Volttack: Control IoT Devices by Manipulating Power Supply Voltage

Kai Wang*, Shilin Xiao*, Xiaoyu Ji*, Chen Yan*‡, Chaohao Li† and Wenyuan Xu*
*Ubiquitous System Security Lab (USSLAB), Zhejiang University
†Hangzhou Hikvision Digital Technology Co., Ltd.
{eekaiwang, xshilin, xji, yanchen, wyxu}@zju.edu.cn, lichaohao@hikvision.com

***Abstract*—This paper analyzes the security of Internet of Things (IoT) devices from the perspective of sensing and actuating. Particularly, we discover a vulnerability in power supply modules and propose `Volttack` attacks. To launch a `Volttack` attack, attackers may compromise the power source and inject malicious signals through the power supply module, which is indispensable in most devices. Eventually, `Volttack` attacks may cause the sensor measurement irrelevant to reality or maneuver the actuator in a way disregarding the desired command. To understand `Volttack`, we systematically analyze the underlying principle of power supply signals affecting the electronic components, which are building blocks to constitute the sensor or actuator modules. Derived from these findings, we implement and validate `Volttack` on off-the-shelf products: 6 sensors and 3 actuators, which are used in applications ranging from automobile braking systems, industrial process control to robotic arms. The consequences of manipulating the sensor measurement or actuation include doubled car braking distance and a natural gas leak. The root cause of such a vulnerability stems from the common belief that noises from the power line are unintentional, and our work aims to call for attention to enhancing the security of power supply modules and adding countermeasures to mitigate the attacks.**

1. Introduction

The Internet of Things (IoT) is a network of billions of connected devices, ranging from autonomous vehicles to robotic arms in the assembly lines. With advances in sensing and actuating technologies, these IoT devices allow the digital world to interact with the physical world at a level of autonomy that was never seen before. The correct measurement of sensors and maneuvering of the actuators are the foundation to ensure the safe operation of IoT-enabled applications, e.g., consumer or industrial applications. For instance, a batch reactor at a British dye factory was reported to be exploded because the temperature was over-cooled by around 10°C [1]. In this paper, we analyze the security of IoT devices from the perspective of sensing and actuating. Particularly, we discover a vulnerability in power supply modules, which are indispensable inside IoT devices to drive the hardware of sensing and actuating.

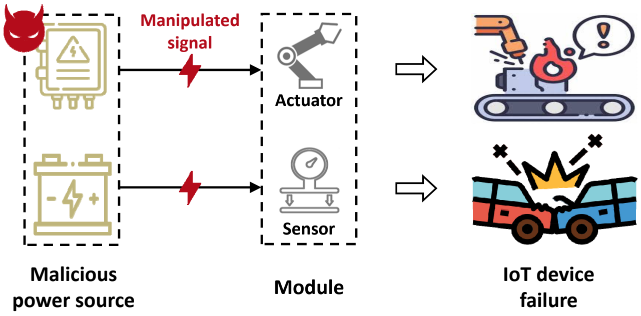


Figure 1. An illustration of `Volttack`. An attacker injects a malicious signal through the power source and eventually tampers the output of critical modules inside IoT devices, e.g., sensors or actuators, causing device failures.

As shown in Figure 1, we envision that an attacker may compromise the power source and inject malicious signals through the power supply module. As these malicious signals propagate through the circuits of both sensors and actuators, they affect the outputs of electronic components constituting the underlying circuit one by one and may eventually cause the sensor measurement irrelevant to reality or maneuver the actuator in a way disregarding the desired command. We call such an attack `Volttack`, and `Volttack` exploits a new type of attack surface that has far-reaching consequences, because it allows attackers to manipulate IoT devices from the physical world, i.e., possibly through a wall socket, unlike from the counterpart digital world that requires compromising the firmware [2–4] or injecting fault data [5–7].

`Volttack` may sound infeasible because modern power supply modules should have adopted abundant noise reduction measures, e.g., voltage regulators and filters, to ensure a stable voltage supply, and thus should eliminate the malicious signals, if any. Not to mention that the large variety and complexity of IoT device hardware will make it difficult, if not impossible, to predict the sensor or actuator operation for a given injected signal over the power supply. Nevertheless, we implemented `Volttack` and validated on 6 sensors and 3 actuators, which are used in applications ranging from automobile braking systems to industrial process control to robotic arms. In summary, we have achieved the following manipulations.

‡. Corresponding author

- For a force sensor (DYTB-002) that is used to measure the force pressure of a driver onto the brake pedal, injecting a signal of 1V at a frequency of 342MHz to the 24V operating voltage can decrease the sensor output by 122N, which is half of the real force and can cause the braking distance to be doubled.
- For a temperature sensor (DHT11) that is used to measure industrial environment temperature, injecting a signal of 0.5V at a frequency of 121MHz to the 12V operating voltage can increase the sensor output by 139°C, which may lead to false excess cooling, a key cause of the British dye factory explosion.
- For a servo (Futaba S9602) that is used to control the joint rotation of robotic arms, injecting a signal of 1.3V at a frequency of 314MHz to the 5.5V operating voltage can rotate the joint 58.4 degrees clockwise, which may jeopardize production or even injure the nearby operator.
- For a valve (Fulaite 05) that is used in the flow control of natural gas, injecting a signal of 0.5V at a frequency of 75MHz to the 5V operating voltage can open the closed valve to 34%, which may cause a gas leak.

To understand the root causes of Volttack, we answer the following questions.

Why can malicious signals be successfully injected over a power supply regardless of the noise reduction or electromagnetic compatibility (EMC) test? Power supply modules are designed with a common belief that noises from the power line are unintentional and thus EMC tests suffice. However, EMC test signals are recommended to cover the frequency range of 150kHz to 80MHz according to the EMC test standard for power supply [8], and the frequencies of most the Volttack signals are between 80MHz and 500MHz. Thus, EMC tests are insufficient to cope with intentional noise injection on the power supply. Moreover, although low-pass filters inside the power supply are supposed to remove high-frequency noises, the filters in reality may fail to eliminate such signals due to the non-ideal characteristics of electronic components and unavoidable parasitic components. Finally, the trend of miniaturization and cost constraints of IoT devices is not helping the noise reduction performance of the power supply module.

How does the power supply affect the output of sensors or actions of the actuators? Injecting noises will cause the power supply to output a signal that has a frequency or amplitude higher or lower than the designed range. To understand the underlying principle of Volttack, we investigate the behaviors of the building blocks of sensors and actuators, i.e., the electronic components, when the power supply is outside of the recommended range. We discover that the power supply signal can affect the components in two ways: it can act as an interfering input that is superimposed to the real input of a component, and it can also change the transfer function of a component, i.e., modifying the input/output relationship.

In summary, this work serves as an initial attempt that challenges the common design principle of power supplies and shows that the EMC test is insufficient to ensure security. We recommend designers pay attention to the high-frequency noises on the power line and the consequences of non-ideal characteristics of electronic components. Our main contributions are as follows:

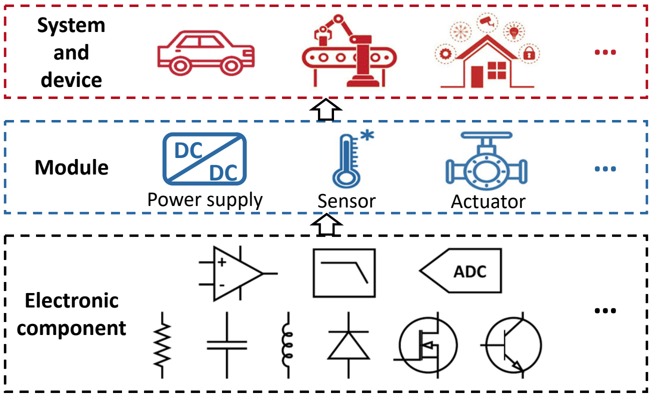


Figure 2. An illustration of the building blocks of an IoT system, and from top to bottom, they are IoT systems or devices, modules, and electronic components, whereby electronic components form the modules that constitute IoT devices.

- We discovered a vulnerability in the power supply, i.e., manipulating power supply signals can affect the output of IoT devices, and call for attention in designing future power supply modules.
- We systematically analyze the underlying principle of power supply signals affecting the electronic components and the output of IoT devices.
- We propose Volttack which can control IoT devices by injecting elaborated power supply signals. We demonstrate Volttack on off-the-shelf products, including 6 sensors and 3 actuators, and provide suggestions to cope with such attacks.
- We perform end-to-end attacks with three methods[1]: fabricating a malicious battery with the attack devices embedded, placing a current injection probe on the power cable, and connecting the attack devices to the power network using a customized coupler.

2. Background

To understand the underlying principle of Volttack, this section introduces the background of IoT devices from three levels, and from large to small they are the IoT device and system level, the module level, and the electronic component level, respectively, as illustrated on Figure 2.

2.1. IoT Devices

The Internet of Things (IoT) is the network of physical objects that are capable of connecting and exchanging data with other devices over the Internet for the purpose of serving various applications, e.g., smart manufacturing, home automation, or self-driving [9]. IoT devices, such as smart

[1] Video demo: https://github.com/USSLab/Volttack

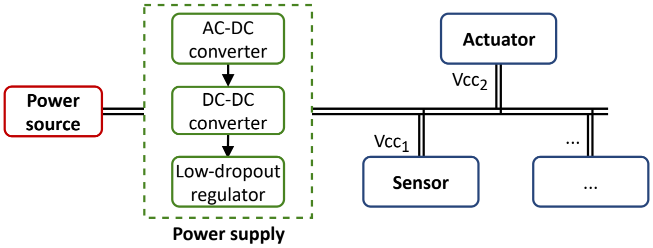


Figure 3. An illustration of the power supply. The power supply circuits draw power from the power source and provide multiple power supply voltage rails to other modules, such as sensors and actuators.

speakers, consist of multiple modules, e.g., at least a power supply module, a sensing module, a computing module, and an actuation module, such that they can perceive the environment, make decisions, and control the physical world. We introduce these modules in the following subsections.

2.2. Power Supply Module

A power supply module is responsible for providing electricity to a device and is indispensable to most IoT devices. As shown in Figure 3, a power supply module typically draws electricity from an *electrical power source* and outputs multiple levels of voltage rails to satisfy the various requirements of the circuits. An *electrical power source* can be categorized into two types: Alternating Current (AC) source and Direct Current (DC) source. A low-power device typically directly draws power from a DC source, e.g., batteries or a USB socket, and a high-power device typically acquires power from an AC source, e.g., socket outlets connected to the power grid. The circuit of a power supply module may include an AC-DC converter, a DC-DC converter, and a low-dropout regulator (LDO). Ideally, the LDO and filters are added to eliminate all power supply noise to protect devices from interference [10, 11], yet we will demonstrate that these protection methods can not completely eliminate elaborated noises from the power supply. As these noises are propagated through multiple voltage rails to affect numerous modules, they may cause widespread failure.

PSRR: Power Supply Rejection Ratio (PSRR) is an important electrical parameter used to describe the ability of the power supply module to reject fluctuations such as noise and ripple [12]. PSRR can be defined as the log ratio of voltage change at the input ΔV_{input} to the voltage change at the output ΔV_{out}. An ideal power supply module has an extremely large PSRR, indicating that the output voltage remains unchanged when the input voltage fluctuates. PSRR varies with the frequency of ΔV_{input}. It is unlikely to obtain excellent PSRR performance in the full frequency band, considering the design cost and technical difficulty. To be realistic, designers focus on improving PSRR performance over the frequency range of the noises that are most likely to present, e.g., switching noise. Generally, PSRR worsens with the increases of the frequency [13]. Thus, the higher frequency noises are, the easier it is to affect the output of the power supply module.

2.3. Sensor and Actuator Module

The sensor and actuator modules are the interfaces between the physical world and the digital world. The sensors measure the process variables such as pressure, temperature and humidity, and they typically perceive analog signals in the real world and convert them into digital signals. The output of sensors determines the system's decision. Actuators convert the energy from pneumatic, hydraulic, or electric to mechanical. In this paper, we focus on electric actuators and refer to them as actuators.

2.4. Electronic Components

The power supply, sensor, and actuator modules are all composed of electronic components, which are elements of the circuit and include resistors, capacitors, inductors, amplifiers, etc. We divide the electronic components into two categories: *elementary electronic components* and *compount electronic components*. Elementary electronic components are the smallest unit of electronic circuits, e.g., resistors and transistors. Compound electronic components are composed of multiple elementary electronic components with the goal of performing complex functions, e.g., transducers, amplifiers, filters, and data converters.

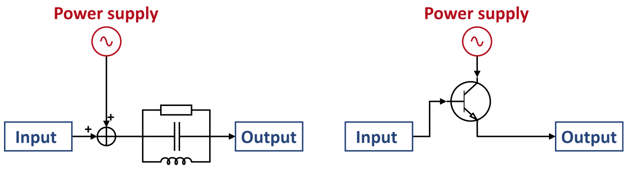
A transducer transforms physical quantity into an electrical quantity or vice versa. An amplifier increases the power of a signal and the most commonly used amplifier is an operational amplifier (op-amp). An op-amp is frequently used for signal amplification, signal conditioning, active filter, etc. [14]. A filter is typically designed to eliminate the undesired noise, and a data converter is the bridge of analog signal and digital signal.

The aforementioned compound electronic components are composed of elementary electronic components, and can be divided into passive components and active components. The passive components do not require energy to operate, and include resistors, capacitors, inductors, and diodes. Active components, such as transistors, require a source of energy to perform their functions of signal processing.

3. Threat Model

This work studies the vulnerability of the power supply that drives sensors and actuators, and the effect of power supply noise on electronic components to reveal a widespread vulnerability. By exploiting the vulnerabilities, an attacker can control the victim's IoT devices by manipulating the power supply voltage. We assume that the attacks have the following goal and capabilities.

- **Manipulating IoT devices:** The goal of the attacker is to control the sensor output and actuator behavior such that she can achieve malicious consequences, e.g., tampering with the decision of the IoT system by



(a) Interfering with input signal.
(b) Modifying the behaviour.

Figure 4. Illustration of two methods in which the power supply signals affect the output signal. (a) Power supply signals may interfere with the processed signal through a network of electronic components. (b) Power supply signals may change the behavior of the electronic components, thereby modifying the input/output relationship.

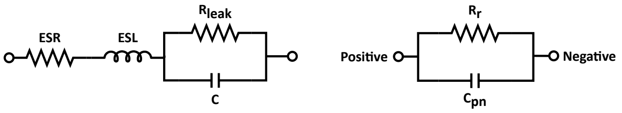
spoofing the environmental perception or causing an accident by controlling the behavior of the actuators.

- **Accessibility to power source:** The attacker may be a malicious employee, a maintenance worker or a guest who has one-time access to the power supply source of the target IoT device. To set up the attack, the attacker can add an attack device to the power supply source, e.g., a power socket, charging station or power distribution cabinet, or replace the original power supply source. For example, the attacker may place a current injection probe on the power cable or connect the attack devices to the power network using a customized coupler. She may also fabricate malicious power adapters or batteries with the attack device embedded and replace the original ones during maintenance. After deployment, the attack device can be controlled remotely by the attacker.
- **Device awareness:** The attacker knows the victim's device model and can acquire a device of the same model to study beforehand.

4. How Does Power Supply Affect Electronic Components?

Sensing and actuating are enabled by analog circuits that are made of various interconnected electronic components. To understand why power supply can affect the output and behavior of sensors and actuators, it is essential to first characterize how power supply affects the underlying electronic components. In this section, we break analog circuits into the most common types of elementary electrical components, i.e., resistors, capacitors, inductors, diodes, and transistors, and study the power supply's impact on them. Moreover, we investigate whether such effects still exist when elementary electrical components are packed into compound electronic components that are common in sensors and actuators, such as voltage regulators, amplifiers, and data converters.

For elementary electronic components, we categorize the power supply's effect into two basic mechanisms: ***interfering with the input*** and ***modifying the behavior***, as illustrated in Figure 4. In the first mechanism, the power supply signal is superimposed on the input of an electronic component, and power noises may act as an interfering input that directly changes the component's output. In the second mechanism, the power supply signal drives the electronic component and may modify its input/output relationship. As a result, power noises may indirectly change the component's output even if the input is kept still. In practice, the specific mechanism that takes effect depends on the electronic component and its signal path to the power supply, and both mechanisms may apply to a component at the same time. In the following, we elaborate on the two mechanisms by their effects on individual elementary electronic components.



(a) Capacitor model.
(b) Diode model.

Figure 5. Equivalent model for a real capacitor and a reverse-biased diode. (a) A real capacitor is equivalent to an RLC network. (b) A reverse-biased diode is equivalent to a reverse resistor in parallel with a depletion layer capacitance and shows low impedance to high-frequency signal.

4.1. Interfering with the Input

This mechanism can apply to most elementary electronic components, especially the passive ones such as resistors, capacitors, inductors, and diodes. In our study, we focus on whether and how much of an interfering power noise input can go through these components and change their output.

4.1.1. Resistors, Capacitors and Inductors. Resistors, capacitors, and inductors are the most common passive electronic components. The combination of these passive components is essentially a passive filter. A power signal can go through these components by the principles of electric circuits. The major influence is their impedance, i.e., opposition to current, to the power signal. When the signal frequency f is equal to the resonance frequency f_r of the circuit, the impedance will reach the minimum and the power supply signal will be attenuated minimally.

Note that there is no ideal passive filter due to the parasitic elements and non-ideal properties of capacitors and inductors. For instance, in the high-frequency range, a real capacitor is equivalent to a combination of the Equivalent Series Resistance (ESR), Equivalent Series Inductance (ESL), leakage resistance R_{leak} and capacitance, as shown in Figure 5(a). This may lead to a passband different from the theoretical value.

Remark 1: Power supply signals can be superimposed on the input of the resistors, capacitors and inductors that are connected to the power supply. These electronic components act as a passive filter. Power supply signals whose frequency is within the filter's passband can go through the components.

4.1.2. Diodes. A diode has two terminals and can conduct current primarily in one direction, a.k.a. the forward direction. Ideally, a power signal can go through the diode only in the forward direction if there is a sufficient voltage between the two terminals. However, in practice, a signal may also go through the diode in the reverse direction. Referring to the equivalent circuit of a diode [15] shown in Figure 5(b), a reversed-biased diode can be simply represented by a large resistor R_r in parallel with the depletion layer capacitor C_{pn}. As the impedance of the capacitor decreases with increasing frequency, a high-frequency signal can go through the diode even if it is reversed-biased. We verify the assumption by conducting a simulation using TINA-TI [16]. The setup and results are shown in Appendix A.

Remark 2: Power supply signals can act as an interfering input and change the output of diodes. They can go through a diode in the forward direction. High-frequency power supply signals can also pass the diode in the reverse direction due to the equivalent capacitance.

4.2. Modifying the Behavior

This mechanism mainly applies to active elementary electronic components, which require an energy source to perform their functions. Among them, transistors are a major category, which is a type of semiconductor used to amplify and switch electronic signals. Herein, we study the effect of power supply on the transistors as an amplifier and a switch, respectively.

4.2.1. Transistor as an Amplifier. As an amplifier, small changes in a transistor's input signal will produce large changes in the output signal. We take the Bipolar Junction Transistor (BJT) as an example to study the influence of power supply signals. A BJT consists of three terminals, namely the emitter, base and collector. When acting as an amplifier, the collector-emitter current, i.e., output signal, is controlled by the base-emitter current or voltage, i.e., input signal. In an amplifier circuit, the power supply V_{cc} and the load R_L are connected between the collector and emitter terminals of the transistor, as shown in Figure 7(a). We investigate whether power supply signals can affect the transistor's output signal.

Figure 6(a) shows a simplified hybrid-π model, which is a commonly used small-signal model for BJTs [17]. We explore the relationship between the power supply signal V_{cc} and the collector-emitter current I_{out}, which is controlled by the base-emitter voltage V_{be} as:

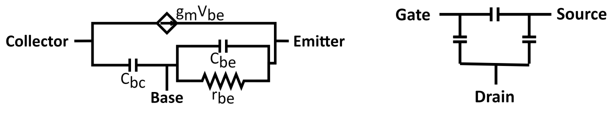
$$I_{out} = g_m \times V_{be} \tag{1}$$

where g_m is a constant. Assuming the input signal is zero, V_{be} can be calculated as:

$$V_{be} = V_{ce} \frac{C_{bc} r_{be}}{C_{bc} r_{be} + \frac{1}{2\pi f} + r_{be} C_{be}} \tag{2}$$

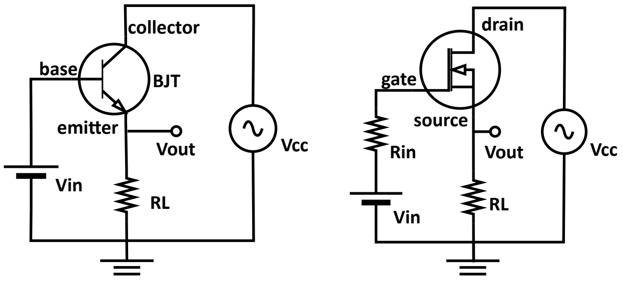
where f is the frequency of power supply signals. In this circuit, the collector-emitter voltage V_{ce} is:

$$V_{ce} = V_{cc} - I_{out} \times R_L \tag{3}$$



(a) Transistor as an amplifier. (b) Transistor as a switch.

Figure 6. Equivalent models of Transistors. (a) Equivalent model of BJT acting as an amplifier (b) Equivalent model of MOSFET working as a switch.



(a) Setup of an amplifier. (b) Setup of a switch.

Figure 7. Illustration of the simulation setup of transistors. (a) Simulation setup of BJT 2N1420 as an amplifier. (b) Simulation setup of MOSFET 2N6762 as a switch.

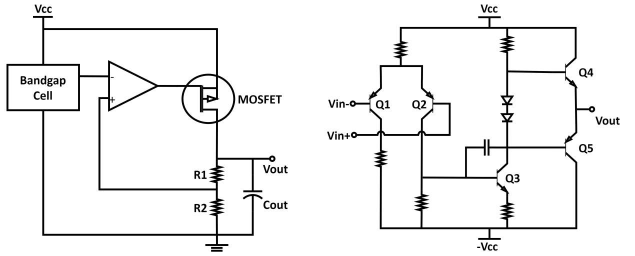
Combining the above equations, we obtain the relationship between the power supply signal and the output current as:

$$I_{out} = \frac{g_m C_{bc} r_{be}}{C_{bc} r_{be} + \frac{1}{2\pi f} + r_{bc} C_{be} + g_m C_{bc} r_{be} R_L} V_{cc} \tag{4}$$

It shows that the amplifier's output current is proportional to the power supply voltage, and the gain between the power supply and the output current increases with a higher frequency f. Therefore, power supply signals of higher frequencies have a greater impact on the BJT's output. We verify the theoretical analysis by conducting a simulation, as shown in Figure 7(a). The details of the simulation are shown in Appendix B.

Remark 3: Power supply signals can modify the relationship between the input and output of the transistor as an amplifier. They can change the output of an amplifier proportionally, and a higher-frequency signal can achieve a higher gain in such transformations.

4.2.2. Transistor as a Switch. As a switch, a transistor controls the "on" and "off" state of the output signal. We take the Metal–Oxide–Semiconductor Field-Effect Transistor (MOSFET) as an example to study the influence of power supply signals. A MOSFET consists of three terminals, namely gate, source and drain. The on and off of the drain-source path is controlled by the gate-source voltage. As shown in Figure 7(b), the power supply is between the source terminal and the drain terminal. Figure 6(b) is the small-signal model of the MOSFET in the off state [18]. It shows that the drain and source terminals are connected by an equivalent capacitor, which will have a low impedance to high-frequency signals. Therefore, a high-frequency power supply signal can go through a MOSFET switch even if



(a) Low-dropout regulator. (b) Operational amplifier.

Figure 8. Schematics of a low-dropout regulator and an operational amplifier. (a) Schematics of a low-dropout regulator. (b) Schematic of an operational amplifier.

it is in the off state. We verify the theoretical analysis by conducting a simulation, as shown in Figure 7(b). The details of the simulation are shown in Appendix B.

Remark 4: Power supply signals can change the output whether the switch is open or closed. They can go through an open switch. They can also penetrate through a closed switch if the signal frequency is sufficiently high.

4.3. Effects on Compound Electronic Components

The above analysis shows how power supply affects common elementary electronic components. In the following, we investigate whether power supply signals can affect the output of compound electronic components that are composed of various elementary electronic components, such as the low-dropout regulator, operational amplifier and data converter, by conducting simulation and real-world experiments.

4.3.1. Low-dropout Regulator. A low-dropout (LDO) regulator is used to eliminate the power supply noise, such as the switching noise. We investigate whether power supply signals can go through the low-dropout regulator without being eliminated. As shown in Figure 8(a), a low-dropout regulator consists of a MOSFET and several compound electronic components composed of transistors and passive components. By design, the MOSFET is switched off to decrease the output voltage when it exceeds the desired value, and switched on to charge the capacitor at the output terminal and increase the output voltage when it is lower than the desired value. Based on our previous analysis of MOSFET in **Remark 4**, we conjecture that a high-frequency power supply signal may go through the MOSFET regardless of its on/off state and affect the output of the regulator. We verify the assumption by conducting a simulation on TPS79501, a common low-dropout linear voltage regulator. The setup and results are shown in Appendix C.

Real-world experiment: We further validate this effect by conducting real-world experiments on another high-performance low-dropout linear regulator, the Analog Devices LT3042. We inject the attack signal into the 6V DC power supply using the direct power injection method in [19]. We sweep the frequency from 10MHz to 130MHz and measure the attack signal's gain in the regulator's output. As shown in Figure 9, the gain reaches a maximum of 4.1dB when the frequency is 110MHz, meaning that the power supply signals are amplified by the LDO regulator instead of being eliminated. We suspect a possible reason is that the operational amplifier and transistor inside the LT3042 amplify the signal.

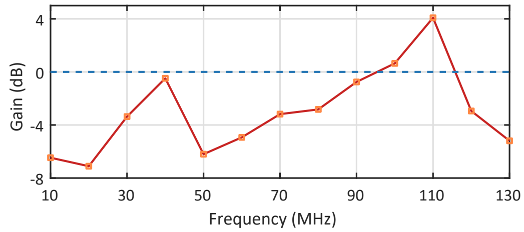


Figure 9. Frequency response of the low-dropout regulator LT3042. Power supply signals in the range of 10MHz to 130MHz can go through LT3042 with an average gain of -3.0dB. There is a positive gain of 4.1dB at 110MHz, where the noise is amplified.

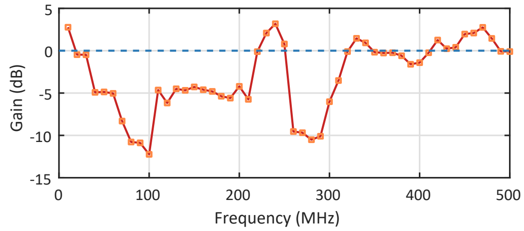


Figure 10. Frequency response of the operational amplifier TSH82. The average gain is -2.9dB in the range of 10MHz to 500MHz. Attack signals at certain frequencies can be amplified by the amplifier.

4.3.2. Operational Amplifier. Operational amplifiers (op-amps) are used for basic amplification, signal conditioning and various mathematical operations. We investigate whether power supply signals can affect the output of an operational amplifier. As shown in Figure 8(b), an operational amplifier consists of several transistors and passive components like diodes, resistors, and capacitors. Based on our analysis in **Remark 1&2&3**, it is possible for the power supply signals to go through the transistors and passive components and affect the op-amp's output. We verify the assumption by conducting a simulation on OPA4H014-SEP, a state-of-the-art operational amplifier, as shown in Appendix D.

Real-world experiment: We further validate this effect by conducting experiments on a SparkFun TSH82 op-amp with a default closed-loop gain of 4.7. The unipolar power supply voltage is 5V and the input signal is 0V. We inject the attack signal into the power supply voltage and sweep the frequency from 10MHz to 500MHz while measuring the signal gain. The results in Figure 10 show that a high-frequency attack signal on the power supply can go through the op-amp. e.g., with a signal gain of 3.2dB at 240MHz.

4.3.3. Data Converters. Data converters include digital-to-analog converters (DAC) and analog-to-digital converters

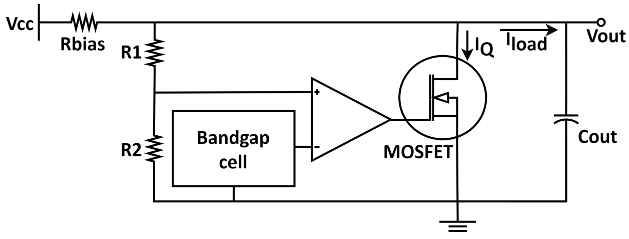


Figure 11. Schematic of a shunt reference.

(ADC). We take the ADC as an example to investigate whether power supply signals can affect the conversion result. The ADC quantifies an analog signal by comparing its voltage with a series of constant reference voltages, which are generated by a voltage reference component consisting of a number of MOSFETs, resistors, capacitors, etc., as shown in Figure 11. Based on our analysis in **Remark 1**, high-frequency power supply signals may go through resistors and change the reference voltage, thereby affecting the ADC's output. The shunt reference may fail to eliminate such power supply signals due to the decreasing gain of the operational amplifier and the MOSFET in the high frequency range. We verify the assumption by conducting a simulation on a shunt reference TL431. The setup and results are shown in Appendix E.

Real-world experiment: To validate that power supply signals can eventually affect the output of ADC, we conduct experiments on ADS1100, a delta-sigma ADC with a -5V to 5V differential input. We set the ADC's input signal to 1V DC, and inject 1.5V attack signal into the ADC's 3.3V power supply while sweeping the frequency from 1MHz to 200MHz. Different from the simulation where the output is also a high-frequency signal, the attack signal causes a DC bias in the ADC's output. For example, the output decreases by 1V when injecting a signal of 2V at 135MHz. This is because the delta-sigma ADC has nonlinear components that convert AC attack signals into a DC bias in the output.

5. How to Control Sensors and Actuators?

After analyzing the effects of power supply signals on electronic components, we seek to control IoT devices by manipulating the output of sensor and actuator modules. First, we analyze how attack signals reach the module output, then we design `Volttack` which controls sensors and actuators by injecting elaborated power supply signals.

5.1. Attack Signal's Path to the Module Output

Before designing `Volttack`, we first investigate how attack signals from the power source can (1) reach the module output without being eliminated by the power circuits and (2) maintain a sufficient signal intensity.

5.1.1. Breaking through the Power Circuits. Most devices are designed with power circuits that can protect them from the interference of power supply noises. Therefore, the attack signals need to go through the power circuits without being eliminated, e.g., by an AC-DC converter, a low-dropout regulator and filters designed for removing AC signals. We discuss these power circuits, respectively.

The AC-DC converter is enabled mainly by a rectifier that converts a two-directional signal into a single-directional signal. Typical rectifiers are composed of diodes as they make signals flow in one direction. For example, the diode in Figure 17(a) in Appendix acts as a half-wave rectifier. As discussed in Section 4.1.2, attack signals that exceed a certain frequency can go through the diode in both directions, and thus can penetrate the AC-DC converter.

The low-dropout regulator is applied to eliminate the power supply noise. As discussed in Section 4.3.1, attack signals can go through the low-dropout regulator without being eliminated, and are even amplified in some cases.

Filters allow signals of predetermined frequencies (pass-band) to pass through and reject signals of other frequencies (stop-band). Passive filters are composed of passive electronic components, thus high-frequency attack signals may go through the low-pass filters due to the non-ideal characteristic of real capacitors as discussed in Section 4.1.1 and the existence of parasitic capacitors. Active filters amplify the pass-band signals using operational amplifiers, which the attack signal can also penetrate. To verify, we conduct a simulation on a low-pass filter shown in Figure 22 in Appendix. The results show that a 25MHz attack signal can go through the low-pass filter with a gain of -10.6dB.

5.1.2. Amplifying the Attack Signal. To increase the intensity of the attack signal and achieve a better attack performance, we manage to amplify the attack signal by exploiting the vulnerability of negative feedback, which is a way of connecting electronic components to increase output stability. As shown in Figure 12, a negative feedback circuit consists of a forward path and a feedback path. In the forward path, the signal is processed by blocks with a transfer function of G_1G_2. In the feedback path, the output of the circuit is fed back via a block with a transfer function of G_3. This feedback signal subtracts from the input. We assume the power supply noise is injected between the G_1 and G_2 and investigate whether the power supply noise can be amplified by the negative feedback circuit.

Suppose that the power supply noise is x_{in} and the compensation signal of negative feedback is x_{com}. The transfer function $G(s)$ is a linear mapping of the Laplace transform of x_{in} to the Laplace transform of x_{com}. $G(s)$ can be calculated as:

$$G(s) = -\frac{G_1G_3G_2}{1 + G_1G_3G_2} \tag{5}$$

According to the transfer function, we can obtain the gain G_f and phase delay $\Delta\varphi$ at a frequency f. Suppose that $x_{in} = \sin(2\pi ft)$, the signal after the compensation can be calculated as:

$$V_{sum} = \sin(2\pi ft) - G_f \sin(2\pi ft + \Delta\varphi) \tag{6}$$

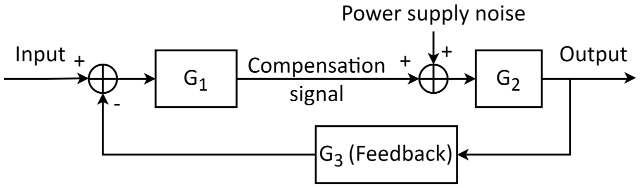


Figure 12. Illustration of a negative feedback circuit. The power supply noise is injected between the G_1 and G_2. The high-frequency power supply noise may not be effectively compensated by the circuit due to the phase delay.

where the phase delay $\Delta\varphi$ depends on the processing time τ of the circuit and the period T of the signal. $\Delta\varphi$ can be calculated as:

$$\Delta\varphi = \frac{\tau}{T} \tag{7}$$

As τ is small, $\Delta\varphi$ is approximately zero when T is large, i.e., f is small. In this case, the power supply noise can be compensated effectively. However, $\Delta\varphi$ increases as the T decreases. When $\Delta\varphi$ reaches π, the power supply noise will be amplified instead. Therefore, the negative feedback circuit can amplify the power supply noise in dedicated frequencies. Our experiment results in Section 4.3.2 are consistent with the above conclusion. For example, in Figure 10, a 240MHz power supply signal can be amplified by the opamp with a gain of 3.2dB.

5.2. `Volttack` Design

We design `Volttack` to control the output of sensor and actuator modules in a predictable way. To achieve the goal, we need to tackle the following challenges. (1) *Effective injection of attack signals:* Although attack signals can go through the various compound electronic components, the optimal frequencies are not the same. We need to optimize the frequency of the attack signal to achieve an effective signal injection. (2) *Predictable control of the module output:* By injecting the high-intensity attack signal into the output, we can realize a Denial-of-Service (DoS) attack against the IoT devices. However, to realize a more controllable attack effect, we need to shape the high-frequency out-of-band attack signal into the in-band frequencies, i.e., the intended frequency band of the module's output.

5.2.1. Effective Attack Signal Injection. To address the challenge that the optimal attack frequencies are not necessarily the same for different components, we manage to obtain the overall frequency response from the power supply to the output. The transmission path can be divided into three parts: power supply, injection point and subsequent signal path. The injection point is an electronic component where the attack signal can enter the signal path that processes the input signal. Then the attack signal goes through the subsequent signal path and reaches the output.

Supposing the frequency responses of the power supply, injection point and subsequent signal path are respectively $G_p(f)$, $G_i(f)$ and $G_s(f)$ in dB, the overall frequency response $G(f)$ can be calculated as follows.

$$G(f) = G_p(f) + G_i(f) + G_s(f) \tag{8}$$

To maximize the intensity of the attack signal, we need to obtain the frequency response of various signal transmission paths and find the optimal frequency with the largest gain.

5.2.2. Control the Output in a Predictable Way. To upgrade from a DoS attack to a controllable attack, the attacker needs to shape high-frequency attack signals to in-band, e.g., DC to 20kHz for a microphone sensor. We exploit the nonlinear properties of the electronic components which can convert the attack signal from the high frequency band to low frequency band. Then we control the output by adjusting the amplitude of the attack signal. We assume the optimal frequency is f_a. Without loss of generality, we want to inject an in-band signal $m(t) = Acos(2\pi f_m t)$, as a complex signal can be expressed as a sum of cosine waves. In the following, we study how to adjust the attack signal amplitude to obtain the $m(t)$ at the output.

(1) Researchers have been studying the nonlinear properties of electronic components [20, 21]. One typical nonlinear property can be simplified as follows [22].

$$V_{out} = c_1 \times V_{in} + c_2 \times V_{in}^2 \tag{9}$$

where c_1 and c_2 are the gains of fundamental and quadratic terms. We amplitude-modulate the signal as follows.

$$V_{in} = [m(t) + 1] \times cos(2\pi f_a t) \tag{10}$$

where V_{in} is the attack signal we inject from the power source. Now we want to exploit the nonlinear property to demodulate the attack signals V_{in}. Combining the above equations, we can calculate the V_{out}. It contains the intended in-band signal $m(t)$ with a gain of c_2. In conclusion, by amplitude-modulating the signal as shown in Eq. 10, an attacker can obtain the intended signal.

(2) ADCs show a nonlinear property called aliasing [23]. According to the Nyquist-Shannon sampling theorem, if the frequency of a sampled signal is higher than half of the sampling rate, it would be reconstructed into a lower-frequency signal. An attacker can exploit this property to convert the high-frequency signals to in-band signals. Assume that the sampling rate of the ADC is F_s and the frequency of the attack signal is fine-tuned to nF_s, where n is an integer. Similarly, we amplitude-modulate the intended in-band signal $m(t)$ into the attack signal V_{in} as follows.

$$V_{in} = [m(t) + 1] \times cos(2\pi nF_s t) \tag{11}$$

Due to the aliasing effect, the attack signal is sampled into $V(N)$ as follows.

$$\begin{aligned} V(N) &= [m(NT_s + T_0) + 1] \times cos(2\pi nF_s(NT_s + T_0)) \\ &= V_0 \times m(NT_s + T_0) + V_0 \end{aligned} \tag{12}$$

$$V_0 = cos(2\pi nF_s T_0) \tag{13}$$

where $V(N)$ is the N^{th} sample point, V_0 is a constant, T_s is the sampling interval, and T_0 is the sampling time of the first point. Eq. 12 indicates that by amplitude-modulating the signal as shown in Eq. 11, an attacker can obtain the sampled intended signal $m(NT_s + T_0)$.

For the nonlinear property that has not been studied yet, the attacker may model the property by inputting signals of different amplitudes and recording the output. Then she can amplitude-modulate the signal by referring to the mapping relation. Note that the nonlinear property varies among different components. For certain components and frequencies f_a, the in-band signal can only be positive or negative, which means the attacker can only increase or decrease the output.

6. Evaluation

We evaluate the performance of Volttack in this section. An automated system relies on sensors and actuators to perform the designed functions. We implement the Volttack attack on 6 sensors and 3 actuators to demonstrate the real-world threat of the attack.

6.1. Experiment Setup

As shown in Figure 13, the experiment setup includes the victim's devices and the attacker's devices. The victim's devices are critical sensors and actuators that require an electrical supply. The attacker's devices are used to inject the elaborated attack signals into the power supply of the victim's devices.

6.1.1. Victim's Devices. We implement Volttack on a variety of widely used sensors and actuators to evaluate the performance of Volttack, including (1) a force sensor Daysensor DYTB-002 50kg [24] used in cars, chemical plants and pharmaceutical factories, (2) a number of sensor modules that are used to measure the factories environment variables, such as light, pressure, humidity, and temperature, (3) servos [25, 26] used in robotics, aerospace industry and automobile industries, and (4) an electric valve [27] used in critical factories such as chemical plant and nuclear power plant.

6.1.2. Power supply. The AC-to-DC converter [28] converts the 220V AC power into a DC power supply voltage adjustable from 0V to 24V. DC-DC converters and linear-dropout regulators may be applied to the victim's devices.

6.1.3. Attacker's Devices. The attacker's devices are used to generate and amplify the attack signal. The signal generator Keysight N5172B [29] can generate a signal in a range of 9kHz to 6GHz. The amplifier Mini-Circuits ZHL-100W-GAN+ [30] can amplify the signal in a range of 20MHz to 500MHz with a typical gain of 42dB. For safety reasons, we inject the attack signals at the output terminal of the AC-DC converters using a bias tee, instead of the 220V AC input terminal. The attack signals still need to pass through the power supply circuits inside the attacked devices.

TABLE 1. Attack results of 10 experiments on each of 5 instances (N1 $\sim$ N5) of the force sensor. The attack frequency is 342MHz.

Amplitude(V)		0.5	1	1.5	2
N1 $\sim$ N4	**Deviation(kg)**	-0.2	-0.8	-2.1	-5.7
	Stdev.(kg)	0.04	0.5	1.3	3.0
N5	**Deviation(kg)**	-1.7	-12.4	-27.2	-41.4
	Stdev.(kg)	0.02	0.1	3.6	10.5

6.2. Attack on Sensors

We evaluate Volttack attack on a force sensor and a number of sensor modules measuring the environment variables.

6.2.1. Force Sensor. We evaluate the Volttack attack on a force sensor Daysensor DYTB-002 used in cars, chemical plants, etc. It can measure the force in a range of 0N to 50kgf (1kgf = 1kg*9.8N/kg). We measure a 9.8kg piece of metal using the sensor and the theoretical result is 9.8kg. We inject the attack signal into the 24V power supply and sweep the frequency of the attack signal from 20MHz to 500MHz to find out the optimal attack parameters. To evaluate the attack predictability, we repeat the experiments 10 times at different times of the day on each of the 5 instances and calculate the average deviation and standard deviation.

According to the results, we can deviate the sensor output in the range of -41.4kg to 1.0kg. The sensor output decreases at a frequency of 342MHz and increases at a frequency of 463MHz. For example, injecting a signal of 180mV at a frequency of 463MHz can increase the output from 9.8kg to 10.8kg.

We show the statistical results, i.e., average deviation and standard deviation, of the 5 instances at different times in Table 1. With the increase of signal amplitude, the average deviation and the standard deviation increase. Compared with the other 4 instances, instance N5 shows a more significant attack effect. For example, injecting a signal of 1V can decrease the output from 9.8kg to -2.6kg. We analyze the reasons for this in Section G in Appendix.

Supposing a driver breaks sharply with a force of 20kgf and an attacker tampers with the sensor output to 10kgf, the braking distance will double, increasing the possibility of a car crash.

6.2.2. Sensor Modules. We evaluate the Volttack attack on different types of sensor modules driven by an Arduino Uno. We use a laptop to power and communicate with Arduino by USB port and read the measured value of sensors. We inject attack signals into the 12V power supply and sweep the frequency of the attack signal from 20MHz to 600MHz to find out the optimal attack parameters. To evaluate the attack predictability, we repeat the experiments 10 times at different times of the day on each of the 5 instances of each sensor module and calculate the average deviation, average rate and standard deviation.

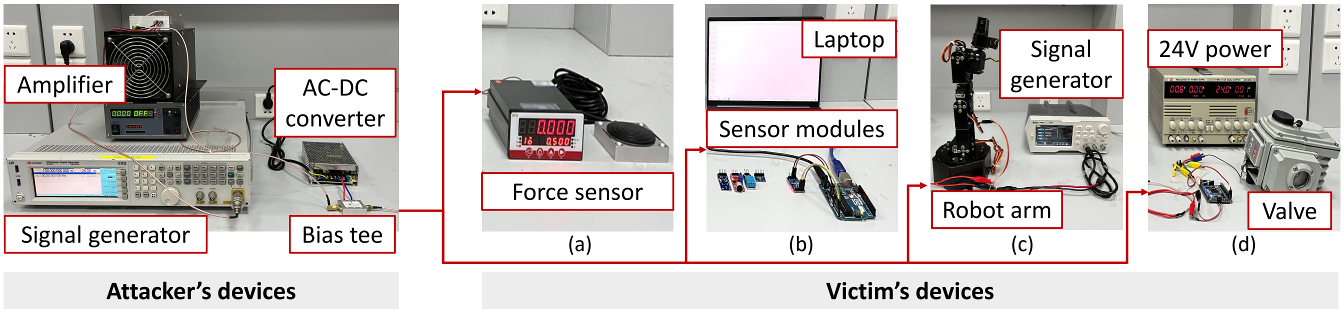


Figure 13. An illustration of the Volttack system setup. The attacker's devices inject attack signals into the DC power supply of the victim's devices. The victim's devices include (a) a force sensor, (b) a variety of sensor modules used to measure the environment variables, (c) servos used in the robot arm, and (d) an electric valve.

TABLE 2. STATISTICAL RESULTS ON A VARIETY OF SENSORS. THE ATTACK FREQUENCY IS SWEPT FROM 20MHZ TO 600MHZ.

Type	Model	Measurement span	Attack parameters		Output			
			Freq.(MHz)	Amp.(V)	Original	Deviation	Rate	Stdev.
Light	GY-30	1 ∼ 65535 lx	195	0.5	1030 lx	-196 lx	-19.1%	47 lx
Acceleration	MMA7361	±1.5 g	392	0.5	1.00 g	+0.41 g	+40.5%	0.08 g
Sound	MK519	\	192	0.5	0.14 V	+0.29 V	+209.7%	0.07 V
Pressure	BMP280	30000 ∼ 110000 Pa	568	0.25	98300 Pa	-146 Pa	-0.1%	138 Pa
Temperature	BMP280	-40 ∼ 85°C	568	0.25	27.2°C	-1.0°C/0.5°C	-3.7%/+1.8%	0.5°C/0.1°C
Temperature	DHT11	0 ∼ 50°C	121	0.5	28°C	+139°C	+497.4%	25°C
Humidity	DHT11	20 ∼ 90%	121	0.5	72%	+96%	+132.7%	29%

[1] For each sensor, we repeat the experiments 10 times on each of the 5 instances and calculate the average deviation and standard deviation.
[2] The original power supply is 12V and the amplitude of the attack signal is at most 0.5V.
[3] We list the tampered output under specific attack signal amplitudes. The attack performance can be improved with a higher amplitude.

We list the attack parameters and original and tampered output in Table 2. By fine-tuning the amplitude, the attacker can control the output of the sensors within a certain range. The tampered output of DHT11 exceeds the measurement span. This is because Volttack may attack the signal processing components of the sensor and make the processed signal out of the normal range.

For each sensor module, we show the statistical results, i.e., average deviation and standard deviation, of the 5 instances at different times in Table 2. On the one hand, GY-30, MMA7361, MK519, and DHT11 as a temperature sensor show relatively low standard deviation, e.g., 47 lx for GY-30. On the other hand, for BMP280, the standard deviation is relatively high. And for BMP280 as a temperature sensor, the output of 3 instances increases while the output of the other 2 instances decreases. We analyze the reasons for this in Section G in Appendix.

Supposing the sensor modules in critical industrial factories are compromised, environmental factors such as temperature and humidity may be incorrectly adjusted. This may lead to industrial control process failure. For example, an attacker can increase the output of DHT11 by 139°C, which may lead to false excess cooling, a key cause of the British dye factory explosion.

6.3. Attack on Actuators

In addition, we evaluate Volttack attack on servos and an electric valve.

6.3.1. Servo. Electric servo is widely used in robotic arms that cover a variety of fields, such as the manufacturing industry and medical treatment. It can rotate or push objects with high precision. In the following, we evaluate the attack performance on a stand-alone servo Futaba S9602 and a servo DSS-M15S mounted in a robotic arm.

First, we evaluate the attack on the servo Futaba S9602 powered by 5.5V DC and controlled by a PWM signal with a frequency of 50Hz. The rotation angle of the servo ranges from 0° to 220°, and the duty of PWM should be configured as 2.5% to 12.5% correspondingly. As shown in Figure 13(c), a signal generator (right) is used to output the control signal. The initial angle of the servo is set to 0°. We inject the attack signal into 5.5V supply and monitor the rotation of the servo with a gyroscope attached to it. To evaluate the attack predictability, we repeat the experiments 10 times at different times of the day on each of the 5 instances and calculate the average deviation and standard deviation.

We sweep the frequency of the attack signal from 1MHz to 500MHz and find out the vulnerable frequency of 314MHz. Then we set the frequency to 314MHz and change the amplitude of the attack signal. According to the result, the servo rotates clockwise in the range of 0° to 58.4°. As shown in Table 3, the standard deviation is 3.9° at most, which is 6.7% of the rotation range of 58.4°. An attacker may control the rotation angle of the servo by injecting a 314MHz attack signal with a specific amplitude based on Table 3.

TABLE 3. Attack results of 10 experiments on each of 5 instances of the servo. The attack frequency is 314MHz.

Amplitude(V)	0.5	0.7	0.9	1.1	1.3
Average deviation(°)	10.5	24.0	36.3	48.3	58.4
Standard deviation(°)	3.0	3.0	3.9	2.8	3.1

TABLE 4. Attack results of 10 experiments on each of 5 instances of the valve. The attack frequency is 75MHz.

Initial opening(%)	0	25		50	
Amplitude(V)	0.5	0.3	0.5	0.5	0.7
Average deviation(%)	34	-14	13	-17	10
Standard deviation(%)	3.3	4.2	5.4	4.2	6.9

Moreover, we implement the attack on DFRobot 6DOF Robotic Arm as shown in Figure 13(c). Specially, we attack the DSS-M15S, one of the six servos. By injecting a 213MHz attack signal with an amplitude of 1.4V, the corresponding robotic arm is rotated 32° falsely. As a consequence, this may jeopardize production or even the nearby operator.

6.3.2. Valve. Electric valves can control the flow of various types of fluids. We evaluate the attack performance on an electric valve [27] with the setup shown in Figure 13(d). The controller STM32F407VET6 decides the valve opening and outputs an analog control signal using the ADC. The control signal is amplified and transmitted to the valve. The valve is powered by a 24V supply and changes opening based on the control signal. The valve opening is $(10 \times V_c)$ % where V_c is the DC voltage of the control signal. We inject the attack signal into the 5V supply. To evaluate the attack predictability, we repeat the experiments 10 times at different times of the day on each of the 5 instances and calculate the average deviation and standard deviation.

We sweep the frequency of the attack signal from 1MHz to 500MHz to find the vulnerable frequencies of 75MHz. The attacker may increase or decrease the valve opening by controlling the signal amplitude. We evaluate the attack performance at 0%, 25% and 50% initial openings. The results are shown in Table 4. The deviation range varies at different initial openings, e.g., 34% at 0% initial opening and 27% at 25% initial opening. In addition, the standard deviation varies at different initial openings. For example, the standard deviation is 3.3% at 0% initial opening, around 1/10 of the deviation range of 34%.

Supposing the valve is used to control the flow of natural gas, injecting a signal of 0.5V at a frequency of 75MHz can open the closed valve to 34%, which may cause a natural gas leak.

6.4. End-to-end Attack

To demonstrate the practicality, we perform end-to-end attacks with three methods: fabricating a malicious battery with the attack devices embedded, placing a current injection probe on the power cable, and connecting the attack devices to the power network using a customized coupler.

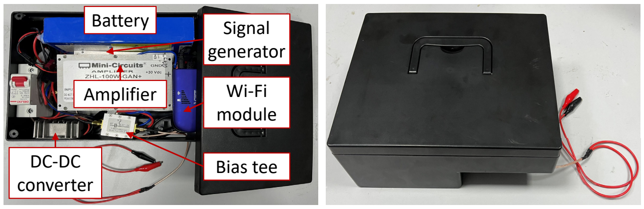


Figure 14. Illustration of the counterfeit battery consisting of a small battery and attack devices. It adds attack signals to the DC supply voltage.

6.4.1. Counterfeit Battery. An attacker may fabricate a malicious battery to manipulate the power supply voltage, as shown in Figure 14. The structure diagram is shown in Figure 23 in Appendix. It comprises a small battery and attack devices. First, to power the attack devices, a DC-DC converter is applied to output the desired power supply voltage. Second, to control the attack devices remotely, a Wi-Fi module is applied to forward the attack parameters from the attacker's PC to the attack devices. Finally, we use a bias tee to add the attack signals to the DC supply voltage. An attacker may be a maintenance worker and replace the original battery with a counterfeit one. After that, she can launch a `Volttack` attack remotely. We attack the force sensor DYTB-002 by injecting 342MHz attack signals using the counterfeit battery. The original measurement output is 9.8kg. We can deviate the output in the range of 8.6kg to 9.8kg by launching the attack. In the bench-top experiments, we can deviate the output in the range of 4.1kg to 9.8kg. Compared to the bench-top experiments, the maximum deviation range becomes smaller. This is because the counterfeit battery has a lower output power than the attack devices in the bench-top experiments.

6.4.2. Current Injection Probe. A noninvasive way is to apply a current injection probe, which is used in the EMC immunity test. An attacker may place a current injection probe on the power cable to inductively couple the attack signal into the power supply line. In this way, the attacker can protect the attack devices from the high voltage of the power network. As shown in Figure 15, the attack devices include a signal generator, an amplifier, and a current injection probe [31]. The attack devices can be powered by a portable battery or the victim's power supply source. The attacker may connect a Wi-Fi module to the signal generator to control the device remotely. Using the setup, we attack the valve by injecting 75MHz attack signals. The original valve opening is 48%. We can deviate the valve opening in the range of 28% to 48%. In the bench-top experiments, we can deviate the valve opening in the range of 33% to 60% at 50% initial valve opening. Compared to the bench-top experiments, the maximum deviation range becomes smaller. This is because the attack signal is attenuated when

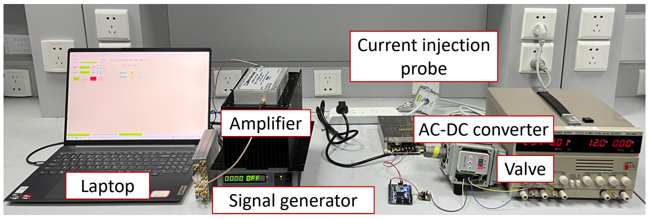


Figure 15. Illustration of the setup with a current injection probe. The probe is placed on the power cable between the power supply source and the victim's device.

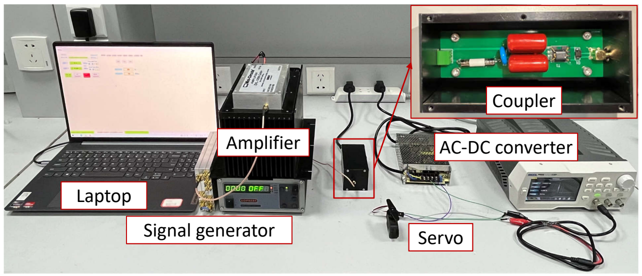


Figure 16. Illustration of the setup with a customized coupler. The attack devices and the victim's device are connected to the same power network.

it is emitted by the current injection probe and received by the power supply line.

6.4.3. Customized Coupler. An attacker may inject the attack signal into the power network to which the attacked IoT devices are connected. In this case, the attack devices act as a malicious peripheral sharing the power network with the victim's IoT devices. The attacker needs to protect the attack devices from the high voltage of the power network. Therefore, we implement a customized coupler to reduce the impact of the power network on the attack devices. The schematic is shown in Figure 24 in Appendix. To verify the practicality, we use the experiment setup as shown in Figure 16. The attack devices include a signal generator, an amplifier, and the customized coupler. The attack devices and the victim's device are connected to the same power network. The attacker may connect a Wi-Fi module to the signal generator to control the device remotely. Using the setup, we attack the servo Futaba S9602 by injecting 314MHz attack signals. The initial angle of the servo is set to 0°. We can rotate the servo clockwise in the range of 0° to 15°. In the bench-top experiments, we can rotate the servo clockwise in the range of 0° to 58.4°. Compared to the bench-top experiments, the maximum rotation range becomes smaller. This is because the attack signal is attenuated during transmission through the coupler and the power network.

6.4.4. Summary. We successfully conduct the end-to-end attack using the above three sets of attack devices. Specifically, for the vehicle scenarios with batteries, the attacker can fabricate malicious batteries with the attack device embedded and replace the original ones during maintenance. In addition, for the industrial plant attack scenarios, the attacker may be a malicious employee or a maintenance worker who can place a current injection probe on the power cable or connect the attack devices to the power network using a customized coupler. In real-world attacks, factors for the attacker to consider include portability, detectability, and output power. First of all, the attack devices should be small in size. The counterfeit battery we make is around 260 × 82 × 185 mm in size. It can be miniaturized furthermore by using a customized circuit board to generate signals at fixed frequencies and a narrow-band amplifier. In addition, the devices should be concealed. An attacker may apply sound insulation and exterior camouflage. Moreover, as the power supply circuit may attenuate the attack signal, the attack devices should meet the output power requirements, especially when attacking an IoT system with many devices and with the intention of achieving widespread manipulation.

7. Discussion

7.1. Attacking a Full System

Attacking a full system with multiple sensors and actuators with different susceptibilities is more complex and challenging for the attacker to achieve precise manipulation. First of all, the attacker needs to acquire information about the system composition and obtain the vulnerable frequency of each device. Then she needs to determine the attack strategy according to the attack goal, including the target device selection and signal design. (1) She may select direct or indirect target devices to achieve the attack goal. For example, to control the rotation angle of a robotic arm, she may attack the servo directly or the angle sensor indirectly. Factors to be considered include the attack cost and attack performance. (2) She needs to design the attack signal based on the target device selection. IoT devices with different susceptibilities may have overlapping vulnerable frequencies. Therefore, it is required to select the attack frequency that has a minimal effect on irrelevant IoT devices. When there is more than one device to attack, she may inject the attack signals of different frequencies simultaneously or sequentially.

7.2. Countermeasures

To protect IoT devices from such attacks, we propose two potential countermeasures. For legacy devices, a defender may add a voltage sensor to monitor the power supply voltage and detect `Volttack` in real time. For future devices, a defender may apply an LDO with high power supply rejection performance, and verify the performance by conducting EMC tests in the wideband frequency range.

7.2.1. Monitoring the Power Supply Voltage. Since Volttack attack requires modifying the power supply voltage, one method of defense is to monitor the power supply voltage. The defenders may sample the voltage of the power supply by applying a voltage sensor. The controller of the IoT device processes the measured data and discriminates the abnormal state of the power supply. This affects the performance of the IoT device minimally as the detection algorithm can be very simple, e.g., determining whether the voltage exceeds a threshold. Another way to monitor the supply voltage is to apply a voltage detector, an IC which integrates an internal comparator and reference voltage to perform a power-management supervisory function [32]. When the supply voltage fluctuation exceeds the normal range, the monitor reports an impending power supply failure to the system [33]. The cost of such a voltage sensor or voltage detector is around $1.

7.2.2. Improving the Noise Rejection Performance. In addition, a defender may improve the noise rejection performance of the power supply to eliminate the attack signals. This involves two steps. First, the defender should carefully design the power supply and improve the PSRR over a wider frequency range. It is required to reduce the size and cost constraints of the power supply so that better electronic components and layout can be applied. Specifically, a defender may improve the PSRR by modifying the architecture of the LDO [34]. The cost of an LDO with a high PSRR is around $2. This will not affect the performance of the IoT device, as it is independent of the subsequent circuits. After that, the defender may verify the noise rejection performance by conducting EMC tests in the wideband frequency range, e.g., 150kHz-500MHz.

8. Related Work

In this section, we review the related works of fault injection attacks based on power supply manipulation. We divide the related works into two categories according to the different attack targets, digital circuits and analog circuits.

8.1. Attacks on Digital Circuits

Fault injection attacks on digital circuits by manipulating the power supply signals have been investigated previously. The research object ranges from cryptographic modules to True Random Number Generator (TRNG). (1) Cryptographic modules are a focus of research. Selmane et al. [35] realized a practical fault attack on a smart card that preserves an AES function by underpowering it using a peripheral power supply. Some researchers have proposed fault injection attacks on Intel SGX and AMD SEV. Qiu et al. [36] proposed a fault attack against TrustZone of ARM processor, named VoltJockey. It can infer the AES key and subvert the RSA signature chain verification by manipulating the CPU's core voltage from privileged software. Murdock et al. [37] realized a similar fault attack against SGX enclaves of Intel CPU. In addition to key extraction, it can fault a list of hardware-level key derivation instructions and violate memory safety. Chen et al. [38] realized a hardware-based fault injection attack on Intel CPU. It controls the CPU core voltage by injecting messages on the Serial Voltage Identification bus between the CPU and the voltage regulator. Bohren et al. [39] proposed a voltage glitching attack on AMD Secure Encrypted Virtualization (SEV) which can deploy customized programs on AMD Secure Processor (AMD-SP) and decrypt the memory of the virtual machine. (2) Moreover, researchers [40–46] have investigated the fault injection attacks on True Random Number Generator which is used to generate confidential keys and other critical security parameters in cryptographic modules. The entropy of the TRNG can be reduced by manipulating the power supply. Compared to the above works, the Volttack focuses on analog circuits. In addition, the Volttack does not require compromising the firmware.

8.2. Attacks on Analog Circuits

Researchers have demonstrated that power supply disturbance can tamper with certain sensors. Tu et al. [19] proposed an attack that can spoof the temperature sensors by transmitting radiated EMI. They demonstrated that power supply noise can induce a DC offset at the output of the amplifier. Esteves et al. [47] proposed a voice command injection attack against smartphones by injecting attack signals into the power line. Tsang et al. [2] provided a firmware attack that can cause data corruption of a pressure sensor by misconfiguring the Power Management Integrated Circuits (PMIC). Compared to the above attacks against specific sensors, we discovered a vulnerability in the power supply and analyzed the influencing mechanism of power supply signals on the electronic components and the output of IoT devices. The Volttack we proposed can spoof the sensors and maneuver the actuators.

9. Conclusion

In this paper, we discover a vulnerability in the power supply that can be exploited to control the sensing and actuating processes of IoT devices. We systematically analyze the principle of how power supply signals affect the underlying electronic components constituting the sensors and actuators. Furthermore, we propose Volttack that can control the output of sensors or the behavior of the actuators by compromising the power source and injecting elaborated signals through the power supply module. To demonstrate the real-world threat of Volttack, we implement and validate the attack on 6 sensors and 3 actuators used in applications such as industrial control systems. Finally, we discuss potential countermeasures to mitigate the attack.

Acknowledgments

We thank the anonymous reviewers for their valuable comments. This work is supported by China NSFC Grant 62222114, 61925109, 62071428, and 62201503.

References

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

[2] R. Tsang, D. Joseph, Asmita, S. Salehi, N. Carreon, P. Mohapatra, and H. Homayoun, "Fandemic: Firmware attack construction and deployment on power management integrated circuit and impacts on iot applications," in *Network and Distributed Systems Security (NDSS) Symposium*, 2022.

[3] S. Kulandaivel, S. Jain, J. Guajardo, and V. Sekar, "Cannon: Reliable and stealthy remote shutdown attacks via unaltered automotive microcontrollers," in *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2021, pp. 195–210.

[4] K.-T. Cho and K. G. Shin, "Fingerprinting electronic control units for vehicle intrusion detection," in *25th USENIX Security Symposium (USENIX Security 16)*, 2016, pp. 911–927.

[5] ——, "Error handling of in-vehicle networks makes them vulnerable," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016, p. 1044–1055.

[6] ——, "Viden: Attacker identification on in-vehicle networks," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, p. 1109–1123.

[7] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," *Black Hat USA*, vol. 2015, no. S 91, 2015.

[8] "Electromagnetic compatibility (EMC) - Part 4-31: Testing and measurement techniques - AC mains ports broadband conducted disturbance immunity test," Standard, 2016.

[9] ORACLE, "What is iot?" https://www.oracle.com/internet-of-things/what-is-iot/,.

[10] B. Yang, B. Drost, S. Rao, and P. K. Hanumolu, "A high-psr ldo using a feedforward supply-noise cancellation technique," in *2011 IEEE Custom Integrated Circuits Conference (CICC)*. IEEE, 2011, pp. 1–4.

[11] S. Ye, W. Eberle, and Y.-F. Liu, "A novel emi filter design method for switching power supplies," *IEEE Transactions on Power Electronics*, vol. 19, no. 6, pp. 1668–1678, 2004.

[12] ScienceDerict, "Power supply rejection ratio," https://www.sciencedirect.com/topics/engineering/power-supply-rejection-ratio.

[13] P. Wilson, *The circuit designer's companion*. Newnes, 2017.

[14] O. N. Pandey, *Operational Amplifier (Op-Amp)*. Cham: Springer International Publishing, 2022, pp. 233–270. [Online]. Available: https://doi.org/10.1007/978-3-030-78995-4_5

[15] EEEGUIDE.COM, "Ac equivalent circuit of semiconductor diode," https://www.eeeguide.com/ac-equivalent-circuit-of-semiconductor-diode/.

[16] TINA-TI, https://www.ti.com/tool/TINA-TI.

[17] C. C. McAndrew and L. W. Nagel, "Bjt small-signal equivalent circuit representation," in *2010 IEEE Bipolar/BiCMOS Circuits and Technology Meeting (BCTM)*, 2010, pp. 153–156.

[18] D. Lovelace, J. Costa, and N. Camilleri, "Extracting small-signal model parameters of silicon mosfet transistors," in *1994 IEEE MTT-S International Microwave Symposium Digest (Cat. No. 94CH3389-4)*. IEEE, 1994, pp. 865–868.

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

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

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

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

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

[24] Daysensor DYTB-002, http://www.dyloadcell.com/product/clcgq/79.html.

[25] DFRobot 6DOF Robotic Arm, https://www.dfrobot.com/product-192.html.

[26] Futaba S9602, https://www.ebay.com/itm/284139429886.

[27] Fulaite 05 Electric Valve, https://item.taobao.com/item.htm?spm=a1z09.2.0.0.43452e8doxmYHA&id=650625135383&_u=72eps17fe651.

[28] Huayao HYK-150, https://www.huayaody.com/a/chanpinzhanshi/ketiaodianyuan/469.html.

[29] Keysight N5172B, https://www2.keysight.com/us/en/howtobuy/N5172B/exg-x-series-rf-vector-signal-generator-9-khz-6-ghz.html.

[30] Mini-Circuits ZHL-100W-GAN+, https://www.minicircuits.com/WebStore/dashboard.html?model=ZHL-100W-GAN%2B.

[31] EM5011, http://www.lemaiyi.net/lemaiyi-Products-30766207/.

[32] TI, "Voltage supervisor and reset ics: Tips, tricks and basics," https://www.ti.com.cn/lit/eb/slyy167/slyy167.pdf, 2019.

[33] ANALOG DEVICES, *Monitoring and Sequencing*

Supply Voltages in High-Reliability Systems, https://www.maximintegrated.com/en/design/technical-documents/app-notes/3/3567.html, 2005.

[34] Saptarshi Banerjee, "Power supply rejection (psr) enhancement techniques for fully integrated low-dropout (ldo) regulators," https://liu.diva-portal.org/smash/get/diva2:1502860/FULLTEXT01.pdf, 2020.

[35] N. Selmane, S. Guilley, and J.-L. Danger, "Practical setup time violation attacks on aes," in *2008 Seventh European Dependable Computing Conference*. IEEE, 2008, pp. 91–96.

[36] P. Qiu, D. Wang, Y. Lyu, and G. Qu, "Voltjockey: Breaching trustzone by software-controlled voltage manipulation over multi-core frequencies," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp. 195–209.

[37] K. Murdock, D. Oswald, F. D. Garcia, J. Van Bulck, D. Gruss, and F. Piessens, "Plundervolt: Software-based fault injection attacks against intel sgx," in *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2020, pp. 1466–1482.

[38] Z. Chen, G. Vasilakis, K. Murdock, E. Dean, D. Oswald, and F. D. Garcia, "{VoltPillager}: Hardware-based fault injection attacks against intel {SGX} enclaves using the {SVID} voltage scaling interface," in *30th USENIX Security Symposium (USENIX Security 21)*, 2021, pp. 699–716.

[39] R. Buhren, H.-N. Jacob, T. Krachenfels, and J.-P. Seifert, "One glitch to rule them all: Fault injection attacks against amd's secure encrypted virtualization," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, 2021, pp. 2875–2889.

[40] A. T. Markettos and S. W. Moore, "The frequency injection attack on ring-oscillator-based true random number generators," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2009, pp. 317–331.

[41] N. Bochard, F. Bernard, V. Fischer, and B. Valtchanov, "True-randomness and pseudo-randomness in ring oscillator-based true random number generators," *International Journal of Reconfigurable Computing*, vol. 2010, 2010.

[42] D. Mahmoud and M. Stojilović, "Timing violation induced faults in multi-tenant fpgas," in *2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2019, pp. 1745–1750.

[43] P. Bayon, L. Bossuet, A. Aubert, V. Fischer, F. Poucheret, B. Robisson, and P. Maurine, "Contactless electromagnetic active attack on ring oscillator based true random number generator," in *International Workshop on Constructive Side-Channel Analysis and Secure Design*. Springer, 2012, pp. 151–166.

[44] S. Buchovecká and J. Hlaváč, "Frequency injection attack on a random number generator," in *2013 IEEE 16th International Symposium on Design and Diagnostics of Electronic Circuits & Systems (DDECS)*. IEEE, 2013, pp. 128–130.

[45] P. Bayon, L. Bossuet, A. Aubert, and V. Fischer, "Fault model of electromagnetic attacks targeting ring oscillator-based true random number generators," *Journal of Cryptographic Engineering*, vol. 6, no. 1, pp. 61–74, 2016.

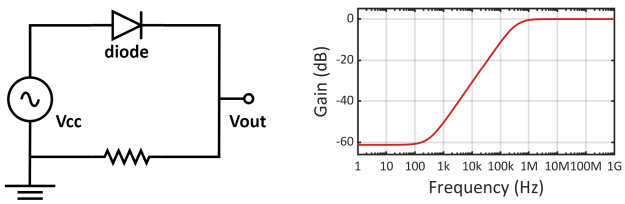
[46] S. Osuka, D. Fujimoto, Y.-i. Hayashi, N. Homma, A. Beckers, J. Balasch, B. Gierlichs, and I. Verbauwhede, "Em information security threats against ro-based trngs: The frequency injection attack based on iemi and em information leakage," *IEEE Transactions on Electromagnetic Compatibility*, vol. 61, no. 4, pp. 1122–1128, 2018.

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

Appendix

A. Diode Simulation

Simulation: To verify our assumption, we conduct a simulation using TINA-TI [16], an analog circuit simulation software. The simulated circuit is shown in Figure 17(a). We perform AC analysis in which the V_{CC} frequency sweeps from 1Hz to 1GHz logarithmically, and in the meantime we measure the signal's gain in the diode's reverse direction. Ideally, the diode should eliminate all signals in the reverse direction. However, the frequency response shown in Figure 17(b) validates that a high-frequency signal can pass the diode. For example, in the simulated case, a signal above 2MHz can go through the diode in the reverse direction without being attenuated.



(a) Setup.

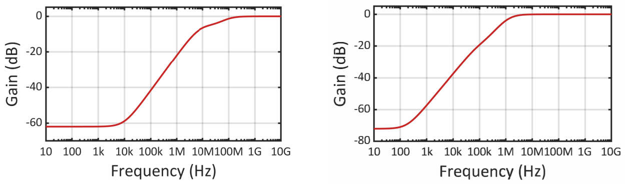
(b) Frequency response.

Figure 17. Illustration of the simulation of diode 1N1183. (a) The simulation setup. The power supply signal is a sine wave with an amplitude of 3V. (b) The frequency response of the diode.

B. Transistor Simulation

Transistor as an amplifier: To validate the theoretical analysis, we conduct a simulation as shown in Figure 7(a). The power supply is a sine wave with an amplitude of 3V and a 5V DC bias. We sweep the signal frequency from 10Hz to 10GHz logarithmically and measure the output voltage, which is proportional to the output current. In the meantime, we calculate the gain between the peak-to-peak value of the output voltage and the power supply signal at different frequencies. The results in Figure 18(a) validate that power supply signals of higher frequencies can affect the amplifier's output with a higher gain. For example, a power supply signal above 1GHz can go through the BJT without attenuation.

Transistor as a switch: To verify our analysis, we conduct a simulation as shown in Figure 7(b). We set the power supply as a 10V DC voltage superimposed by a 3V sine wave. We sweep the frequency of the power supply signal from 10Hz to 10GHz to measure the frequency response as shown in Figure 18(b). It shows that similar to the previous simulations, power supply signals of higher frequencies are more likely to penetrate a closed MOSFET switch. For example, when the frequency is larger than 4MHz, the power supply signal will appear in the switch's output as if the switch is turned on.



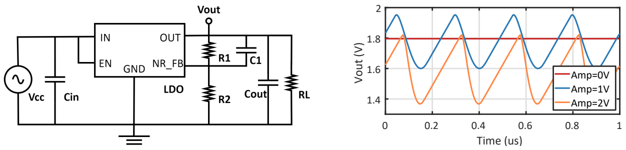
(a) Frequency response of an amplifier.

(b) Frequency response of a switch.

Figure 18. Illustration of the simulation results of transistors. (a) The frequency response of BJT 2N1420 as an amplifier. (b) The frequency response of MOSFET 2N6762 as a switch.

C. LDO Simulation

Simulation: We conduct a simulation on TPS79501, a common low-dropout linear voltage regulator, as shown in Figure 19(a). It requires a 5V DC power supply and outputs 1.8V voltage. We add a sine wave with an amplitude of 2V into the power supply and sweep its frequency from 10Hz to 100GHz logarithmically. Then we measure the V_{out} and calculate the gain at different frequencies. The results indicate that power supply signals can go through the LDO and affect the outputs. The gain achieves a maximum of -19dB at 4MHz and shows a similar frequency response below 4MHz with the MOSFET. However, the gain decreases when the frequency is above 4MHz due to the existence of C_{out} in the circuit. Apart from the AC output, there is also a DC bias in the output signal in Figure 19(b), which is due to the impedance difference between the MOSFET's on and off states.



(a) Setup.

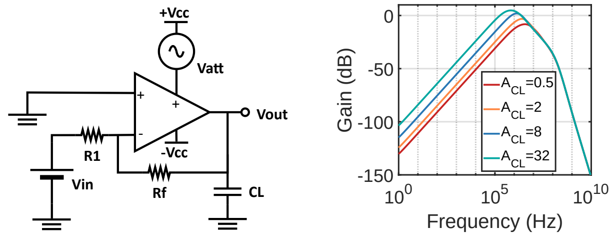
(b) Output signal.

Figure 19. Illustration of the simulation of LDO TPS79501. (a) The simulation setup. (b) The output signal of the LDO under different amplitude of 4MHz power supply signal.

D. Operational Amplifier Simulation

Simulation: We conduct a simulation on OPA4H014-SEP, a state-of-the-art operational amplifier, as shown in Figure 20(a). The input signal is a 100mV DC signal, and the power supply voltage is ±9V. We add a sine wave signal with an amplitude of 3V to the positive power supply voltage. We measure the op-amp's output and calculate the signal gain between the peak-to-peak value of the output voltage and the positive power supply at different frequencies. The results shown in Figure 20(b) indicate that power supply signals of high frequencies can affect the output of an operational amplifier. For example, when the closed-loop gain A_{CL} is 0.5, the signal gain reaches the maximum of

-8.2dB at the frequency of 3.8MHz. It shows a similar frequency response as the transistor below 3.8MHz. However, the signal gain decreases if the frequency is above 3.8MHz because the capacitor C_L acts as a low-pass filter. Moreover, the results also show that the signal gain increases with the close-loop gain A_{CL}, indicating that the power supply signal is more likely to affect the op-amp's output if it has a higher amplification ratio.



(a) Setup. (b) Frequency response.

Figure 20. Frequency response of the operational amplifier OPA4H014. With a close loop gain A_{CL} of 0.5, the attack signal at 3.8MHz can affect the output with a gain of -8.2dB. The attack signal is more likely to affect the output when the A_{CL} increases.

E. Shunt reference

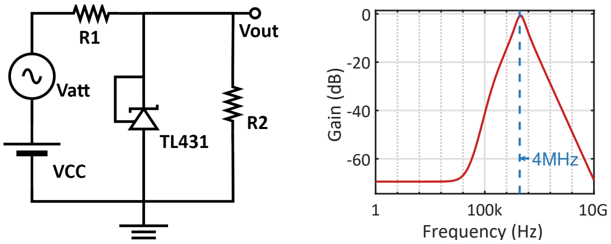
A shunt reference maintains a constant output voltage by shunting excess current to the ground. When the power supply voltage increases, the excess current flows into the ground through the triode $Q1$. The power supply voltage V_{cc} should satisfy the following equation.

$$\frac{(V_{ccmax} - V_{out})}{R_{bias}} \leq I_{loadmax} + I_{Qmax} \tag{14}$$

$$\frac{(V_{ccmin} - V_{out})}{R_{bias}} \geq I_{loadmin} + I_{Qmin} \tag{15}$$

where V_{out} is the generated voltage reference, V_{ccmax} and V_{ccmin} are the maximum and minimum power supply voltage, $I_{loadmax}$ and $I_{loadmin}$ are the maximum and minimum current flowing through the load, and I_{Qmax} and I_{Qmin} are the maximum and minimum current flowing through $Q1$. When the power supply voltage exceeds the valid range, the generated voltage reference V_{out} will not remain the same.

Simulation: We take the shunt reference as an example and simulate a circuit shown in Figure 21(a). The shunt reference is TL431, a precision programmable reference component designed by TI. The power supply voltage is 5V, and we add an attack signal V_{att} with an amplitude of 2V and measure the frequency response between 1Hz-10GHz. The results in Figure 21(b) indicate that power supply signal, e.g., at 4MHz, can go through the shunt reference with a gain of -0.6dB and affect the output. However, power supply signals above 4MHz can hardly go through the shunt reference, because the MOSFET has a low impedance to high-frequency signals.



(a) Setup. (b) Frequency response.

Figure 21. Simulation on the shunt reference TL431. (a) The simulation setup. (b) Result shows 4MHz attack signal can affect the output with a gain of -0.63dB.

F. Active Filter

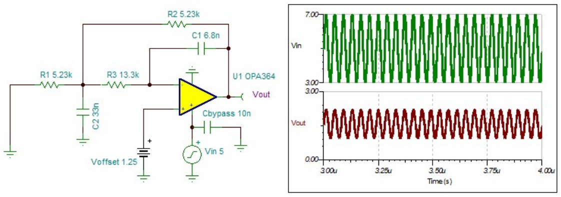


Figure 22. Simulation of filters.

G. Analysis of DYTB-002 and BMP280

We investigate the reason of high standard deviations in the DYTB-002 and BMP280 experiments. First, we evaluate 5 more instances of these sensors. For the force sensor DYTB-002, we measure a 9.8kg piece of metal and inject attack signals at a frequency of 342MHz. The experiment results are shown in Table 5. The statistical results are similar to those of instances N1 $\sim$ N4. For the sensor BMP280, we inject attack signals of 0.25V at a frequency of 568MHz. The experiment results are shown in Table 6. We attribute the high standard deviations to differences in component selection, circuit layout, and soldering processes, which affect the electrical parameters of the sensor circuits. For example, we measure the equivalent impedance of the DYTB-002 instances at the power input terminal and observe that the fifth instance (N5) has a smaller impedance at the attack frequency.

TABLE 5. ATTACK RESULTS OF 5 INSTANCES (N6 $\sim$ N10) OF THE FORCE SENSOR. THE ATTACK FREQUENCY IS 342MHZ.

Amplitude(V)	0.5	1	1.5	2
Deviation(kg)	-0.4	-1.3	-3.2	-5.5
Stdev.(kg)	0.07	0.2	0.8	1.4

TABLE 6. ATTACK RESULTS OF 5 INSTANCES OF SENSOR BMP280. THE ATTACK FREQUENCY IS 568MHZ AND THE AMPLITUDE IS 0.25V.

Type	Output			
	Original	Deviation	Rate	Stdev.
Pressure	98300 Pa	-63 Pa	-0.06%	20 Pa
Temperature	27.2°C	-0.7°C	-2.5%	0.2°C

H. Counterfeit Battery

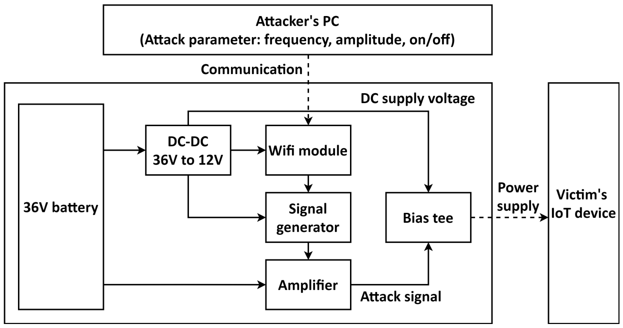


Figure 23. Structure diagram of the counterfeit battery.

I. Customized Coupler

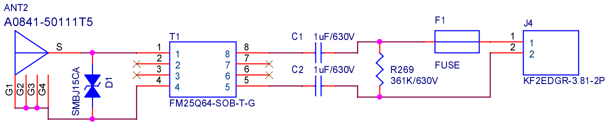


Figure 24. Schematic diagram of the customized coupler.