LightThief: Your Optical Communication Information is Stolen behind the Wall

Xin Liu, *The Ohio State University;* Wei Wang, *Saint Louis University;*
Guanqun Song and Ting Zhu, *The Ohio State University*

https://www.usenix.org/conference/usenixsecurity23/presentation/liu-xin

This paper is included in the Proceedings of the
32nd USENIX Security Symposium.

August 9–11, 2023 • Anaheim, CA, USA

978-1-939133-37-3

Open access to the Proceedings of the
32nd USENIX Security Symposium
is sponsored by USENIX.

LightThief: Your Optical Communication Information is Stolen behind the Wall

Xin Liu[1], Wei Wang[2], Guanqun Song[1], Ting Zhu[1,*]
[1]The Ohio State University, [2]Saint Louis University

Abstract

Optical Wireless Communication (OWC) is a viable and promising alternative to traditional Radio Frequency (RF) based communication links. Especially for the security issue, since light does not penetrate through opaque objects, OWC is considered gaining certain intrinsic security benefits. The only related work eavesdrops on OWC by detecting the electromagnetic signal leaking from an open-source research platform for OWC. However, electromagnetic compatibility (EMC) regulations require Commercial Off-The-Shelf (COTS) OWC products to minimize electromagnetic leakage, securing OWC from the previous eavesdropping. In this paper, we propose a new class of eavesdropping, *LightThief*, that can directly convert optical signals into RF signals without complicated baseband processing circuits and power consumption, making it lightweight, unlimited lasting, and easy to disguise. Specifically, *LightThief* is constructed by coupling a photodiode (PD) to an antenna. Since OWC adopts intensity modulation to transmit data, light intensity change can modify the PD impedance, causing the antenna to reflect different amounts of RF signals to enable data breaches. The attacker outside the room can then detect and decode the RF signals without resistance by EMC regulations. We demonstrate the effectiveness of our attack on a COTS OWC product, which shows successful eavesdropping through physical barriers such as walls. We also discuss potential defense strategies to secure OWC systems from *LightThief*.

1 Introduction

OWC is an innovative method that utilizes light emitted from light-emitting diodes (LEDs) to establish efficient networked communication. Compared to traditional RF communication links, OWC boasts numerous advantages, including lower implementation costs and reduced energy consumption, primarily attributed to the affordability and energy-saving characteristics of LEDs. These benefits elevate OWC as a promising and viable alternative to RF communication, propelling the OWC market towards an impressive compound annual growth rate of 101% through 2026 [8]. With rapid market expansion and the proliferation of applications, addressing the critical security concerns associated with OWC products has become increasingly vital.

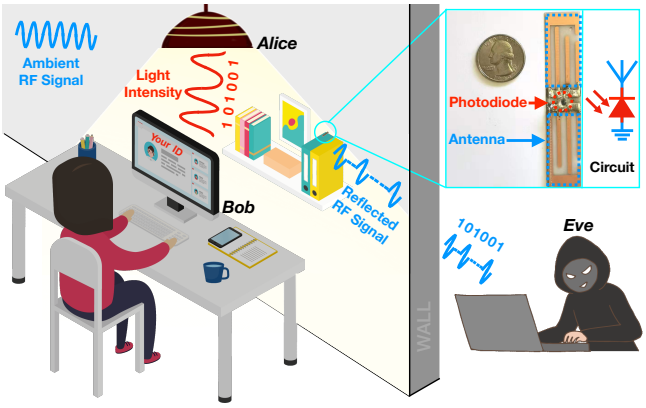
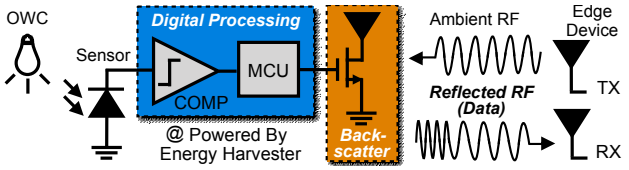


Figure 1: *LightThief* can smuggle the OWC data through walls by passively reflecting ambient RF signals. The attacker outside the room then detects and decodes the reflected RF signals, gaining access to the indoor OWC data.

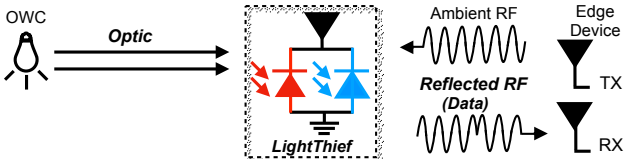
However, OWC is commonly taken for granted as highly secure with inherent advantages such as being sniff-proof [45, 46]. This is because light propagates directionally and cannot penetrate physical barriers like walls. As a result, recent work [15] explored the use of non-optical media for eavesdropping purposes. Specifically, the attacker in [15] attempted to eavesdrop on an open-source OWC research platform [40] by detecting leaked electromagnetic signals, which stemmed from current fluctuations in the LED connection cable.

In spite of its effectiveness on the open-source platform, the eavesdropping method proposed in [15] may prove challenging to apply to COTS OWC products. This is because COTS products are subject to stringent EMC regulations [4–6], requiring the minimization of electromagnetic leakage. In con-

*Corresponding author: Prof. Ting Zhu (zhu.3445@osu.edu)



(a) Latest optic-to-RF conversion design [17, 31]



(b) Our passive optic-to-RF conversion approach

Figure 2: Comparison between different optic-to-RF conversion approaches.

trast, open-source platforms can circumvent these restrictions. For example, [15] employs two long unshielded wires as the LED connection cable, arranged at an angle of 180°. This arrangement effectively forms a dipole antenna [3], amplifying the leaked electromagnetic signals. As the wire length increases, the efficiency of the antenna system also increases. However, such designs are not permissible in the majority of COTS products. In practice, engineers consistently employ various techniques to minimize electromagnetic leakage in order to comply with EMC regulations. Consequently, the combination of impenetrable physical barriers and adherence to EMC regulations seems to offer a reasonable degree of security for OWC systems.

In contrast to prior non-optical-based attacks, our goal in this paper is to develop the first battery-free optical-based eavesdropping approach, *LightThief*. Battery-free eavesdropping allows for indefinite eavesdropping duration while reducing maintenance and minimizing the exposure risk of the attacker. Furthermore, the new eavesdropping attack should be efficient to deploy and simple to conceal. Nevertheless, achieving these goals presents challenges, specifically regarding the following three questions:

(a) What to smuggle OWC data through walls with? Our goal is to leverage RF signals to smuggle OWC data through walls. Intuitively, the attacker should deploy an RF signal generator inside the victim's room. However, generating RF signals is energy expensive, demanding a power cord, a battery, or solar cells to supply power, increasing the exposure risk of eavesdropping or allowing for only short-lived eavesdropping. This paper leverages the backscatter technology [27] that reflects different amounts of ambient RF signals to transmit data. Since reflecting RF signals only consumes micro-watts' level of power, the backscatter system can enable batteryless wireless communication. By using the backscatter technology, *LightThief* piggybacks OWC data onto the RF signals through the wall, as shown in Fig. 1, allowing batteryless and unlimited lasting eavesdropping.

(b) How to piggyback OWC data onto RF signals? To piggyback OWC data from optical signals onto RF signals, we need to conduct an optic-to-RF conversion. The recent solution [17] uses a complicated baseband processing circuit to conduct the conversion. As shown in Fig. 2a, it first uses a threshold circuit to digitize the optical signals and then uses a micro-controller to recover OWC data from the threshold output. Finally, it uses an RF switch to control the antenna to reflect ambient RF signals. However, since its power consumption and circuit size (including solar cells) increase as the data rate increases, it is not suitable for eavesdropping. Unlike the previous solution, *LightThief* borrows the ideas from hybrid fiber-coaxial cable TV systems [21] and the Great Seal bug [36] to explore a passive optic-to-RF conversion. To be more specific, we found that IEEE Std 802.15.7 for OWC mainly adopts On-Off Keying modulation to transmit data, where the On and Off states of the light represent the data bits '1' and '0', which can significantly change the impedance of a PD. When we couple the PD to an antenna as shown in Fig. 2b, it is equivalent to a conventional backscatter system, allowing the antenna to reflect different amounts of RF signals according to the incident light intensity. Therefore, the optic-to-RF conversion is realized using only two passive components, eliminating the complicated baseband circuit and the energy harvester.

(c) How to decode OWC data from RF signals? Since OWC adopts a different physical layer operating mode from RF signals, we need a new demodulation scheme to decode OWC data from the reflected RF signals. In this work, the reflected RF signals are demodulated on a software defined radio platform with specified physical layer operating modes, such as modulation scheme, clock rate, and bandwidth.

Our key contributions are summarized as follows:

- We designed a new class of OWC eavesdropping, *LightThief*, that can eavesdrop on OWC systems without resistance by EMC regulations. To the best of our knowledge, this is the first battery-free optical-based attack for next-generation optical communication scenarios.
- We built a hardware prototype of *LightThief*, which is composed of only two passive components and can directly convert OWC data from optical signals to RF signals. It is lightweight, unlimited lasting, and easy to disguise.
- We extensively evaluate the effectiveness of *LightThief* on a COTS OWC product, and the experiment results show the vulnerability of current OWC systems. To defend against *LightThief*, we also provide defense strategies and suggestions to enhance the security of OWC systems.

2 Models and Assumptions

In this section, we first introduce the system model. Then, we define the threat model and assumptions.

2.1 System Model

Our design considers scenarios consisting of OWC systems, such as conference room or cubicle arangements. In these scenarios, a typical OWC system can comprise of OWC senders and receivers to support various applications (e.g., high-speed communication [39], smart sensing [30], localization [24], etc.). Specifically, the sender uses light-emitting diodes (LEDs) to support lighting applications and leverage the intensity modulation scheme to embed the data into the visible light. The receiver is placed in the line of sight with the sender to receive the OWC data.

Fig. 1 shows an example, in an office environment, an OWC sender, such as an LED ceiling light, which not only provides illumination for the office space but also serves as a data transmitter using intensity modulation. The modulated light carries the data to be transmitted and is then received by an OWC receiver integrated into the target device, such as a laptop or a smartphone. In this smart office, the OWC system can be utilized to enable a secure and high-speed wireless network for employees to connect their devices, as well as for indoor localization or smart sensing applications.

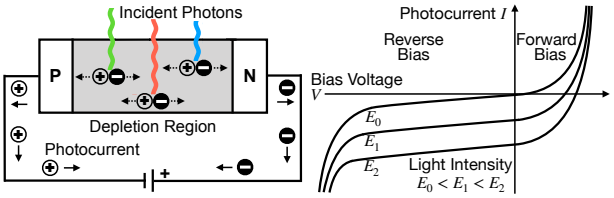
We further consider that the OWC system is working on its own schedule according to the applications. In addition, we also consider that there are other wireless communication systems (e.g., WiFi, Bluetooth, ZigBee, FM, LTE, 5G, etc.) working in these scenarios.

2.2 Threat Model and Assumptions

In this work, we consider an adversary (Eve) whose primary objective is to eavesdrop on OWC between legitimate devices - Alice (OWC transmitter) and Bob (OWC receiver) while concealing its presence without resistance from EMC regulations. To orchestrate such an attack, we assume that the attacker is fully aware of the characteristics of the target OWC device, such as the physical operating mode and the peak wavelength. The attacker can get such knowledge by acquiring a model of the target device and analyzing the model device before launching attacks.

We also assume that the attacker can deploy *LightThief* in shared areas, such as conference rooms or cubicles to convert the OWC signal into RF signal. For example, as shown in Fig. 1, the attacker can deploy the *LightThief* on the victim's desktop, or on the victim's shelf in advance. Then, since the converted RF signal can be detected through the wall, the attacker can easily eavesdrop on the ongoing communication without being seen by the legitimate user. Moreover, our *LightThief* tag is very small and battery-free. It can harvest the energy from the OWC signal and passively convert the OWC signal into RF signal, which makes the legitimate user even less likely to notice the ongoing attack.

Finally, we neither impose any restrictions on the OWC applications that the legitimate user is using nor on the work schedules of the legitimate OWC senders. We also do not impose any restrictions on the light (i.e., diffuse light or direct light) that the OWC system will use. As long as the OWC system uses intensity modulation scheme, *LightThief* should be able to eavesdrop on the ongoing communication between legitimate OWC senders and receivers.



(a) (b)

Figure 3: Working and characteristic I-V curves of PDs.

3 Background

To fully reveal the working mechanism of *LightThief*, it is necessary first to understand the unique features of PDs and OWC physical operating modes.

3.1 Variable Impedance in PD

A PD is a semiconductor p-n junction device that converts light into a photocurrent. As shown in Fig. 3a, when incident photons fall on the PD, the depletion region absorbs most of the photon energy because of its broad width. The photon hits the atom with high energy, resulting in free electrons and holes in the atom structure. Because of the electric field formed by an applied bias voltage, free electrons move towards the n-side, whereas holes move towards the p-side, generating photocurrents. Higher light intensity means that more photons are hitting the depletion region, resulting in a higher photocurrent.

Since the photocurrent changes depending on the light intensity, it enables the PD to be used as a light-intensity-based variable-impedance device. Fig. 3b shows the typical characteristic I-V curves of PDs. For a fixed bias voltage, when the PD is in reverse biased mode, an increase in light intensity E will induce growth in photocurrent I. The impedance is negative linear to the light intensity. When there is no incident light, the photocurrent is almost negligible and introduces a large impedance. When a forward bias mode is applied to the PD, there is an exponential increase in the photocurrent. Although it reveals a non-linear property, we can still observe a variable impedance feature in this figure. As a result, we can use the PD as a variable impedance device with either *reverse bias voltage* or *forward bias voltage*.

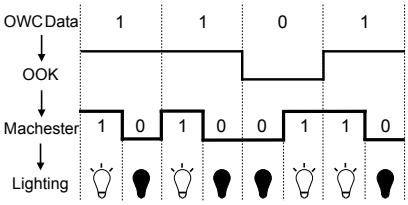
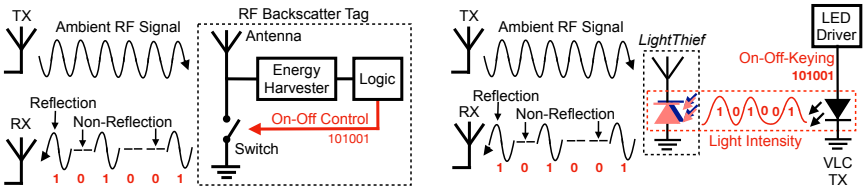


Figure 4: OWC standards encode OOK with Manchester codes to achieve lightness balanced (50%).



(a) Working of RF backscatter tag.

(b) Working of *LightThief*.

Figure 5: Compared to the conventional RF backscatter tag, *LightThief* is controlled by a remote light source and does not need the energy harvester.

3.2 Intensity Modulation for OWC

LightThief can eavesdrop on IEEE standard-based OWC because IEEE Std 802.15.7 mainly adopts an intensity modulation scheme - On-Off Keying (OOK). Due to the physical properties of LEDs, it is difficult for OWC to transmit data by modulating the phase of the light. In contrast, OWC can only encode data in the light intensity [37]. Moreover, OOK modulation can be easily achieved by turning LEDs on and off. Therefore, the data is transmitted as two states of light intensity: bright and dark.

Besides the intensity modulation, OWC standards encode OOK with Manchester code to achieve a balanced lightness (50%). As shown in Fig. 4, the long OOK stream of "0" or "1" produces dimming or flicker, which is not acceptable for lighting purposes. Manchester code encodes each OOK data bit either low then high or high then low, for equal time, creating a balanced lightness. This balanced lightness improves the visual quality of the transmitted light while also making the eavesdropping more effective, as the attacker can more easily distinguish between the "0" and "1" bits based on the light intensity. Moreover, Manchester code is essentially a binary phase-shift keying (BPSK) modulation scheme [32], which has been widely adopted by backscatter techniques [48–51]. The attacker can leverage similar backscatter techniques to demodulate the reflected RF signals to obtain the OWC data.

4 Feasibility Analysis

In this section, we first investigate the feasibility of *LightThief*. We then model *LightThief* to quantify parameters that will affect the eavesdropping. Finally, we validate the proposed model with feasibility experiments.

4.1 Intuition Underlying *LightThief*

We leverage the backscatter technology to convey the OWC data by reflecting RF signals. As shown in Fig. 4a, a conventional RF backscatter tag controls an RF switch to change the antenna's impedance. When the antenna picks up RF signals, it can convert the RF signals to an electromagnetic wave traveling through the antenna. When the control signal is '1', the switch is on, which shorts the antenna and the ground. Since the wave encounters an impedance discontinuity between the antenna and the ground, part of the wave is reflected out of the antenna, which can then be picked up by another antenna. When the control signal is '0', the switch is off, and the antenna's impedance are matched, limiting the reflected wave. Using this approach, the backscatter tag controls the RF switch toggling between the reflection and non-reflection states of the RF signals to transmit data.

When two terminals of the PD couple two branches of the antenna, it is equivalent to the conventional backscatter circuit. Because of the intensity change of the incoming light, the PD impedance is also changing significantly. Therefore, the PD can behave like the RF switch to change the antenna's impedance. Fig. 4b shows the working mechanism of *LightThief*. The light intensity (i.e., OWC data) determines the amount of the reflected RF signals. The major advantage of *LightThief* is that its "switch" is controlled by a remote light source, eliminating the logic circuit. Another advantage is that it does not need the energy harvester anymore, enabling unlimited lasting eavesdropping.

4.2 Mathematical Model

As discussed in Sec. 4.1, when two terminals of PD couple two branches of the dipole antenna, the PD behaves like an RF switch for the antenna. Meanwhile, the antenna acts like a bias voltage for the PD. Fig. 6 shows the equivalent circuit of *LightThief*, which is formed by coupling the equivalent circuit of the antenna to the equivalent circuit of the PD.

Antenna Side. Our goal is to find the related parameters that will increase the eavesdropping range of *LightThief*. Specifically, the eavesdropping range can be defined as the maximum distance from which the attacker equipped with the *LightThief* receiver can detect the reflected RF signals. The range can be modeled by the Friis path loss formula [34]:

$$d_r = \sqrt{\left(\frac{P_t G_t}{4\pi d_t^2}\right)\left(\frac{c^2 G_{passive}^2}{4\pi f_c^2}\frac{|\Delta\Gamma|^2}{4}\alpha_{loss}\right)\left(\frac{1}{4\pi P_{th}}\frac{c^2 G_r}{4\pi f_c^2}\right)} \quad (1)$$

This formula has three essential parts: the term in the first parenthesis models the signal propagation from the RF trans-

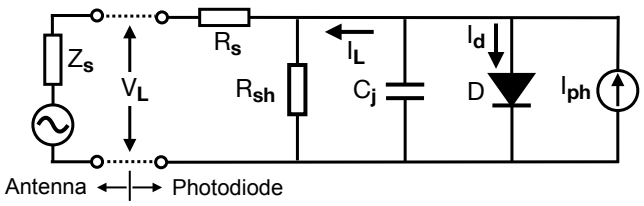


Figure 6: Equivalent Circuit of *LightThief*.

mitter with the transmitted power P_t and the transmitting antenna's gain G_t to *LightThief*'s antenna at a transmission distance d_t away. Similarly, the third part models the signal propagation from *LightThief*'s antenna to the attacker's receiver with the receiving antenna's gain G_r and the signal strength threshold P_{th}. In this part, c represents the speed of light and f_c represents the center frequency of the RF signal. If we choose a lower center frequency, the eavesdropping rage can increase. Finally, the middle parenthesis models the RF signal that *LightThief* reflects with an antenna gain $G_{passive}$. $|\Delta\Gamma|^2$ is the backscatter coefficient which is a measurement of the efficiency. α_{loss} models the energy loss due to backscattering. It considers half of the power lost due to the side lobes generated by backscattering (detailed in Sec. 4.5).

Our current design utilizes a continuous wave (CW) as the RF signal to validate the proof-of-concept. When the RF signals are ambient, P_t, G_t, and d_t are almost fixed. Moreover, the attacker can tune G_r and P_{th} at the receiver side during eavesdropping. Therefore, the most critical factors in determining the eavesdropping range are the *LightThief* antenna's gain $G_{passive}$ and the backscatter coefficient $|\Delta\Gamma|^2$. In principle, one can achieve a more extended eavesdropping range by designing *LightThief*'s antenna with a high gain. However, the design and fabrication of *LightThief*'s antenna are outside this paper and left for future work. In this paper, we use a COTS omnidirectional antenna as *LightThief*'s antenna without loss of generality. We mainly discuss the backscatter coefficient $|\Delta\Gamma|^2$, which is given by [23]:

$$|\Delta\Gamma|^2 = \frac{|\Gamma_1^* - \Gamma_0^*|^2}{4} \tag{2}$$

where Γ_1^* and Γ_0^* are the complex conjugates of the reflection coefficients corresponding to the two impedance states when the switch is on and off. Consider the equivalent circuit of an antenna shown in Fig. 6, representing a generator–load circuit with a complex generator and a complex load impedance. The equivalent circuit of the PD is just the load impedance. The reflection coefficient between a complex generator and a complex load impedance is given by:

$$\Gamma_i = \frac{Z_i - Z_s}{Z_i + Z_s} \quad , \quad i \in \{0,1\} \tag{3}$$

where Z_i is the complex PD impedance corresponding to the two impedance states when the light is on and off, and Z_s is the complex antenna impedance.

Therefore, in terms of the backscatter coefficient $|\Delta\Gamma|^2$, we need to maximize the difference between the two impedance states of the PD to increase the eavesdropping range.

PD Side. From the above analysis, we know we need to maximize the difference between the two impedance states of the PD. We can calculate the PD impedance using the ratio of the bias voltage to the photocurrent. The antenna provides the bias voltage.

Fig. 6 shows the photocurrent path in the PD. The PD can be represented by a current source (I_{ph}), a parallel junction capacitance (C_j), a parallel shunt resistance (R_{sh}), a series resistance (R_s), and a parallel normal p-n junction (D). The current source represents the current generated by the incident light, which is given by:

$$I_{ph} = \frac{R_\lambda P}{4\pi d_{ph}^2} \tag{4}$$

where P is the total power radiated from a light source, and d_{ph} is the distance between the PD and the light source. R_λ is the responsivity of a PD. It measures the effectiveness of the conversion of the light power into a photocurrent at a given light wavelength. It varies with the light wavelength.

The prominent noise of the PD is the dark current (I_d), which is a relatively small photocurrent from background radiation that flows through the p-n junction when there is no incident light. It can be calculated by using:

$$I_d = I_{SAT}(e^{\frac{qV_L}{k_B T}} - 1) \tag{5}$$

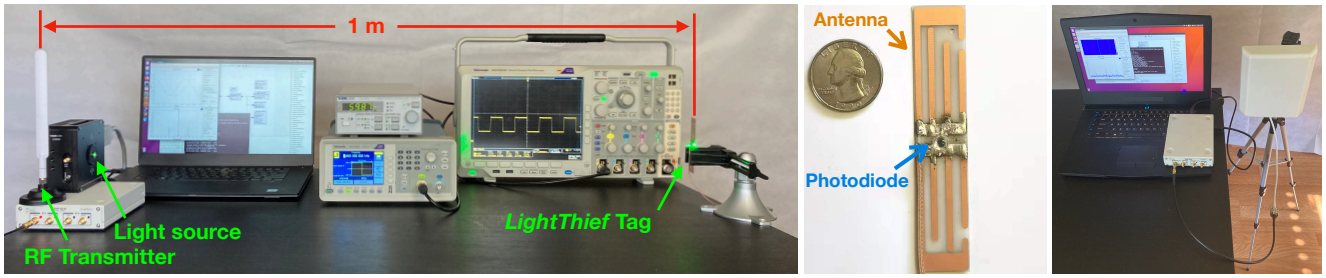
where I_{SAT} is the reverse saturation when a reverse bias applies to the PD, q is the electron charge, V_L is the applied bias voltage across the two terminals, $k_B$is the Boltzmann Constant, and T is the absolute temperature.

Thus, the PD impedance is:

$$Z_i = \frac{V_L}{I_{ph} - I_d} = \frac{V_L}{\frac{R_\lambda P}{4\pi d_{ph}^2} - I_{SAT}(e^{\frac{qV_L}{k_B T}} - 1)} \tag{6}$$

From Eqn. 6, we can observe that only a small dark current survives when there is no incident light ($P = 0$), and the corresponding impedance will be enormous. Therefore, to maximize the difference between the two impedance states, we need to minimize the impedance when there is incident light ($P \neq 0$). In other words, the photocurrent generated by the incident light (I_{ph}) should be as large as possible. As we can observe in Eqn. 6, an increased responsivity R_λ or a reduced distance d_{ph} will produce a high photocurrent and result in a small impedance.

Summary. As introduced in Eqn. 1 and 6, to increase the eavesdropping range, the attacker needs to either i) design *LightThief*'s antenna with a high gain $G_{passive}$, ii) select the RF signal with a lower center frequency f_c, iii) increase the responsivity R_λ of *LightThief*'s PD, or iv) reduce the distance



(a) Light source, RF transmitter, and *LightThief* Tag (b) Tag with single PD (c) Attacker's receiver

Figure 7: Feasibility experiment setup for the model validation

Color	Laser Diode (LD)	Band	Wavelength (nm)			Phototdiode (PD)	Band	Sensitivity (nm)			Sensitive Area (mm^2)	Responsitivity (A/W)
			Min	Peak	Max			Min	Peak	Max		
Blue	PLT5 450B	Osram	440	450	460	MTPD4400D-1.4	Marktech	190	440	570	1.2	0.13
Green	L515A1	Thorlabs	510	515	525	TEMD6010FX01	Vishay	430	540	610	0.27	0.39
Red	L650P007	Thorlabs	640	650	660	PDB-C156	API	400	870	1100	8.07	0.53
Infrared	L904P010	Thorlabs	890	904	920	BPV10	Vishay	380	920	1100	0.78	0.55

Table 1: Selected Components for Feasibility Experiments

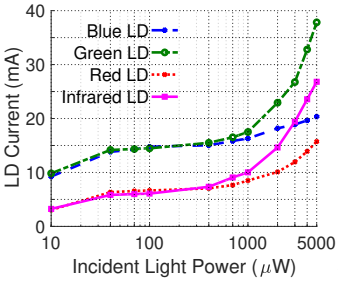


Figure 8: LD current vs. light intensity

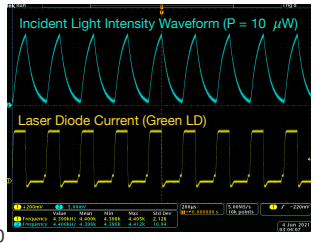


Figure 9: LD current waveform vs. light intensity waveform

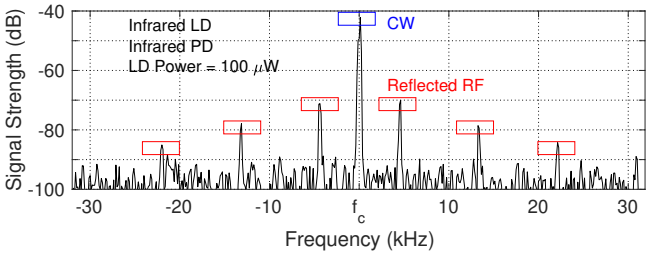


Figure 10: FFT spectrum of received RF signals.

d_{ph} from *LightThief* to the light source. Since the design and fabrication of *LightThief*'s antenna are outside this paper, we mainly evaluate the effects of last three factors on the eavesdropping range.

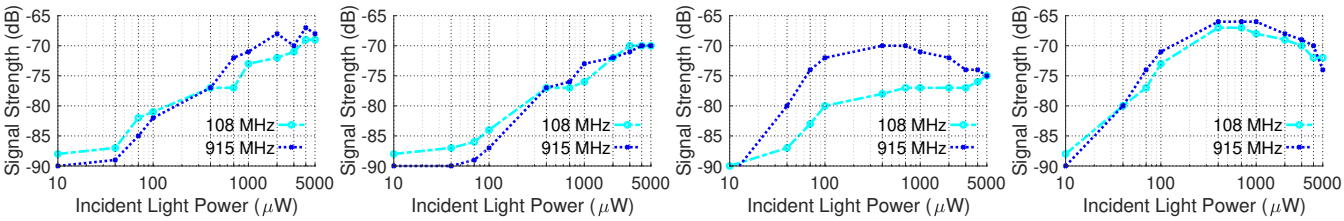
4.3 Feasibility Experiment Setup

The setup is shown in Fig. 7. We chose components with different parameters to compare the effects on *LightThief*.

Light Source. To accurately evaluate different parameters that affect *LightThief*, we employ lasers as the light sources for controlled experiments. In the latter evaluation and applications, we utilize the most common lighting fixtures, such as LED and lamps, as our light sources.

As shown in Table 1, we select laser diodes (LDs) with wavelengths corresponding to four different colors, which can cover most of the wavelength range used for OWC. To precisely control the light power incident on *LightThief*, we use a Thorlabs LDC205C laser current controller to provide a constant current for LDs and use a function generator Tektronix AFG1062 to modulate the controller to emulate OOK modulation. As mentioned in Sec. 3.2, since OOK encoded by Manchester code is essentially a square wave, we make the function generator continuously modulate the controller with a square wave. We select the optical clock rate in IEEE Std 802.15.7 PHY V Mode 3 (4.4 kHz) as the square wave frequency.

We fix the distance d_{ph} between the LD and *LightThief* and tune the incident light power with the controller to emulate the obscuration level. We use the Thorlabs S130C PD power sensor to measure the incident light power. Fig. 8 shows the diode current vs. incident light power curves. The horizontal axis is the incident light power ranging from 10 μW to 5000 μW, emulating the real-world light intensity. Since the 3 dB bandwidth of the current controller is DC to 150 kHz based on a small signal, the output laser waveform may be distorted at the optical clock rate. Therefore, we use a 2 GHz free space photo-detector with 400 $\sim$ 1100 nm Thorlabs DET025A/M to observe the laser waveform. Fig. 9 shows the compari-



(a) Blue LD & Blue PD. (b) Green LD & Green PD. (c) Red LD & Red PD. (d) Infrared LD & Infrared PD.

Figure 11: Effect of RF center frequency.

son of diode current waveform and incident laser waveform. Compared with the square wave from diode current, the laser waveform has some amount of distortion and is still acceptable to realize the OOK modulation.

Laser Safety. Due to the risk of laser radiation, we have received comprehensive laser safety training. During the experiment, a laser interlock system was used to prevent unauthorized access to the laser operation area. The laser was operated at the lowest power setting required for the experiment. The beam path was closed or shielded as much as possible and non-reflective surfaces were used around the laser unit. Warning signs and labels were clearly displayed, and only trained and authorized personnel had access to the laser area. We also used personal protective equipment to protect the safety of the authorized personnel.

RF Transmitter. *LightThief*'s antenna can pick up RF signals in FM band (87.5 $\sim$ 108.0 MHz) and license-free band (902 $\sim$ 928 MHz). To prove the basic concept of passive optic-to-RF conversion, we use USRP B210 to create CWs at 108 MHz and 915 MHz. We note that FCC regulations allow weak unlicensed personal transmitters in FM bands [16, 38]. As shown in Fig. 7, we fix the distance d_t between the transmitting antenna and *LightThief* at 3.28 ft.

***LightThief* Tag.** We implement four *LightThief* tags, each with a different PD to compare the effect of the responsivity R_λ. As shown in Table 1, although the sensitivity wavelength ranges overlap, the responsivity differs from each other.

4.4 Avoiding Self-Interference

In this experiment, we first present how *LightThief* leverages the frequency shift to avoid the self-interference. The RF transmitter transmits a CW with a central frequency f_c. *LightThief* reflects the CW under laser irradiation. The laser is modulated using a square wave at an optical clock rate. Fig. 10 shows the FFT spectrum of the received RF signals at the receiver. We see *LightThief* creates reflected RF signals (the red marks) on both sides of the transmitting CW (the blue mark). The reflected signals are copies of CW with the same modulation information as the laser (i.e., OWC data). We can observe that the minimum frequency gap between reflected RF signals and CW is 4.4 kHz, i.e., the optical clock rate. The minimum frequency gap among reflected RF signals is 8.8 kHz. Therefore, the attacker can demodulate the reflected RF signals to obtain the OWC data without self-interference.

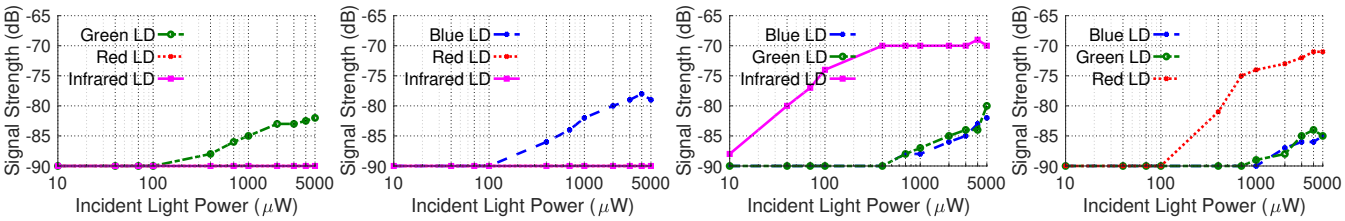
We next explain how *LightThief* realizes frequency shift. When the laser modulated by square waves changes the impedance of *LightThief*'s antenna to reflect the RF signals, it essentially uses a square wave with the phase of 0 or π to modulate the phase of incoming RF signals [28]. We use θ_n to represent the phase of each square wave. As described in Sec. 3.2, the phase of a square wave represents the transmitted OWC data bit. If the transmitted bit is '1' or '0', the phase is 0 or π, respectively. A square wave can be represented using Fourier series as follows [13]:

$$S_{sqw}(f_o,\theta_n) = 0.5 + \frac{2}{\pi}\sum_{m=1,3,5...odd}^{\infty}\frac{1}{m}cos(2\pi m f_o t + \theta_n) \quad (7)$$

Where, f_o is the square wave frequency, i.e., optical clock rate. We assume the transmitting CW as $sin(2\pi f_c t)$. The reflected RF signal can be calculated by multiplying the CW and the harmonics of a square wave [48]:

$$\begin{aligned} S_r &= S_{cw} \times S_{sqw} \\ &= sin(2\pi f_c t) \times \frac{2}{\pi}\sum_{m=1,3,5...odd}^{\infty}\frac{1}{m}cos(2\pi m f_o t + \theta_n) \\ &= \frac{1}{\pi}\sum_{m=1,3,5...odd}^{\infty}\frac{1}{m}\{sin(2\pi(f_c + m f_o)t + \theta_n) \\ &\quad + sin(2\pi(f_c - m f_o)t - \theta_n)\} \end{aligned} \quad (8)$$

From Eqn. 8, we see the reflected RF signals S_r are shifted $f_c \pm m f_o$ ($m = 1,3,5...odd$) away from the center frequency of the incoming CW, avoiding self-interference. Therefore, we can find the reflected RF signals at $\pm$4.4 kHz (m=1), $\pm$13.2kHz (m=3), and $\pm$22 kHz (m=5) in Fig. 10. More importantly, the phase θ_n representing OWC data is embedded into the reflected RF signals. Since θ_n is the only unknown value in Eqn. 8 and has only two states, it is easy for the attacker to demodulate the reflected RF signal to obtain θ_n.



(a) Blue PD. (b) Green PD. (c) Red PD. (d) Infrared PD.

Figure 12: Effect of responsivity.

4.5 Effect of RF Center Frequency

We study the effect of the RF center frequency on the received signal strength in Fig. 11. When the peak sensitivity wavelength of the PD is close to the peak wavelength of the LD, the received signal strength increases with the increase of the incident light power. Constrasting with Fig. 11a and 11b , Fig. 11d and 11c show *LightThief* implemented with the infrared and red PDs can create higher received signal strength even the incident light power is lower than 100 μW. Specifically, when the incident light power increases from 10 μW to 1000 μW, the received signal strength increases. While the incident light power keeps increasing to 5000 μW, the corresponding received signal strengths are slightly decreasing.

As we can observe from these sub-figures, the received signal strengths range from -88 $\sim$ -70 dB as long as the incident light power is higher than 100 μW, which is sufficient for the attacker to eavesdrop on OWC outside the room .

4.6 Effect of Responsivity

Because of the overlapping responsivity, the PD can sense light in the adjacent spectrum. The closer the peak wavelength of the LD is to the peak sensitive wavelength of the PD, the stronger the received signal strength and vice versa. We first show the effect of the responsivity for a blue PD in Fig. 12a. As we can observe in this figure, since the spectrums of blue and green light are close to each other, *LightThief* can reflect RF signals using a blue PD under the green LD irradiation. The corresponding signal strength is as high as -83 dB when the incident LD power reaches 5000 μW. However, since the minimum emitted wavelengths of the red or infrared LD (640 and 840 nm) are even greater than the maximum sensitive wavelength of the blue PD (460 nm), the reflected signal strength under the irradiation from the red or infrared LD is lower than the noise floor (-90 dB).

Similarly, a PD with a larger sensitive area and wavelength range can help an attacker obtain a stronger received signal strength. As shown in Fig. 12c, *LightThief* with the red PD can reflect RF signals under the irradiation of a shorter wavelength LD (i.e., blue and green) and a longer wavelength LD (i.e., infrared). When the incident power reaches 5000 μW, the corresponding received signal strengths for the blue and infrared LD are -70 dB and -82 dB, respectively.

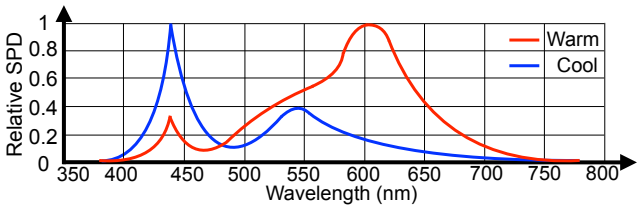


Figure 13: SPDs of cool and warm white LEDs [33]

Therefore, to effectively reflect the RF signals, we should i) utilize the PD with the peak sensitivity wavelength closest to the strongest energy spectrum of the light source; ii) place *LightThief* with small sensitive-area PDs closer to the light source than that with large sensitive-area PDs.

4.7 Effect of Source-to-*LightThief* Distance

The incident light power increases as the distance from the light source to *LightThief* decreases and vice versa. Therefore, the analysis of the effect of the source-to-*LightThief* distance is equivalent to analyzing the effect of the incident light power. As we can observe from Fig. 11 and 12, the received signal strength increases as the incident light power increases. Since the incident light power is negatively correlated with the source-to-*LightThief* distance, we can conclude that deploying *LightThief* close to the light source can increase the eavesdropping range.

5 Attack Design

The design is composed of two stages. We begin by selecting the PD and the center frequency of the RF signal. We then present the RF signal demodulation.

5.1 PD Choice

As analyzed in Sec. 4.6, the attacker should use the PD with the peak sensitivity wavelength closest to the strongest energy spectrum of the light source. However, the LED light we see, often perceived as white, comprises a multitude of

wavelengths. An approach to generate white light is to incorporate the phosphor in the body of a blue LED. Some of the blue light will be converted to yellow light by the phosphor. The remaining blue light, when mixed with the yellow light, results in white light. By making slight changes to the phosphor chemistry, manufacturers can alter the peak wavelength of a white LED. Fig. 13 shows typical cool and warm LEDs' spectral power distributions (SPDs). We can see a cool white LED with a peak wavelength around 450 nm and a warm white LED with a peak wavelength around 650 nm. Therefore, *LightThief* uses dual optic wavelength technology to detect optical signal. The tag integrates a blue PD (MTPD4400D) and a red PD (PDB-C156), which can sense most of LEDs.

5.2 RF Signal Choice

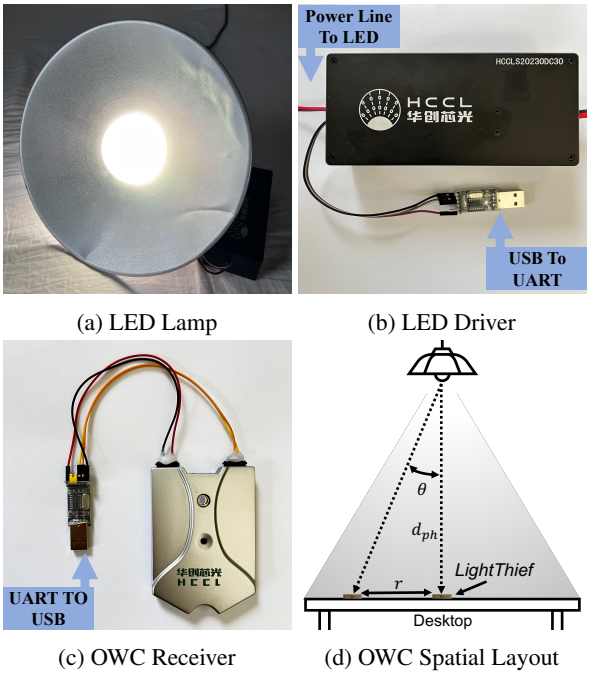
From the analysis in Sec. 4.5, *LightThief* can reflect CW in FM band or license-free band (902 $\sim$ 928 MHz). Since the opaque objects absorb a portion of RF signal energy as the signal passes through them, we take advantage of a lower center frequency (FM band) to conduct the eavesdropping because its long wavelength tends to suffer less signal absorption.

5.3 RF Signal Demodulation

As elaborated in Sec. 4.4, the reflected RF signal is fundamentally a BPSK signal generated by the multiplication of a continuous wave (CW) and square waves with two distinct phases (0 and π). In order to recover the OWC data, we utilize the signal processing techniques associated with BPSK demodulation [12, 25]. Initially, we down-convert the signal to baseband using a quadrature down-conversion mixer, focusing on the first harmonic frequency, i.e., $f_c + f_o$. Following this, we eliminate the DC offset and apply a low-pass filter to reduce high-frequency noise and unwanted components in the signal. We then employ the timing recovery method to accurately recover the symbol clock, which helps to identify the correct sampling points. During the symbol detection stage, we estimate and correct the signal's phase and amplitude to improve the accuracy of the recovered data. Next, we perform a cross-correlation analysis on the recovered data with the preamble codes to establish frame synchronization. Once the frame sync pulses have been identified, we proceed to recover the OWC data while parsing the frame structure. This comprehensive approach ensures a more accurate and reliable recovery of the OWC data under various conditions, taking into account factors such as noise, interference, and signal distortion that might affect the data recovery process.

6 Implementation

COTS OWC Device. To validate the effectiveness of *LightThief*'s eavesdropping capabilities, we conduct experiments using a COTS OWC device, (i.e., HCCLS2023ODC [1]), in our experimental setup. This device is considered ideal for providing secure, non-radio frequency wireless links in highly sensitive areas, effectively handling confidential information, and ensuring the integrity of critical communications [2].



(a) LED Lamp (b) LED Driver

(c) OWC Receiver (d) OWC Spatial Layout

Figure 14: Implementation

In the following two subsections, we provide the detailed specifications of the COTS OWC device (HCCLS2023ODC), which consists of two primary components: an OWC transmitter and an OWC receiver.

(1) *OWC Transmitter.* As shown in Fig.14a and Fig.14b, the OWC transmitter comprises an LED lamp and an LED driver, respectively. The white LED lamp's power rating is 40 W and its size is 30cm by 17cm. The LED driver converts AC current into a constant current suitable for powering the LED. By controlling the current converter, the driver can employ OOK modulation to regulate the light intensity of the LED, allowing for simultaneous communication and illumination. By using UART communication software, the driver can set the physical layer transmission data rate to four different rates: 400 kbps, 300 kbps, 200 kbps, and 100 kbps. Specifically, it goes through the following three steps: i) it converts the transmitted data into 8-bit ASCII codes; ii) it transforms the 8-bit ASCII codes into 12-bit Hamming codes and 1-bit parity check code for error detection and correction; and iii) it converts the 13-bit codes into 26-bit Manchester codes to ensure balanced lightness. To facilitate packet detection and synchronization, each packet consists of a 10-bit preamble with a fixed pattern of "1111000010".

(2) *OWC Receiver.* As shown in Fig.14c, the OWC receiver can be powered by a USB interface, which is a 5V DC power

supply or a 5V battery for mobile applications. The Power consumption of the receiver is less than 1W. The OWC receiver contains a 3.7 mm by 3.7 mm photosensitive sensor, which is capable of detecting light wavelengths between 320 and 1050 nm. Same as the transmitter, the receiver also provides the UART interface. The receiver achieves a communication rate of approximately 400 kbps within a 2-meter communication distance and a 1.5-meter communication coverage diameter. While this confined coverage area restricts the communication range, it guarantees that the emitted light does not disrupt other ongoing optical communication systems, thus maintaining a reliable communication channel.

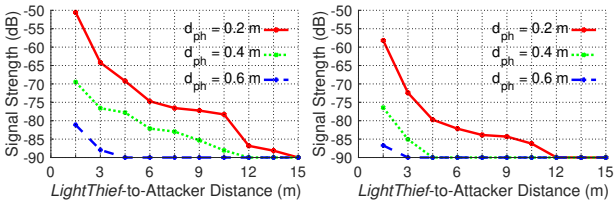
Experiment Setup. We conduct the experiment in an office setting, simulating a real-world scenario, and established two separate communication links: one between the OWC transmitter and receiver, and another between LightThief and the attacker's receiver.

(1) *Victim.* We first establish communication between the OWC transmitter and receiver. Using the UART interface, we send commands to the transmitter to control the data rate for various experimental scenarios. We then evaluate the performance of the communication link. This process provides baseline information, such as the limitations of communication distances and angles for OWC, allowing us to effectively assess the performance of *LightThief*.

(2) *Attacker.* As shown in Fig. 14d, we place *LightThief* on a desktop within a cubicle. To adjust the eavesdropping distance and angle, we modify the distance between the lamp and the desktop, as well as the position of *LightThief* on the desktop. When the LED directly illuminates *LightThief*, the distance between the LED and *LightThief* is denoted as d_{ph}, and the angle is 0 degrees. By changing the position of *LightThief* along a circular path with a radius r around a central point, we can adjust the angle θ, which can be calculated as $\arctan(\frac{r}{d_{ph}})$. We then evaluate the eavesdropping performance at different positions with factors including signal strength, data rate, and reliability.

(3) *Barriers.* In our experiments, we utilize two types of walls as barriers to evaluate the performance of *LightThief* under various conditions. The first type is an office partition wall, commonly used to divide workspace areas, while the second type is room drywall, typically found in residential and commercial buildings. These walls differ in material composition and structure, which allows us to assess the effectiveness of *LightThief* in different scenarios.

Since there may be particle diffusion in the victim's room, such as mist or smoke, we also evaluate the impact of the particle diffusion on eavesdropping. We emulate particle diffusion using mist created by a humidifier. To control the particle concentration, the LED, *LightThief* and the humidifier are placed in a cubicle. After the mist is sprayed from the humidifier, it spreads between the LED and *LightThief*.



(a) Office partition wall. (b) Room dry wall.

Figure 15: Distance vs. Signal Strength.

7 Evaluation

In this section, we comprehensively evaluate *LightThief*'s performance across a range of scenarios and settings. Initially, we investigate the detected signal strength on the attacker's side, taking into account various LED-to-*LightThief* and *LightThief*-to-attacker distances. We then proceed to decode the received signal, disassemble the packet, and compute the bit error rate to verify the effectiveness of *LightThief*. Subsequently, we delve into the influence of multiple factors on eavesdropping performance, including the data rates, light source angle, and particle diffusion.

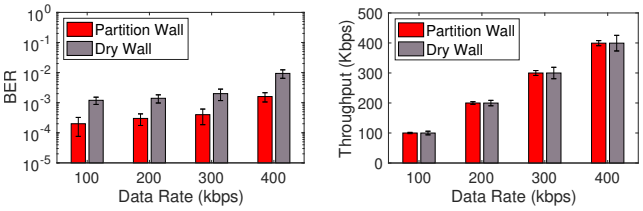
7.1 Detecting the Signal

In this section, we demonstrate *LightThief*'s performance in smuggling OWC data through various opaque objects, considering different LED-to-*LightThief* and *LightThief*-to-attacker distances. These experiments are conducted with the LED light directly illuminating the *LightThief*. For these experiments, we set the OWC data rate to 400 kbps.

Fig. 15a demonstrates the signal strength detected by the attacker when an office partition wall is positioned between the *LightThief* and the attacker. As the distance from *LightThief* to the attacker grows, the detected signal strength diminishes. However, even when the *LightThief*-to-attacker distance reaches approximately 10 m, the detected signal strength maintains a level above -80 dB. This ensures that the attacker can effectively eavesdrop on the communication while minimizing exposure risk.

Furthermore, when the LED-to-*LightThief* distance (d_ph) extends from 0.2 to 0.6 m, the detected signal strength declines due to the reduction in incident light power. It is worth noting that the OWC device itself only supports a communication range of up to 2 m, which subsequently limits the LED-to-*LightThief* distance.

Fig. 15b presents a similar trend in the reflected signal strength when room drywall is placed in between. We can observe that *LightThief* exhibits better performance in environments with office partition walls compared to those with room dry walls. This is attributed to the thinner structure and lower electromagnetic signal absorption properties of partition walls.



(a) Bit Error Rate (b) Throughput

Figure 16: Eavesdropping Performance

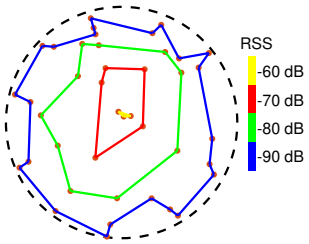


Figure 17: Impact of Light Source Angle

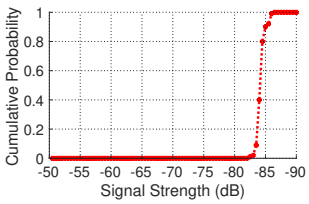


Figure 18: Impact of Particle Diffusion

From these experiments, we can conclude that increasing the signal strength can be achieved by reducing either the LED-to-*LightThief* distance or the *LightThief*-to-attacker distance. To effectively eavesdrop on OWC while remaining covert, an attacker can decrease the LED-to-*LightThief* distance, thereby allowing for an increased *LightThief*-to-attacker distance.

7.2 Decoding the Signal

Fig. 16a demonstrates the eavesdropping performance at a *LightThief*-to-attacker distance of 10 m. As observed from the left figure, the attack with an office partition wall in between exhibits the best performance. At a data rate of 400 kbps, the BER is around 0.1%, indicating that our proposed attack method can effectively eavesdrop on OWC systems with high data rates.

The BER reduces when the data rate increases. This can be attributed to the fact that the maximum data rate of 400 kbps approaches the response limit of the LED. As the optical clock rate increases, the time allocated for powering the LED decreases, leading to a reduced response time for the LED to reach its maximum brightness. Consequently, when the optical clock rate approaches or falls below the response time, the LED cannot achieve its highest brightness, resulting in a lower light intensity entering the *LightThief*.

We also assess the throughput at the attacker's receiver under varying data rates. As illustrated in Fig. 16b, the throughput rises as the data rates of the OWC transmitter increase, closely approaching the data rates themselves. It's worth noting that *LightThief* has a straightforward design, consisting of only two passive analog components: an antenna and a photodiode. With the photodiode's response speed exceeding MHz, *LightThief* is well-equipped to eavesdrop on communication with higher data rates.

7.3 Impact of Light Source Angle

In this experiment, we alter the position of *LightThief* along a circular path with a radius r around the central point of the LED light spot on the desktop (shown in Fig. 14d). We maintain the LED-to-*LightThief* distance at 0.2 m, enabling us to adjust the angle θ. We measure the reflected signal strength to evaluate the impact of the light source angle. We observed that the light intensity is not uniformly distributed around the circle's center. As illustrated in Fig. 17, to obtain the same light intensity, measurements must be taken at varying radii from the center.

The uneven light intensity distribution can be attributed to the arrangement of multiple LEDs in the COTS LED lamp. These LEDs are placed in a radial pattern, and when they have non-identical characteristics such as brightness, beam angle, or color temperature, they can cause uneven light distribution when illuminated simultaneously. Manufacturing tolerances and the aging of individual LEDs can also result in slight performance differences. When combined in a single lighting fixture, these discrepancies can lead to an irregular light distribution pattern, as seen in the experiment. Although a white LED diffuser helps distribute the light more evenly, its effectiveness is limited.

The maximum radius *LightThief* can reach corresponds to an angle of 11 degrees, while the OWC device supports up to 20 degrees. Consequently, our *LightThief* can utilize up to 48% of the available illumination range.

7.4 Impact of Particle Diffusion

We set the optical clock rate of the OWC transmitter to 400 kbps and the LED-to-*LightThief* distance to 0.6 m with an office partition wall in between. We turn on the humidifier and adjust the reflected signal strength to the same value as the previous experiment. A Thorlabs S130C PD power sensor is placed close to *LightThief* to measure the incident light power.

Fig. 18 shows the impact of the particle diffusion on reflected RF signal strength. As we can see, the average reflected RF signal strength is reduced compared to the performance without particle diffusion shown in Fig. 15a. This is because the particles tend to absorb and scatter light, disturbing the light environment. As a result, the incident light power reduces, lowering the reflected RF signal strength. As we can see from Fig. 18, the detected signal strength with particle diffusion is around 5 dB lower than that without particle diffusion. We set the threshold value as -83. Since particle diffusion is a slow process, we combine the rate of change

in the received signal strength and the threshold to ensure detection accuracy.

8 Defense Strategy

In this section, we discuss strategies to defend against the proposed attack.

Light Source-Based Approach. Reducing the light scattering angle of the OWC product can serve as a defense against *LightThief*. From Sec. 7.3, we know that *LightThief* can exploit up to 48% of the illumination area. However, if the OWC product's scattering angle were even smaller, the available space to deploy *LightThief* would be extremely limited, even when taking advantage of the 48% area. If *LightThief* is placed between the LED and the OWC receiver, *LightThief* will block the light signal before it reaches the OWC receiver. Therefore, the OWC receiver cannot receive the photoelectric signal, which exposes the eavesdropping. Therefore, we can use a highly directional light source, such as directional & spotlight LED, to conduct OWC and avoid being detected by *LightThief*. However, it is not suitable for free-space optics because they also need to illuminate the entire room.

Physical Barrier-Based Approach. It is possible to use a Faraday Cage to shield the reflected RF signals penetrating through walls from inside the room. However, completely enclosing a room with a Faraday Cage may not be practical. For example, the victim cannot receive the RF signals from outside the room anymore, such as FM radio and LTE. A more feasible approach is to apply electromagnetic shielding material to thinner walls or to the wall where the attacker is most likely to be hiding. This material can effectively block the transmission of RF signals, preventing the attacker from eavesdropping on the OWC communication while maintaining a more reasonable level of practicality in implementation.

RF Medium-Based Approach. Victims can actively create RF interference to defend against *LightThief*'s eavesdropping. To improve the efficiency of *LightThief*, attackers choose clean frequency bands to transmit their continuous wave (CW), ensuring that the reflected RF signal also falls within a clean frequency band. This is easily achievable, as there are many vacant frequency bands within the RF spectrum. However, victims can proactively generate RF noise within these vacant bands, raising the noise floor without interfering with others' legitimate RF signals. This approach can effectively disrupt the attacker's eavesdropping while minimizing any negative impact on other users in the spectrum.

Encryption. Since the proposed eavesdropping captures optical signals in the physical layer, once the data is encrypted at a higher layer, the attackers cannot decode meaningful data from the raw signal.

We note that the above strategies have not been empirically evaluated. We leave the task of implementing these strategies to future work.

9 Discussion

Higher Data Rates. *LightThief* can eavesdrop on communication with higher data rates. This is because *LightThief* has a straightforward design, consisting of only two passive analog components: an antenna and a photodiode. The photodiode has a response speed exceeding MHz, enabling *LightThief* to sense data rates of multiple megabits per second. However, our attack scenario focuses on OWC systems that deliver both illumination and communication. Due to the high-power nature of illumination systems, achieving MHz-level optical clock rates is challenging. We have made extensive efforts to look for OWC systems with illumination and higher data rates, but to no avail. The OWC product we used in our experiment is a COTS OWC product with a moderate illumination power of 40 W and the highest data rates of 400 kbps we can find thus far. Moreover, our evaluation results demonstrate that the throughput of *LightThief* is closely approaching the data rates of the targeted OWC product.

Ambient Light Interference. It is possible for *LightThief* to eavesdrop in the presence of strong ambient light. Because the ambient light is also essentially noise for OWC, OWC needs to choose a specific wavelength to increase the SNR. *LightThief* can eavesdrop by selecting PDs with a similar peak wavelength. However, the performance of *LightThief* working in strong ambient light is bound to degrade.

10 Related Work

Researchers aim to improve sensor network performance through building heterogeneous IoT networks, primarily by developing cross-protocol techniques [14, 41–43]. Our work, however, focuses on a different aspect: the intersection of two fundamental mediums of wireless networks:

RF medium. Recently, backscatter has played an attractive role in the RF medium communication field because it leverages ambient RF signals to achieve communication with notable performances on low cost and energy efficiency. Ambient Backscatter [27] is the first work of backscatter communication, which utilizes OOK modulation to reflect TV signals and achieve communication between two backscatter tags with up to 10 kbps bit rates. WiFi Backscatter [22] also uses OOK modulation, but it is the first work that uses commodity devices (i.e., Wi-Fi receivers) to decode the backscatter signal. Passive Wi-Fi [23] is the first work of reflecting single tones to enable communication between backscatter tags and WiFi receivers. BackFi [10] designs a self-interference cancellation on WiFi receivers to allow high throughput and long-range communication. HitchHike [48], FreeRider [49], Passive ZigBee [26], VMscatter [29], TScatter [28], and LScatter [13] serve as comprehensive studies that systematically elucidate how to reflect RF signals by controlling the phase of square waves, how to avoid self-interference, and how to extract the phase of square waves on commodity receivers.

The design of *LightThief* is inspired by the aforementioned backscatter techniques. By transferring OWC's OOK modulation onto a sine wave, *LightThief* essentially creates a BPSK RF signal. Modulation, demodulation, and self-interference avoidance techniques for this type of BPSK signal are quite common in the realm of backscatter. Consequently, we can employ these techniques to effectively implement *LightThief*.

Optical Medium. The field of optical medium networks hosts numerous key studies, tackling aspects like communication, optimization, and security. For instance, Turboboosting [45] and PassiveVLC [46] examine uplink communication via modulated optical reflection in visible light mediums. ChromaLux [18], seeking performance optimization, increases communication range and data rate through reduced switching time without major contrast reduction. Light Commands [35] uses light to attack devices, injecting malicious commands into smart speakers via laser beams, highlighting potential security threats in this domain. ICSL Attack [44] investigates the features of Infrared light to alter environment perception results and introduce SLAM errors to the AV.

However, since light cannot penetrate through opaque objects, researchers [45, 46] consider optical medium intrinsically addresses the security and privacy problems RF communication systems bring in room-level networking [11, 47]. As a result, there is a scarcity of studies investigating the security aspects of light communication. One related study [15] attempts to eavesdrop on an open-source OWC research platform by detecting electromagnetic signals that leak from the power lines of OWC products. However, the EMC regulations [4–6], found in an annex to IEEE Std 802.15.7 for OWC [9], require the COTS OWC products to prevent their electromagnetic signals from leaking out and interfering with surrounding electronics. Unlike the COTS products, the open-source research platforms can circumvent EMC regulations. For example, [15] chooses two long unshielded wires as the power line and places them at an angle of 180°. For two long wires with an angle of 180°, it is essentially a dipole antenna [3], which can strengthen the leaked electromagnetic signals. As the length of wire increases, the efficiency of the antenna system will increase significantly. In contrast, EMC engineers of COTS products routinely shorten the length of the power line as much as possible, choose shielded cable rather than unshielded wires, and use twisted pairs instead of 180° placement to reduce the electromagnetic leakage. Some COTS products [7] even eliminate the power line by directly soldering LEDs onto the power supply PCB. Therefore, the EMC regulations protect the COTS OWC products from detecting the leaked electromagnetic signals by attackers.

We challenge the prevailing assumption that OWC systems are immune to eavesdropping via optical signals. In contrast to the approach in [15], we present *LightThief*, a novel eavesdropping technique that employs backscatter techniques to detect optical signals and transmit OWC data through walls, circumventing the limitations imposed by EMC regulations. Our proposed method demonstrates that even in scenarios where there is no side-channel electromagnetic leakage, attacks can still be launched.

Intersection of optical and RF mediums. Few studies have investigated communication methods combining the strengths of both RF and optical media. Works like [20] integrate RFID readers into smart LED bulbs, simplifying deployment, while others like [17, 19, 31] incorporate a backscatter modulator circuit into light processing circuit, using light and radio's complementary properties for passive communication. Distinct from the aforementioned approaches, *LightThief* is the first to achieve cross-medium backscatter communication, negating the need for complex circuits and power use. It offers a long-lasting, highly sensitive, easy-to-conceal eavesdropping method.

11 Conclusion

In this paper, we propose the first battery-free optical-based eavesdropping, *LightThief*, which directly transfers OWC data to RF signals without requiring complex circuits and power consumption, making OWC vulnerable to eavesdropping by attackers outside the room. The structure and deployment of *LightThief* are exceptionally simple, and it boasts high sensitivity, longevity, ease of disguise, and near-zero maintenance. We demonstrate the effectiveness of our proposed approach by building a *LightThief* prototype and conducting extensive evaluations on commercial OWC products under various real-world settings. Our evaluation results reveal that *LightThief* can successfully eavesdrop on OWC through physical room boundaries such as walls, emphasizing the need for enhanced security measures in OWC systems. While the performance of our prototype represents a modest beginning, we hope that the passive cross-medium eavesdropping methods we present will contribute to the development of alternative eavesdropping approaches for various systems, especially in situations lacking electromagnetic leakage.

12 Disclosure Statement

To ensure that the security vulnerability is properly addressed and the OWC product's security is improved, we have disclosed our findings and the details of *LightThief* methodology to the manufacturer. We are committed to working collaboratively with the manufacturer to resolve this issue and protect the privacy and security of users.

13 Acknowledgments

This work is partially supported by NSF grants CNS-1652669 and CNS-2305246. We thank the anonymous shepherd and reviewers for their valuable input in improving this manuscript.

References

[1] Broad coverage visible light communication system. http://www.hccltech.com/products-detail/i-50.html.

[2] Commercial application of hccl - secure communication. http://www.hccltech.com/application-detail/i-69/.

[3] Dipole antenna. https://en.wikipedia.org/wiki/Dipole_antenna.

[4] Iec 1000-3-5, electromagnetic compatibility. part 3: Limits—section 5: Limitation of voltage fluctuations and flicker in low-voltage power supply systems for equipment with rated current greater than 16 a. 1994.

[5] Iec en 61000-3-3, electronic compatibility (emc) part 3: Limits—section 3: Limitation of voltage fluctuations and flicker in low voltage supply systems for equipment with rated current 16 a and smaller. international electrotechnical commission, 1994.

[6] Iec/ts 61000-3-5, ed. 2.0b, cor.2:2010, corrigendum 2—electromagnetic compatibility (emc)— part 3-5: Limits—limitation of voltage fluctuations and flicker in low-voltage power supply systems for equipment with rated current greater than 75 a.

[7] https://www.microchip.com/developmenttools/ProductDetails/PartNO/ADM00641.

[8] https://www.mordorintelligence.com/industry-reports/visible-light-communication-market.

[9] Ieee standard for local and metropolitan area networks–part 15.7: Short-range optical wireless communications. IEEE Std 802.15.7-2018 (Revision of IEEE Std 802.15.7-2011) (2019).

[10] Bharadia, D., Joshi, K. R., Kotaru, M., and Katti, S. Backfi: High throughput wifi backscatter. In ACM SIGCOMM (2015).

[11] Chi, Z., Li, Y., Liu, X., Wang, W., Yao, Y., Zhu, T., and Zhang, Y. Countering cross-technology jamming attack. In ACM WiSec (2020).

[12] Chi, Z., Li, Y., Liu, X., Yao, Y., Zhang, Y., and Zhu, T. Parallel inclusive communication for connecting heterogeneous iot devices at the edge. In ACM SenSys (2019).

[13] Chi, Z., Liu, X., Wang, W., Yao, Y., and Zhu, T. Leveraging ambient lte traffic for ubiquitous passive communication. In ACM SIGCOMM (2020).

[14] Chi, Z., Yao, Y., Xie, T., Liu, X., Huang, Z., Wang, W., and Zhu, T. Ear: Exploiting uncontrollable ambient rf signals in heterogeneous networks for gesture recognition. In ACM SenSys (2018).

[15] Cui, M., Feng, Y., Wang, Q., and Xiong, J. Sniffing visible light communication through walls. In ACM MobiCom (2020).

[16] FCC. Permitted forms of low power broadcast operation. "public notice 14089".

[17] Galisteo, A., Varshney, A., and Giustiniano, D. Two to tango: Hybrid light and backscatter networks for next billion devices. In ACM MobiSys (2020).

[18] Ghiasi, S. K., Zamalloa, M. A. Z. n., and Langendoen, K. A principled design for passive light communication. In ACM MobiCom (2021).

[19] Giustiniano, D., Varshney, A., and Voigt, T. Connecting battery-free iot tags using led bulbs. In ACM HotNets (2018).

[20] Gummeson, J., Mccann, J., Yang, C. J., Ranasinghe, D., Hudson, S., and Sample, A. Rfid light bulb: Enabling ubiquitous deployment of interactive rfid systems.

[21] Hatamian, M., and Bowen, E. G. Homenet: A broadband voice/data/video network on catv systems. AT T Technical Journal (1985).

[22] Kellogg, B., Parks, A., Gollakota, S., Smith, J. R., and Wetherall, D. Wi-fi backscatter: Internet connectivity for rf-powered devices. In ACM SIGCOMM (2014).

[23] Kellogg, B., Talla, V., Gollakota, S., and Smith, J. R. Passive wi-fi: Bringing low power to wi-fi transmissions. In USENIX NSDI (2016).

[24] Koonen, T., Mekonnen, K. A., Cao, Z., Huijskens, F., Pham, N. Q., and Tangdiongga, E. Beam-steered optical wireless communication for industry 4.0. IEEE Journal of Selected Topics in Quantum Electronics (2021).

[25] Li, Y., Chi, Z., Liu, X., and Zhu, T. Chiron: Concurrent high throughput communication for iot devices. In ACM MobiSys (2018).

[26] Li, Y., Chi, Z., Liu, X., and Zhu, T. Passive-zigbee: Enabling zigbee communication in iot networks with 1000x+ less power consumption. In ACM SenSys (2018).

[27] LIU, V., PARKS, A., TALLA, V., GOLLAKOTA, S., WETHERALL, D., AND SMITH, J. R. Ambient backscatter: Wireless communication out of thin air. In ACM SIGCOMM (2013).

[28] LIU, X., CHI, Z., WANG, W., YAO, Y., HAO, P., AND ZHU, T. Verification and redesign of ofdm backscatter. In USENIX NSDI (2021).

[29] LIU, X., CHI, Z., WANG, W., YAO, Y., AND ZHU, T. Vmscatter: A versatile mimo backscatter. In USENIX NSDI (2020).

[30] MANIE, Y. C., YAO, C.-K., YEH, T.-Y., TENG, Y.-C., AND PENG, P.-C. Laser-based optical wireless communications for internet of things (iot) application. IEEE Internet of Things Journal (2022).

[31] MIR, M. S., GUZMAN, B. G., VARSHNEY, A., AND GIUSTINIANO, D. Passivelifi: Rethinking lifi for low-power and long range rf backscatter. In ACM MobiCom (2021).

[32] [N. D.]. Manchester code. https://en.wikipedia.org/wiki/Manchester_code.

[33] [N. D.]. Xlamp xm-l2 leds. https://cree-led.com/media/documents/XLampXML2.pdf.

[34] NIKITIN, P., AND RAO, K. Theory and measurement of backscattering from rfid tags. IEEE Antennas and Propagation Magazine (2006).

[35] SUGAWARA, T., CYR, B., RAMPAZZI, S., GENKIN, D., AND FU, K. Light commands: Laser-based audio injection attacks on voice-controllable systems. In USENIX Security (2020).

[36] THEREMIN, L. The thing (also known as the great seal bug). https://en.wikipedia.org/w/index.php?title=The_Thing_(listening_device)&oldid=1043635720.

[37] TSONEV, D., VIDEV, S., AND HAAS, H. Light fidelity (Li-Fi): towards all-optical networking. In Broadband Access Communication Technologies VIII (2014), International Society for Optics and Photonics, SPIE.

[38] WANG, A., IYER, V., TALLA, V., SMITH, J. R., AND GOLLAKOTA, S. Fm backscatter: Enabling connected cities and smart fabrics. In USENIX NSDI (2017).

[39] WANG, K., NIRMALATHAS, A., LIM, C., AND SKAFIDAS, E. High-speed optical wireless communication system for indoor applications. IEEE Photonics Technology Letters (2011).

[40] WANG, Q., GIUSTINIANO, D., AND PUCCINELLI, D. An open source research platform for embedded visible light networking. IEEE Wireless Communications (2015).

[41] WANG, W., LIU, X., YAO, Y., PAN, Y., CHI, Z., AND ZHU, T. Crf: Coexistent routing and flooding using wifi packets in heterogeneous iot networks. In IEEE INFOCOM (2019).

[42] WANG, W., LIU, X., YAO, Y., AND ZHU, T. Exploiting wifi ap for simultaneous data dissemination among wifi and zigbee devices. In IEEE ICNP (2021).

[43] WANG, W., XIE, T., LIU, X., AND ZHU, T. Ect: Exploiting cross-technology concurrent transmission for reducing packet delivery delay in iot networks. In IEEE INFOCOM (2018).

[44] WANG, W., YAO, Y., LIU, X., LI, X., HAO, P., AND ZHU, T. I can see the light: Attacks on autonomous vehicles using invisible lights. In ACM CCS (2021).

[45] WU, Y., WANG, P., XU, K., FENG, L., AND XU, C. Turboboosting visible light backscatter communication. In ACM SIGCOMM (2020).

[46] XU, X., SHEN, Y., YANG, J., XU, C., SHEN, G., CHEN, G., AND NI, Y. Passivevlc: Enabling practical visible light backscatter communication for battery-free iot applications. In ACM MobiCom (2017).

[47] YAO, Y., LI, Y., LIU, X., CHI, Z., WANG, W., XIE, T., AND ZHU, T. Aegis: An interference-negligible rf sensing shield. In IEEE INFOCOM (2018).

[48] ZHANG, P., BHARADIA, D., JOSHI, K., AND KATTI, S. Hitchhike: Practical backscatter using commodity wifi. In ACM SenSys (2016).

[49] ZHANG, P., JOSEPHSON, C., BHARADIA, D., AND KATTI, S. Freerider: Backscatter communication using commodity radios. In ACM CoNEXT (2017).

[50] ZHAO, J., GONG, W., AND LIU, J. Spatial stream backscatter using commodity wifi. In ACM MobiSys (2018).

[51] ZHAO, J., GONG, W., AND LIU, J. X-tandem: Towards multi-hop backscatter communication with commodity wifi. In ACM MobiCom (2018).