Towards Adversarial Process Control on Inertial Sensor Systems with Physical Feedback Side Channels

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

Sara Rampazzi
srampazzi@ufl.edu
University of Florida
Gainesville, Florida, USA

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

ABSTRACT

Real-world process control requires continuous sensor measurements and automatic control of the environment. Typical process control systems consist of three main components: controllers functioning as the system's "brain", sensors acting as measurement devices, and final control elements that modify the environment. Prior works showed that adversaries could inject signals into analog sensors to affect the control process; however, an adversarial controller that is necessary to achieve process control is inherently missing in conventional physical-level sensor signal injection attacks, which revealed mechanisms to perturb sensor systems but did not describe the computations necessary to adjust and regulate the process over time.

This paper introduces an adversarial control loop approach that computes attack signals during the attack to guide the adversarial process control. Our approach allows constructing the external "brain" of the adversarial process control with programs. Further, we characterize the Physical Feedback Side Channel (PFSC) in out-of-band signal injection attacks, and study how the adversarial prototype system can be constructed non-invasively to gain control over two types of inertial sensor-actuator systems, including a MegaWheels self-balancing scooter. We demonstrate proof-of-concept process control without accessing or tampering with internal modules of the victim system.

CCS CONCEPTS

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

KEYWORDS

Adversarial Control Loop, Physical Feedback Side Channel, Sensors, Attacks

ACM Reference Format:
Yazhou Tu, Sara Rampazzi, and Xiali Hei. 2023. Towards Adversarial Process Control on Inertial Sensor Systems with Physical Feedback Side Channels. In *Proceedings of the 5th Workshop on CPS&IoT Security and Privacy (CPSIoTSec '23), November 26, 2023, Copenhagen, Denmark*. ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3605758.3623494

CPSIoTSec '23, November 26, 2023, Copenhagen, Denmark

ACM ISBN 979-8-4007-0254-9/23/11…$15.00
https://doi.org/10.1145/3605758.3623494

1 INTRODUCTION

Process control is widely applied in various industrial, robotic [5, 6, 35, 41], and medical systems [15, 16]. The main objective of process control is to stabilize and adjust the output of a process over a certain period despite variations in input, disturbances, or other changing environmental conditions. It involves continually monitoring the process, making necessary adjustments to the input or operational variables, and concurrently evaluating the outcomes to reach the desired results throughout the process.

In process control systems, there are three main components: 1) controllers that decide the necessary course of action when there is any deviation from the desired state (*e.g.*, the set point). Such decisions are made based on the input from the sensor and using a pre-determined algorithm, 2) sensors that measure the process variable, such as temperature, pressure, or angle, and provide such feedback to the controller, and 3) final control elements that can physically change the process, like a heater, valve, or motor.

Prior works show that adversaries could manipulate sensors by affecting their analog components with physical signal injections [26, 38, 53, 58]. However, unlike control systems that can continuously adjust the system status with a control algorithm, such attacks inherently rely on 1) fixed or manually tuned attack signals and 2) access to internal sensor data or readings illustrated on a screen. Due to these inherent limitations, prior attacks on sensors can disrupt the victim control system or induce targeted actuation, but it remains challenging to gain adversarial process control, which requires an accurate methodology that computes the attacker's desired input and continuously adjusts the process over time.

Drawing inspiration from control systems that manage physical-domain properties using algorithms, we propose an adversarial control loop (ACL) approach to sensor-dependent process control systems. Instead of a legitimate internal control loop, we study an external, physical adversarial control loop that has no digital connections to the targeted system and lacks access to data from the victim system's internal modules.

To achieve the adversarial control loop, we utilize a Physical Feedback Side Channel (PFSC) and an external attack system. We first characterize the physical feedback side channel, which allows non-invasively assessing the target's responses under signal injections. We then investigate how to construct an adaptive attack system that computes attack signals with programs to control the victim process. Our approach is designed for continuous processes that have sensors subjected to physical signal injections and actuators leading to PFSCs. In our attacks, the time series of the system's side-channel physical feedback are automatically extracted from physical-domain signals and used by programs to adjust attack

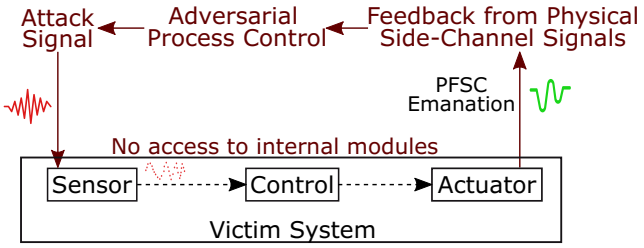

Figure 1: An illustration of the proposed approach. We identify the necessary, concurrent operations to construct the non-invasive, physical adversarial control loop: 1) signal injection, 2) PFSC feature extraction, and 3) adversarial control and computation.

signals. The perturbations induced by attack signals transmit to the control system's output to induce changes to the environment. We characterize the three main necessary components to construct the adversarial control loop: 1) signal injection, 2) PFSC feature extraction, and 3) adversarial control and computation (Figure 1).

We conduct case studies to investigate how the ACL can be constructed on inertial sensor-actuator systems. We then develop an attack system that captures and processes physical-domain signals related to the actuation of the victim system; it performs signal capturing, feature extraction, and attack signal generation in multiple threads while the victim system is running. We demonstrate the proof-of-concept software-based process control on two kinds of control processes based on inertial sensors, including a closed-loop control process of a self-balancing system (a Megawheels self-balancing scooter) and an open-loop speed control process of a motor based on the sensed heading angle. The adversary's goal is to manipulate such processes in a continuous manner to achieve the desired accumulated attack effects over time. Processes with similar control principles can be found in robotic systems [5, 6, 35], gimbals [7, 52], platform stabilization [34, 41], and telepresence control systems [17, 29].

In summary, our approach allows an adversarial control system to be constructed externally and non-invasively to control a victim process. In addition, our methodology is necessary because 1) many physical properties (*e.g.*, speed, angle, temperature) are accumulated during the entire process, and their control over time requires continuous monitoring instead of sporadically induced events, and 2) naive attacks cannot succeed over complex and long-duration processes that change their operations based on external stimuli. In comparison, we characterize PFSC as a complementary technique for out-of-band signal injections [26, 38, 52] to retrieve physical feedback from the target and provide reference inputs for adversarial process control without accessing the victim system's internal statuses. Finally, different from existing works [45, 46, 51–53] that rely on previously recorded or manually tuned signals, our attack automatically computes the PFSC features and physical attack signals during the adversarial control process.

This paper makes the following contributions.

- We propose an adversarial control loop-based approach for manipulating inertial sensor-based control processes. Unlike the legitimate internal control loop, the adversarial control loop has no digital connections to the target system and cannot access data from the system's internal modules.
- We characterize the physical feedback side channel under signal injections. We study how to utilize this channel to extract features and guide adversarial process control.
- We explore the adversarial process control with proof-of-concept attacks on two types of real-world inertial sensor-actuator systems. We develop a prototype testing system to facilitate the evaluation of the threats.

2 BACKGROUND

Process Control. Process control is essential in various industrial systems, robots, and medical devices to ensure stable, repeatable, and optimized performance. It involves continuously monitoring, maintaining, and adjusting variables, such as temperature, pressure, flow, humidity, pH levels, and angles, to achieve consistent, desired results.

In a typical process control system, there are three main components. First, a controller is an indispensable component that performs computations to decide the necessary course of action when there is deviation from the desired state. Second, a sensor measures the physical property, such as temperature or angle, and provides feedback to the controller. Third, the final control element, such as a valve or motor, can physically change the process over time according to the instructions from the controller.

Inertial Sensors. Inertial sensing and control processes are used in a wide range of applications like platform stabilization of types of machinery [14], telepresence control [17, 29], robotics [5, 6, 35], virtual/augmented reality, and the guidance of rockets and airplanes [42, 50], etc. They are crucial for maintaining stability, precision, and safety in motion-dependent systems, enabling seamless interaction with the physical world. These processes provide precise control over an object's orientation, position, and movement over time.

Micro-electromechanical system (MEMS) inertial sensors are susceptible to acoustic resonance [21, 22]. Prior work explored using acoustic resonance to intentionally interfere with inertial sensors to crash drones [46]. Further, researchers manipulated accelerometers' outputs by visually observing the internal sensor data and manually tuning the acoustic signals [51]. Moreover, attacks on gyroscope-based embedded systems such as self-balancing scooters, camera stabilizers, and gyroscopic screwdrivers achieved targeted actuation by manually adjusting attack signals [52].

3 THREAT MODEL

The adversary aims to manipulate the course of action of the victim system automatically through programs in the external adversarial control loop and gain adversarial process control without accessing the victim's internal modules or digital interfaces. The ultimate attacker's goals can vary, from rendering the victim system ineffective under actual environmental stimuli or user operation inputs, continuously controlling a physical property that was expected to be regulated by the victim system, to causing harm to a person in the environment. To realize these objectives, the attacker aims to obtain reliable malicious control over the victim system, resulting in a sequence of adverse outcomes that might diverge from the system's originally designed behaviors. This is achievable by

the ability to manipulate the process in a continuous manner to produce the desired cumulative attack effects.

Non-Invasive Adversarial Process Control. We assume adversaries cannot tamper with or access the internal firmware/hardware of the victim system. They also cannot directly modify the actual physical properties, such as by directly moving or damaging the victim system. To achieve process control, the adversary needs to utilize software (*e.g.*, multi-threaded programs) to continuously adjust attack signals. In this process, the attack system is designed to manipulate the victim system to apply changes to continuous physical properties (*e.g.*, heading angle and speed).

This attack approach differs from others, which use digital channels to directly send control commands to the victim system with digital-domain data communication. Furthermore, the adversary cannot access the victim system's internal sensor measurements, sampling intervals, clock, and timer signals. We assume that the adversaries can only analyze external physical-domain signals like the acoustic emissions from the victim system's actuators. They can deploy devices such as directional microphones [39, 43] and microphone arrays [12] to capture such side-channel signals from a long distance. Due to the time-varying nature of injected signals and other statuses in continuous process control systems, the extraction of physical side-channel feedback and adjustment of the attack signals are performed when the victim system is being continually influenced by the attacker's injected perturbations and the subsequent states are yet to be determined.

Acoustic Signal Injection. To inject malicious signals, attackers can use consumer-grade speakers, directivity horns, transducers, and amplifiers to produce sound waves. The signal source can be a sound card. A computer such as a laptop or Raspberry Pi runs the attack program. Attackers can optimize the acoustic transmitting power and directivity with customized sound sources. Capable attackers could use professional acoustic devices or highly customized acoustic amplification techniques to further improve the attack range. For instance, adversaries may launch the attack by using long-range acoustic devices [4, 10, 13, 25]. The resonant frequencies of MEMS gyroscopes are usually above 19 kHz [46, 52]. Thus, the attack signals are beyond the audible range of most adults [48].

4 METHODOLOGY

This section introduces the proposed methodology and describes the mechanisms to form an external adversarial loop over an inertial sensor-actuator system.

4.1 Adversarial Control Loop Structure

Fig. 2 illustrates the structure and basic modules in our approach. We model the victim system as a black-box sensor-actuator system that controls its actuation based on sensor measurements. The attack system is external to the victim system and can only affect the target system by emitting physical-domain signals.

The main modules in the attack system include the physical observer, the feature analyzer, the adversarial control program, and the attack signal generator.

The physical feedback is provided by the physical observer and the feature analyzer modules. The physical observer of the attack

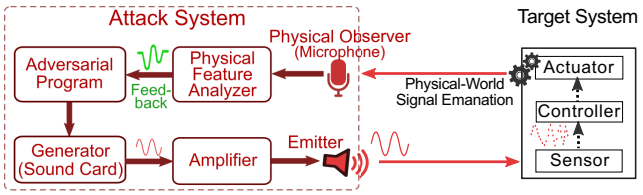

Figure 2: An illustration of the structure and basic modules of the proposed method. The attack system computes the attack signals during the attack. The input to the victim system is the perturbation caused by the attack signals. The output of the victim control system is the changes it applies to the environment. The attack system automatically captures and analyzes the side-channel physical signal emanation to guide the attacks.

system consists of sensor modules that measure physical signals related to the actuator of the target system. The data is streamed to the feature analyzer, which extracts the physical feedback by analyzing physical signal features.

The attacker's program on a computer or an embedded device will adjust the attack signals based on the extracted feedback. The program then generates the attack data and writes the attack signal streams to a signal generator hardware. (*e.g.*, a sound card). Additionally, an amplifier is used to regulate the power of the emitted signal. Depending on the type of injection (*e.g.*, acoustic or electromagnetic), a transducer or antenna can be used to emit the attack signals.

During the attack process, the modules of the adversarial process will not pause and wait for other modules. To form an adversarial control loop, we implement the attack system's software with multi-threaded programs that handle the inputs and outputs of each module. Sections 5 will discuss the details of implementing the attack system on inertial sensor systems.

4.2 Adversarial Control Loop Formalization

The adversarial control is enabled by a loop that injects signals to perturb the victim system and extract the system feedback from physical-domain signals, such as acoustic side-channel emanations of the victim actuator. In this section, we characterize the general mechanisms, including analysis and control, injection of perturbations, and physical feedback extraction.

4.2.1 ***Analysis and Control.*** We provide the following analysis and formalization to understand how to guide the perturbation injection to control the victim system by leveraging the extracted system feedback from physical domain signals.

Assuming the perturbation injected into the input of the victim system is $p(t)$, the perturbed system input $X'(t)$ is

$$X'(t) = X(t) + p(t), \tag{1}$$

where $X(t)$ is the original status without the perturbation. The actuation output of the system under perturbation is $Y(t) = G(X'(t))$, where G is the transfer function of the victim control system. For control systems that rely on the sensor measurements to perform

real-time process control, the injected perturbations $p(t)$ will be transmitted to the output of the system via

$$Y(t) = G(X(t) + p(t)). \tag{2}$$

When the goal is to control a continuous process over time, the time-varying effect of the perturbation on the victim process has to be considered. By extracting and analyzing the time series $y[n]$ of the physical feedback $y(t)$ from physical-domain signal emanations related to $Y(t)$, the injection of perturbations can be guided and adjusted to gain process control over the target system.

4.2.2 ***Injection of Perturbations.*** The injection of perturbation $p(t)$ is conducted as previous works [52, 53] by influencing analog sensor components with physical-level signals, such as acoustic signals emitted at the resonance frequency of MEMS inertial sensors. The internal statuses of the victim system are not accessible to external attackers.

4.2.3 ***Side-Channel Physical Feedback Extraction.*** As defined in the previous sections, We consider the PFSC as the side-channel signal emanations of the victim actuators, which we use to monitor and control the victim system's responses under out-of-band signal injection attacks. This is a complementary methodology to traditional out-of-band signal injection attacks [26, 52] to achieve an external non-invasive adversarial control loop. It can be utilized to retrieve the time series of $y(t)$ under signal injections without directly accessing its internal data. For instance, radars/sonars can detect and measure the movements of the actuator; infrared sensors can remotely monitor the temperature of the target actuator/environment; laser-based devices can measure the distance and speed of the target system. In this study, we explore the use of actuator acoustic emanations as the PFSC. Section 4.4 will discuss the specific mechanisms applied to inertial sensor systems.

4.3 Model Generalization

In continuous process and actuation control systems, the system controls a continuous physical property such as temperature, air pressure, pH value, position, speed, and heading angle. These properties are measured by sensors. For instance, a robotic system continuously measures the heading angle with a gyroscope and actuates the system to maintain a certain speed or balanced position [5, 6, 35]. Telepresence control systems continuously actuate an object in a remote environment based on the inertial sensor system's orientation, speed, and position [17, 29]. The heading angle or the other kinematics properties of these systems are continuous because they cannot be changed instantly but require a control process for the system to apply changes to the physical environment over time.

In addition, process actuators such as motors in actuation systems can result in a change in the process variables and states. Actuators typically transduce electricity into other forms of physical properties. The operation of the mechanical and electrical parts of the actuator will generate changes in environmental physical signals. An external attacker can measure the induced changes in the signals of the physical environment. Examples of such signals include but are not limited to heat, sound, and electromagnetic signals.

Formalization of System Properties. In process control, $Y(t)$ is the control system's output and is directly related to the actuator status. For example, $Y(t)$ can be the acceleration or speed of the motor. Additionally, we use $Z(t)$ to represent the process variables of the control system. Depending on the application, $Z(t)$ can be equal to $Y(t)$ or be affected by $Y(t)$. For instance, when the control goal is to reach a certain motor rotation speed, we have $Z(t) = Y(t)$. In many other scenarios, the process variable $Z(t)$ is not equivalent to the status of the actuator. For example, when the goal is to maintain the pH level at a specific value, the actuator status $Y(t)$ of the peristaltic motor will determine the volume of acid or alkaline solutions delivered to the environment in a certain amount of time. This further determines how the actual pH value $Z(t)$ will be changed.

Based on these premises, we can provide a generalization of our adversarial close loop process by characterizing our approach with the following stages. First, adversaries can extract physical signals in the environment depending on the control system. In scenarios where the physical signals are directly related to the actuator, the extracted feedback will be denoted as $y(t)$, which is directly correlated to the control system output $Y(t)$. This applies to kinematics-based control systems and many other process control systems. For instance, pH or temperature control systems' actuators (*e.g.*, pumps, heaters) can generate side-channel acoustic, electromagnetic, or heat signals. The extracted time series of the physical signals will be directly related to the process variable being controlled by the victim system. Usually, the actuation will generate environmental changes that can be measured from acoustic, electromagnetic, current, heat, or vibration signals, etc.

Second, the adversaries will inject physical-domain signals to induce malicious current or voltage signals in the analog sensor of a victim system. For example, adversaries can inject out-of-band acoustic signals to inertial sensors to perturb their readings [46, 51, 52, 56] or affect the output of pH, temperature, and pressure sensors by electromagnetic interference (EMI) injection attacks [53].

Finally, the injected perturbation $p(t)$ can be adjusted with algorithms to control the victim system by processing and analyzing the extracted feedback. The methodology provides a systematic approach to control the victim system without connecting to the internal statuses or modules. Unlike relying on empirical observation and manual signal tuning, this approach provides a formalized, universal framework to enable non-invasive adversarial process control.

4.4 ACL Mechanisms on Inertial Sensor Systems

In this section, we study how our method applies to real-world systems. We investigate ACL-based attacks to gain targeted process control over inertial sensing and control systems such as a self-balancing scooter. The attack system perturbs the sensor data with acoustic signals at the resonance frequency of the victim inertial sensor and adjusts the adversary injection signals based on the physical feedback side channel. We specify the mechanisms as follows.

4.4.1 System Feedback Extraction. We utilize a microphone to capture the side-channel acoustic emanations of the victim actuator.

Through experiments and analysis, we find that the sound emanation of motors can be leveraged to extract the physical feedback to guide the adversarial control process. Specifically, we provide the following formalization.

Assuming the output mechanical power of a motor is P, measured in watts (W), the rotational speed is rpm in revolutions per minute. The work done per revolution in Joule is $Work = Force \cdot Distance = \frac{\tau}{Radius} \cdot 2\pi Radius = \tau \cdot 2\pi$, where τ is the torque of the system. The output power of the motor P is related to its speed rpm in the following formula:

$$P = \tau \cdot rpm \cdot 2\pi/60, \tag{3}$$

where P and rpm are directly correlated. Since the energy of acoustic emanations P_s is also related to the power of the motor (*e.g.*, by friction, vibration, coil noise), for simplicity, we assume that P_s is related to P by $P = \alpha P_s$, where α is a constant value to describe the ratio between the acoustic emanation power and the motor power. We have $\alpha P_s = \tau \cdot rpm \cdot 2\pi/60$. The formula may not accurately determine the acoustic energy or the speed but can serve as an empirical tool in relative estimations. Our experimental results in later sections also show that the extracted time series $y[n]$ from side-channel acoustic emanations are highly correlated with the actual motor speed and movement patterns. Therefore, we can utilize the extracted and processed features to guide the attacks. In addition, both power and frequency-related features can be analyzed to provide useful feedback that can be incorporated into the adversarial control loop. The details of automatically extracting and utilizing these features are described in Sections 5 and 6.

4.4.2 Injection of Perturbations. The measurements of MEMS inertial sensors can be interfered with by acoustic signals due to their susceptibility to acoustic resonance [21, 46]. The high-frequency acoustic signals injected into the sensors can be converted to low-frequency in-band signals, such as Direct Current (DC) signals, by aliasing [51]. Further, this conversion process is imperfect and can be subject to the disturbance caused by the drifts of sampling intervals in embedded systems [52].

Assuming the attack signal $m(t)$ is:

$$m(t) = A \cdot sin(2\pi f(t)t + \phi_m), \tag{4}$$

where A and $f(t)$ are the amplitude and frequency of the attack signal. ϕ_m is the initial phase. After being transduced into the sensor, the injected signal becomes $V(t)$.

$$V(t) = A_0 \cdot sin(2\pi f(t)t + \phi_0), \tag{5}$$

where A_0 and ϕ_0 are the amplitude and initial phase of $V(t)$. While attackers have full knowledge about the signal $m(t)$, they may not have full knowledge about $V(t)$. For instance, the initial phase ϕ_0 is not certain for attackers after signal transmission and conversion. Moreover, the frequency of the injected signal after aliasing is also not fully deterministic. Assuming $\Delta T[i] = \delta[i] + \frac{1}{F_{S0}}$ are the sampling intervals. F_{S0} is the ideal sample rate. $\delta[i]$ is the drift in the sampling interval. The exact value of $\delta[i]$ can be affected by imperfect clock signals or other kinds of software delays or interrupts in the victim system. Therefore, adversaries are unlikely to fully predict the values of the exact sampling intervals during the control process. $t_0 = 0, t_1 = \Delta T[1], ..., t_i = \sum_{j=1}^{i} \Delta T[j], ...$, are sampling times. The digitized signal $V[i]$ will be

$$V[i] = A_0 \cdot sin(2\pi\epsilon(t_i)t_i + 2\pi n F_{S0}(\textstyle\sum_{j=1}^{i} \delta[j]) + \phi_0). \tag{6}$$

Ideally, the digitized signal would have a frequency of $\epsilon(t)$, assuming $f(t) = nF_{S0} + \epsilon(t)(-\frac{1}{2}F_S < \epsilon \leq \frac{1}{2}F_S, n \in \mathbb{Z}^+)$. However, due to the drifts in sampling intervals, the digital signal frequency is also subject to disturbance. We can observe a non-constant term $2\pi n F_{S0}(\sum_{j=1}^{i} \delta[j])$ in the signal. This is an accumulated term amplified by n. It changes over time and brings disturbance to the converted signal.

Because of drifts in sampling intervals, the induced sensor signals will oscillate. The values of the signal fluctuate as the phase of the signal changes. Such fluctuating signals can be interpreted as noises by inertial sensor-based systems. Thus, we model the injected signals as perturbations that influence the inputs on the victim system. Further, the victim control system affected by the perturbation will make changes in the environment in real-time. We then leverage the physical feedback side channel to adjust the perturbation over time to achieve adversarial process control.

4.4.3 Analysis and Control. In our case studies, we observed that the control systems affected by the injection exhibit an oscillating pattern in actuation. This is because the injected signal is oscillating and the changes in sensor data are transmitted to the output of the victim control system via the transfer function (Eq. 2). The extracted physical feedback $y(t)$ that describes $Y(t)$ can provide necessary information for controlling the attack process. For instance, the relative time-varying power and frequency of the actuation under the perturbation can be analyzed and used by programs to gain process control.

Based on the physical feedback time series $y[n]$, we can develop our automatic approach, which continuously applies signal injection techniques to adjust $p(t)$. For example, researchers have proposed two kinds of attacks to manipulate systems based on inertial measurement units (IMUs). The *Switching attack* manipulates the oscillating digitized signal by repetitively switching the out-of-band attack signal frequency $f(t)$ [52]. The *Side-Swing attack* adjusts the attack signal amplitude A within each oscillation cycle of the induced perturbation to manipulate the accumulated effect [52]. Our prototype attack system will selectively apply these signal injection techniques to continuously adjust $p(t)$ during the attack in Sections 5 and 6.

Instead of focusing on a specific module (such as the injection), we focus on a system-level approach utilizing automatic mechanisms guided by physical side-channel feedback time series in the context of a continuous adversarial control loop.

5 SYSTEM DESIGN AND ATTACK VALIDATION

In this section, we design and implement the prototype attack system. We discuss the procedure to achieve the external adversarial control loop (ACL) on inertial sensor-actuator systems and validate the methodology on a self-balancing scooter.

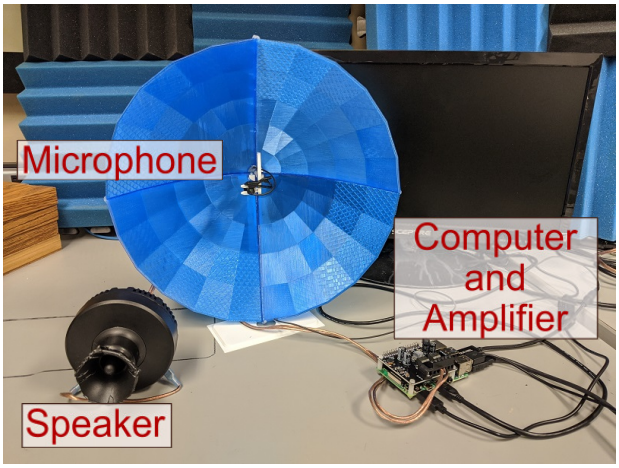

Figure 3: The hardware components of the testing system. The computer can be a desktop/laptop or an embedded device such as a Raspberry Pi.

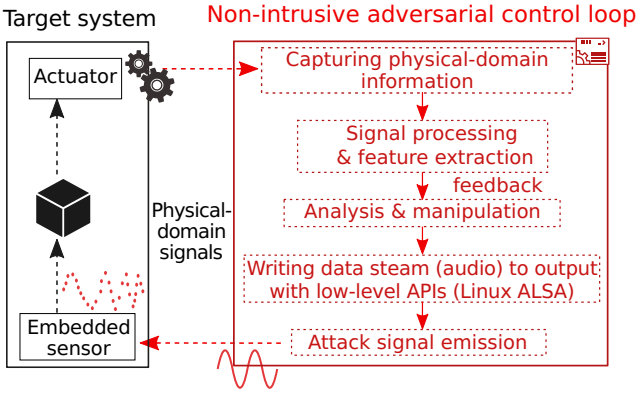

Figure 4: An illustration of the ACL implementation with the procedure and main modules used for our real-world case studies. The multi-threaded programs perform the functionalities in parallel.

5.1 Settings

Our ACL extracts the physical side-channel feedback automatically and utilizes the feedback to adjust the signal injection. The attack signals are fed to an external digital-to-analog converter (sound card) that connects to an amplifier. We use a high-output-resolution (≥96kHz) sound card and a tweeter speaker to generate the attack signals. Additionally, a microphone captures the physical side-channel acoustic signals emanated by the target system. We use a 3D-printed [9] parabolic microphone (Fig. 3) to pick up the signals.

We implement the software modules of our ACL in Python and run them on a Raspberry Pi to perform signal processing, feedback extraction, analysis, and attack signal adjusting. We implement the software signal injector module in C. This allows attack signals to be generated and continuously adjusted while writing data to the sound card without introducing extra latency. Such latency can lead to glitches and discontinuity in the attack signals. The module directly uses the low-level sound APIs (Linux ALSA [11]) to control the sound card.

Additionally, the ground truth of the victim system's motor speed is measured with a hall effect switch. It is used to provide quantitative analysis only, and its data is not used for the actual threat model.

5.2 Adversarial Control Loop Implementation

We characterize here the steps that constitute the ACL process depicted in Fig. 4 for the case study of achieving adversarial control of a Megawheels self-balancing scooter.

Capturing physical-domain signals. We capture acoustic signals emanated by the actuator of the target system. We use the parabolic microphone as a directional receiver of signals the target scooter emits.

Signal Processing and Feedback Extraction. The program first applies fast Fourier transform (FFT) to get frequency-domain features with a window size of 4,096 samples. If this window size is too small, the spectrum analysis can be less effective. However, if it is too large, the system reaction time will be slow. We select a window size of 4,096 samples to allow an update time under 0.1 seconds (0.093s with a recording sample rate of 44.1 kHz).

Fig.5 shows the frequency analysis results of acoustic signals recorded while the motor of the Megawheels self-balancing scooter is moving. We can identify that the range of sound frequencies of the actuator is from 14, 600 Hz (F_l) to 16, 900 Hz (F_h). By utilizing a Butterworth bandpass filter, we removed the noises in other frequency ranges and observed the relationship between the motor speed and the frequency-domain features more easily.

Since the strength of frequency components in the identified range $[F_l, F_h]$ is highly related to the speed of the motor (Fig.5 right), we use the sum of the magnitude of all frequency components in this range as the feedback. The ACL module extracts the feedback $y(t)$ data stream in time series

$$y[n] = \sum_{f=F_l}^{F_h} R(f, n \cdot T_c), \tag{7}$$

where $T_c \approx 0.093$ is the duration of each chunk of signals being processed, and $R(f, t)$ is the magnitude of the frequency component f at a time window $[t - T_c, t]$. Given a specific time t, only the time series of $y[1], ..., y[n]$ with $n \cdot T_c < t$ ($n \in \mathbb{Z}^+$) are available during the attack process.

Additionally, we observe that the actuator generates a part of electrically and mechanically induced acoustic noises that are not correlated to its speed. Such noises can lead to small spikes in the time series of $y[n]$. We thus effectively mitigate this effect with a simple weighted moving average filter. In detail, we get $y_0[n] = \sum_{i=0}^{k} w_i y[n-i]$. A small window size (*e.g.*, $k = 4$) works well to reduce the noise while maintaining the sensitivity.

Then we have $y_0[n] = \frac{6}{18}y[n] + \frac{5}{18}y[n-1] + \frac{4}{18}y[n-2] + \frac{3}{18}y[n-3]$. A larger value of k could increase the signal smoothness but would make the feature less sensitive to reflect the actual changes. During

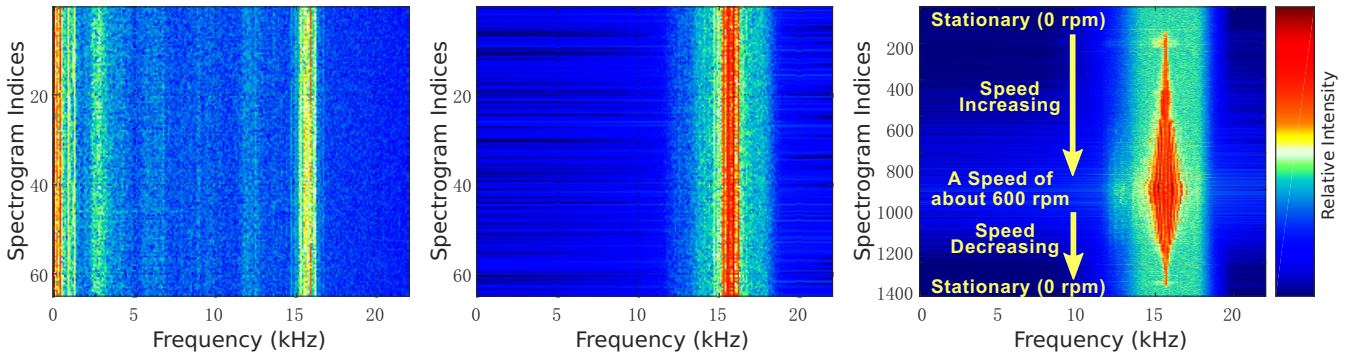

Figure 5: Left: The spectrogram of the captured acoustic signals (unfiltered) in a segment of 15 seconds while the motor is rotating with a speed of about 300 rpm. Middle: The spectrogram of signals under the same condition but with Butterworth band-pass filtering. Right: The spectrogram of the filtered acoustic signals when the motor speed is changing. We gradually change the motor speed by manually adjusting the actual heading angle of the self-balancing scooter.

the attack, the ACL module automatically processes the signals and computes the feedback.

Analysis and Manipulation. We observe that the injection induces perturbations in the system input by $X'(t) = X(t) + p(t)$ (Eq. 1), the perturbations will then be transferred to the output of the system via $Y(t) = G(X(t) + p(t))$ (Eq. 2). Therefore, the functionality of this module is to selectively adjust the attack signals to change input perturbations $p(t)$ based on the extracted feedback $y(t)$ in order to achieve targeted adversarial process control over the victim system.

We develop an automatic mechanism to adjust the injected perturbations, by designing a dynamic threshold setting method and utilizing the signal injection technique of the Switching attack [52] to inject phase offsets by repetitively switching the attack frequency.

Dynamic threshold setting. We develop a dynamic mechanism for the attack system to set a threshold and perform frequency-switching operations automatically during the manipulation stage as follows.

The attack system monitors the value of the most recent peak (K) in the time series of the side-channel feedback $y_0[n]$ and sets the threshold as $T_h = \alpha K - \beta K^2$. Then, it switches the frequency when the value of $y_0[n]$ drops and crosses this threshold. Since we want the program to switch the attack frequency when the signal is at a higher level for efficiency, we set α as a value close to 1.0 (such as 0.95). Selecting a higher threshold can also help compensate for the slight delay (δ) in the control system and the signal streaming in the ACL. We set β as 0 (or a minimal value) to adjust the threshold when $y_0[n]$ reaches a large value (such as when the motor is rotating with the maximum speed).

We also observe a drift of sample rates, which can cause disturbance in the signals and accumulate over time (Eq. 6). To mitigate this effect, our ACL automatically records two intervals between the last frequency switching operations and uses their ratio to adjust the center frequency.

In addition, we notice that implementing Switching attacks with a smaller difference (step size) between the injection frequencies results in a lower frequency of the induced movements which

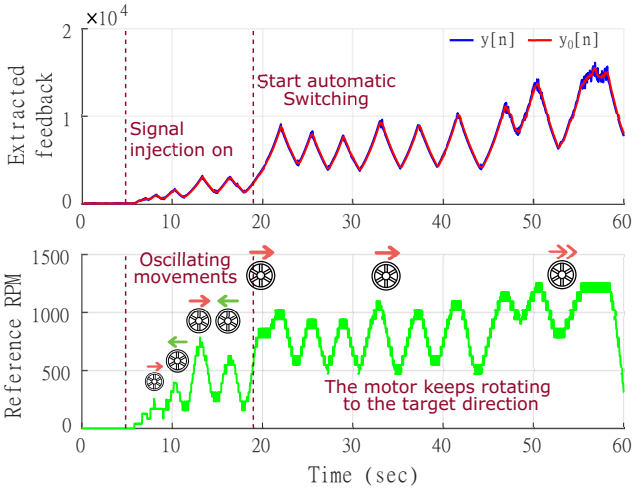

Figure 6: Before the signal injection, the scooter motor is stationary (0-5 seconds). The signal injection induces oscillating movements in the system (5-19 seconds). The automatic Switching process starts at 19 seconds. Our ACL adjusts the perturbation (attack signals) based on the extracted physical feedback to accumulate and maintain the physical property (motor speed). The reference RPM is measured with a hall effect switch to show the motor's actual speed and is not used by the attack system.

can be used to induce larger accumulative effects in the victim system within a certain amount of time. Therefore, the manipulation process can start with a larger step size and update by $step' = \gamma \cdot step, 0.8 < \gamma < 1.0$ in the adaptation rounds until a minimum step size is reached. In our experiments, we set the initial step size as 1.5 Hz, and the program would decrease it until it reaches a minimum value of 0.85 Hz during the automatic manipulation process.

Validation. We demonstrate the proof-of-concept attack on the Megawheels self-balancing scooter without accessing or tampering

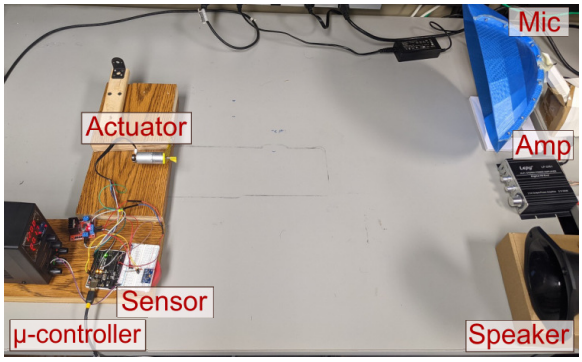

Figure 7: Our prototype testing system. In the victim system (on the left), a microcontroller controls the actuator based on the sensor measurements. The attack system (on the right) manipulates the victim system via the external adversarial control loop. The two systems are not interconnected with any communication or control interfaces.

with its internal modules. We place the speakers in proximity to the scooter. The distance range of the attack can be extended by using a higher volume and directivity horns [8, 52]. Under acoustic signal injections at its sensors' resonance frequency, the scooter presents an oscillating movement pattern that alternatively turns the wheel in different directions. This is because the oscillating signals induced in the sensor are perturbing the system, inducing shaking and oscillating movements.

Fig.6 illustrates this process. When the acoustic signal is emitted, the injected perturbations induce oscillating movements in the motor of the scooter. After the automatic switching process starts, the ACL controls the attack process based on the time series of $y_0[n]$.

During this manipulation process, the attack system automatically extracts the feedback and adjusts the attack signals to turn the scooter wheel into a target direction and manipulate its speed [1]. As shown in Fig. 6, from 19 s, the motor keeps rotating in the direction desired by the attacker and reaches a high speed by the end of the attack. The induced speed can be further adjusted in automatic Switching processes by adjusting the injected signal amplitude. The manipulation is a continuous process because the victim control system is not controlled with an instant value or event, but requires continuous control to selectively perturb the time-varying statuses and apply changes to the environment.

6 PROTOTYPE TESTING SYSTEM

In this section, we develop a prototype to study attacks on inertial sensor-actuator systems with our ACL approach. We then evaluate a proof-of-concept continuous adversarial process control over a prototype motor system. This prototype system can record how the sensor measurements change in the adversarial control process, allowing for analyzing and illustrating the quantitative results.

[1]Demos of the proof-of-concept attacks on a real-world self-balancing scooter are available at https://www.youtube.com/playlist?list=PL_l1Kb3yQ2-ZllwC31CqIG5dNzJTXObF_.

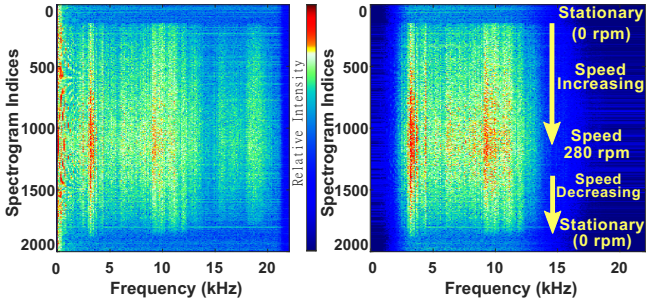

Figure 8: The spectrogram of the captured acoustic signals before (left) and after (right) filtering while the motor speeds up and slows down.

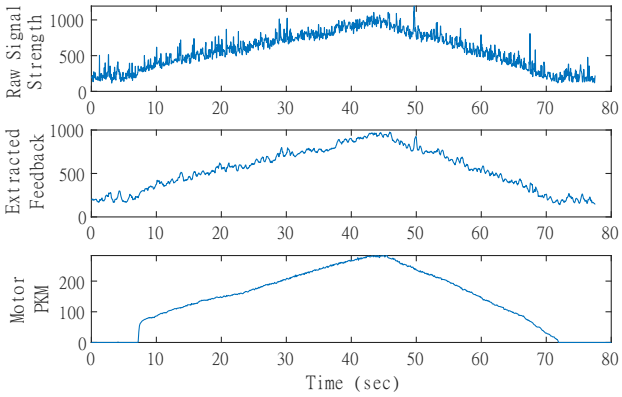

Figure 9: The extracted feedback from physical-domain signals (top and middle) is correlated with the motor speed of the victim (bottom).

6.1 Prototype Testing System Design

Fig. 7 shows our experimental setup, including a victim system and an attack system.

The victim system is composed of a microcontroller (Arduino Uno) which controls a motor in real-time based on inertial sensor measurements. The microcontroller sets the motor speed based on the heading angle measured with an IMU gyroscope sensor (MPU-9250). Unlike the self-balancing scooter, the actuator is a brushed-geared DC motor with an encoder driven by the L298N motor driver.

The attack system includes a microphone, a tweeter speaker, an audio amplifier, and a high-output-resolution sound card (*e.g.*, Sound Blaster Z). The software of the attack system runs on a Linux desktop computer. It can also run on a Raspberry Pi or laptop. The distance between the attack system and the victim system is set to 0.6 meters.

6.2 Experimental Evaluation with PFSC

We analyze the PFSC generated by the victim DC motor system. Our experimental results suggest that the motor speed can be analyzed from its physical side-channel signal emanations (Fig. 8). To prove it, we record the actual speed using the motor encoder and show that the extracted feedback is correlated with the motor speed (Fig.

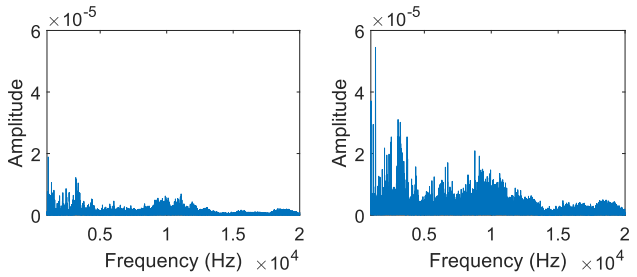

Figure 10: Signal spectrum of the motor acoustic emanations in a low speed (left)(about 100 rpm) and a high speed (right)(about 280 rpm).

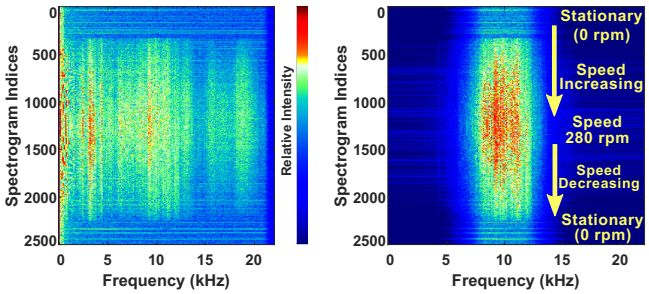

Figure 11: The spectrogram of the captured acoustic signals using a subset of the motor sound components before (left) and after (right) filtering, while the motor speeds up and slows down.

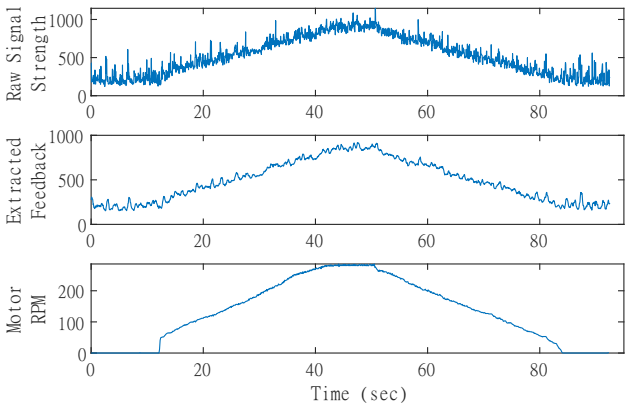

Figure 12: The extracted feedback from physical-domain signals is correlated with the motor speed even using a subset of the motor sound components.

9). Our analysis of the motor speed and sound energy in Section 4.4.1 explains this correlation.

We use the same methods as in the self-balancing scooter evaluation to derive the physical side-channel feedback. In real-world attacks, the frequency range of the motor can be identified using a few seconds of audio recorded from the motor of the victim system (Fig. 10). We also observe that using a subset of the motor sound components, we can derive similar results (Fig. 11 and Fig. 12).

6.3 Attack Evaluation

Under the effect of resonant acoustic signals, the motor of the victim system accelerates and decelerates in an oscillating pattern. This is because the perceived heading angle of the system fluctuates under the perturbation of the injected signal as observed for the scooter motor.

Fig. 14 shows the internal statuses of the victim system in this continuous process. We can observe that under the effect of acoustic resonant signals, the system's perceived heading angle fluctuates and falls back after each cycle. Under the interference, the victim system periodically accelerates and decelerates, and its speed fluctuates in an oscillating pattern.

The attack system leverages the physical feedback (Fig. 13) automatically extracted from physical-domain signals to guide the attack. Then, it adjusts the attack signals in relation to the motor speed without accessing the internal statuses of the victim system. After the automatic Side-Swing process starts, the attack system automatically performs amplitude adjusting of the attack signals within each cycle of the induced oscillation to selectively increase or decrease the heading angle.

Specifically, the ACL utilizes the most recent physical feedback time series before starting the automatic Side-Swing attacks. It computes the period of the oscillation p_0 and an average value as a threshold $\sum_{j=0}^{N} \frac{y_0[n-j]}{N}$ in the recent N samples of the time series (we use $N = 100$ samples). It then records the most recent time T_0 and direction when the feedback signal crosses the threshold. After the automatic Side-Swing attack starts, the system will adjust the amplitudes alternatively at an interval of half of the oscillation period ($\frac{p_0}{2}$) at specific times: $T_0 + k\frac{p_0}{2} - T_{offset} (k = 1, 2, 3, ...)$, where T_{offset} is the sum of a phase delay and a small real-time delay in the systems. The phase delay is $\frac{p_0}{4}$ between the oscillating injected signal in the gyroscope and the accumulated heading angle. Leveraging the time intervals, the system can adjust the amplitude of attack signals to drive the motor in the direction desired by the attacker.

To further demonstrate program-controlled processes in the ACL, we program the following procedure: The program in the attack system first controls the motor to speed up twice and maintain the speed. Then it controls the motor to slow down, and finally speed up twice and maintain the speed. The attack system automatically analyzes the extracted feedback and adjusts the attack signals to complete the procedure (Fig. 14).

7 DISCUSSION

7.1 Limitations

We implemented the proof-of-concept ACL methodology with limited signal power and off-the-shelves hardware components. Our proof-of-concept implementation does not address the attacker's distance from the victim challenge. However, the usage of the parabolic microphone would allow for the execution of our approach at a further distance. Additionally, motivated attackers can launch more powerful attacks with more sophisticated equipment such

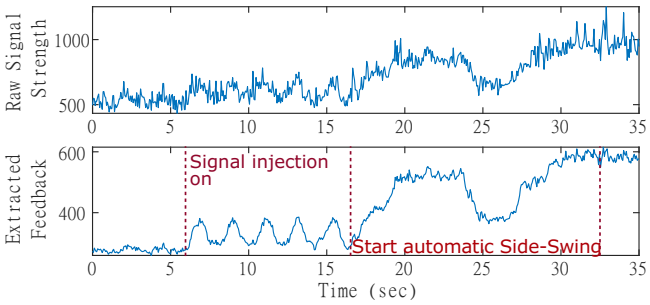

Figure 13: The physical side-channel feedback is automatically extracted from acoustic emanations of the victim motor. The induced oscillating movements (5.5-17 s) in the victim system perturbed by the signal injection can also be observed from the time series of the feedback. After the automatic Side-Swing process starts (after 17 s), the attack system automatically adjusts the attack signals to control the victim system.

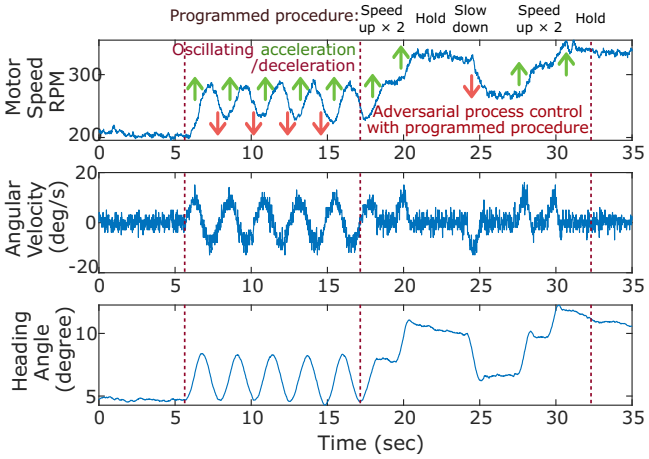

Figure 14: The speed and internal sensor measurements of the victim system in the process of adversarial control. We can observe how the induced perturbations in the sensor (middle) affect the perception (bottom) and the actuation (top) of the victim control system in a continuous process. The attack system performs the programmed procedure to continuously control the motor speed (from 17 s).

as long-range acoustic devices [4, 10] and sonars/radars that can transmit the attack signals over long distances.

We show that it is possible to construct an external adversarial control loop for process control to significantly increase the attacker's capabilities, even though the adversarial process control is not as precise as having access to data from the victim's internal control loop in the victim system. This is also due to the fact that our control mechanism is constructed externally, based on implicit analog channels instead of explicit digital interfaces that directly control the system. Because the nature of most actuators is to transduce electricity into other forms of physical properties, the actuators will inevitably emit electromagnetic or mechanical (*e.g.*, acoustic) signals during their operations. This paper focuses on proving the concept of such an attack scenario. Generally, the PFSC will exist, but making use of it can be difficult, depending on the attacker's capability and available budget to retrieve it (*e.g.*, using more sensitive and accurate equipment).

Finally, because the adversarial control loop is built externally over the original internal control loop (Fig. 1), the adversarial control loop will almost always exhibit a delay compared to direct digital control. Adjustments over time may be necessary if high-speed responses are required. Future research could explore whether incorporating more advanced control methods into the adversarial control loop can mitigate such delay.

7.2 Future Work Directions

In the future, the methodology could be applied to other process control systems (such as self-balanced platforms and telepresence control systems that control robotic devices based on the inertial sensor measurements) that have sensors that are subject to physical signal injections and actuators that have PFSCs.

By developing our ACL, future research can construct testbeds that enable automatic security testing of sensor-based control systems in programmed, continuous processes without connecting to the internal modules of embedded systems. Additionally, more robust physical feedback extraction methods can be developed using a combination of measuring devices in attacks on complex systems. Further, future works can extend our approach to processes that continuously control other physical properties such as blood glucose level [28, 44].

Future works can investigate shielding or obfuscating the side-channel signal emanations to mitigate/disrupt the physical feedback side channel. However, it may be challenging to completely shield the emanations of actuators in the physical world. It might be possible to obfuscate the side-channel signals by intentionally generating physical signals with additional signal-emitting devices or conducting obfuscated/randomized operations with the actuator to mask the side channel. This, however, will require carefully evaluating the trade-off between security and performance of the system to be protected.

7.3 Countermeasures

Low-pass filtering was recommended to mitigate or eliminate out-of-band injections [37, 51]. However, sensors with low-pass filters can still be vulnerable to the attacks. For instance, the datasheets of certain inertial sensors [2, 3] specified the use of analog low-pass filters, but these sensors were still found vulnerable to attacks [52]. Realizing ideal anti-aliasing filters that eliminate all out-of-band signals may be non-trivial. For instance, a high-order filter that removes all signals above the cutoff frequency will cause signals that change rapidly to ring on for a long time. Moreover, analog filters lead to an unequal time delay as a function of frequency [1]. If the phase delay introduced by filters is large, the circuit performance may not be desirable [24].

Researchers studied **sampling-based methods** to obfuscate attack effects with randomized sampling [51] or cancel a frequency component by adding two samples based on a delay calculated from

a known frequency [51]. However, it can be challenging to cancel injected signals because the sensors are usually vulnerable in one or more frequency ranges instead of a single, previously determined frequency [46, 51, 52]. Further, these methods did not necessarily detect and report the attacks.

Recent work studied **purely software-based detection methods** [49] including a machine learning method and a sensor fusion method using the magnetometer and gyroscope. However, false positives/negatives can occur under environmental movements or when injected data differ from the assumed patterns. The researchers also noted that attacks that influence more than one sensor [40] can defeat fusion-based detection methods [49]. Another strategy is to implement **signal processing techniques**, like filtering or machine learning algorithms, to detect and eliminate the effects of acoustic interference on the sensor's output. This can be combined with redundant sensor arrays to provide more reliable and accurate motion tracking in the presence of interference. However, this approach usually assumes only one sensor is under attack. Moreover, it remains to be investigated how to detect the attacks without false alarms that may affect the usability and safety of the system. For instance, the system may fail to respond to an emergent or sudden event, such as a crash, if the inertial sensor data were falsely classified as the result of an attack.

Moreover, **shielding** can mitigate malicious acoustic or EMI signals by a finite amount. However, it can be difficult to completely shield the sensors without causing heat dissipation, cost, size, and usability issues. Although shielded sensors may still be vulnerable to attacks [53], isolating the sensor from the surrounding environment using damping materials or enclosures can help mitigate the effect of acoustic resonance on MEMS inertial sensors by reducing the exposure to external noise sources.

Additionally, recent works [54, 61] proposed detection and correction methods for electromagnetic signal injection attacks on sensors. These defense methods can work for post-transducer stage sensor signal injection attacks [20, 27, 28, 30, 36, 37, 53, 57], but may not apply to transducer-stage attacks such as acoustic attacks that inject signals via the resonance of the sensing-mass transducer structure of inertial sensors.

8 RELATED WORK

Acoustic Attacks on Inertial Sensors. Prior works showed that resonant acoustic attacks can disrupt inertial sensor-based systems [18, 31, 46, 56]. Accelerometer measurements can be manipulated by monitoring and adjusting the induced signals in the sensor output [51]. Researchers demonstrated attacks on embedded systems to control the actuation [52]. However, these attacks on inertial sensor-actuator systems were typically based on manually tuning the acoustic signals. Moreover, the researchers investigated automated attacks with digital sensor data feedback using JavaScript and mobile apps to manipulate navigation systems (Google Maps) and VR applications [52].

Physical-Domain Signal Injection Attacks on Sensors. Researchers have utilized different kinds of physical signals such as electromagnetic, ultrasonic, and light signals in sensor attacks [19, 26, 58] on smart voice assistants [23, 32, 33, 37, 47, 55, 57, 59, 60]. These attacks explored the physical-level risks of exploiting sensors by transmitting determined signals (*e.g.*, recorded voice) modulated in specific, out-of-band carriers to maliciously trigger an event in the victim system. Different from triggering instant events, our work studies the threats in continuous control processes. Many physical properties, such as temperature, pH levels, and angles, are controlled in a continuous process rather than an instantly triggered event.

In comparison to prior works, this paper focuses on adversarial process control over inertial sensor-actuator systems without digital sensor data feedback. Our attack system analyzes the time series of physical feedback coming from the victim system in the form of side-channel signals, and leverages software-controlled mechanisms to adjust the adversarial control process. To the best of our knowledge, this work is the first to 1) construct an external adversarial control loop that continuously computes the attack signals to control the process without accessing the internal statuses or digital interfaces of the victim system, and 2) characterize the physical feedback side channel as a complementary methodology in out-of-band signal injection attacks [26] and explore its use on continuous process control systems.

9 CONCLUSION

This research investigated an external, physical adversarial control loop methodology for manipulating inertial sensor-actuator systems in continuous attack processes. Unlike conventional control systems, the adversarial control loop mechanisms are constructed externally without connecting to the internal modules and statuses of the system. In our case studies, we developed an attack system comprising various parallel modules. By automatically extracting and utilizing the time series of physical side-channel feedback, the external attack system can continuously adjust the attack signals to achieve the desired process control over the victim system.

ACKNOWLEDGEMENT

The authors thank the anonymous reviewers and our shepherd Marina Krotofil for their valuable comments that improved this paper. This work is supported in part by the US NSF under grants OIA-1946231, CNS-2117785, OIA-2229752, CNS-2231682, and two gifts from Meta.

REFERENCES

[1] 1996. Problems with the Anti-aliasing Filter. https://ccrma.stanford.edu/CCRMA/Courses/252/sensors/node35.html. Tim Stilson, 1996-10-17.
[2] 2012. STMicroelectronics LSM330 datasheet. www.st.com/resource/en/datasheet/dm00037200.pdf. Accessed: 2018-06-14.
[3] 2013. STMicroelectronics L3GD20 datasheet. http://www.st.com/en/mems-and-sensors/l3gd20.html. Accessed: 2017-06-12.
[4] 2015. L. Corporation, LRAD 2000X datasheet. https://genasys.com/wp-content/uploads/2015/06/LRAD_Datasheet_2000X.pdf. Accessed: 2022-01-12.
[5] 2019. Boston Dynamics' Handle robot brings mobile manipulation to logistics. https://www.therobotreport.com/boston-dynamics-handle-robot-pallets/. Steve Crowe, 2019-03-28.
[6] 2019. Handle - ROBOTS. Boston Dynamics. https://robots.ieee.org/robots/handle/. 2019.
[7] 2020. DJI Osmo Mobile 3 review. https://www.techradar.com/reviews/dji-osmo-mobile-3-review. Basil Kronfli, 2020-01-15.
[8] 2021. Myskunkworks 10" Long-Range Horn. http://myskunkworks.net/index.php?route=product/product&path=61&product_id=63. Accessed: 2021-05-05.
[9] 2021. An open-source parabolic reflector design. https://www.thingiverse.com/thing:2721955. Accessed: 2021-08-28.
[10] 2022. UltraElectronics HyperShield datasheet. https://www.nixalite.com/SiteContent/Documents/PDFs/HyperShield.pdf. Accessed: 2022-01-07.

[11] 2023. Advanced Linux Sound Architecture (ALSA) project homepage. https://www.alsa-project.org/wiki/Main_Page.

[12] 2023. DIRECTIONAL MICROPHONE FOR LONG-RANGE SURVEILLANCE. https://ampflab.com/. Accessed: 2023-08-28.

[13] Jürgen Altmann. 2001. Acoustic weapons-a prospective assessment. *Science & Global Security* 9, 3 (2001), 165–234.

[14] Riccardo Antonello, Roberto Oboe, et al. 2011. *MEMS gyroscopes for consumers and industrial applications*. InTech.

[15] Roberto Antonucci, Annalisa Porcella, and Vassilios Fanos. 2009. The infant incubator in the neonatal intensive care unit: unresolved issues and future developments. *Journal of perinatal medicine* 37, 6 (2009), 587–598.

[16] Edward F Bell. 2006. Servocontrol: Incubator and radiant warmer. *Iowa Neonatology Handbook* (2006).

[17] Ariful Islam Bhuyan and Tuton Chandra Mallick. 2014. Gyro-accelerometer based control of a robotic Arm using AVR microcontroller. In *9th International Forum on Strategic Technology (IFOST)*. IEEE.

[18] 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.

[19] Yulong Cao, Chaowei Xiao, Benjamin Cyr, Yimeng Zhou, Won Park, Sara Rampazzi, Qi Alfred Chen, Kevin Fu, and Z Morley Mao. 2019. Adversarial sensor attack on lidar-based perception in autonomous driving. In *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*. 2267–2281.

[20] Gökçen Yilmaz Dayanikli, Rees R Hatch, Ryan M Gerdes, Hongjie Wang, and Regan Zane. 2020. Electromagnetic sensor and actuator attacks on power converters for electric vehicles. In *2020 IEEE Security and Privacy Workshops (SPW)*. IEEE, 98–103.

[21] Robert Neal Dean, Simon Thomas Castro, George T Flowers, Grant Roth, Anwar Ahmed, Alan Scottedward Hodel, Brian Eugene Grantham, David Allen Bittle, and James P Brunsch. 2010. A characterization of the performance of a MEMS gyroscope in acoustically harsh environments. *IEEE Transactions on Industrial Electronics* 58, 7 (2010), 2591–2596.

[22] Robert N Dean, George T Flowers, A Scotte Hodel, Grant Roth, Simon Castro, Ran Zhou, Alfonso Moreira, Anwar Ahmed, Rifki Rifki, Brian E Grantham, et al. 2007. On the degradation of MEMS gyroscope performance in the presence of high power acoustic noise. In *2007 IEEE International Symposium on Industrial Electronics*. IEEE, 1435–1440.

[23] 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).

[24] M. Sami Fadali and Antonio Visioli. 2020. Chapter 12 - Practical issues. In *Digital Control Engineering (Third Edition)* (third edition ed.), M. Sami Fadali and Antonio Visioli (Eds.). Academic Press, 567–614. https://doi.org/10.1016/B978-0-12-814433-6.00012-0

[25] Juan A Gallego-Juárez, G Rodriguez-Corral, and L Gaete-Garreton. 1978. An ultrasonic transducer for high power applications in gases. *Ultrasonics* 16, 6 (1978), 267–271.

[26] 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.

[27] 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 (ESORICS)*. 512–532.

[28] Xiali Hei and Yazhou Tu. 2021. Glucose monitorying method and system. US Patent App. 16/952,692.

[29] Yusuke Hirao, Weiwei Wan, Dimitrios Kanoulas, and Kensuke Harada. 2023. Body Extension by Using Two Mobile Manipulators. *Cyborg and Bionic Systems* 4 (2023), 0014.

[30] Md Imran Hossen, Yazhou Tu, and Xiali Hei. 2023. A First Look at the Security of EEG-based Systems and Intelligent Algorithms under Physical Signal Injections. In *Proceedings of the 2023 Secure and Trustworthy Deep Learning Systems Workshop*. 1–8.

[31] Xiaoyu Ji, Yushi Cheng, Yuepeng Zhang, Kai Wang, Chen Yan, Wenyuan Xu, and Kevin Fu. 20201. Poltergeist: Acoustic Adversarial Machine Learning against Cameras and ComputerVision. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE.

[32] Xiaoyu Ji, Juchuan Zhang, Shui Jiang, Jishen Li, and Wenyuan Xu. 2021. CapSpeaker: Injecting Voices to Microphones via Capacitors. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. 1915–1929.

[33] 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.

[34] PK Kavale, Mohini Amritkar, and Sakshi Joshi. 2022. DESIGN AND DEVELOPMENT OF SELF BALANCING PLATFORM. (2022).

[35] Victor Klemm, Alessandro Morra, Ciro Salzmann, Florian Tschopp, Karen Bodie, Lionel Gulich, Nicola Küng, Dominik Mannhart, Corentin Pfister, Marcus Vierneisel, et al. 2019. Ascento: A two-wheeled jumping robot. In *2019 International Conference on Robotics and Automation (ICRA)*. IEEE, 7515–7521.

[36] Sebastian Köhler, Richard Baker, and Ivan Martinovic. 2021. Signal Injection Attacks against CCD Image Sensors. *arXiv preprint arXiv:2108.08881* (2021).

[37] 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.

[38] Yan Long, Sara Rampazzi, Takeshi Sugawara, and Kevin Fu. 2021. Protecting COVID-19 Vaccine Transportation and Storage from Analog Cybersecurity Threats. *Biomedical Instrumentation & Technology* 55, 3 (2021), 112–117.

[39] Ralph P Muscatell. 1984. Laser microphone. *The Journal of the Acoustical Society of America* 76, 4 (1984), 1284–1284.

[40] Shoei Nashimoto, Daisuke Suzuki, Takeshi Sugawara, and Kazuo Sakiyama. 2018. Sensor CON-Fusion: Defeating Kalman filter in signal injection attack. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*. 511–524.

[41] Steven Nasiri. 2009. A critical review of MEMS gyroscopes technology and commercialization status. (2009). InvenSense whitepaper (2009).

[42] Vittorio MN Passaro, Antonello Cuccovillo, Lorenzo Vaiani, Martino De Carlo, and Carlo Edoardo Campanella. 2017. Gyroscope technology and applications: A review in the industrial perspective. *Sensors* 17, 10 (2017), 2284.

[43] Gianni Pavan, Gregory Budney, Holger Klinck, Hervé Glotin, Dena J Clink, and Jeanette A Thomas. 2022. History of sound recording and analysis equipment. *Exploring Animal Behavior Through Sound: Volume 1: Methods* (2022), 1–36.

[44] Md Fazle Rabby, Yazhou Tu, Md Imran Hossen, Insup Lee, Anthony S Maida, and Xiali Hei. 2021. Stacked LSTM based deep recurrent neural network with kalman smoothing for blood glucose prediction. *BMC Medical Informatics and Decision Making* 21 (2021), 1–15.

[45] 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.

[46] 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.

[47] 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.

[48] Shintaro Takeda, Ikuharu Morioka, Kazuhisa Miyashita, Akeharu Okumura, Yoshiaki Yoshida, and Kenji Matsumoto. 1992. Age variation in the upper limit of hearing. *European journal of applied physiology and occupational physiology* 65, 5 (1992), 403–408.

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

[50] Jing Tian, Wenshu Yang, Zhenming Peng, Tao Tang, and Zhijun Li. 2016. Application of MEMS accelerometers and gyroscopes in fast steering mirror control systems. *Sensors* 16, 4 (2016), 440.

[51] 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.

[52] 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.

[53] 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.

[54] 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.

[55] Yuanda Wang, Hanqing Guo, and Qiben Yan. 2022. GhostTalk: Interactive Attack on Smartphone Voice System Through Power Line. *arXiv preprint arXiv:2202.02585* (2022).

[56] 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).

[57] Zhifei Xu, Runbing Hua, Jack Juang, Shengxuan Xia, Jun Fan, and Chulsoon Hwang. 2021. Inaudible Attack on Smart Speakers With Intentional Electromagnetic Interference. *IEEE Transactions on Microwave Theory and Techniques* 69, 5 (2021), 2642–2650.

[58] 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.

[59] Qiben Yan, Kehai Liu, Qin Zhou, Hanqing Guo, and Ning Zhang. 2020. Surfingattack: Interactive hidden attack on voice assistants using ultrasonic guided waves. In *Network and Distributed Systems Security (NDSS) Symposium*.

[60] 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.

[61] 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.