain extent, but it can be difficult to maintain the correct functioning of the system.

Correction Module. When an attack is detected, the correction module can correct the corrupted sensor data, which helps maintain the functioning of the system.

The correction module receives the corrupted sensor output $s'(t)$ and the TS output $d(t)$. With a matched dummy sensor design, the TS output $d(t)$ would be highly similar to the malicious signal $m(t)$ injected into the sensor. This allows us to use light-weight computations based on in-band signals to mitigate the injected errors with low computation overhead. We can use a linear model to correct the sensor data with low complexity. The corrected sensor data would be

$$c(t) = s'(t) - p \cdot (d(t) - b) = s(t) + m(t) - p \cdot (d(t) - b)$$

p is a parameter that could be adjusted to compensate for mismatching between the TS circuit and the sensor circuit. By default, we have $p = 1$. Therefore, we would have $c(t) = s(t) + m(t) - (d(t) - b)$. Assume the TS circuit and sensor circuit are designed and fabricated to be identical; ideally, we would have $m(t) \approx d(t) - b$. Thus, we would also have $c(t) \approx s(t)$, indicating that the corrected sensor

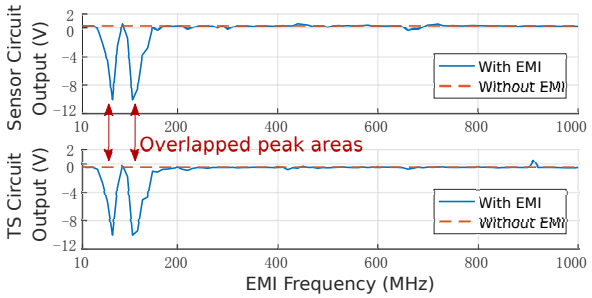


Figure 9: The outputs of the load cell pressure sensor circuit and the TS circuit under EMI attacks with different frequencies. The transmitting power is 10 dBm (10.00 mW).

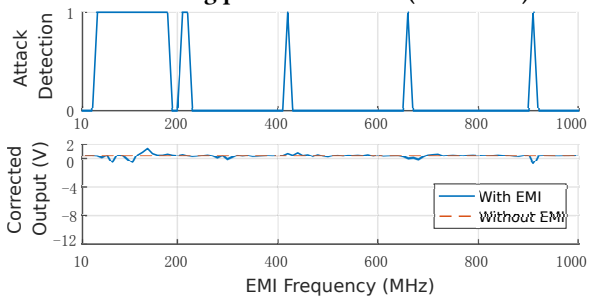


Figure 10: The detection and correction of EMI attacks with different frequencies. The detection module can successfully detect the most vulnerable frequencies around the peak areas (*e.g.*, $[50, 80]$ and $[100, 140]$ MHz). The correction module can mitigate the injected errors of the corrupted sensor data to a much lower level.

data $c(t)$ would be close to the original sensor data if EMI signal injections do not corrupt them.

In practice, the correction module corrects the sensor data with a certain error reduction rate, but would usually not eliminate errors. In another word, without the Transduction Shield, the injected error is $e_1(t) = s'(t) - s(t) = m(t)$. With the Transduction Shield, the error would be mitigated to $e_2(t) = c(t) - s(t) = m(t) - (d(t) - b)$.

5.4 Defense of Pressure Sensor

Circuit. First, we implement the prototype circuit. Figure 7 shows the circuit diagram. The load cell pressure sensor is based on strain gauges, and we connect it to a Wheatstone bridge circuit. The pressure applied to the sensor transducer would change its resistance, causing a voltage difference that would be amplified by the LM 1458 amplifier. By detecting the voltage change, the force applied to the sensor transducer can be measured.

As shown in Figure 7, the TS circuit has the same topology and shares the same power and ground lines with the sensor. Figure 8 shows the physical circuit we implement. We use similar components (similar lengths of wires, the same type of amplifier) in the TS circuit so that it has similar properties as the sensor circuit. As shown in Figure 8, one of the load cells is for real pressure measurement. This one is the sensor that we try to protect. Another one is deployed in the TS circuit for attack detection and correction.

We make this prototype circuit with off-the-shelf components, jumper wires, and a breadboard. We manually twist and bind the wires of the two circuits together to reduce mismatch. The circuits

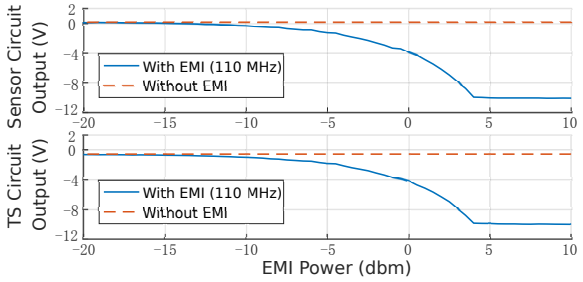


Figure 11: The outputs of the load cell pressure sensor circuit and the TS circuit under EMI attacks with different transmitting power at a fixed frequency of 110 MHz.

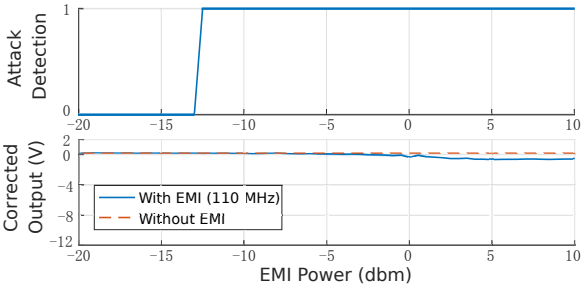


Figure 12: The detection and correction of EMI attacks on the pressure sensor with different transmitting power.

on the breadboard are quite similar, although they are not exactly symmetrical. We use this circuit for proof-of-concept purposes. In practice, manufacturers can integrate a real sensor and a matched dummy sensor into one package, and the circuits can be fabricated with high accuracy to reduce mismatch.

Defense. In our experiments, we inject a DC voltage offset into the sensor data by emitting EMI signals at a fixed frequency using a dipole antenna at a 1-meter attack distance. We test the effect of EMI signals with different frequencies and power to manipulate the sensor measurement and evaluate the defense against the intentional EMI attack.

We sweep the frequency range from 10 to 1000 MHz with a step of 10 MHz. Compared to the sensor output, the TS output shows a very similar response under EMI with different frequencies. As shown in Figure 9, the peak areas corresponding to EMI frequencies that cause the most significant DC voltage offsets are highly overlapped in the TS and sensor circuit outputs.

The default value of the TS output is $b = -449$ mV. The range of the circuit noise is about 30 mV in both directions. We can set $h = 50$ mV. We set the sensitivity parameter $a = 5$. Therefore, we would have $H = 250$ mV. When $|d(t) - b| > H$, we can identify that there is an attack at time t. As shown in Figure 10, attacks with the most vulnerable frequencies around the peak areas (at the ranges of $[50, 80]$ and $[100, 140]$ MHz) are successfully detected.

The detection module also detects several other higher frequencies with less significant attack effects (*e.g.*, 420, 660, and 910 MHz). However, due to the mismatch between the sensor circuit and TS circuit in our prototype implementation, the detected frequency positions of the less significant attack frequencies may not be very accurate.

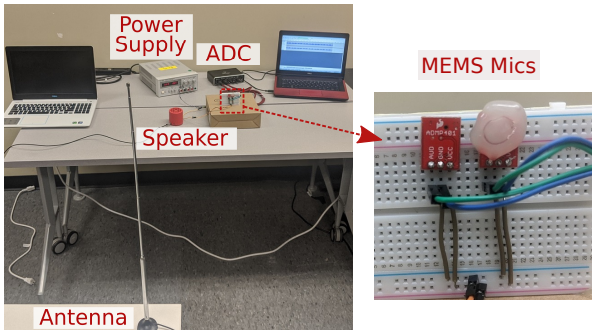


Figure 13: The experiment setup to evaluate the defense method on a microphone against EMI signal injections. In the experiment, we use two MEMS microphones: one for real sound measuring (sensor transducer); one is glued and placed in the matched dummy sensor circuit for attack detection and correction (TS transducer).

The correction method we use is linear subtraction. We compute the corrected data based on $c(t) = s'(t) - [d(t) - b]$. As shown in Figure 10, the errors in the corrected output are much lower compared to the sensor circuit output. The absolute value of the maximum injected error is mitigated from $|e_1|_{max} = 10.39$ V to $|e_2|_{max} = 1.07$ V. The error reduction rate is 89.7%. If we compare the average error in the frequency range $[50, 140]MHz$ covering the peak areas, the average error is mitigated from: $|e_1|_{mean} = 4.88$ V to $|e_2|_{mean} = 0.50$ V. The error reduction rate is 88.7%.

Next, we evaluate our method using different transmitting power at a fixed frequency of 110 MHz (Figure 11). As illustrated in Figure 12, the detection module can successfully detect the attack that can induce a deviation in the TS circuit that is larger than H (250 mV). The correction module can mitigate the maximum error from $|e_1|_{max} = 10.2$ V to $|e_2|_{max} = 0.84$ V. The error reduction rate in this case is 91.8%.

5.5 Defense of Microphones

As shown in Figure 13, we use two SparkFun ADMP 401 MEMS microphone breakout boards in our experiments. We plug them into a breadboard, and the two microphone boards share the same power (3.3 V) and ground lines. We use an Agilent E3630A power supply to provide the power to microphones.

The outputs of both the sensor circuit and the TS circuit are digitized by a Behringer umc202hd 2-channel audio ADC and recorded by a laptop using a sample rate of 48 kHz. In our experiments, we use a simple method (applying glue to the TS transducer) to block acoustic signals.

We analyze and evaluate the defense of EMI signal injection attacks with different waveforms, including sine waves, white noises, and malicious voice signals. All these scenarios would compromise the sensor data integrity because adversaries manipulate the sensor measurements without changing the actual physical property being sensed. We use a dipole antenna to emit amplitude-modulated EMI signals at an attack distance of 1 meter with a transmitting power of 1 mW, and the carrier frequency is 70 MHz.

We measure the maximum value of the RMS deviation of the TS output TS_{RMS} without EMI signal injection for 10 seconds. The

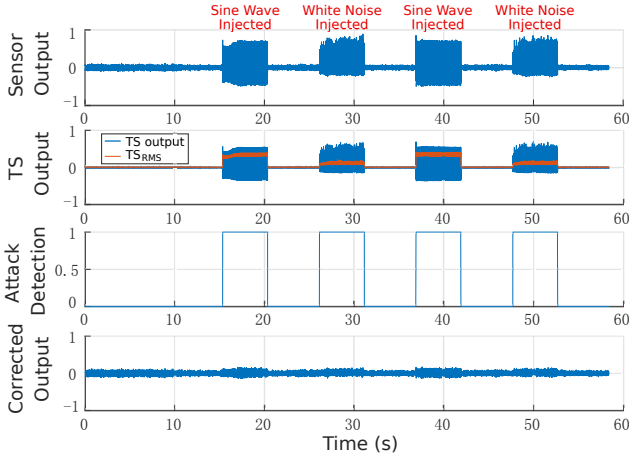


Figure 14: The outputs of the microphone sensor and TS circuit under EMI signal injection attacks. We inject sine wave signals and white noises alternatively. Each injection session lasts 5 seconds and there is a 5-second interval between two sessions. With our method, the injected signals can be detected and mitigated to a much lower level.

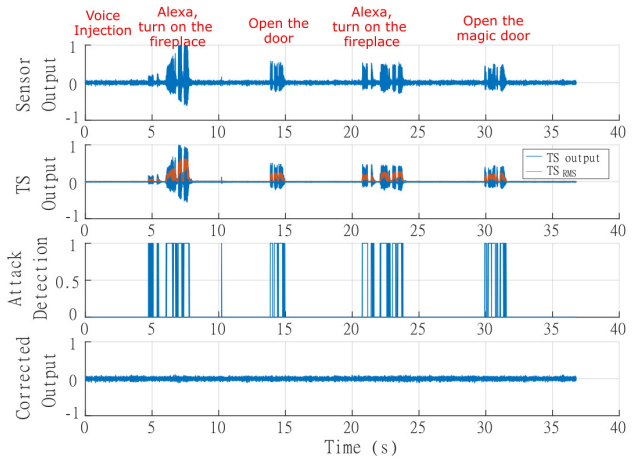


Figure 15: The outputs of the microphone sensor and TS circuit under EMI attacks to inject voice signals. We inject one sentence of voice signals in 5-second sessions, and there is a 5-second interval between two sessions. With our method, the injected signals can be detected and mitigated to a much lower level.

maximum value of TS_{RMS} in 10 seconds is 0.0191. Therefore, we can set $h = 0.02$ to bound this value and set sensitivity adjusting parameter as $a = 2$. Therefore, we would have the detection threshold $H = 0.04$. When $TS_{RMS}(t) > H$, an attack would be detected at time t. TS_{RMS} is calculated with a window of $n = 100$ samples. The default value of the TS circuit is $b = 0$.

Attack Detection and Mitigation. We inject sine wave signals (600 Hz) and white noise alternatively using intentional amplitude-modulated EMI. As shown in Figure 14, while there is no such sound in the real world, the corrupted sensor data shows strong noise signals we inject. The TS output also shows the malicious

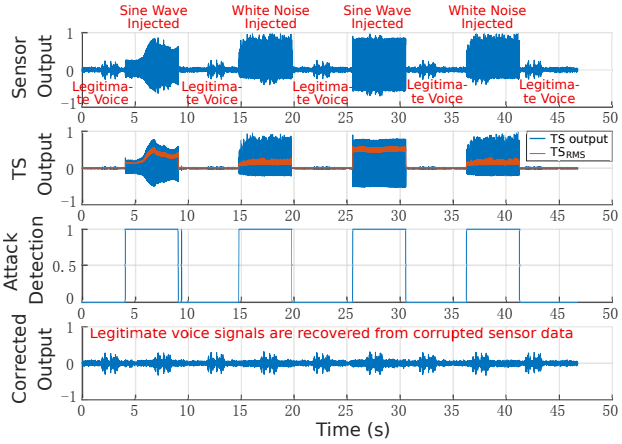


Figure 16: The outputs of the microphone sensor and TS circuit under EMI signal injection attacks. A speaker is playing "Hey Google, what time is it" every 5 seconds as the legitimate signals. We inject sine wave signals and white noises alternatively. Each injection session lasts 5 seconds, and there is a 5-s interval between two sessions.

injected signals. By comparing TS_{RMS} with the threshold H, the detection module can precisely detect all the attack sessions.

Moreover, the correction module can mitigate the injected noises to a much lower value (Figure 14). We use linear subtraction and compute the corrected data based on $c(t) = s'(t) - p \cdot (d(t) - b)$. Due to the mismatch between the sensor and TS circuits, we set $p = 1.1$. The default value of the TS circuit is $b = 0$. The RMS value of the sine wave injection session (from 15.3 s to 20.3 s) is mitigated from 0.424 to 0.055. The RMS of the white noise injection session is mitigated from 0.128 to 0.029.

As shown in Figure 15, we also inject voice signals into the microphone, and the attack can be successfully detected. The correction module can mitigate the injected voice information. For instance, the RMS of the voice injection session from about 14 s to about 15 s is mitigated from 0.140 in the sensor data to 0.027 in the corrected data.

Attack Detection and Mitigation with Active Environmental Sound. Next, we evaluate our method in scenarios with active environmental sound. We use a speaker to play "Hey Google, what time is it" every 5 seconds as the source of legitimate signals.

We inject sine wave signals and white noises alternatively using intentional amplitude-modulated EMI. As shown in Figure 16, under the signal injection, the legitimate signals are completely buried by the injected strong noise. Using the same parameters as experiments without the active environmental sound, the detection module can detect all the attack sessions. Moreover, the correction module can significantly mitigate the injected noise. We can clearly observe the pattern of the legitimate signals in the corrected sensor data.

We then inject malicious voice signals, including "Hey Google, turn on the fireplace" and "open the door" alternatively. After the injection, the sensor output is dominated by the injected strong signals. As shown in Figure 17, the injected signals are effectively detected and mitigated to a much lower level. After correction, the pattern of the legitimate signals can be clearly observed in the corrected sensor data.

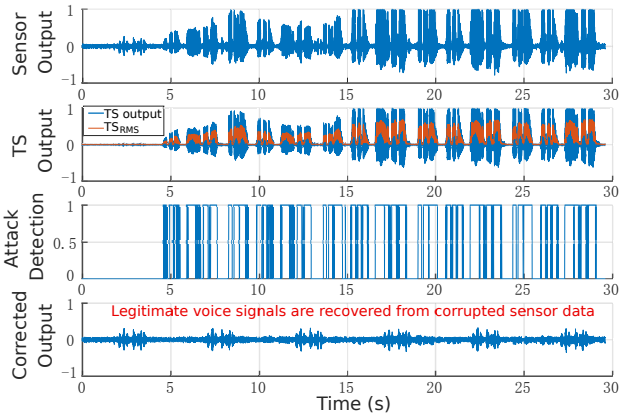


Figure 17: The outputs of the microphone sensor and TS circuit under EMI signal injection attacks. A speaker is playing "Hey Google, what time is it" every 5 seconds as the legitimate signals. The adversary injects malicious voice signals to dominate the sensor data. After correction, the originally masked legitimate signals can be recovered.

We play the corrupted audio to the Google Assistant voice recognition system on an Android smartphone, and the system could not recognize the legitimate commands. We then play the corrected data to the voice recognition system, and the legitimate signals can be correctly recognized. More details of the experiments are in Appendix B (Figure 22 and Figure 23).

6 DISCUSSION

6.1 Cost and Complexity

The hardware components we use are common in sensors. In practice, the TS transducer can also be replaced with simple components such as resistors. Due to the similarity between the TS circuit and the original sensor circuit, the matched dummy sensor can share a large part of the circuit with the original sensor. The added hardware components are also very cheap in terms of price. Therefore, the proposed method can enhance the reliability of sensing systems subject to EMI signal injection attacks with minimum cost and redundancy.

The detection and correction methods can be implemented in real time with lightweight computations. The methods can be implemented in hardware or software. For instance, the correction method can be realized with a differential amplifier circuit. If the correction is delayed to the digital domain, the processing can be done in real time due to straightforward logic. Since our method will not require adding relatively complex modules or functionalities, it is suitable for resource-constrained devices. Our method helps to keep the functionality of sensing systems simple, secure and reliable.

6.2 Limitations and Future Work

In our experiments, we notice that although a large part of the injected errors can be mitigated, they are not completely removed. This might be due to mismatches between the sensor and TS circuits. In the future, the TS circuit can be fabricated and integrated during manufacturing. For instance, the TS and sensor circuit could be

manufactured into the same package to reduce the mismatch. In addition, non-sensor elements can be used as the TS transducer so that the TS circuit will not respond to the legitimate signals. For microphones, it might be possible to achieve more effective mitigation by using frequency-domain signal processing methods (*e.g.*, filtering) based on the frequency information extracted from the TS output.

For the pressure sensor, when the default value of the TS circuit significantly deviates from the sensor setpoint, the correction could be less effective. As shown in Figure 21, the error after correction becomes larger as the EMI power increases and the voltage of the TS circuit reaches the limit of the operating range. In this scenario, an alarm signal would be sent to the system. To compensate for this effect, we can replace one of the resistors in the TS circuit with a variable or programmable resistor to adjust the default value.

In the future, we plan to conduct more extensive tests on different kinds of sensor circuits to develop an optimal design. It will be interesting to investigate and understand how to limit the mismatch of the paired dummy sensor circuit design under EMI signal injections with detailed experiments and analysis.

EMI attacks can be a general threat to different kinds of sensors. This work aims to detect and correct the effects of EMI signal injection attacks with a general low-complexity method. However, in this paper, we do not consider other kinds of transduction attacks such as acoustic attacks [40, 53] and light commands [41].

7 RELATED WORK

Recent studies have investigated the sensor data integrity issue caused by intentional EMI attacks on analog sensing components. In this section, we discuss related studies about EMI signal injections on sensors and countermeasures.

EMI Attacks on Analog Sensors. Foo Kune et al. exploited EMI signal injections on sensors as an unchecked entry point to gain adversarial control over the system [33]. They proposed baseband EMI attacks and amplitude-modulated (AM) attacks to craft specific signals in the sensor output. The AM attack exploited the generation of harmonics and cross-products in non-linear microphone circuits. It can induce bogus audio signals in several consumer devices at a distance of 1 to 2 m with a low transmitting power (100 mW). With higher power and usually from a closer range, they investigated in-band EMI attacks on cardiac implantable electrical devices (CIEDs) to inhibit pacing and induce defibrillation shocks [33]. Kasmi et al. [27] investigated intentional EMI attacks on microphones with a front-door coupling setting and studied the threats on voice interfaces of smartphones. They proposed several attack scenarios of injecting malicious voice commands into the headphone microphone to manipulate the voice control system. In another interesting work, Esteves et al. [20] demonstrated EMI voice command injections on smartphones through a conducted propagation path. It is also worth noting that Rasmussen et al. observed that EM emanations could "induce a current in the audio receiver circuit just as if the IMD received a sound signal" and pointed out adversarial usage of this effect to invalidate security properties of acoustic-based distance bounding protocols in an early work [35].

Selvaraj et al. [37] investigated EMI attacks to modify the input voltage of GPIO pins in microcontrollers. More specifically, the attack induced signal clippings in Electro-Static Discharge (ESD) protection circuits of ADC inputs of a microcontroller, resulting in a rectification effect in the ESD protection circuit. Tu et al. [46] studied EMI attacks to inject and manipulate the DC voltage in the sensor signal amplification stage. The attack can trick the internal temperature control system of devices such as an infant incubator to heat up or cool down. The attack could affect different classes of analog sensors that share similar signal conditioning processes.

Researchers investigated the effect of intentional EMI attacks on different applications such as radar [52], sensor network [17], drones [19], and magnetic encoders of anti-lock braking systems [38]. In addition, the effects of near-field EMI attacks with a relatively high power were investigated on touchscreens [34], power converters [16], and hall sensors [13]. Recent works conducted detailed security analysis with EMI signal injections on sensor components such as ADCs [24] and amplifiers [46] using a direct power injection (DPI) setting to understand the vulnerabilities. Additionally, Rouf et al. [36] exploited the unauthenticated wireless transmission to spoof the pressure of car tires and trigger warning lights. While the topic of pressure monitoring is related, the attack vector investigated differs from EMI signal injection attacks on pressure sensors. The threats of physical-level signal injection attacks on pressure sensors have not been investigated in the context of a control process.

Countermeasures to EMI attacks on Analog Sensors. We will discuss attack mitigation methods, including 1) conventional methods such as shielding, filtering, sensor redundancy, and sensor fusion. 2) defense methods specifically designed in the context of intentional EMI attacks on sensors.

Shielding and filtering can be effective ways to mitigate EMI. However, in practice, there can be many factors (*e.g.*, cost and design) that limit the effectiveness of such methods. Moreover, in intentional EMI attacks, information about the malicious EMI signal source is unknown. The attacks are not limited to a specific frequency range or a certain transmitting path since adversaries can intentionally adjust the attack parameters. Therefore, filtering circuits designed for a specific device and tested for known EMI sources with a certain frequency range or transmitting path may not work effectively for intentional EMI attacks on different kinds of sensors. Sensor fusion and sensor redundancy-based methods could be used to detect the anomaly and to improve the resilience of the system. However, such methods often require modeling and testing based on the specific application scenario and system. It may not be a trivial task to deploy such methods on consumer electronics with different kinds of sensors and application scenarios. Moreover, the attack surface would increase when multiple sensors are added. In comparison, our method can achieve effective detection and correction of the EMI attack effects by introducing minimal redundancy and complexity.

Researchers have proposed methods designed to mitigate intentional EMI signal injection attacks on sensors. Foo Kune et al. proposed a general framework composed of a series of analog and digital defenses to improve the security of analog sensors. The researchers proposed to capture the malicious EMI signals with an

antenna or a reference conductor. The received electromagnetic signals will be processed to determine the signal contamination level and filter the attack signal [33]. However, this approach requires the use of specific modules to monitor and process EM signals in the attack frequency range. Moreover, it could be challenging to recover the legitimate sensor signal by directly analyzing out-of-band EMI signals that are non-linearly transformed in the circuits.

Tu et al. [46] proposed a tunable anomaly detector leveraging the superheterodyne technique to detect EMI attack signals in vulnerable frequency ranges. Additionally, Shoukry et al. [39] presented a physical challenge-response authentication method to detect attacks on active sensors. Wang et al. [48] and Bolton et al. [14] recommended to use a microphone to detect attack signals in the context of resonant acoustic attacks [44, 45]. Recently, Zhang and Rasmussen [54] proposed to detect EMI attacks on sensors by modulating the sensor output in a way that is unpredictable to the adversary. By selectively turning sensors on and off based on an encoded secret bit sequence, the system can detect the presence of EMI attacks that cause inconsistent or unexpected non-zero samples.

Unlike methods that primarily focused on detecting EMI attacks, this paper aims to detect and correct the corrupted sensor data, which helps to maintain the functioning of sensor-based systems in the presence of EMI signal injection attacks. Moreover, our defense method leverages a matched dummy sensor design with components that are usually no more complex than an original sensor circuit and is suitable for securing different kinds of low-end sensor systems.

8 CONCLUSION

Sensing and control systems fundamentally rely on sensor measurements to make accurate and real-time decisions. EMI signal injection attacks can cause security issues to different classes of sensors. This paper proposed a low-complexity defense method for sensing systems that often have simple functionalities and constrained resources. Our method leveraged a matched dummy sensor circuit design to detect and correct the effects of EMI signal injection attacks. We analyzed and evaluated the defense method with attack experiments using various attack parameters on different kinds of sensors. Our experimental results showed that the proposed defense method could be a simple but effective approach to ensure the security and reliability of sensing systems in the presence of EMI signal injection attacks.

Acknowledgments. The authors thank the anonymous reviewers for their valuable comments that improved this paper. This work is supported in part by US NSF under grant OIA-1946231.

REFERENCES

[1] 2018. RFSpace LPDAMAX Wide-band PCB Log Periodic Antenna . http://rfspace.com/RFSPACE/Antennas_files/LPDA-MAX.pdf.
[2] 2020. https://onezero.medium.com/the-u-s-military-is-building-voice-controlled-war-robots-dcf4f98b63bd.
[3] 2020. Common Types of Pressure Sensors. https://www.thomasnet.com/articles/instruments-controls/pressure-sensors/.
[4] 2020. Datasheet of Honeywell Basic Board Mount Pressure Sensors: ABP Series. https://sensing.honeywell.com/honeywell-sensing-pressure-board-mount-abp-series-ventilator-datasheet-32350389.pdf.
[5] 2020. Datasheet of Sensata P1J Low Pressure Sensor. https://www.alliedelec.com/m/d/db1e910878b0367f4c9ffd5b1e6f47cd.pdf.
[6] 2020. HackRF One. https://greatscottgadgets.com/hackrf/one/.
[7] 2020. How does a Pressure Sensor Work - Physics of Probeware . https://www.thepocketlab.com/educators/lesson/how-does-pressure-sensor-work-physics-probeware.
[8] 2020. Load Cell Applications. https://www.flintec.com/applications.
[9] 2020. Load Cells & Force Sensors. https://www.omega.com/en-us/resources/load-cells.
[10] 2020. MEMS pressure sensors. https://www.microsensorcorp.com/Details_mems_pressure_sensor.html.
[11] 2020. MEMS pressure sensors. https://www.avnet.com/wps/portal/abacus/solutions/technologies/sensors/pressure-sensors/core-technologies/mems/.
[12] Ahmed M Almassri, WZ Wan Hasan, Siti Anom Ahmad, Asnor J Ishak, AM Ghazali, DN Talib, and Chikamune Wada. 2015. Pressure sensor: state of the art, design, and application for robotic hand. *Journal of Sensors* 2015 (2015).
[13] 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)*. 1273–1290.
[14] 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.
[15] Q Chen, BW Jones, SM Loo, WW Nazaroff, RA Overfelt, CP Weisel, and CJ Weschler. 2010. Report to the FAA on the Airliner Cabin Environment. *Report No. RITE-ACER-CoE-2010-1. National Air Transportation Center of Excellence for Research in the Intermodal Transport Environment (RITE)-Airliner Cabin Environmental Research (ACER) Program* (2010).
[16] Gokcen Y Dayanikli, Rees R Hatch, Ryan M Gerdes, Hongjie Wang, and Regan Zane. 2020. Electromagnetic Sensor and Actuator Attacks on Power Converters for Electric Vehicles. *IEEE Workshop on the Internet of Safe Things* (2020).
[17] Jerker Delsing, Jonas Ekman, Jonny Johansson, Sofia Sundberg, Mats Bäckström, and T Nilsson. 2006. Susceptibility of sensor networks to intentional electromagnetic interference. In *International Zürich Symposium on Electromagnetic Compatibility.*
[18] Fatemeh Ejeian, Shohreh Azadi, Amir Razmjou, Yasin Orooji, Ajay Kottapalli, Majid Ebrahimi Warkiani, and Mohsen Asadnia. 2019. Design and applications of MEMS flow sensors: A review. *Sensors and Actuators A: Physical* 295 (2019), 483–502.
[19] José Lopes Esteves, Emmanuel Cottais, and Chaouki Kasmi. 2018. Unlocking the Access to the Effects Induced by IEMI on a Civilian UAV. In *2018 International Symposium on Electromagnetic Compatibility (EMC EUROPE)*. IEEE, 48–52.
[20] J Lopes Esteves and C Kasmi. 2018. Remote and silent voice command injection on a smartphone through conducted IEMI: Threats of smart IEMI for information security. *Wireless Security Lab, French Network and Information Security Agency (ANSSI), Tech. Rep* (2018).
[21] AS Fiorillo, CD Critello, and SA Pullano. 2018. Theory, technology and applications of piezoresistive sensors: A review. *Sensors and Actuators A: Physical* 281 (2018), 156–175.
[22] Kevin Fu and Wenyuan Xu. 2018. Risks of trusting the physics of sensors. *Commun. ACM* 61, 2 (2018), 20–23.
[23] Ilias Giechaskiel and Kasper Rasmussen. 2019. Taxonomy and challenges of out-of-band signal injection attacks and defenses. *IEEE Communications Surveys & Tutorials* 22, 1 (2019), 645–670.
[24] Ilias Giechaskiel, Youqian Zhang, and Kasper B Rasmussen. 2019. A framework for evaluating security in the presence of signal injection attacks. In *European Symposium on Research in Computer Security*. Springer, 512–532.
[25] Hashem Mehrdad Hashemian. 2011. On-line monitoring applications in nuclear power plants. *Progress in Nuclear Energy* 53, 2 (2011), 167–181.
[26] Yaser Javed, Mohtashim Mansoor, and Irtiza Ali Shah. 2019. A review of principles of MEMS pressure sensing with its aerospace applications. *Sensor Review* (2019).
[27] Chaouki Kasmi and Jose Lopes Esteves. 2015. IEMI threats for information security: Remote command injection on modern smartphones. *IEEE Transactions on Electromagnetic Compatibility* 57, 6 (2015), 1752–1755.
[28] Walt Kester. 1999. *Practical design techniques for sensor signal conditioning*. Analog devices.
[29] Chih-Hung King, Martin O Culjat, Miguel L Franco, James W Bisley, Gregory P Carman, Erik P Dutson, and Warren S Grundfest. 2008. A multielement tactile feedback system for robot-assisted minimally invasive surgery. *IEEE Transactions on Haptics* 2, 1 (2008), 52–56.
[30] Charles Kitchin and Lew Counts. 2004. *A designer's guide to instrumentation amplifiers*. Analog Devices.
[31] S Konishi, S Otake, H Kosawa, A Hirata, and F Mori. 2019. The Combination of Soft Microfingers and Wearable Interface Device for Haptic Teleoperation Robot System. In *2019 International Conference on Manipulation, Automation and Robotics at Small Scales (MARSS)*. IEEE, 1–6.
[32] Uwe Kruger and Lei Xie. 2012. *Statistical monitoring of complex multivatiate processes: with applications in industrial process control*. John Wiley & Sons.
[33] 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.
[34] Seita Maruyama, Satohiro Wakabayashi, and Tatsuya Mori. 2019. Tap'n Ghost: A Compilation of Novel Attack Techniques against Smartphone Touchscreens. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 620–637.
[35] Kasper Bonne Rasmussen, Claude Castelluccia, Thomas S Heydt-Benjamin, and Srdjan Capkun. 2009. Proximity-based access control for implantable medical devices. In *Proceedings of the 16th ACM conference on Computer and communications security*. 410–419.
[36] Ishtiaq Rouf, Robert D Miller, Hossen A Mustafa, Travis Taylor, Sangho Oh, Wenyuan Xu, Marco Gruteser, Wade Trappe, and Ivan Seskar. 2010. Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study. In *USENIX Security Symposium*, Vol. 10.
[37] Jayaprakash Selvaraj, Gökçen Yılmaz Dayanıklı, Neelam Prabhu Gaunkar, David Ware, Ryan M Gerdes, and Mani Mina. 2018. Electromagnetic induction attacks against embedded systems. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*. 499–510.
[38] 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.
[39] 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.
[40] 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 *Proceedings of USENIX Security Symposium*.
[41] Takeshi Sugawara, Benjamin Cyr, Sara Rampazzi, Daniel Genkin, and Kevin Fu. 2020. Light commands: laser-based audio injection attacks on voice-controllable systems. In *29th {USENIX} Security Symposium ({USENIX} Security 20)*. 2631–2648.
[42] Subramanian Sundaram, Petr Kellnhofer, Yunzhu Li, Jun-Yan Zhu, Antonio Torralba, and Wojciech Matusik. 2019. Learning the signatures of the human grasp using a scalable tactile glove. *Nature* 569, 7758 (2019), 698–702.
[43] Mohsin I Tiwana, Stephen J Redmond, and Nigel H Lovell. 2012. A review of tactile sensing technologies with applications in biomedical engineering. *Sensors and Actuators A: physical* 179 (2012), 17–31.
[44] 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.
[45] 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.
[46] Yazhou Tu, Sara Rampazzi, Bin Hao, Angel Rodriguez, Kevin Fu, and Xiali Hei. 2019. 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*. 2301–2315.
[47] BR Upadhyaya, K Zhao, and B Lu. 2003. Fault monitoring of nuclear power plant sensors and field devices. *Progress in nuclear energy* 43, 1-4 (2003), 337–342.
[48] Zhengbo Wang, Kang Wang, Bo Yang, Shangyuan Li, and Aimin Pan. 2017. Sonic gun to smart devices: Your devices lose control under ultrasound/sound. *BlackHat USA* (2017).
[49] Qingxiong Xiong and Shaojie Zhang. 2018. Fault Injection and Diagnosis for Civil Aircraft Cabin Pressure Control System. In *2018 Prognostics and System Health Management Conference (PHM-Chongqing)*. IEEE, 314–318.
[50] Xiaodong Xu, Shaojie Zhang, and Xiaohang Hai. 2017. Cabin pressurization control system design of civil aircraft by model based systems engineering. In *2017 Chinese Automation Congress (CAC)*. IEEE, 3035–3040.
[51] 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)*. 480–495.
[52] Chen Yan, Wenyuan Xu, and Jianhao Liu. 2016. Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle. *DEF CON* 24 (2016).
[53] 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.
[54] Youqian Zhang and Kasper Rasmussen. 2020. Detection of electromagnetic interference attacks on sensor systems. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 203–216.
[55] Kateryna Zinchenko, Chien-Yu Wu, and Kai-Tai Song. 2016. A study on speech recognition control for a surgical robot. *IEEE Transactions on Industrial Informatics* 13, 2 (2016), 607–615.

APPENDIX

A. Results of EMI Attack Experiments

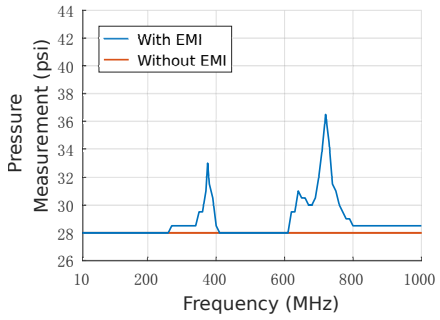


Figure 18: The attack effect with different frequencies of EMI on inflation pump #2 with an attack distance of 0.5 m and a transmitting power of 4 W.

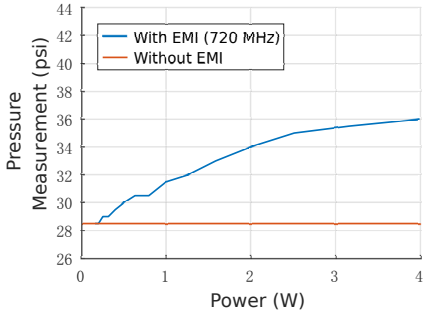


Figure 19: The attack effect with varying transmitting power of EMI on inflation pump #2 with an attack distance of 0.5 m.

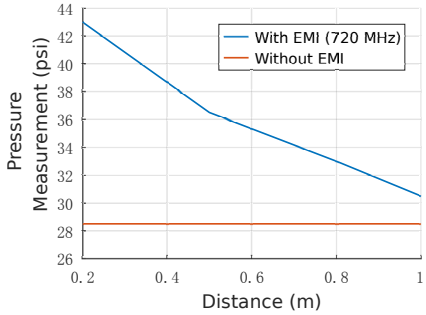


Figure 20: The effect of EMI attacks on inflation pump #2 in different distances at a frequency of 720 MHz with a 4-W transmitting power.

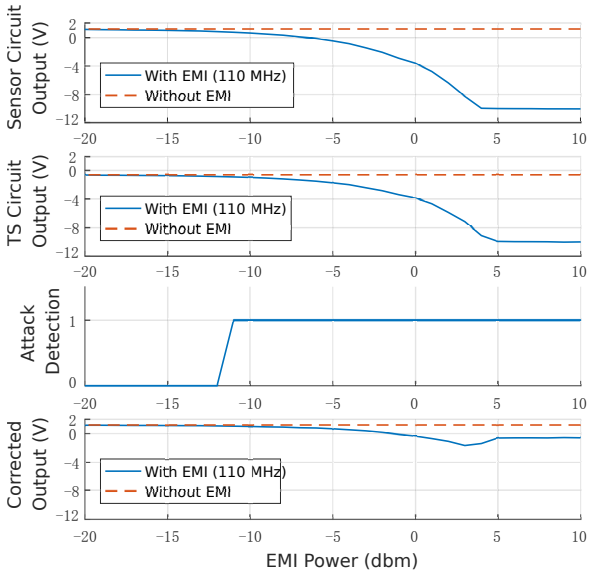


Figure 21: The detection and correction of EMI attacks on the load cell pressure sensor with different transmitting power. A constant force is applied on the sensor transducer to cause a voltage offset. Due to the difference between the default values of the TS and sensor circuits, the error after correction becomes larger as the EMI power increases and the voltage of the TS circuit reaches the limit of the operating range.

B. Experiments with the Corrected Microphone Sensor Data on a Voice Recognition System

We play the corrupted and corrected microphone sensor data respectively to evaluate our defense method. We play the audio data using a laptop. We use a smartphone (Google Pixel 2 XL) voice recognition system (Google Assistant) to recognize the sound. The data we use correspond to the experiments illustrated in Figure 16 and Figure 17.

The legitimate signal is "Hey Google, what time is it". As shown in Figure 22, when the sine wave and white noise signals are injected, the legitimate signals cannot be recognized. With the corrected sensor data, the legitimate voice signals are correctly recognized.

The experiment of Figure 23 uses the data illustrated in Figure 17. In this experiment, the legitimate signal is still "Hey Google, what time is it". The adversary injects malicious voice signals including "Hey Google, turn on the fireplace" and "open the door" alternatively. As shown in Figure 23, the legitimate signals cannot be correctly recognized from the microphone sensor data due to the EMI injected voice signals. With our defense method, most of the legitimate signals are correctly recognized.

C. Ethical Consideration

Conducting experiments with vehicle tires and manipulating the tire air pressure could come with risks of tire explosion. In our experiments, we keep the tire pressure in a range below 40 psi to reduce risks. Researchers involved in these experiments have taken safety precautions including wearing safety helmets, polycarbonate face shields, and earmuffs.

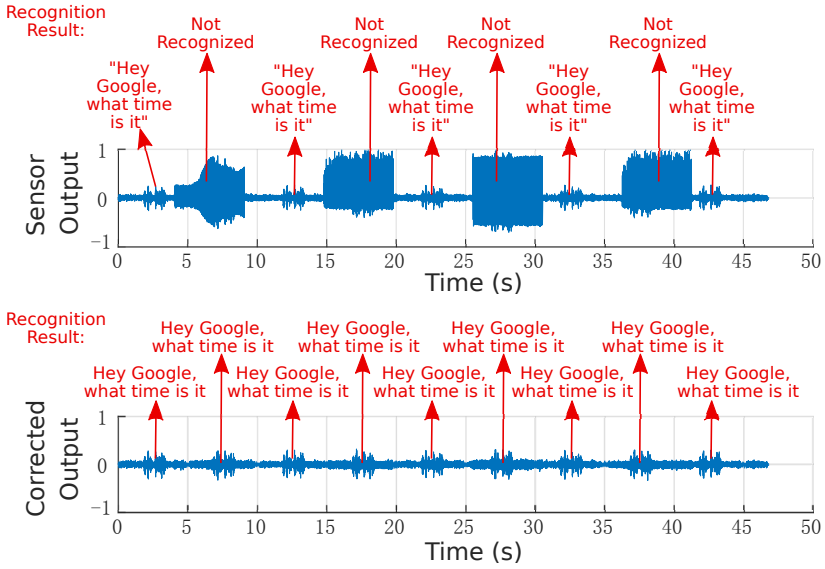


Figure 22: We use a laptop to play the audio data to a smartphone voice recognition system (Google Assistant). Up: The legitimate signals cannot be recognized from the microphone sensor data due to the EMI injected sine wave and white noise signals. Bottom: With our defense method to mitigate the EMI injected signals, the legitimate signals are correctly recognized. This experiment corresponds to the experiment illustrated in Figure 16.

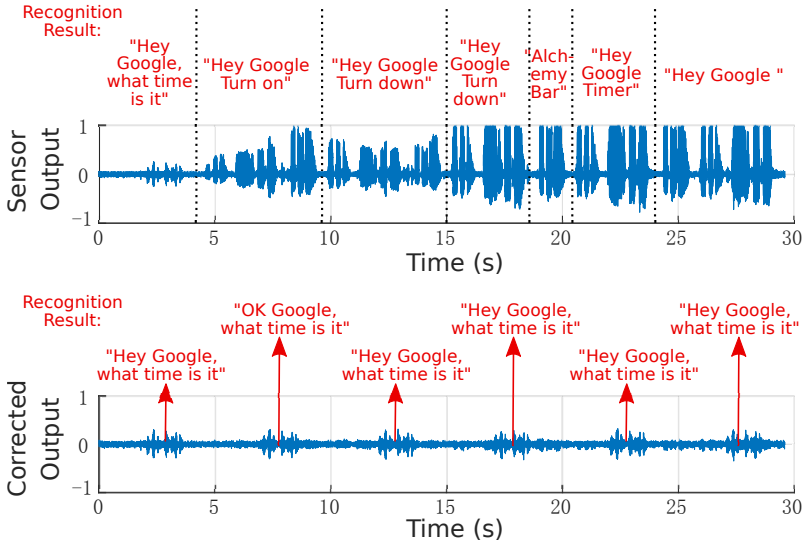


Figure 23: We use a laptop to play the audio data to a smartphone voice recognition system (Google Assistant). Up: The legitimate signals cannot be correctly recognized from the microphone sensor data due to the EMI injected voice signals. Bottom: With our defense method to mitigate the EMI injected signals, most of the legitimate signals are correctly recognized (in one case, it is recognized as "OK Google,what time is it" instead of "Hey Google,what time is it"). This experiment corresponds to the experiment illustrated in Figure 17.