LightAntenna: Characterizing the Limits of Fluorescent Lamp-Induced Electromagnetic Interference

Fengchen Yang, Wenze Cui, Xinfeng Li, Chen Yan†, Xiaoyu Ji, and Wenyuan Xu
Zhejiang University
{yangfengchen, wenze, xinfengli, yanchen, xji, wyxu}@zju.edu.cn

***Abstract*—Fluorescent lamps are almost everywhere for electric lighting in daily life, across private and public scenarios. Our study uncovers a new electromagnetic interference (EMI) attack surface that these light sources are actually able to manipulate nearby IoT devices in a contactless way. Different from previous EMI attempts requiring a specialized metal antenna as the emission source, which can easily alert victims, we introduce `LightAntenna` that leverages unaltered everyday fluorescent lamps to launch concealed EMI attacks. To understand why and how fluorescent lamps can be exploited as malicious antennas, we systematically characterize the rationale of EMI emission from fluorescent lamps and identify their capabilities and limits in terms of intensity and frequency response. Moreover, we carefully design a covert method of injecting high-frequency signals into the fluorescent tube via power line transmission. In this way, `LightAntenna` can realize controllable EMI attacks even across rooms and at a distance of up to 20 m. Our extensive experiments demonstrate the generality, practicality, tunability, and remote attack capability of `LightAntenna`, which successfully interferes with various types of sensors and IoT devices. In summary, our study provides a comprehensive analysis of the `LightAntenna` mechanism and proposes defensive strategies to mitigate this emerging attack surface.**

I. Introduction

Fluorescent lamps have been pervasive in industrial production and everyday life for decades. They consume less energy than incandescent lamps and are more available and affordable than LEDs [21]. In addition, their large lighting angle, uniform lighting effect, and diverse light colors make fluorescent lamps preferable in places demanding low-cost, long-time, and large-area lighting, such as factories, hospitals, offices, libraries, etc. Although LEDs are more efficient and eco-friendly, it is reported that consumers prefer fluorescent lighting to a greater extent [42], [11], especially in developing countries, and the global fluorescent lighting market is predicted to grow with a compound annual growth rate of 9.5% from 2023 to 2030 and reach 14.8 billion USD [45]. Ideally, fluorescent lamps are designed to convert electrical energy into light. However, in this paper, we uncover a troubling reality: fluorescent lamps can also be maliciously exploited as antennas to emit electromagnetic interference (EMI) and control neighboring Internet of Things (IoT) devices in a contactless manner. For instance, an adversary with control of the lighting in a victim's home may invisibly inject EMI into a voice assistant's microphone and instruct it to "open the door". Even more worrisome is the use of fluorescent lamps in hospitals. If an adversary controls these lights, she may use them to emit EMI and tamper with the measurement of temperature sensors in infant thermostats [51], [25], causing incorrect temperature control and possibly fatal consequences.

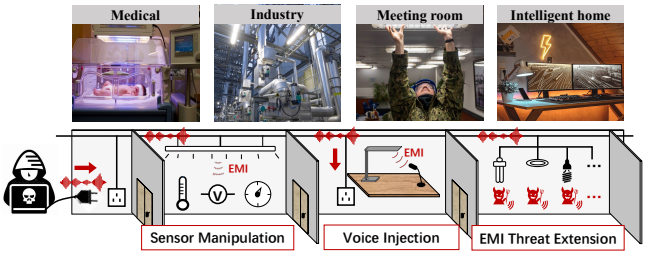


Fig. 1. An illustration of `LightAntenna`. The attacker can inject high-frequency signals into the power grid, control the pre-existing fluorescent lamps to emit EMI and manipulate sensors, inject voice into microphones, or cause other EMI threats.

Existing EMI attacks require the adversary to bring a specialized metal antenna and deploy the attack equipment locally to emit signals from at most a few meters away from the target device [62], [63], [26], [59], [22]. However, the requirement to access the local environment is usually challenging in everyday life, and the adversary's antenna and attack equipment are likely to alert victim users onsite.

This work makes the first attempt to reveal a new EMI attack threat model, i.e., by exploiting fluorescent lamps that are already installed in the local environment as antennas to emit malicious EMI signals. Since lamps are present in almost every room in medical, industrial, and home scenarios, such attacks can be launched in various locations and are intrinsically difficult to notice. To achieve such effects without making any modifications to fluorescent lamps or the local environment, we design `LightAntenna`, a technique that can remotely control ordinary fluorescent lamps to emit EMI in desired waveforms, by injecting carefully crafted high-frequency signals into the shared power lines. `LightAntenna` enables long-range EMI attacks across rooms as depicted in Fig. 1, which can manipulate sensor readings, inject voice commands,

† Chen Yan is the corresponding author.

Network and Distributed System Security (NDSS) Symposium 2025
24-28 February 2025, San Diego, CA, USA
ISBN 979-8-9894372-8-3
https://dx.doi.org/10.14722/ndss.2025.242334
www.ndss-symposium.org

etc. Nonetheless, realizing LightAntenna is challenging in two aspects: (1) *How to make fluorescent lamps generate EMI attack signals?* Fluorescent lamps are not designed to emit EM signals like antennas. Though they are known for unintentional EM radiation below 50 kHz, it is unclear whether these lamps can emit signals of sufficient intensity and at the frequency range (usually MHz) required for EMI attacks [26], [8], [48], [57]. (2) *How to control the EMI signals emitted by a fluorescent lamp and use them to manipulate other IoT devices?* Fluorescent lamp circuits generally do not contain MCUs, which makes it impossible to realize controllable attacks by implanting malicious codes like in [18], [68].

To tackle the first challenge, we begin by analyzing the operating principles of fluorescent lamps, which consist of two primary components: the ballast and the fluorescent tube. Our theoretical analysis and measurement experiments confirm that the fluorescent tube, rather than the ballast, is the predominant source of EMI emissions. To systematically characterize the limits of fluorescent lamps as antennas for EMI attacks, particularly in terms of radiation intensity and frequency response, we conduct feasibility analysis experiments. The comparative experiments involving various combinations of ballasts and fluorescent tubes reveal that the ballast's operating frequency directly affects the frequency of the emitted EMI. We also examine the impact of distance, power, and tube shape on EMI strength. By performing frequency sweeps with injected signals, we generate broad-spectrum frequency response curves, which establish a foundation for identifying optimal coupling frequencies for subsequent attacks on IoT systems.

To tackle the second challenge, we identify the power line as a promising channel to transmit attack signals since fluorescent lamps are inherently connected to the grid. By modeling the transmission of the attack signal in power lines, we understand the mechanisms and limitations of the signal transmission in the complex power grid. We also characterize the attenuation of the attack signal due to the built-in rectification and filtering circuits when it is transmitted through the ballast, so that the attack signal can be successfully injected into the fluorescent tube for further controllable attacks. For the above signal transmission stage, we design DC and AC couplers to inject high-frequency attack signals into the DC power or AC power of off-the-shelf fluorescent lamps. We set the LPF (low-pass filter) to isolate the experimental grid from the public grid, prevent polluting the grid and damaging extraneous equipment. Finally, we develop two signal crafting methods, namely tampering attacks and manipulation attacks, that enable controllable attacks on various types of sensors, ranging from general data tampering to precise value manipulation. Our experiments showed that these attacks could effectively alter sensor measurements and behaviors in a predictable manner.

The extensive experiments involve 8 different types of sensor modules, an industrial sensor, and a conference gooseneck microphone. These sensors are widely used in various of IoT devices, and once they are attacked, it will directly or indirectly lead to security issues for IoT devices. In summary, our evaluation comprehensively validates four aspects of LightAntenna: (1) **Generality**: We utilized the fluorescent lamps to achieve tampering attacks on 8 different sensor modules. (2) **Practicality**: We utilized the fluorescent lamps to achieve a controllable manipulation attack on an industrial PT100 thermocouple temperature sensor. (3) **Tunability**: We utilized fluorescent lamps to inject voice commands into a gooseneck microphone and successfully spoof the voice recognition model. (4) Finally, we implemented a **remote attack** by injecting signals into the power grid at a distance from 10 m to 20 m and successfully impacted the thermocouple temperature sensor, and we evaluated the impact of realistic power grid on LightAntenna. In addition, we discuss the mechanics of LightAntenna attacks and propose defensive strategies to mitigate this novel threat to sensor integrity and security.

We summarize our contributions as follows:

1) We reveal a novel optical-electromagnetic covert channel that leverages fluorescent lamps for EMI injection attacks, eliminating the need for specialized antenna equipment.
2) We analyze the EMI produced by fluorescent lamps, characterizing its applicability and limitations.
3) We explore the potential impact of EMI injection attacks on IoT devices and propose corresponding defense strategies.

II. Background

In this section, we introduce the underlying principle of fluorescent lamps and their potential characteristics as non-certified antennas, including the principle of ballast, fluorescent tubes, and plasma antennas.

A. Fluorescent Lamps

Fluorescent lamps are widely used lighting devices that rely on the excitation of mercury vapor to produce light. A fluorescent lamp mainly consists of a ballast and a fluorescent tube.

1) Ballast: Ballast serves as the driver to provide high-frequency voltage for the fluorescent tube's operation. Currently, electronic ballasts are the most commonly used to supply discharge lamps [2], offering numerous advantages, such as improved efficiency or flicker-free operation of the lamp. A typical circuit of electronic ballast is shown in Fig. 2, including three main stages:

- The rectification stage rectifies AC to DC by a rectifier bridge circuit, which is usually used in AC-powered fluorescent lamps.
- The self-excited oscillation stage is the most critical stage, which generate high-frequency voltage to ensure the lighting of the lamp, the output frequency of the self-excited oscillation stage is usually from 40 kHz $\sim$ 50 kHz [15].
- The transformer stage provides a high voltage of 600 V $\sim$ 800 V to ionize the rare gases inside the lamp at the moment of lighting up. After the fluorescent lamp is lightened, the transformer stage outputs the voltage with a stabilized amplitude in the range of 200 V $\sim$ 300 V.

Power supply methods of electronic ballasts. To support further analysis, we investigated the power supply method of commercially available fluorescent lamps. Most fluorescent

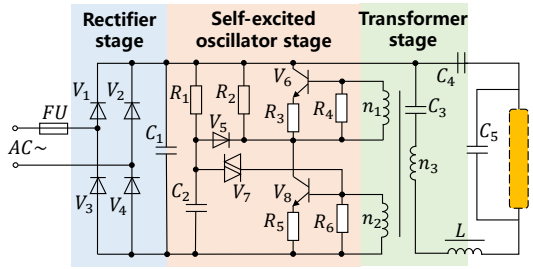


Fig. 2. A typical circuit of electronic ballasts. Mainly including the rectifier stage, the self-excited oscillator stage, and the transformer stage.

lamps are designed for alternating current (AC) power systems, as they are originally developed for use in standard AC power grids. Recently, with technological advances and specific application demands, some electronic ballasts have also been designed for direct current (DC) power systems, particularly in solar and emergency lighting systems. We examined 61 ballasts on the market, covering major fluorescent brands such as GE, Philips, Osram, Panasonic, and others. According to our survey, 60 ballasts adopt 220 V AC power, and 1 ballast adopts 24 V DC power.

2) Fluorescent Tube: The fluorescent tube is the light-emitting component of fluorescent lamps, which consists of glass tubes coated with phosphor on the inner wall, mercury vapor inside, and electrodes, as shown in Fig. 3. When powered on, the ballast provides an instantaneous high voltage on the electrodes of the fluorescent tube, ionizing the gas around the electrodes and forming electric arcs. This process ionizes the mercury vapor, producing ultraviolet light, which then excites the phosphor coating to emit visible light. In a steady state, the voltage ranges from 100 V for tubes under 30 W and 100 V $\sim$ 175 V for tubes of 30 W or more [27].

Notably, the ionization of the gas inside the fluorescent tube can be also called plasma. Plasma is the fourth state of matter, in which atoms are split into free negative electrons and positive ions by DC discharge, RF discharge, or laser excitation [66]. For a lightening fluorescent tube, the interior free electrons can flow swiftly and create current under the electric field, then form the plasma. Thus, similar to the conductivity concept of metal antennas, fluorescent tubes have the capacity to transmit and receive electromagnetic signals with the conversion of electric and magnetic. Besides, as the current in the fluorescent tube has a high frequency (40 kHz $\sim$ 50 kHz), it will generate EMI in the same frequency range.

B. Plasma Antenna

The plasma antenna is a specialized type of antenna that uses ionized gas (plasma) as its conducting medium instead of traditional metal elements. Compared to conventional metal antennas, plasma antennas offer the key advantage of adjustable electrical properties through modifications in plasma density and other parameters. They can be rapidly switched on and off, providing stealth capabilities by becoming virtually invisible to radar when deactivated. Additionally, they are resistant to electromagnetic interference, making them suitable for both civilian and military communications where low observability and high performance are essential. Consequently, plasma antennas are often employed in scenarios requiring stealth, such as in military aircraft.

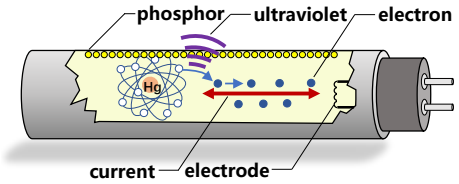


Fig. 3. The structure of a fluorescent tube. A fluorescent tube mainly includes a glass tube, the inside mercury vapor, and the electrodes.

Fluorescent tubes and plasma antennas share many similarities in their operating principles. This similarity suggests that fluorescent lamps could potentially be used as covert antennas by adversaries to launch EMI attacks on IoT devices.

C. EMI Threats on Sensors of Cyber-physical Systems

Sensors are the entry points of cyber-physical systems (CPS) and serve as the connectors between cyber systems and the physical world. Existing research has demonstrated that EMI can affect sensor performance, leading to security and privacy issues. However, previous work required specialized antennas to transmit EMI signals, which made the attack easy to be detected. In this paper, we show that fluorescent lamps can be repurposed as antennas to launch EMI attacks, introducing a new attack vector for CPS.

III. Threat Model

This article reveals that fluorescent lamps can be exploited as malicious antennas to launch EMI attacks. We make the following assumptions about the adversary and the victim.

Attack goal: The adversary's goal is to utilize fluorescent lamps to create EMI threats on CPS, such as maliciously manipulating temperature sensors to cause runaway temperatures in critical systems (e.g., the infant thermostats and industrial reactors), or injecting voice signals into the microphone to cause security and privacy issues.

Attack scenarios: We consider two scenarios. In the first scenario, the attacker injects attack signals through the power grid shared with the victim, where the attacker can be a neighbor or even a passerby. In the second scenario, the attacker uses a malicious external mobile power source to inject attack signals into the fluorescent lamps.

Non-invasive attack: The attacker cannot modify the software or hardware of the target fluorescent lamps or victim sensors. Instead, she can only inject attack signals through the power grid or external mobile power source. For remote attacks, the distance between the fluorescent lamps and the injection node should be within 20 m.

Victim fluorescent lamps and sensors: We assume that the fluorescent lamp is connected to the malicious power source and is in the operation state, with the target sensor within 15 cm of the fluorescent lamps.

Prior knowledge about the target: The attacker does not need information about the victim's fluorescent lamps but should conduct pre-tests on the victim's sensors, such as frequency sweep tests, to determine the attack frequency. Since the sensors are on sale, the attacker can purchase them from the market for these pre-tests, similar to most EMI attacks.

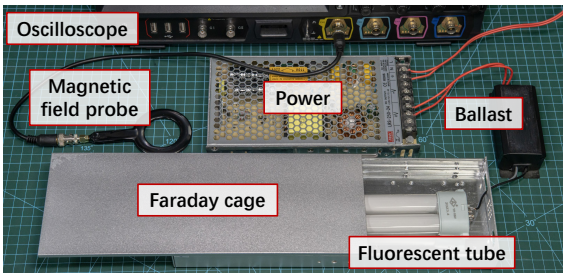


Fig. 4. The experiment setup of ballast and fluorescent tubes. Include the test ballasts and fluorescent tubes, the Faraday cage, and the measurement devices.

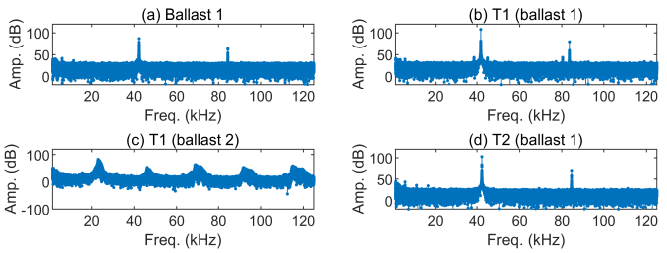


Fig. 5. The unintentional EMI of ballast and fluorescent lamps. (a) Only ballast 1; (b) ballast 1 drives fluorescent tube 1; (c) ballast 2 drives fluorescent tube 1; (d) ballast 1 drives fluorescent tube 2. () means that the ballast is shielded.

IV. Analysis of the EMI of Fluorescent Lamps

To understand why fluorescent lamps can be utilized as malicious antennas, we need to investigate the source of a lamp's unintentional EMI. It is essential to first address the following 2 questions: *A.* How do fluorescent lamps generate EMI? *B.* How are the EMI performances of the fluorescent lamps? In this section, we will systematically analyze the EMI generation mechanism of fluorescent lamps and test the EMI performance of fluorescent lamps.

A. The EMI Generation of Fluorescent Lamps

Since fluorescent lamps rely on high-frequency voltage to ionize the mercury vapor, they are likely to produce unintended electromagnetic interference. For a fluorescent lamp in a working state, there are mainly two EMI sources: One is the high-speed switching of semiconductor components inside the electronic ballast, and another is the high-frequency currents inside the fluorescent tube. Although these kHz-level EMI signals cannot be utilized in our attack, they have been reported to affect iPhone [41], Microsoft Surface [7], [53], radio signals [35], TV signals [44], and Internet [56], and figuring out the main EMI source can guide the following attack designs and the defense of threats.

1) EMI of Electronic Ballasts: It is known that current alternating at high frequency in the circuits of most electronic equipment can produce radiated and conducted EMI. Similarly, the high-frequency switching semiconductor elements in the electronic ballasts will also cause conducted and radiated EMI noise. Of course, the EMC developers have noticed this problem and have taken proper EMC measures to control it within safe limits. For example, custom-designed filters are required to meet the limits for conducted and radiated EMI noise. In the European Union, the relevant standards for lighting systems are EN55015 for conducted and radiated EMI in the range $9\,\mathrm{kHz} \sim 30\,\mathrm{MHz}$ and EN55015 or EN55022 for radiated noise in the range $30\,\mathrm{MHz} \sim 1\,\mathrm{GHz}$ [15]. So we infer that the electronic ballasts of fluorescent lamps may not be able to serve as effective antennas.

2) EMI of Fluorescent Tubes: With the driving of ballasts, the mercury vapor in the fluorescent tubes will be ionized and form the plasma. Notably, plasma is one of four states of matter (the other three are solid, liquid, and gas) characterized by a significant portion of charged particles in any combination of ions or electrons [32]. The presence of charged particles makes plasma electrically conductive [60]. Thus, it can be used in electromagnetic applications such as antennas, transmitting and receiving RF signals. Besides, fluorescent tubes are exposed to the air due to their work, and most RF shielding materials are opaque, making it difficult to resist the EMI of fluorescent tubes.

3) Test of the EMI Source: To investigate: ① Whether the EMI of fluorescent lamps is produced by ballasts or fluorescent tubes? ② Whether the EMI characteristics are determined by the ballasts or fluorescent tubes? We conducted a control test on 2 different ballasts (a $220\,\mathrm{V}$ AC ballast and a $24\,\mathrm{V}$ DC ballast) and 2 different fluorescent tubes (a $25\,\mathrm{W}$ tube and a $18\,\mathrm{W}$ tube) disassembled from off-the-shelf fluorescent lamps. We called them ballast 1, ballast 2, T1 and T2. The experiment setup is shown in Fig. 4. The AC-DC converter is used to convert the $220\,\mathrm{V}$ AC power into $24\,\mathrm{V}$ DC power, the ballast is used to drive the fluorescent tubes, and the Faraday cage is used to shield the EMI of ballasts or fluorescent tubes to form controlled experiments. Finally, the magnetic field probe and oscilloscope are used to measure and record the EMI.

To answer question ①, we first shielded T1 using the Faraday cage and measured the EMI of ballast 1 at a distance of $10\,\mathrm{cm}$; then, we shielded ballast 1 and measured the electromagnetic field of T1 at a distance of $10\,\mathrm{cm}$. The result is shown in Fig. 5 (a) and Fig. 5 (b), as we can see, without T1, ballast 1 can generate EMI with the amplitude of $85\,\mathrm{dB}$, while T1 can generate EMI with the amplitude of $110\,\mathrm{dB}$, the EMI intensity generated by fluorescent tubes is about $25\,\mathrm{dB}$ higher than that generated by ballasts. Thus, we can conclude that the EMI of fluorescent lamps is mainly produced by fluorescent tubes rather than ballasts.

To answer question ②, we used the same ballast (ballast 1) to drive different fluorescent tubes (T1 and T2), the result is shown in Fig. 5 (b) and (d); and used different ballasts (ballast 1 and ballast 2) to drive the same fluorescent tube (T1), the result is shown in Fig. 5 (b) and (c). According to the result, we can find that: (1) different ballasts can drive the same fluorescent tube to generate EMI at different frequencies, e.g., ballast 1 drives fluorescent tubes to generate EMI at around $41\,\mathrm{kHz}$, while ballast 2 drives fluorescent lamps to generate EMI at around $22\,\mathrm{kHz}$; (2) the same ballast can drive different fluorescent tubes to generate EMI at the same frequency but different amplitude, which is because different fluorescent tubes have different rare gas density and form plasma antennas with different characteristics. Thus, we can conclude that the EMI frequency of fluorescent tubes is determined by the ballasts, while the EMI intensity is determined by both the ballast and the fluorescent tubes.

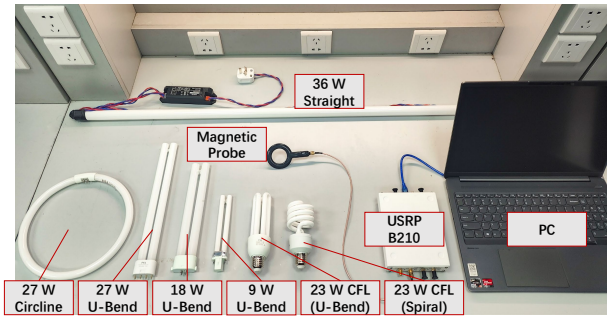


Fig. 6. The experiment setup of unintentional EMI intensity test of different fluorescent tubes. We tested 7 fluorescent tubes with different power and shapes with a magnetic probe, a USRP B210, and a PC.

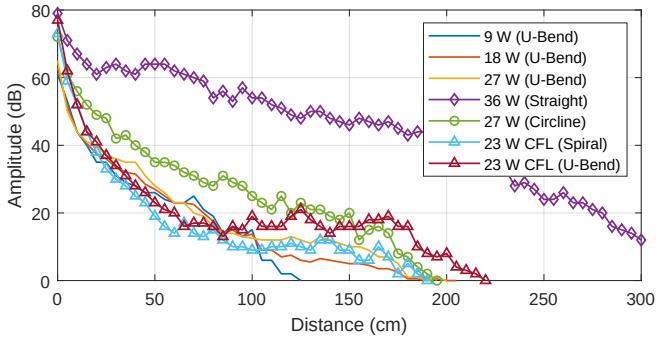


Fig. 7. The result of unintentional EMI intensity of different distances. Include 7 fluorescent tubes with different power and shapes. The amplitude is referenced to the EMI noise intensity in the environment, which is set to 0 dB.

B. The EMI Performance of the Fluorescent Lamps

The antenna is the interface between radio waves propagating through space and electric currents moving in metal conductors [16]. For EMI attacks, the EMI intensity and frequency range are the two main performances of antennas. To investigate whether fluorescent lamps can replace metal antennas in EMI attacks, we need to test the EMI intensity and frequency range of fluorescent lamps.

1) Unintentional EMI Intensity: It is known that all metal conductors carrying a high-frequency current can produce EMI. However, the main difference between antennas and metal conductors is that antennas can convert electric signals into electromagnetic signals with higher intensity. Thus, the unintentional EMI intensity of the fluorescent lamp is an essential indicator. We conduct the following experiment to test the unintentional EMI intensity of the fluorescent lamps.

To investigate the impact of the distances, power, and tube shapes on the unintentional EMI intensity, we selected 7 fluorescent tubes with different power and shapes to test the EMI intensity from 0 m to 3 m, including 3 U-Bend fluorescent tubes (9 W, 18 W, and 27 W), a 36 W straight fluorescent tube, a 27 W circline fluorescent tube, and 2 compact fluorescent lamps (CFL) with spiral and U-Bend shapes. We use the USRP (Universal Software Radio Peripheral) B210 and a near-field magnetic probe to measure the EMI intensity and calculate the amplitude gain relative to the environment EMI noise with MATLAB. The experiment setup is shown in Fig. 6.

The result is shown in Fig. 7: By comparing the unintentional EMI of 3 U-Bend fluorescent tubes with the power of 9 W, 18 W, and 27 W, we can find that higher power fluorescent tubes can produce stronger EMI, this is because higher power leads to higher ionization of the mercury vapor and forms higher density plasma; By comparing the U-Bend and circline fluorescent tubes with the same power of 27 W, we can find that circline fluorescent tubes can produce stronger EMI than U-Bend lamps, this is due to the larger radiating area of the circline tubes; By comparing the 2 compact fluorescent lamps with the same power, we can find that the EMI intensity of spiral and U-Bend CFLs are not significantly different. In conclusion, we can conclude that: ① the unintentional EMI generated by fluorescent lamps can radiate 2 m $\sim$ 3 m away (The EMI amplitude is referenced to the EMI noise intensity in the environment, which is set to 0 dB); ② the power and tube shape are the 2 main impact factors of the fluorescent tube's EMI, the higher power and larger radiating area can cause stronger EMI.

2) Intentional EMI Frequency Range: According to the previous analysis in the Background, fluorescent tubes only produce EMI at a single frequency between 20 kHz to 50 kHz in normal operation, which varies depending on the ballasts. However, most EMI attacks [26], [8], [48], [57] are usually at MHz level. Thus, if we want to utilize the fluorescent lamps to launch EMI attacks, we need to test the frequency response of the fluorescent lamps' intentional EMI. Notably, unlike lighting the fluorescent lamps, ionizing the rare gases inside the fluorescent tubes and generating EMI only needs about a 10 W power [34], so there are two ways to drive the fluorescent tubes: One is to inject the RF signals into the power supply, and another is to use the RF signals to directly drive the tubes. To compare the two methods, we conducted the following experiments: ① using the power source coupled with a 20 W signal to drive the fluorescent tubes; ② directly using a 20 W signal to drive the fluorescent tubes, which will not light them up. In detail, we designed the following steps:

First, we used the signal generator N5171B [54] to generate signals from 700 MHz $\sim$ 1500 MHz and amplified it to 20 W with RF amplifier HPA-50W-63+; then we used a customized coupler to inject the signals into the 24 V power source or directly used them to drive the fluorescent tubes. Finally, we used the near-field magnetic probe and the USRP B210 to measure the EMI spectrogram and record the signal intensity at different frequencies with a distance of 10 cm.

However, we need to note that the signal generator, RF amplifier, and power line also produce EMI. To eliminate these interference factors, we customized an RF shielding box to isolate the fluorescent lamps, the shielding box has a size of 50 cm $\times$ 50 cm $\times$ 50 cm and shielding effect of more than 70 dB in the range of 100 MHz $\sim$ 3 GHz. Then, we put the tested fluorescent tubes and magnetic probes into the shielding box, as shown in Fig. 13.

The result is shown in Fig. 8, as we can see: Fluorescent lamps have a stable gain in all frequency bands, like a broadband antenna; By comparing the intentional EMI intensity of "only RF" and "Power + RF" at different frequencies, we can find that inject RF signals into the power source

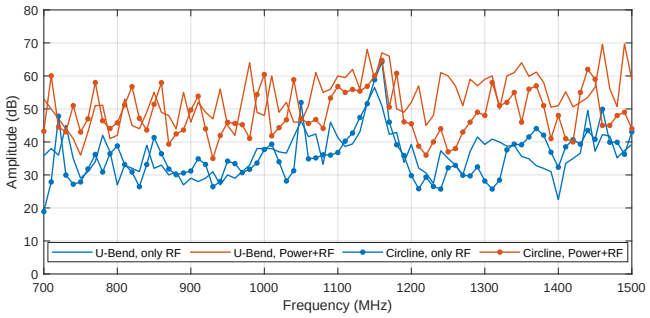


Fig. 8. The frequency response of the fluorescent lamps' intentional EMI. We tested 2 fluorescent tubes (a 27 W U-Bend fluorescent tube and a 27 W circline fluorescent tube) with 2 signal injection methods (inject signals into the tube without ballast, and inject signals into the power under normal working state).

can improve the intentional EMI intensity of the fluorescent tubes, compared with directly using RF signals to drive the fluorescent tubes. This is because the gas can be ionized more adequately when the RF signals are injected into the power source, while only injecting RF signals into the fluorescent tubes will consume some energy to ionize the gas; For the same power, circline fluorescent lamps have slightly better gain than the U-Bend fluorescent lamps, which matches the result of the previous test. Thus, we can conclude that: ① Fluorescent lamps have a wide bandwidth in the EMI attack band and are promising to be used as antennas for EMI attacks. ② Injecting RF signals into the power source of the fluorescent tubes can achieve a better effect in generating EMI.

V. How to Achieve Controllable Attacks?

After analyzing the EMI of fluorescent lamps, we seek to achieve controllable EMI attacks on sensors. First, we analyze how attack signals reach the fluorescent tubes; then we design `LightAntenna`, which controls sensors by utilizing the fluorescent lamps to generate EMI signals.

A. Transmission of the Attack Signals

Before the attack design, we need to analyze the transmission process of high-frequency attack signals from the power grid to the fluorescent lamp tube. Mainly including: *1)* the transmission of the high-frequency signals in the power grid; *2)* the transmission of the high-frequency signals in the lamp's circuit (a.k.a. electronic ballast).

1) Transmission in the Power Grid: Compared with the EMI attacks with metal antennas, one important advantage of utilizing fluorescent lamps to generate EMI is that the fluorescent lamps leave the power source as a hidden path for the transmission of attack signals, which opens a door for remote manipulations.

The transmission of the MHz-level attack signals in power lines has been proved feasible by the power line carrier communication (PLCC). PLCC employs modulation techniques like Amplitude Shift Keying (ASK), Frequency Shift Keying (FSK), or Phase Shift Keying (PSK) to encode data onto the carrier wave, usually from tens of kHz to tens of MHz. These methods vary the carrier's characteristics based on the data to be transmitted, allowing for efficient use of the power line

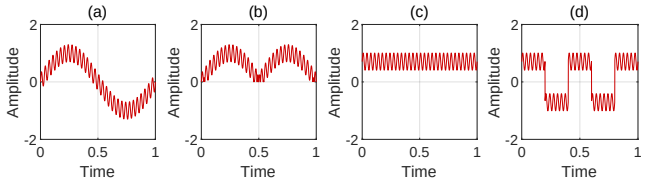


Fig. 9. Transmission of power signal superimposed with attack signal $v(t)+v_a(t)$ in electronic ballasts: (a) power input, (b) after rectification, (c) after filtering, (d) after self-excited oscillation.

channel. Of course, the impulsive noises from other loads [1] may affect the signal transmission of `LightAntenna`, and we will evaluate the impact of loads and power branches on `LightAntenna` in Section VI.

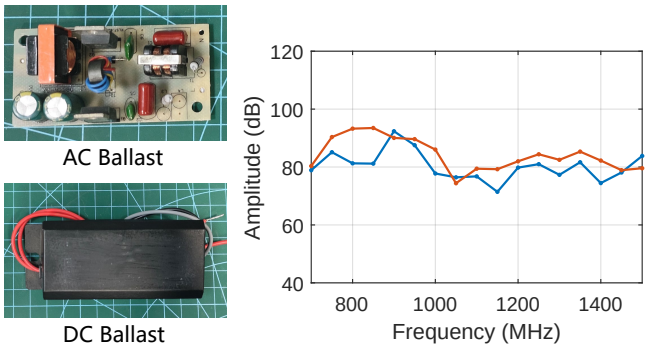
2) Transmission in the Ballast: It is known that most electronic devices have been designed with EMC protection measures to resist noise from the power supply. Thus, another challenge is the transmission of the attack signals in the ballast circuit.

According to Fig. 2, the electronic ballast circuit mainly includes a rectification stage, a filtering stage, and an inverter. We assume the input of the ballast is $v(t)+v_a(t)$, as shown in Fig. 9 (a), where the $v(t)$ is the AC power and $v_a(t)$ is the high-frequency attack signal. In the rectification stage, since the frequency of the attack signal (several hundred MHz) far exceeds the maximum response frequency of the rectifier bridge diode (several kHz), the diodes will only switch on and off according to the AC power, so the rectification stage produces little obstruction to the high-frequency attack signals, generating the signal in Fig. 9 (b); in the filtering stage, because the capacitors and inductors of the low-pass filter circuit are not ideal devices, so it will produce a filter leakage of the Ultral-high-frequency (UHF) signals, and generating bus voltage $v_{bus}+v_a(t)$, as shown in Fig. 9 (c); in the inverter stage, the self-excited oscillation circuit convert mixed bus signal $v_{bus}+v_a(t)$ into drive signal $v_d(t)+v_a(t)$, where $v_d(t)$ is the desired drive signal with the frequency of $40\,\text{kHz} \sim 50\,\text{kHz}$, as shown in Fig. 9 (d), and the attack signal $v_a(t)$ will be carried to fluorescent tubes.

To verify the above inference, we conducted a frequency response test on both AC and DC ballasts in Fig. 10 (a): We injected a sinusoidal signal with the amplitude of 2.5 V and frequency of $700\,\text{MHz} \sim 1500\,\text{MHz}$ into the input of the ballast and recorded the output with an oscilloscope, then we calculated the gain amplitude at each frequency. According to the result in Fig. 10 (b), we can conclude: ① The signals within the test band can pass through the ballast with acceptable attenuation; ② There is a difference in the degree of attenuation of the signals passing through the ballast, which may be due to the frequency selection of the filtering circuits constituted by the internal components of the ballast.

B. Design of `LightAntenna`

Here, we introduce the attack design of `LightAntenna`. `LightAntenna` reveals a brand new EMI attack that utilizes fluorescent lamps as hidden malicious antennas to launch EMI attacks remotely. To realize `LightAntenna`, we need to tackle the following challenges: 1) Effective signal injection: According to our threat model, the attacker is not allowed to



(a) Ballasts. (b) Frequency response of two ballast.

Fig. 10. The frequency response test of 2 ballasts. Including a 220 V AC ballast and a 24 V DC ballast.

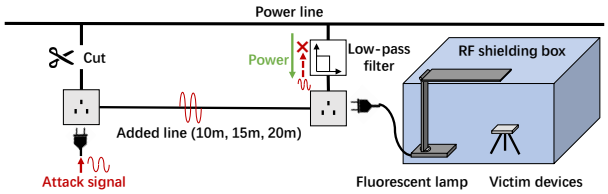


Fig. 11. The design of `LightAntenna`. The attacker remotely injects attack signals into the power grid, the attack signal is transmitted in the power line of 10 m $\sim$ 20 m and arrives at the victim's fluorescent lamps, then the attacker utilizes the fluorescent lamps to emit MEI and attack sensors.

(a) Coupler schematic. (b) 24 V coupler. (c) 220 V coupler.

Fig. 12. The customized couplers for signal injection. Including an AC coupler and a DC coupler.

make any hardware or software manipulation of the victim's fluorescent lamps, so we need to investigate how to inject high-frequency signals into the power of the fluorescent lamps as effective as possible. 2) Controllable attack: It is known that a strong enough EMI can achieve DoS attacks on sensors or other IoT devices. However, if the attacker wants to achieve a controllable attack on the victim device, such as controlling the measurement of the target sensors, we need to investigate how to craft attack signals.

1) Injection of Attack Signals: To design the method to inject high-frequency attack signals into the power, we need to first discuss the power supply methods of fluorescent lamps. According to our market survey, there are two power supply methods for fluorescent lamps: One is AC mains power, usually from 85 V to 270 V, which varies according to country and region, and the other is DC power, e.g. 24 V battery or 24 V AC/DC converter. Among them, most scenarios such as industrial production, medical, and home use 220 V AC-powered ballasts, while in recent years, DC-powered fluorescent lamps are gradually being used in DC-powered systems such as solar lighting systems or emergency lighting. To cover most of the scenarios, we design signal injection methods for AC-powered and DC-powered fluorescent lamps separately.

The injection goal is to generate a controllable high-frequency voltage signal on the power supply of the fluorescent lamps. Directly injecting high-frequency signals into the power source can destroy the RF amplifier. To solve this problem, one possible strategy is to control a load to switch between the on and off modes at a specific frequency and induce corresponding noise in the power grid, as introduced by Yang et al. [64]. However, the frequency of the noise generated by the CPU or GPU can not satisfy the requirements of EMI attacks which are usually at the MHz level.

According to the need for EMI attacks, a compliant coupler needs to be able to both inject high-frequency EMI signals into the power supply and prevent high-voltage signals from the power supply from destroying the signal output device. Based on the frequency selection function of the filter circuit, we finally customized the DC coupler and AC coupler to inject the RF signal into the 24 V DC power and 220 V AC power source. Differently, the 220 V AC coupler is additionally fitted with a voltage amplifier, this is because load variations and noise on power lines can affect attack signal transmission, and higher voltage allows for longer distance attack signal transmission. The 24 V and 220 V couplers are shown in Fig. 12 (b) and Fig. 12 (c).

2) Crafting the Attack Signals: The key to achieving a controllable EMI attack is to craft the attack signals. According to previous EMI attacks, the EMI attacks on sensors of IoT devices can be divided into tampering attacks and manipulation attacks. The tampering attack can tamper with the normal operation of the victim, while the manipulation attack can quantitatively manipulate the victim sensor's output. Here we respectively discuss the crafting of tampering attack signals and manipulation attack signals. **Tampering Attack.** For general analog sensors such as temperature sensors, humidity sensors, voltage sensors, Hall current sensors, etc., we only need to adjust the amplitude and frequency of single-frequency EMI signals, then we can achieve tampering attacks on these sensors. Existing work [57] has demonstrated that some electronic components have a rectification effect on high-frequency signals and will produce deviation in the output. We assume that the EMI coupling frequency of the victim sensor is f, which can be obtained by frequency sweep tests, and then the attack signal can be expressed as Equation (1):

$$s(t) = c(t) = A \cdot sin(2\pi ft), \tag{1}$$

where A is the amplitude of the attack signal, which can be adjusted based on the feedback of the attack result, or roughly determined according to the pre-tests.

Manipulation Attack. More refined EMI attacks need a quantitative manipulation of the target sensors. For example, if an attacker wants to control the output of a temperature sensor to vary sinusoidally, or inject a piece of voice into a microphone, then she needs to set the desired sensor output as baseband signal and craft attack signals.

We select the AM (Amplitude modulation) to craft attack signals and utilize the nonlinear properties of the victims' sensors to demodulate the desired baseband signals. The modulation of the attack signal $s(t)$ can be expressed as Equation (2):

$$s_t = (m(t) + 1) \cdot c(t),\ c(t) = cos(2\pi f_c t), \tag{2}$$

where $m(t)$ represents the baseband signal that the attacker desired, and $c(t)$ represents the carrier signal that can form electromagnetic coupling resonance (ECR) with the circuits of target sensors. Previous works [63], [14], [69] have introduced the nonlinear properties of electronic components: When we inject the modulated signal $s(t)$, the output of microphone will contain the frequency component f_m together with the fundamental frequency components of sin (i.e., $f_c - f_m$, $f_c + f_m$, and f_c), harmonics, and other cross products (i.e., f_m, $2(f_c - f_m)$, $2(f_c + f_m)$, $2f_c$, $2f_c + f_m$, and $2f_c - f_m$), thus carrying the wanted voice control signals.

VI. Evaluation of LightAntenna

In this section, we evaluate the performance of LightAntenna. To evaluate the generality, practicality, and tunability of LightAntenna, we respectively use LightAntenna to perform the EMI attack effect on different sensor modules, industrial sensors, and microphones. Besides, we also investigate the impact of power, distance, and performance of LightAntenna under realistic.

A. Experiment Setup

The experiment setup is shown in Fig. 13. The system of LightAntenna includes the victim devices, attack devices, and test-bed devices. The victim devices are off-the-shelf fluorescent lamps and widely used sensors. The attack devices are used to generate and inject attack signals into the power grid. The test-bed devices are used to eliminate interfering factors in the experimental process and address ethical concerns, ensuring the rigor and legitimacy of experiments.

1) Victim Devices: To evaluate the generality of LightAntenna on various CPS, we selected 8 different sensor modules for evaluation, including a temperature sensor, humidity sensor, sound sensor, photosensitive sensor, infrared sensor, voltage sensor, Hall current sensor, and microphone sensor. Among them, some are used to quantitatively measure the physical variables and output an analog value, such as the value of the temperature, humidity, ultraviolet intensity and current; Some are used to detect the absence of the target physical signal and output a digital signal, such as the sound, light and infrared. These sensors are widely used in various of IoT devices, and once they are attacked, it will directly or indirectly lead to security issues for IoT devices. Besides, to evaluate the practicality of LightAntenna, we select an industrial PT100 thermocouple temperature sensor as the target victim. To evaluate the tunability of LightAntenna, we select a gooseneck microphone as the victim device.

2) Attack Devices: The attack devices are used to generate, amplify, and inject attack signals. We use EXG vector signal generator [54] to generate signals from $1\,\text{MHz} \sim 1.5\,\text{GHz}$. To amplify the signals, we use a 5 W portable amplifier to amplify signals from $1\,\text{MHz} \sim 100\,\text{MHz}$ and use HPA-50W-63+ [38] to amplify signals from $700\,\text{MHz} \sim 1.5\,\text{GHz}$. Finally, to inject the attack signal into the power source, we used the customized $24\,\text{V}$ coupler to inject signals into the $24\,\text{V}$ DC power and use the $220\,\text{V}$ coupler to inject signals into the $220\,\text{V}$ AC power grid.

3) Test-bed Devices: The test-bed devices are used to support the evaluation experiment and eliminate interference and ethical concerns.

Elimination of Interfering Factors. When we use the signal generator and the RF amplifier to generate an EMI signal, the power wires, sockets, and attack devices will generate radiated EMI, so we cannot make sure that the EMI is generated by the fluorescent lamps. To solve this problem and separately study the EMI generated by fluorescent tubes, we use the RF shielding box to isolate the fluorescent lamp and victim sensors in a non-electromagnetic space, which we have introduced in Section IV.

Ethical Consideration. The power grid is a critical public utility where safety and stability are of paramount importance. Disruptions to this system can have far-reaching consequences, affecting other people and essential services. Therefore, injecting interference signals into the power grid is not only irresponsible but also illegal. To avoid impacting the reliability of the grid and pose significant risks to public safety and infrastructure, we injected the attack signal into the plug and set up a fifth-order low-pass filter between the plug and the public power grid, which prevented the attack signal from flowing into the power grid with a leakage current of under $0.65\,\text{mA}$ at $220\,\text{V}$ AC power.

B. Evaluation of the Generality of LightAntenna

We evaluate the performance of LightAntenna on 8 sensor modules that are used to measure physical variables to evaluate the generality of LightAntenna. Embedded sensor modules are the entrance of information for most IoT devices; since the sensed information is usually conducted in the form of analog signals in metallic wires, they are likely to suffer from EMI threats and cause more serious consequences.

Here, we evaluate the manipulation effect of LightAntenna on different analog and digital sensor modules; the sensing range includes basic physical quantities such as sound, light, electricity, magnetism, and heat. The detailed information of these sensors is shown in Table I.

First, we used the signal generator [54] to generate a single-frequency signal of $700\,\text{MHz} \sim 1.5\,\text{GHz}$, then amplified it to $10\,\text{W}$ by RF amplifiers [38], and finally injected into the power line of the fluorescent desk lamp by the customized coupler. The distance between the fluorescent desk lamp and the target sensor is set to about $15\,\text{cm}$. By carefully adjusting the frequency and amplitude of the attack signal within $10\,\text{W}$, we find and record the attack frequency and deviation rate of each sensor. The measurement results are recorded by an Arduino UNO with a sample rate of $9.6\,\text{kHz}$. Electromagnetic isolation measures are taken between the Arduino and the victim sensor to ensure the reliability of the measurements, as described before.

We list specific data results, including the attack frequency, original values, average deviation values, etc., as shown in Table I. As we can see, ① all of the analog sensors can be manipulated by more than 25% compared with their original value; ② all of the digital sensors can be manipulated to output a wrong result.

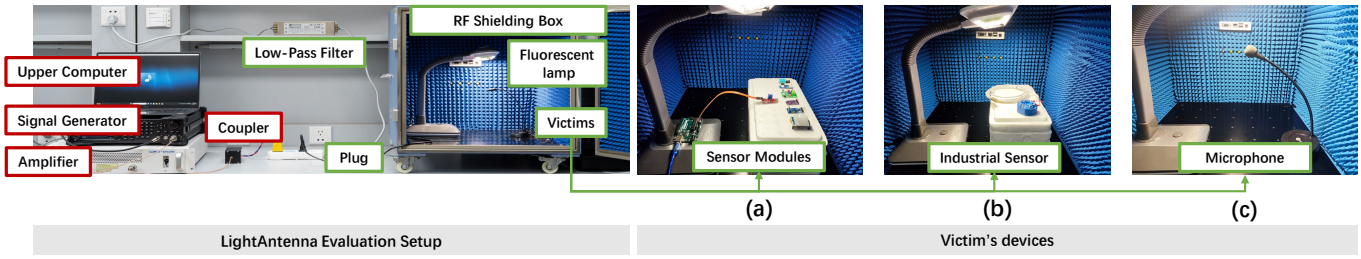


Fig. 13. An illustration of the LightAntenna system setup. The attack devices inject attack signals into the power supply of the fluorescent lamps. The victim devices include (a) 8 different sensor modules used to measure the environment variables, (b) an industrial thermocouple temperature sensor, (c) a gooseneck microphone used in the meeting rooms or home.

TABLE I. RESULT OF EMI ATTACK ON 8 SENSOR MODULES

Sensor type	Sensor model	Output type	Measurement span	Attack parameters		Output		
				Freq.(MHz)	Pow.(W)	Original	Deviation	Rate
Temperature	PT100	Analog	0∼50 °C	966	10	26.5 °C	-11 °C	-41.5%
Temperature	DS18B20	Analog	-55∼+125 °C	876	10	26.5 °C	+9 °C	+34.0%
Humidity	DHT11	Analog	20%∼90%	779	10	61%	+17%	+27.9%
Sound	/	0/1	/	627	10	0	1	+100.0%
Light	LM393	0/1	/	677	10	0	1	+100.00%
Light(Ultraviolet)	S12SD	Analog	0∼11	724	10	2	+4.5	+225.0%
Light(Infrared)	HC-SR501	0/1	/	1322	10	0	1	+100.0%
Current	ACS712	Analog	0∼5 A	1280	10	5 A	+8.2 A	+164.0%

1. For each sensor, we repeat the experiments 10 times and calculate the average deviation and deviation rate.
2. The Sound sensor, Light sensor, and Light (infrared) sensor are used to detect the existence of the target, for these sensors, we only record the output are 0 or 1.
3. We set the injection to be 10 W to verify whether the LightAntenna can impact senors. In fact, the deviation rate can be improved with a higher attacker power.

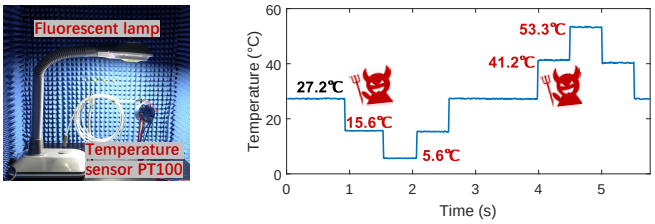
Assuming that these sensors are used for IoT devices, the results of the attacks on the sensors we show can have more serious consequences. For example, injecting a signal into the power supply of an infant thermostat, controlling the inside fluorescent tubes to generate EMI, and maliciously controlling the temperature sensor measurements can lead to the runaway of temperature and cause serious safety incidents.

C. Evaluation of the Practicality of LightAntenna

Compared to sensor modules, industrial sensors are more robust against EMI attacks because they operate in complex electromagnetic environments and are usually adopted with better EMC measures. Here, we use the thermocouple temperature sensor as an example to evaluate the practicality of LightAntenna in real industrial scenarios. We have introduced the method of executing a controllable attack through AM modulation; however, it still needs to be verified whether the attack signals can be transmitted through the power grid and ballasts without being distorted.

We assume that the attacker's goal is to control the increase and decrease of the temperature sensor's measurements with a controllable offset. First, we connect the PT100 thermocouple temperature sensor with its transmitter module and use a metal directional antenna to do an EMI sweep test on the thermocouple temperature sensor to record the attack parameters that can make the thermometer output rise and fall. The temperature sensor is then placed in the RF shielding box 15 cm away from the fluorescent tube. We then turned on the fluorescent lamp and injected an AM-modulated attack signal into the power supply of the fluorescent lamp using a 220 V coupler. We used an Arduino UNO to record the temperature sensor measurements at a sampling rate of 9600 Hz.

The result is shown in Fig. 14. As we can see, before the attack, the indoor temperature can be correctly measured as



(a) Setup. (b) Result.

Fig. 14. The evaluation experiment on industrial thermocouple temperature sensor. The attacker first decreases the measured temperature to 15.6 °C and 5.6 °C, then increases the measured value to 41.2 °C and 53.3 °C.

27.2 °C; when we inject attack signals into the power of the desk fluorescent lamp, the measurement can be decreased to 15.6 °C and 5.6 °C, and increased to 41.2 °C and 53.3 °C. The deviation rate can be controlled by adjusting the amplitude of attack signals. By manipulating industrial temperature sensors, an attacker can trigger a temperature runaway that can lead to safety issues in production or cause financial losses.

D. Evaluation of the Tunability of LightAntenna

One scenario of the LightAntenna is to inject voice signals into microphones of voice systems. Compared to EMI attacks on general sensors, the voice signal injection attack has a higher requirement on the tunability of LightAntenna. To investigate whether LightAntenna can achieve voice injection attacks like metal antennas. We select an off-the-shelf gooseneck microphone to conduct voice injection tests.

1) Chirp Signal Injection Test: To achieve voice manipulation, the injection ability at the full voice frequency band is integral. To investigate the frequency response of LightAntenna in the full voice frequency band, we drew

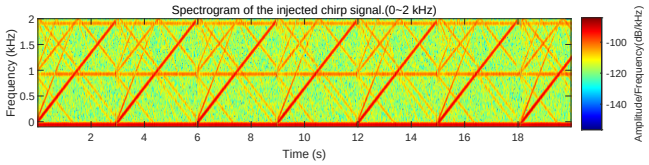


Fig. 15. Chirp signal injection. We injected a chirp signal with a frequency $0 \sim 2$ kHz and a period of 3 seconds playing in a loop.

inspiration from the ultrasound channel modeling mechanism of Vrifle [29] and selected the $0 \sim 2$ kHz chirp signal as the target voice signal and evaluated the injection effect on a gooseneck microphone.

First, we selected the resonant coupling frequency of 112 MHz as the carrier frequency by frequency sweeping test, and modulated it using the AM function built into the signal generator, then amplified it to 4 W using the portable RF amplifier, and finally injected the attack signal into the 220 V AC power source via the 220 V AC coupler. At the same time, we used an oscilloscope to measure and record the analog output of the gooseneck microphone at a sampling rate of 48 kHz, and then recovered it as a speech signal with Matlab. Considering that a general voice system will have filtering and light audio enhancement processing algorithms, we set a low-pass filter with a cutoff frequency of 5 kHz on the original signal. To evaluate the injection effect more realistically, the experiment is not set up with other speech-processing algorithms.

The result is shown in Fig. 15. As we can see, `LightAntenna` can inject voice signals into the gooseneck microphone across the entire voice frequency band and maintain a low harmonic content, which poses advantages over prior ultrasound-based attacks that require specially sparse-frequency design, like Tuner [30], [67].

2) Voice Injection Test: After testing the injection of voice frequency band signal, we next evaluated the effect of `LightAntenna` on injecting voice signals into the microphone. To evaluate whether `LightAntenna` can inject voice signals into voice control systems (VCS) as effectively as previous EMI attacks, such as GhostTalk [26], we compare the effect of injecting "OK, Google" into an off-the-shelf gooseneck microphone using a metal directional antenna and a fluorescent lamp, respectively.

We use a computer to play the pre-recorded voice as the baseband signal and a signal generator to generate a 112 MHz carrier signal based on our frequency sweeping pre-test. The built-in AM modulation function of the signal generator set a 90% modulation depth. The amplifier HPA-25W-272+ is employed to amplify the attack signal to 10 W. The amplified attack signal is then injected into the AC power line of the desk fluorescent lamp. We keep the typical distance of approximately 15 cm between the desk lamp and the gooseneck microphone, as is common in daily life.

The result is shown in Fig. 16. Compared to the original audio signal, both GhostTalk and `LightAntenna` can inject voice signals with relatively complete preservation of the low-frequency part of the voice signal, and the high-frequency part of the voice signal is lost to some extent. In comparison, `LightAntenna` loses more high-frequency detail above

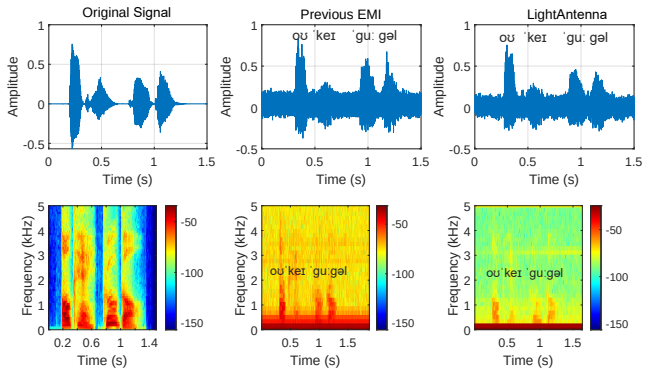


Fig. 16. The experiment result of "Ok Google" injection into an off-the-shelf gooseneck microphone.

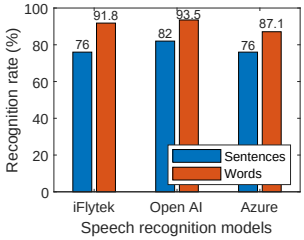


Fig. 17. The recognition result on 3 models.

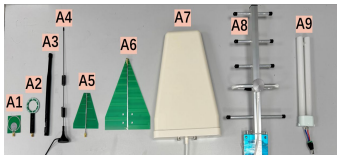


Fig. 18. The 8 metal antennas and tested fluorescent lamp.

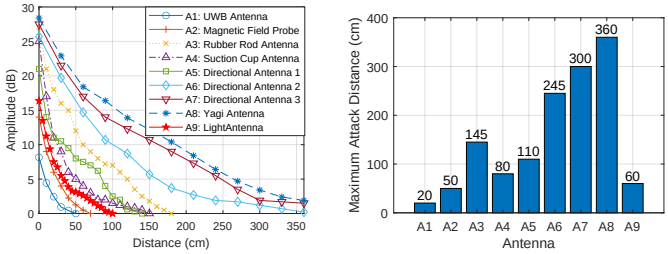
2 kHz, which may lead to changes in timbre.

To further verify whether the voice signals injected into the microphone by `LightAntenna` can spoof the speech recognition model, we selected 50 commonly used voice commands, modulated them with AM, amplified them to 10 W, and finally injected them into the gooseneck microphone at a distance of 15 cm. In a similar setup to NormDetect [28] and SOFTER [31], all voice is recorded at a sampling rate of 48 kHz and then recognized by 3 commercial speech recognition APIs, including IFlytek ASR [17], OpenAI ASR [43], and Microsoft Azure ASR [37]. According to the result in Fig. 17, the recognition rates on the three models are 76%, 82%, and 76% for the 50 sentences, and 91.8%, 93.5%, and 87.1% for the 232 words, respectively. This suggests that `LightAntenna` is able to manipulate voice control systems by injecting malicious voice commands such as "Open the Door". The original and injected audio can be found on our website 1.

E. Comparison with Conventional RF Antennas

We selected 8 metal antennas as shown in Fig. 18, and the detailed parameters are shown in Table II in Appendix G. We conducted 2 experiments with the same input signal (966 MHz and 12.6 W): (1) we compared the EMI intensity at different distances of `LightAntenna` and 8 metal antennas, (2) we compared the maximum attack distance to make the temperature sensor deviate over 5 °C.

The result is shown in Fig. 19. As we can see, the EMI intensity of the fluorescent lamp is higher than the UWB (Ultra-Wide Band) antenna and magnetic field probe and lower than other antennas, which is mainly related to the



(a) Comparison of EMI intensity. (b) Comparison of attack distance.

Fig. 19. The comparison results of LightAntenna and metal antennas.

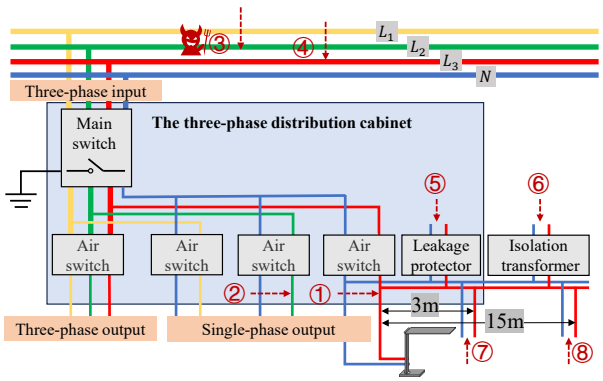


Fig. 20. The topological diagram of the off-grid power distribution system.

geometry, and directional antennas are capable of transmitting longer distances than fluorescent lamps and general antennas. Thus, we can conclude that the fluorescent lights may replace antennas to launch close-range EMI attacks to some extent, e.g. within 50 cm. This is possible in specific scenarios, such as baby incubators in hospitals in Fig. 33 in Appendix H.

F. Evaluation of Attack Distance and Power

In the previous evaluation, to replicate existing EMI attacks using lamps, we choose a moderate lamp-target distance of 15 cm to meet the varying requirements of attacking different sensors, despite more power can achieve better effect. To evaluate the impact of distance and power on LightAntenna, we used the magnetic probe and USRP B210 to measure the EMI intensity of a 27 W fluorescent lamp when injecting signals of 900 MHz and different power. The result is shown in Fig. 23. As we can see, temporally boosting the attack power from 10 W to 15.8 W can lead to an 8 dB increment in the EMI intensity. A higher distance is possible with couplers that support more injection power, which can be custom-made at a higher price.

G. Evaluation of LightAntenna under Realistic Grid

The remote attack of LightAntenna needs to face the challenge of transmitting attack signals in the real power grid, mainly including the impact of power branches and interference from other loads.

1) Impact of Power Branches: To avoid the ethical concerns of injecting attack signals into the real power grid, we analyzed the power distribution cabinet of our lab and built an off-grid power distribution system to investigate the impact of the power branch on the LightAntenna, the topology is

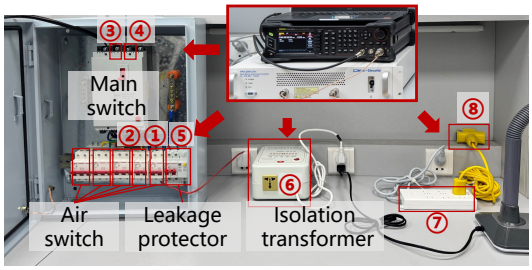


Fig. 21. The experiment setup of the impact of power branches.

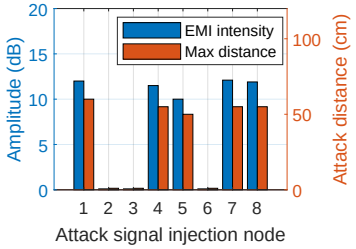


Fig. 22. The result of injection from different power branch nodes.

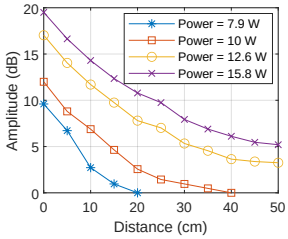
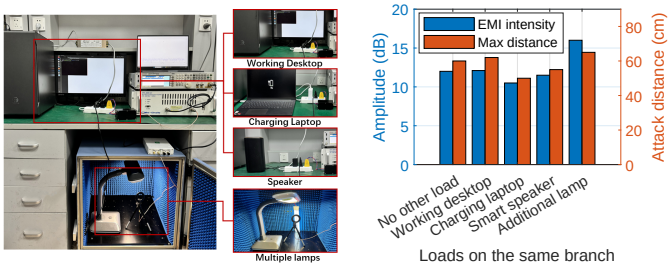


Fig. 23. The impact of distance and power.

shown in Fig. 20. We injected signals into 8 different nodes of the distribution system: Node ① is the reference node that is directly connected to the fluorescent lamp; Node ② is used to compare the effect of injecting from a phase different from the target fluorescent lamp; Nodes ③ and ④ are used to compare the effects of injection from the three-phase public grid. ③ is in a different phase from the target, and ④ is in the same phase; Nodes ⑤ and ⑥ are used to evaluate the impact of leakage protector and isolation transformer. Isolation transformers are used in scenarios where a clean power source is required for sensitive equipment; Nodes ⑦ and ⑧ are used to evaluate the impact of wire length (3 m and 15 m). The experiment setup is shown in Fig. 21. We injected signals of 966 MHz and 12.6 W into the 8 nodes, measured the EMI intensity at 10 cm from the fluorescent lamp and recorded the maximum attack distance to make a temperature sensor deviate more than 5 °C.

The result is shown in Fig. 22. We summarize our observations as follows: (1) By injecting signals into nodes ② and ③, we observed that signals cannot be transmitted across phases, so the attacker should inject signals into the same phase as the target, or inject signals into all phases. (2) By injecting signals into node ⑥, we observed that the isolation transformer can block attack signals. (3) The main switch, air switches, and leakage protectors have little impact on LightAntenna. To further investigate, we measured the equivalent impedance of the main switch, air switch, leakage protector and isolation transformer at 10 kHz (the maximum frequency supported by our device) using an impedance analyzer. The equivalent impedance are 8.6 Ω, 25 Ω, 162 Ω, and −30 kΩ, respectively. The measurement result further validates our conclusions.

2) Impact of Other Loads: To investigate the impact of loads on the EMI intensity and attack distance of LightAntenna, we tested four types of loads: ① a working desktop running a cyclic square root operation; ② a low-battery laptop is charging at 90 W via a switched power supply;



(a) Experiment setup. (b) Result.

Fig. 24. Evaluation of the impact of loads on LightAntenna.

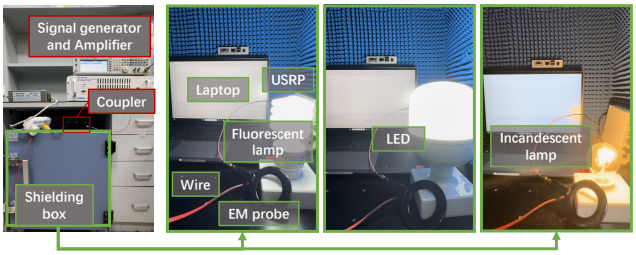


Fig. 25. The measurement setup of the EMI of wires and different lamps.

③ a loudspeaker playing 1 kHz noise; ④ another fluorescent lamp of the same model. These loads share the total injection power at a distance of about 15 cm from the target fluorescent lamp. We injected the signal of 12.6 W and 966 MHz into the power branch, and evaluated from 2 aspects: (1) we used a near-field magnetic probe and USRP B210 to measure the EMI intensity of the fluorescent lamps at a distance of 10 cm, (2) we recorded the maximum distance to successfully attack the temperature sensor (causing a temperature deviation over 5 °C). The experiment setup and result are shown in Fig. 24.(a) and Fig. 24.(b). We can see that (1) different loads have different impacts on LightAntenna, this may be because different loads have different input impedance and can absorb different injected power; (2) two fluorescent lamps can produce stronger EMI, this may be because lamps in parallel have a lower overall impedance and absorb more injected power.

VII. Discussion

In this section, we develop some discussions of LightAntenna from several aspects, in the hope of contributing to the subsequent studies. We mainly focus on the cross-talk, the difficulties of defense, potential countermeasures, limitations , and engineering optimizations of LightAntenna.

A. The EMI of Wires and Other Lamps

Although we adopted a shielding box to isolate the fluorescent lamps and other test-bed devices, the EMI of wires is unavoidable. To investigate whether the fluorescent lamp is the indispensable EMI source of LightAntenna, (1) we measured the unintentional EMI of the wires, a 23 W compact fluorescent lamp, a 23 W LED and a 20 W incandescent lamp; (2) we kept the wire's geometry and the injected signal (700 MHz, 10 W) the same, and measured the intentional EMI intensity of these lamps with the magnetic field probe and the USRP B210 at a distance of about 10 cm, as shown in Fig. 25. The result is shown in Fig. 26 and demo video[1]. We can conclude that the fluorescent lamp is the main EMI source, because it can produce an intentional EMI 7 dB stronger than the metal wire and other lamps.

B. The Difficulty of Defense

The root cause of the difficulty in defending against LightAntenna is the effective detection, because LightAntenna is already around the victim's sensor and cannot be detected by metal detectors when it's off. When injecting attack signals, the gas inside the fluorescent tube will be activated and become a plasma antenna, and when the attack signals are cut off, the gas returns to its original state. Moreover, fluorescent tubes can secretly generate EMI when there is no power and they are not emitting light. These characteristics make LightAntenna difficult to detect by people or normal antenna detectors.

[1] https://tinyurl.com/LightAntenna

C. Potential Countermeasures

We investigate existing works and discuss potential countermeasures.

1) Higher EMC Standards: The proposed EMI threat LightAntenna requires injecting malicious EMI signals into the victim device. If the victim device has good electromagnetic shielding from the outside, such as being placed in a Faraday cage in an ideal scenario, the attack may not be carried out. Although the existing off-the-shelf industrial sensors are satisfied with current EMC standards, such as the IP65 standard requirement according to the International Organization for Standardization ISO 20653:2023 [13] and the International Electrotechnical Commission IEC 60529 [5], we still suggest the manufacturers of crucial sensors develop EMI shielding cases with higher requirements, and the standard-setting organizations should consider revision the EMC measures of fluorescent lamps and sensors.

2) Filter Leakage and Filters with Higher Order: LightAntenna relies on the propagation of high-frequency signals in the power line and electronic ballasts. Although current electronic ballasts have been designed with low-pass filtering circuits to eliminate high-frequency noise from the power supply, we have found that ultra-high-frequency signals can still pass through. This is mainly due to the phenomenon of filter leakage brought about by the nonlinear physical properties of the filter, as shown in Fig. 27.

To solve this problem, we find that a fifth-order filter connected between the power grid and the fluorescent lamp can block the high-frequency signals. Of course, this method will cause a higher cost and complexity.

3) Idle-time Management: Implementing "idle-time management" for potential EMI sources such as fluorescent lights. For instance, unplugging fluorescent lights when not in use to disconnect them from the power grid can physically block the transmission of attack signals and defend against this threat.

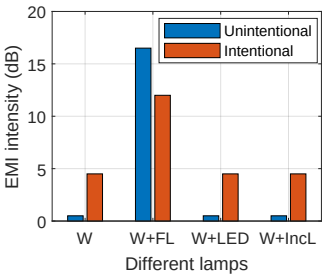


Fig. 26. The EMI comparison of different lamps. W: Wire, FL: Fluorescent lamp, IncL: Incandescent lamp.

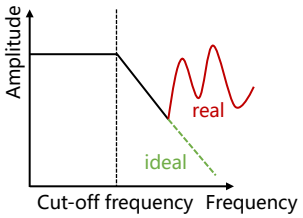


Fig. 27. Filter leakage.

D. Limitations

Although we successfully conducted electromagnetic injection attacks through fluorescent lamps, the `LightAntenna` still has some limitations. Understanding these limitations can help design more threatening attacks and more effective countermeasures.

1) Attack Scenarios: According to our experimental results, the EMI generated by the fluorescent lamp's normal operation can reach a distance of 3 m, while the EMI generated by the malicious signal injection can only reach a distance of a few tens of centimeters, this is mainly limited by the amplitude of the injected signals and the characteristics of the plasma. Even so, we believe the fluorescent lamp can have a better chance of approaching the victim sensors than the extra metal antennas. Therefore, a suitable attack scenario is necessary to implement the `LightAntenna`.

2) Signal Injection Efficiency: In this work, we inject the attack signal into the power grid and DC power source through customized couplers. However, the efficiency of injecting RF signals into the power source depends on the impedance matching between the power source and the attacking equipment. The RF amplifier we used has an output impedance of 50 Ω, while the grid's impedance is typically tens to hundreds of Ω. As a result, a part of the signal power will be reflected back to the RF amplifier, which can even damage the amplifier under certain circumstances. Thus, the attacker can increase the efficiency of the signal injection by targeted impedance-matched design, which is an engineering issue.

3) Signal Transmission Interference: Remote `LightAntenna` relies on the transmission of attack signals in the power grid. However, the attack signal transmission can be interfered with by noise in the power line, such as load variations. Similar to power line carrier communications (PLCC), the signal transmission in the power grid can only achieve a distance of a few tens of meters, which depends on the signal amplitude and power line noise.

E. Engineering Optimization of `LightAntenna`

1) Design of Portable Attack Device: To illustrate that the `LightAntenna` can be developed as a practical attack method, we design a portable and cost-saving attack device, as shown in Fig. 28. The portable attack device mainly includes a signal generator, an RF amplifier, a coupler, and their power source. We select LTDZ MAX2870 [12] based on STM32 as the signal generator that can generate single frequency signal from 1 MHz ∼ 6 GHz and conduct the sweep-frequency test, with a cost of $45. Based on the previous experiment result, we select a portable RF amplifier [65] that can amplify the signal from 100 kHz ∼ 75 MHz, which costs only $10. The 220 V coupler is the one used in the previous experiment. The 5 V mobile power is used for the signal generator and the 12 V battery is used for the amplifier. All device costs about $80 in total, and we customized a portable toolbox to carry the attack equipment. Finally, we successfully implement `LightAntenna` with the designed portable attack device.

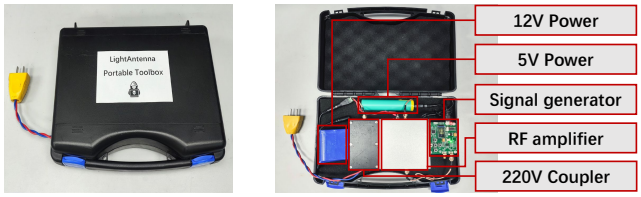


Fig. 28. The designed portable attack device. We design a portable toolbox that can inject attack signals into the power grid of the victim.

2) Wireless Injection: `LightAntenna` injects signals at the port where the victim is connected to the power grid, which can be a socket or a meter, etc. However, sometimes the attacker has no access to such a power port. In this case, we proposed the wireless injection method that does not require any power port. According to the requirements of `LightAntenna`, we select the TBCP2-750 as the injection tool. TBCP2-750 is an RF current monitoring probe that is used for EMC tests. It has a response with a 3 dB bandwidth of 850 MHz and is characterized and usable in the frequency range from 1 kHz ∼ 1 GHz [55]. The injection point can be any power line, whether it is DC or AC power. The wireless injection probe and principle are shown in Fig 32 in Appendix F.

VIII. Related Work

IEMI Attacks against Cyber Physical Systems There are various EMI attacks against analog sensors: microphones [26], [62], [63], implantable cardiac devices [26], CCD and CMOS image sensors [19], [23], [70], touch screens and more involved structures, such as (virtual) keyboards [36], [49], [58], [20] and cellphones [22], [62]. Though digital signals are more difficult to manipulate than analog ones, several EMI attacks against digital signals have been demonstrated as bit-flip attacks on serial communications [9], [48], [46]. Current IEMI works mainly utilize metal antennas to launch attacks near the victim's sensors, which is limited in terms of stealth. We have compared the attack capabilities of some IEMI works with `LightAntenna` as shown in Table III in Appendix J.

Power Manipulation Attacks Recently, power manipulation attacks have been extensively studied, which can address the distance and stealth limitations of IEMI attacks. Yang et al. [64] realize the control of transformers to emit voice signals by injecting attack signals into the power grid. Dai et al. [6] utilize wireless chargers to emit EMI and inject voice into mobile phones by manipulating the power. Our proposed `LightAntenna` is one of this type of threat and can be used in more scenarios.

EMI of Fluorescent Tubes and Countermeasures Some reports have noticed that fluorescent lamps can impact touch screens [7] and radio [44], and researchers have recognized that fluorescent lamps can generate conducted and radiated EMI [15], [4], [33], [40], and have investigated EMC measures. Current countermeasures mainly focus on two aspects: One is to attenuate the conducted EMI from the ballast to the grid, such as Eugen et al. [4]; The other is to design compensating defenses for EMI on the victim's devices, such as Chih et al. [3]. However, `LightAntenna` controls the EMI from fluorescent lamps by injecting signals, remains unnoticed and lacks effective defense measures.

IX. Conclusion

In this paper, we discover a vulnerability of fluorescent lamps that can be utilized to launch EMI attacks on sensors of IoT devices. We systematically analyze the underlying principle of how fluorescent lamps generate EMI and how to control the EMI. Furthermore, we propose `LightAntenna` that can remotely control the fluorescent lamps to launch controllable EMI attacks on sensors by injecting signals into the power grid. To demonstrate the real-world threat of `LightAntenna`, we conduct and evaluate the attack effect on 8 different sensor modules, a thermocouple temperature sensor, and a gooseneck microphone, and evaluate the impact of realistic power grid on `LightAntenna`. Finally, we discuss the potential countermeasures of `LightAntenna` and design a portable attack device.

Acknowledgment

We thank the anonymous reviewers for their valuable comments. This work is supported by the National Natural Science Foundation of China under Grant 62201503, 61925109, 62222114, and 62071428.

References

[1] A. O. Ajibade, I. B. Oluwafemi, A. O. OJO, and K. A. Adeniji, "Theoretical analysis of transmission parameters and interference issues in power line communication systems," *ABUAD Journal of Engineering Research and Development*, vol. 1, no. 1, pp. 95–99, 2017. 6

[2] J. M. Alonso, "22 - electronic ballasts," in *Power Electronics Handbook (Third Edition)*, third edition ed., M. H. Rashid, Ed. Boston: Butterworth-Heinemann, 2011, pp. 573–599. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780123820365000227 2

[3] H.-C. Chih, W.-T. Huang, and K.-C. Yao, "Fluorescent lamp effect correction on capacitive touch panel by timely update predicted covariance matrix," *IEEE Transactions on Industrial Electronics*, vol. 66, no. 7, pp. 5508–5515, 2018. 14

[4] E. Coca, V. Popa, and G. Buta, "Compact fluorescent lamps electromagnetic compatibility measurements and performance evaluation," in *2011 IEEE EUROCON-International Conference on Computer as a Tool*. IEEE, 2011, pp. 1–4. 14

[5] I. E. Commission. (2013) Degrees of protection provided by enclosures (ip code). [Online]. Available: https://webstore.iec.ch/publication/2452 12

[6] D. Dai, Z. An, and L. Yang, "Inducing wireless chargers to voice out for inaudible command attacks," in *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2023, pp. 1789–1806. 13

[7] dankgus. Touchscreen interference issue, confirmed–weird! [Online]. Available: https://www.surfaceforums.net/threads/touchscreen-interference-issue-confirmed-weird.14810/ 4, 14

[8] G. Y. Dayanikli, R. R. Hatch, R. M. Gerdes, H. Wang, and R. Zane, "Electromagnetic sensor and actuator attacks on power converters for electric vehicles," in *2020 IEEE Security and Privacy Workshops (SPW)*. IEEE, 2020, pp. 98–103. 2, 5

[9] G. Y. Dayanıklı, A. Z. Mohammed, R. Gerdes, and M. Mina, "Wireless manipulation of serial communication," in *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*, 2022, pp. 222–236. 13

[10] G. Y. Dayanıklı, S. Sinha, D. Muniraj, R. M. Gerdes, M. Farhood, and M. Mina, "{Physical-Layer} attacks against pulse width {Modulation-Controlled} actuators," in *31st USENIX Security Symposium (USENIX Security 22)*, 2022, pp. 953–970. 18

[11] Energyrating.gov. Household lighting consumer survey report. [Online]. Available: https://www.energyrating.gov.au/industry-information/publications/household-lighting-consumer-survey-report 1

[12] S. B. S. S. E. Firm. Ltdx max2870. [Online]. Available: https://www.alibaba.com/product-detail/MAX2870-23-5-6000MHz-0-96_1600594901578.html?spm=a2700.galleryofferlist.normal_offer.d_image.27c6a4f3SyzgVR 13

[13] I. O. for Standardization. (2023) Degrees of protection (ip code) protection of electrical equipment against foreign objects, water and access. [Online]. Available: https://www.iso.org/standard/76116.html 12

[14] 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. 8

[15] F. Giezendanner, J. Biela, J. W. Kolar, and S. Zudrell-Koch, "Emi noise prediction for electronic ballasts," *IEEE Transactions on Power Electronics*, vol. 25, no. 8, pp. 2133–2141, 2010. 2, 4, 14

[16] R. F. Graf, *Modern dictionary of electronics*. Elsevier, 1999. 5

[17] IFlytek. Iflytek asr. [Online]. Available: https://global.xfyun.cn/products/speech-to-text 10

[18] X. Ji, J. Zhang, S. Jiang, J. Li, and W. Xu, "Capspeaker: Injecting voices to microphones via capacitors," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, 2021, pp. 1915–1929. 2

[19] Q. Jiang, X. Ji, C. Yan, Z. Xie, H. Lou, and W. Xu, "{GlitchHiker}: Uncovering vulnerabilities of image signal transmission with {IEMI}," in *32nd USENIX Security Symposium (USENIX Security 23)*, 2023, pp. 7249–7266. 13, 18

[20] Q. Jiang, Y. Ren, Y. Long, C. Yan, Y. Sun, X. Ji, K. Fu, and W. Xu, "{GhostType}: The limits of using contactless electromagnetic interference to inject phantom keys into analog circuits of keyboards," in *31st Network and Distributed System Security Symposium (NDSS 24)*, 2024. 13

[21] A. Kadam, G. B. Nair, and S. Dhoble, "Insights into the extraction of mercury from fluorescent lamps: A review," *Journal of Environmental Chemical Engineering*, vol. 7, no. 4, p. 103279, 2019. 1

[22] C. Kasmi and J. L. Esteves, "Iemi threats for information security: Remote command injection on modern smartphones," *IEEE Transactions on Electromagnetic Compatibility*, vol. 57, no. 6, pp. 1752–1755, 2015. 1, 13

[23] S. Köhler, R. Baker, and I. Martinovic, "Signal injection attacks against ccd image sensors," in *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*, 2022, pp. 294–308. 13

[24] S. Köhler, R. Baker, and I. Martinovic, "Signal injection attacks against ccd image sensors," in *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*, ser. ASIA CCS '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 294–308. [Online]. Available: https://doi.org/10.1145/3488932.3497771 18

[25] kriang sak. The newborn instrument production project. [Online]. Available: https://www.dr-sak.net/index-eng.html 1

[26] D. F. Kune, J. Backes, S. S. Clark, D. Kramer, M. Reynolds, K. Fu, Y. Kim, and W. Xu, "Ghost talk: Mitigating emi signal injection attacks against analog sensors," in *2013 IEEE Symposium on Security and Privacy*. IEEE, 2013, pp. 145–159. 1, 2, 5, 10, 13, 18

[27] K. Lai. (2003) Voltage of a fluorescent tube. [Online]. Available: https://hypertextbook.com/facts/2003/KarryLai.shtml 3

[28] X. Li, X. Ji, C. Yan, C. Li, Y. Li, Z. Zhang, and W. Xu, "Learning normality is enough: a software-based mitigation against inaudible voice attacks," in *32nd USENIX Security Symposium (USENIX Security 23)*, 2023, pp. 2455–2472. 10

[29] X. Li, C. Yan, X. Lu, Z. Zeng, X. Ji, and W. Xu, "Inaudible adversarial perturbation: Manipulating the recognition of user speech in real time," in *Network and Distributed System Security (NDSS) Symposium*, 2024. 10

[30] X. Li, J. Ze, C. Yan, Y. Cheng, X. Ji, and W. Xu, "Enrollment-stage backdoor attacks on speaker recognition systems via adversarial ultrasound," *IEEE Internet of Things Journal*, vol. 11, no. 8, pp. 13 108–13 124, 2024. 10

[31] X. Li, Z. Zheng, C. Yan, C. Li, X. Ji, and W. Xu, "Toward pitch-insensitive speaker verification via soundfield," *IEEE Internet of Things Journal*, vol. 11, no. 1, pp. 1175–1189, 2024. 10

[32] H. G. Liddell, R. Scott, and S. H. S. Jones, "A greek-english lexicon. clarendon," 1940. 4

[33] C.-S. Lin, "Low power 60 khz electrodeless fluorescent lamp for indoor use," in *2010 Conference Proceedings IPEC*. IEEE, 2010, pp. 682–686. 14

[34] L. L. Liu Ping and J. Q. Deng Jicai, "Research on emission characteristics of plasma antennas," *Journal of Zhengzhou University (Engineering Science)*, vol. 27, no. 3, pp. 126–128, 2006. 5

[35] K. Lundgren. Why does my radio buzz when near fluorescent lights? [Online]. Available: https://www.quora.com/Why-does-my-radio-buzz-when-near-fluorescent-lights 4

[36] S. Maruyama, S. Wakabayashi, and T. Mori, "Tap'n ghost: A compilation of novel attack techniques against smartphone touchscreens," in *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2019, pp. 620–637. 13, 18

[37] Microsoft. Microsoft azure asr. [Online]. Available: https://azure.microsoft.com/en-us/products/ai-services/speech-to-text/ 10

[38] L. Mini-Circuits Technologies Co. High power amplifier hpa-50w-63+. [Online]. Available: https://www.minicircuits.com/pdfs/HPA-50W-63+.pdf 8

[39] A. Z. Mohammed, A. Singh, G. Y. Dayanıklı, R. Gerdes, M. Mina, and M. Li, "Towards wireless spiking of smart locks," in *2022 IEEE Security and Privacy Workshops (SPW)*, 2022, pp. 251–257. 18

[40] J.-D. Mok, S.-B. Jeon, and S.-K. Park, "A consideration on the electrodeless fluorescent lamp and its radio interference characteristics," in *ICTC 2011*. IEEE, 2011, pp. 312–317. 14

[41] L. Norwood. Why does bright fluorescent light affect iphone touch screens? [Online]. Available: https://www.quora.com/Why-does-bright-fluorescent-light-affect-iPhone-touch-screens 4

[42] C. F. of America and O. International. Consumer views and behavior relating to light bulbs: Findings of a national survey. [Online]. Available: https://consumerfed.org/reports/consumer-views-behavior-relating-light-bulbs-findings-national-survey/ 1

[43] OpenAI. Openai asr. [Online]. Available: https://platform.openai.com/docs/guides/speech-to-text 10

[44] Radio and Television. What is the radio and television investigation service? [Online]. Available: https://www.radioandtvhelp.co.uk/help-guides/radio/interference-due-to-lights 4, 14

[45] Z. M. Research. (2023) Fluorescent lighting market size, share, analysis, trends, growth report, 2030. [Online]. Available: https://www.zionmarketresearch.com/report/fluorescent-lighting-market 1

[46] J. Selvaraj, "Intentional electromagnetic interference attack on sensors and actuators," Ph.D. dissertation, Iowa State University, 2018. 13

[47] J. Selvaraj, G. Y. Dayanıklı, N. P. Gaunkar, D. Ware, R. M. Gerdes, and M. Mina, "Electromagnetic induction attacks against embedded systems," in *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, ser. ASIACCS '18. New York, NY, USA: Association for Computing Machinery, 2018, p. 499–510. [Online]. Available: https://doi.org/10.1145/3196494.3196556 18

[48] J. Selvaraj, G. Y. Dayanıklı, N. P. Gaunkar, D. Ware, R. M. Gerdes, and M. Mina, "Electromagnetic induction attacks against embedded systems," in *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, 2018, pp. 499–510. 2, 5, 13

[49] H. Shan, B. Zhang, Z. Zhan, D. Sullivan, S. Wang, and Y. Jin, "Invisible finger: Practical electromagnetic interference attack on touchscreen-based electronic devices," in *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2022, pp. 1246–1262. 13, 18

[50] Y. Shoukry, P. Martin, P. Tabuada, and M. Srivastava, "Non-invasive spoofing attacks for anti-lock braking systems," in *Cryptographic Hardware and Embedded Systems - CHES 2013*, G. Bertoni and J.-S. Coron, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 55–72. 18

[51] M. Sopapan Ngerncham, M. Kriangsak Jirapaet, R. Suvonachai, R. Chaweerat, P. Wongsiridej, and T. Kolatat, "Effectiveness of conventional phototherapy versus super light-emitting diodes phototherapy in neonatal hyperbilirubinemia," *J Med Assoc Thai*, vol. 95, no. 7, pp. 884–9, 2012. 1

[52] L. Sources and LightTech. Medical phototherapy. [Online]. Available: https://www.light-sources.com/solutions/specialty-fluorescent/applications/medical-phototherapy/ 17

[53] L. M. Surface. Surface touchscreen not working with touch? [Online]. Available: https://www.lovemysurface.net/surface-touchscreen-not-working-with-touch/ 4

[54] K. Technologies. (2023, Feb.) Exg x-series signal generators n5171b analog & n5172b vector. [Online]. Available: https://www.keysight.com/us/en/assets/7018-03381/data-sheets/5991-0039.pdf 5, 8

[55] TEKBOX. (2024, Mar.) Rf current monitoring probe. [Online]. Available: https://www.tekbox.com/product/TBCP2_750_Manual.pdf 13

[56] TekkyTG. Fluorescent lights interfering with my internet. [Online]. Available: https://linustechtips.com/topic/1015757-fluorescent-lights-interfering-with-my-internet/ 4

[57] 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. 2, 5, 7, 18

[58] K. Wang, R. Mitev, C. Yan, X. Ji, A.-R. Sadeghi, and W. Xu, "{GhostTouch}: Targeted attacks on touchscreens without physical touch," in *31st USENIX Security Symposium (USENIX Security 22)*, 2022, pp. 1543–1559. 13, 18

[59] K. Wang, S. Xiao, X. Ji, C. Yan, C. Li, and W. Xu, "Volttack: Control iot devices by manipulating power supply voltage," in *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2023, pp. 1771–1788. 1

[60] WikiPedia. (2024, Feb.) Plasma (physics). [Online]. Available: https://en.wikipedia.org/wiki/Plasma_(physics) 4

[61] Z. Xie, C. Yan, X. Ji, and W. Xu, "Bitdance: Manipulating uart serial communication with iemi," in *Proceedings of the 26th International Symposium on Research in Attacks, Intrusions and Defenses*, ser. RAID '23. New York, NY, USA: Association for Computing Machinery, 2023, p. 63–76. [Online]. Available: https://doi.org/10.1145/3607199.3607249 18

[62] Z. Xu, R. Hua, J. Juang, S. Xia, J. Fan, and C. Hwang, "Inaudible attack on smart speakers with intentional electromagnetic interference," *IEEE Transactions on Microwave Theory and Techniques*, vol. 69, no. 5, pp. 2642–2650, 2021. 1, 13, 18

[63] 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. 1, 8, 13

[64] L. Yang, X. Chen, X. Jian, L. Yang, Y. Li, Q. Ren, Y.-C. Chen, G. Xue, and X. Ji, "Remote attacks on speech recognition systems using sound from power supply," in *32nd USENIX Security Symposium (USENIX Security 23)*, 2023, pp. 4571–4588. 7, 13

[65] A. Yutai. 100khz-75mhz 5w rf amplifier. [Online]. Available: https://m.tb.cn/h.gSHNkyh?tk=sWOR3b2OsdhCZ3458 13

[66] S. Zainud-Deen, M. Badaway, H. A. Malhat, and K. Awadalla, "Circularly polarized plasma curl antenna for 2.45 ghz portable rfid reader," in *2014 31st National Radio Science Conference (NRSC)*. IEEE, 2014, pp. 1–8. 3

[67] J. Ze, X. Li, Y. Cheng, X. Ji, and W. Xu, "Ultrabd: Backdoor

attack against automatic speaker verification systems via adversarial ultrasound," in *2022 IEEE 28th International Conference on Parallel and Distributed Systems (ICPADS)*, 2023, pp. 193–200. 10

[68] Z. Zhan, Y. Yang, H. Shan, H. Wang, Y. Jin, and S. Wang, "Voltschemer: Use voltage noise to manipulate your wireless charger," *arXiv preprint arXiv:2402.11423*, 2024. 2

[69] 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. 8

[70] H. Zhang, Q. Jiang, Y. Cheng, X. Ji, and W. Xu, "Intentional electromagnetic interference attack against infrared thermal imaging sensor," in *2022 IEEE 6th Conference on Energy Internet and Energy System Integration (EI2)*. IEEE, 2022, pp. 1748–1753. 13

APPENDIX

A. Ballast

Generally, there are two types of ballasts: magnetic and electronic ballasts.

1) Magnetic Ballast: Magnetic ballasts use a core-and-coil assembly to regulate the current in the lamp. They are characterized by their simplicity and durability but are less efficient than electronic ballasts. Besides, magnetic ballasts will make the fluorescent tubes produce noticeable flickering and humming noises.

2) Electronic Ballast: Using solid state electronic circuitry, an electronic ballast can be smaller and quieter than magnetic ones. Electronic ballasts frequently employ switched-mode power supply (SMPS) topology, initially rectifying the input power and subsequently converting it into high-frequency AC. Advanced electronic ballasts facilitate dimming through pulse-width modulation (PWM) or by increasing the frequency. Ballasts integrated with microcontrollers, known as digital ballasts, often provide capabilities for remote control and monitoring.

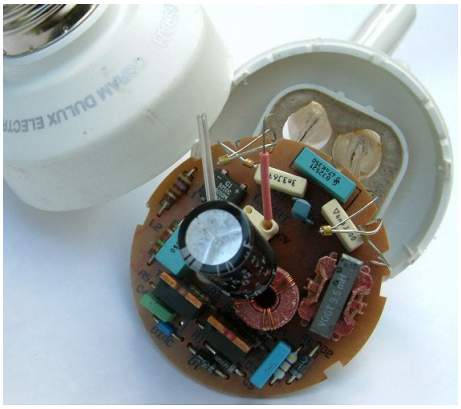


Fig. 29. Electrical Ballast of a Compact Fluorescent Lamp.

B. Plasma Antenna

The working principle of a plasma antenna including:

1) Ionization: When the electrical current or radio frequency (RF) energy is applied, the gas (such as argon, neon, or xenon) in the tube or chamber will ionize and turn into plasma. During the ionization, the gas atoms lose electrons and become charged particles.

2) Plasma formation: The ionized gas forms a conductive plasma that can carry electrical currents. This conductive plasma can interact with electromagnetic waves just like a metal antenna.

3) Signal transmission and reception: The plasma antenna transmits and receives signals by the plasma's conductive properties. When transmitting, the electrical signals cause the plasma to emit electromagnetic waves. When receiving, the plasma captures electromagnetic waves, which are then converted back into electrical signals.

4) Dynamic reconfiguration: One of the key advantages of plasma antennas is their ability to be dynamically reconfigured. By adjusting the ionization level, the shape, size, and conductivity of the plasma can be changed, allowing the antenna to operate on different frequencies and modify its radiation pattern in real-time.

5) On/Off capability: Plasma antennas can be turned on or off by ionizing or de-ionizing the gas, providing a unique stealth capability. When the gas is not ionized, the antenna is invisible to electronic detection.

The plasma frequency in a vacuum depends on the free electron density of the plasma, and can be expressed as Equation (3):

$$\omega_p = \sqrt{\frac{n_e e^2}{\varepsilon_0 m_e}}, \tag{3}$$

where ω_p is the plasma frequency (angular frequency), n_e is the electron density, e is the electron charge, ε_0 is the vacuum permittivity, and m_e is the electron mass.

C. The Customized Coupler

As shown in Fig. 30, the customized 220 V coupler mainly includes an amplification stage and a coupler stage.

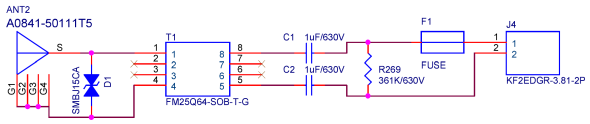


Fig. 30. The schematic diagram of the customized 220 V coupler.

D. DC Battery Injection

Most fluorescent lamps are AC-powered, with a few scenarios using DC power, such as photovoltaic systems that generate electricity that is stored in batteries that then power the fluorescent lamps DC, or mobile fluorescent lamps in emergency scenarios that use DC batteries to power the lamps. To verify that `LightAntenna` can also inject signals into a DC power source (e.g., a battery) and control the fluorescent lamps to generate EMI, we implemented an EMI test for DC fluorescent lamps with the experimental setup shown in Fig. 31. The result shows that using a maliciously modified battery pack to inject a signal into a DC fluorescent lamp can also achieve a similar effect to that of an AC fluorescent lamp.

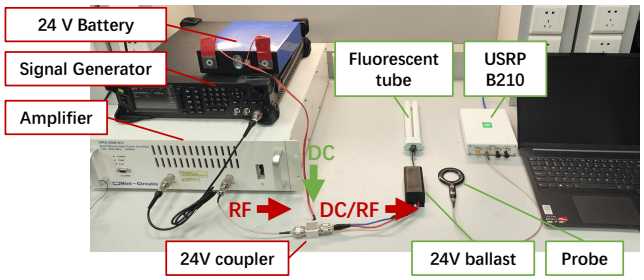


Fig. 31. The experiment setup of the EMI test on DC-powered fluorescent lamps.

E. Power Line Carrier Communication

Power line carrier communication (PLCC) involves transmitting data over electrical power lines using high-frequency carrier signals. Let A_c be the carrier amplitude, ϕ be the phase offset and $m(t)$ represent the message signal. The carrier signal $s(t)$ can be represented as:

$$s(t) = A_c \cos(2\pi f_c t + \phi) \cdot m(t)$$

PLCC employs modulation techniques like Amplitude Shift Keying (ASK), Frequency Shift Keying (FSK), or Phase Shift Keying (PSK) to encode data onto the carrier wave. These methods vary the carrier's characteristics based on the data to be transmitted, allowing for efficient use of the power line channel.

The transmission characteristics are influenced by the electrical properties of the power line, which can be modeled using transmission line theory. The telegrapher's equations describe the propagation of signals along the power line, accounting for impedance Z, propagation constant γ, and characteristic impedance Z_0. For a lossy transmission line, these equations are:

$$V(z) = V^+ e^{-\gamma z} + V^- e^{\gamma z}$$
$$I(z) = \frac{V^+}{Z_0} e^{-\gamma z} - \frac{V^-}{Z_0} e^{\gamma z}$$

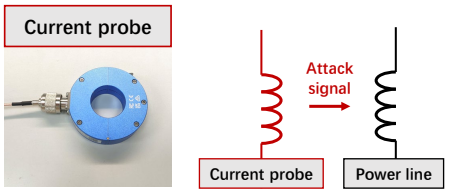
where:

- $V(z)$ and $I(z)$ are the voltage and current along the transmission line,
- V^+ and V^- are the forward and backward traveling voltage waves,
- $\gamma = \alpha + j\beta$ is the propagation constant with attenuation constant α and phase constant β.

The performance of PLCC systems also considers factors like signal attenuation due to line losses and noise interference, impacting the reliability and data rate achievable over the power line channel.

F. Wireless Injection Method

If the attacker cannot find a power port such as an outlet to inject the attack signal, then he can inject the attack signal directly into the power line through the wireless injection probe, as shown in Fig. 32.



(a) The wireless injection probe. (b) The principle of the wireless injection.

Fig. 32. The wireless injection method.

G. Parameters of Antennas

We have summarised the detailed parameters of the eight antennas tested, as shown in Table II.

TABLE II. THE PARAMETERS OF 8 CONVENTIONAL METAL ANTENNAS.

No.	Name	Frequency range (MHz)	Voltage standing wave ratio $\leq$	Input Impedance (Ω)	Gain (dBi)
1	UWB Antenna	3900$\sim$ 10500	2	50	7
2	Magnetic Field Probe	0.009$\sim$ 6000	1.5	50	-
3	Rubber Rod Antenna	868, 915	1.5	50	15
4	Suction Cup Antenna	470	1.5	50	6
5	Directional Antenna 1	0.05 $\sim$ 6500	2	50	7
6	Directional Antenna 2	0.05 $\sim$ 10500	2	50	7
7	Directional Antenna 3	698 $\sim$ 4900	1.5	50	12
8	Yagi Antenna	700 $\sim$ 800	1.5	50	10

H. A Possible Threat Scenario

Despite the fact that the effective attack range of `LightAntenna` is only a few tens of centimeters, it is still possible to get close to the target sensors in some scenarios due to the stealthy nature of the lamps in comparison to traditional antennas. For example, in a baby thermostat in a hospital, a fluorescent lamp can come into close contact with temperature sensor, humidity sensor and oxygen concentration sensor, as shown in Fig. 33 (from [52]), which can cause serious consequences.

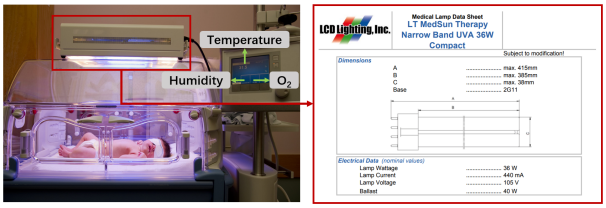


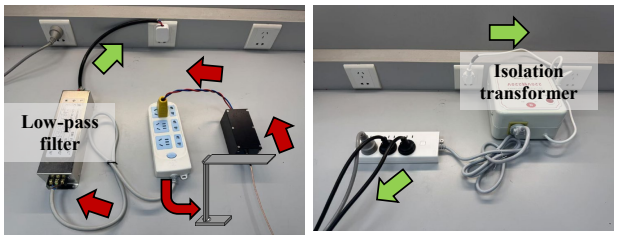
Fig. 33. A possible threat scenario in hospital. There are temperature sensor, humidity sensor, and oxygen concentration sensor in the vicinity of the fluorescent lamp.

I. Avoidance of Conductive Cross-talk

To prevent the attack signal from interfering with the test-bed device, we use a fifth-order low-pass filter to block the attack signal from entering the power grid, and even if there may be a small amount of leakage, we use an isolation transformer on the power supply side of the test-bed device to filter the block again, as shown in Fig. 34.

TABLE III. COMPARISON OF EXISTING IEMI WORKS WITH LIGHTANTENNA.

Work	Attack Target		Attack Parameters			Attack Effect
	Victim	Signal Type	Frequency (MHz)	Power (W)	Distance (m)	
[26]	Microphone	Analog	826	10	$1 \sim 2$	Voice Command Injection
[62]	Microphone	Analog	$8000 \sim 16000$	2.5	2.5	Voice Command Injection
[50]	Magnetic sensor	Digital	0.0005	/	/	Spoof wheel speed sensor
[47]	Embedded system	Digital	$170 \sim 320$	1.8	10	Manipulated analog and digital signals
[57]	Temperature sensor	Analog	$810 \sim 950$	3	3	Manipulate temperature sensors
[36]	Touchscreen	Digital	$0.06 \sim 0.09$	6	0.02	Manipulate touchscreen
[58]	Touchscreen	Digital	$46 \sim 86$	/	0.04	Manipulate touchscreen
[49]	Touchscreen	Digital	0.14	/	$0.7 \sim 2$	Manipulate touchscreen
[24]	CCD image sensor	Digital	190	0.1	0.3	Manipulate CCD image sensor
[19]	Camera signal line	Digital	1000	/	0.3	Manipulate camera signal transmission
[39]	Smart lock	Digital	0.5	/	0.05	Unlock the smart lock
[61]	UART serial	Digital	15.36	/	0.05	UART signal bit flip
[10]	Servo	Digital	$8 \sim 140$	20	0.5	DoS & Control servo
LightAntenna	**Different sensors**	**Analog**	**700 ~ 1500**	**12.6**	**20 (With power line)**	**Sensor manipulation & Voice injection**



(a) Signal injection side. (b) Device power supply side.

Fig. 34. The Blocking measures for unwanted conductive cross-talk.

J. Comparison with Existing IEMI Works

Here we give a detailed comparison of some existing IEMI works with LightAntenna, as shown in Table III.