LeakageScatter

Backscattering LiFi-leaked RF Signals

Mir, Muhammad Sarmad; Cui, Minhao; Guzman, Borja Genoves; Wang, Qing; Xiong, Jie; Giustiniano, Domenico

DOI
10.1145/3565287.3610262

Publication date
2023

Document Version
Final published version

Published in
MobiHoc 2023 - Proceedings of the 2023 International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing

Citation (APA)
Mir, M. S., Cui, M., Guzman, B. G., Wang, Q., Xiong, J., & Giustiniano, D. (2023). LeakageScatter: Backscattering LiFi-leaked RF Signals. In *MobiHoc 2023 - Proceedings of the 2023 International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing* (pp. 290-299). (Proceedings of the International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)). Association for Computing Machinery (ACM). https://doi.org/10.1145/3565287.3610262

LeakageScatter: Backscattering LiFi-leaked RF Signals

Muhammad Sarmad Mir[*★], Minhao Cui[◇★], Borja G. Guzman[△], Qing Wang[†], Jie Xiong[◇], Domenico Giustiniano[△]
[*]Universidad Carlos III de Madrid, [◇]University of Massachusetts Amherst, [△]IMDEA Networks Institute, [†]TU Delft

[*]sarmadmir2003@gmail.com, [◇]{minhaocui, jxiong}@cs.umass.edu,
[△]{borja.genoves, domenico.giustiniano}@imdea.org, [†]qing.wang@tudelft.nl

ABSTRACT

Radio-Frequency (RF) backscatter has emerged as a low-power communication technique. Backscatter systems either rely on active signal generators (spectrum efficient, but dedicated infrastructure) or existing ambient wireless transmissions (existing infrastructure, but spectrum inefficient). In this paper, we aim to make RF backscatter spectrum efficient and at the same time work with existing infrastructure. We propose to leverage the deployment of LiFi networks built upon LED bulbs for pervasive RF backscatter. We experimentally demonstrate that LiFi, which passively leaks RF signals, can be exploited as a radio carrier generator for low-power RF backscatter. We further design **LeakageScatter**, the first backscatter system operating in the ISM band and exploiting LiFi-leaked RF signals, without the need to actively generate the carrier wave. We customize the design of the loop at the LiFi transmitter, as well as the coil antennas at the tag and RF backscatter receiver, to optimize the system performance. We propose to opportunistically enable the oscillator of the backscatter tag in the software that could reduce the energy consumption on backscattering by up to 75%. Experimental results show that LeakageScatter achieves a backscattering distance up to 10 m and 18 m in indoor and outdoor scenarios, respectively, without using a dedicated RF carrier generator.

CCS CONCEPTS

• **Networks** → **Mobile networks**; • **Computer systems organization** → **Sensor networks**.

KEYWORDS

LiFi, leaked RF signals, backscatter, system design, implementation

ACM Reference Format:
Muhammad Sarmad Mir, Minhao Cui, Borja Genoves Guzman, Qing Wang, Jie Xiong, Domenico Giustiniano. 2023. LeakageScatter: Backscattering LiFi-leaked RF Signals . In *International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing (MobiHoc '23), October 23–26, 2023, Washington, DC, USA.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3565287.3610262

★Both authors contributed equally to the paper.

MobiHoc '23, October 23–26, 2023, Washington, DC, USA

ACM ISBN 978-1-4503-9926-5/23/10…$15.00
https://doi.org/10.1145/3565287.3610262

1 INTRODUCTION

The ever-increasing Internet-of-Things (IoT) services lead to a massive deployment of connected devices, where most of them are currently *battery-powered*. According to a prediction by Business Insider, there will be more than 64 billion IoT devices deployed worldwide by 2026 [1]. However, batteries cause severe environmental issues due to a large amount of chemical materials such as lithium, zinc and chloric acid inside the battery. Therefore, a tremendous amount of research effort has been devoted to enabling low-power *battery-free* communication for the era of IoT [7, 19, 25, 29]. Among these solutions, Radio Frequency (RF) backscattering is a particularly promising technique which modifies and reflects surrounding RF signals to enable ultra-low-power battery-free communication.

Emerging RF backscatter techniques either use dedicated RF carriers or exploit ambient carriers to trigger backscattering. Solutions leveraging dedicated RF carriers are more spectrum efficient (only a frequency tone transmitted) [10] but they suffer from high deployment cost and increased power consumption of the dedicated carrier generator. Solutions leveraging ambient RF communication can remove the significant burden of deploying dedicated hardware as the carrier source, making the design much more convenient to be adopted in real-world settings. However, the signal strength of ambient RF carrier is usually very weak. The ambient RF signals from TV broadcast can only enable backscatter communication up to a few meters [18, 23] and ambient WiFi signals only support a backscatter range of 5 m [2, 17]. Also, backscattering with ambient RF signals results in low spectrum efficiency due to doubling the required channel bandwidth [32, 33]. Besides, an issue with backscattering is the dependence of communication performance on tag placement. The backscatter tag needs to be placed either close to the carrier source or the receiver, limiting its application scenarios. The most straightforward solution to this problem is to deploy many carrier generators to reduce the distance between carrier sources and tags [16]. However, this will unavoidably cause a high deployment cost and more RF interference.

In this work, we address the aforementioned issues by utilizing the otherwise wasted ambient RF leakage from modulated Light-Emitting Diode (LED) bulbs, to achieve spectrum efficiency for backscattering. As the most popular lighting technology nowadays, LED bulbs are now pervasively deployed in our environment to achieve efficient illumination. Because LEDs can be easily turned on and off at the order of million times per second, they are also being used to transmit data wirelessly, creating the so-called LiFi networks. Our system is inspired by a recent discovery that LED-based LiFi causes RF leakage [3]. In this work, we propose to utilize RF leakage as the carrier source for backscattering. An illustration of our system is shown in Figure 1. The IoT tag not only receives

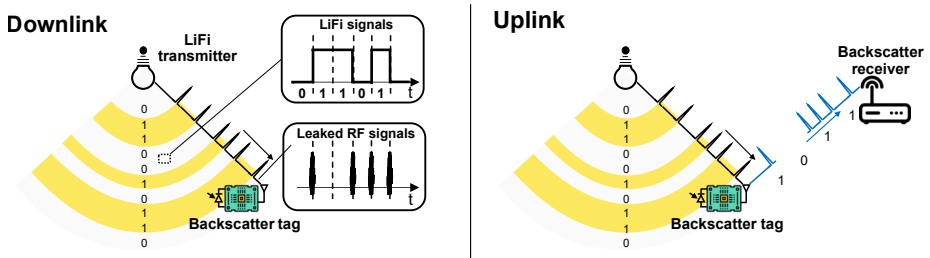


Figure 1: LeakageScatter overview: *(left)* Downlink: The backscatter tag receives the LiFi signals and harvests energy from them; *(right)* Uplink: The tag modulates the received LiFi-leaked RF signals and backscatters them to the receiver.

the light signal (downlink), but also serves as a backscatter tag for the RF leakage (uplink), thus enabling low-power bi-directional communication without the need for a dedicated device as the RF carrier source. Although the idea sounds promising, several challenges need to be addressed before the idea can be turned into a working system.

The first challenge is that the LiFi-leaked RF signal is very weak and cannot support backscattering. The RF leakage is a "by-product" of the LiFi modulation process. As the LiFi transmitter circuit is designed for sending out light signals instead of the RF leaked signals, the amplitude of the leaked signals is too weak —about -100 dBm when the transmitter-tag distance is 1 m—and thus it is not able to support backscatter communication. To address this issue, we study the key factors affecting the signal strength of the RF leakage. We find that parameters such as the length and shape of the powerline inside the LiFi transmitter affect the strength of the RF leakage. Thus, we add an extra loop at the transmitter to have a control over it. Our solution does not affect the LiFi links but helps boost the backscattering performance. We carefully design the parameters of the added loop, which significantly increases the backscattering distance from a few centimeters to 10 m and 18 m in indoor and outdoor environments, respectively, without using a dedicated RF carrier.

Increasing the signal strength of leakage is a critical step to increase the backscattering distance. However, such leaked RF signals with larger amplitude, which are low-frequency RF signals, could cause interference with licensed RF communications in the corresponding frequency band. One potential solution is to make it work in an ISM band. However, as leaked RF signals are not emitted by the LiFi transmitter on purpose, the relationship between the leaked frequencies and LiFi transmitter hardware is hard to control. Besides, it is also unwanted to modify the LiFi devices to make leaked signals fall in the ISM band at the cost of degrading the LiFi performance. Fortunately, we find that the extra conductive loop which we connect to the LiFi transmitter for enlarging the signal strength of leakage also affects the leaked RF frequency. Based on the observation, we carefully design the added conductive loop to shift the frequency of the leaked RF signal to the ISM band to avoid interfering with other licensed transmissions.

Our design of using an extra conductive loop makes LiFi leak RF signals in the 27 MHz ISM band. Detecting the leaked signals would require specialized antennas in the 27 MHz band, which are very costly (around a hundred dollars) and oversized (around one-meter height) for IoT applications. In this work, we design a low-cost small-size coil antenna and carefully tune its frequency and impedance matching to achieve efficient backscattering. Besides, the leaked RF signals to be backscattered in our system are pulse-liked signals, which are different from the continuous RF signals. Thus, the backscatter tag needs to accurately control the timing of reflecting/absorbing of the leaked RF signals; otherwise, even the tag successfully switches impedance for backscattering modulation, there might be no leaked RF signals in that time window to carry the backscattering information.

By addressing the aforementioned challenges, we introduce LeakageScatter, the first system leveraging the LiFi-leaked signals for backscattering. The only modification to the LiFi transmitter is to connect a cheap (less than 10 cents) copper loop to the power line of the LED bulb, which does not influence the original LiFi communication and can be easily implemented on existing LiFi systems. We also carefully design the backscatter tag and receiver to ensure efficient backscattering. By re-purposing the "wasted" leaked signals from LiFi transmitter as the backscatter carrier, LeakageScatter achieves an uplink data rate of 22.2 kb/s and an outdoor backscattering distance of 18 m. Besides, the proposed LeakageScatter can enable bi-directional communication for current LiFi systems. To summarize, our main contributions are as follows.

- We present the first RF backscatter design exploiting the RF leakage from LiFi as the carrier. The widespread deployment of LEDs presents a great potential for the proposed system to be adopted in real-world settings.
- We employ dedicated designs to tune the frequency of the RF leakage in the ISM band to avoid interfering with other RF technologies. The RF leakage power is well below the permitted maximum power in such band, complying with FCC regulations.
- We propose a joint design considering LiFi transmitter, backscatter tag, and backscatter receiver simultaneously. We achieve the backscatter communication with a range suitable for many indoor and outdoor applications by only connecting an additional single loop copper wire at the LiFi transmitter power line. Our approach can be easily implemented on existing LiFi systems. Besides, it does not affect the original LiFi communication.
- We propose to control in software the opportunistic enabling of oscillator at the backscatter tag. This approach can save 75% of the energy consumption in backscattering communication.
- We implement LeakageScatter and evaluate the full system comprehensively in a variety of scenarios, including *indoors, outdoors, multi-tag, and under dimming conditions.*

2 SYSTEM OVERVIEW

The system overview of LeakageScatter is shown in Figure 1. It has three components: *LiFi transmitter*, *backscatter tag*, and *backscatter receiver*. Below we describe each component briefly.

LiFi transmitter. It is equipped with an LED and the necessary circuitry to provide both communication and illumination. It transmits data by modulating the light intensity of the LED bulb. The modulation is performed by turning on/off the LED rapidly. While transmitting data in the LiFi channel, the LiFi transmitter also *leaks RF signals to the surrounding environment*. This is because when the LED bulb is turned on/off to transmit data wirelessly, the current flowing through the LED of the LiFi transmitter also changes rapidly. According to the Maxwell Equations, such a current change further induces electromagnetic signals in the environment, *creating a leaked RF channel* [3]. This is illustrated in Figure 1. In this work, we exploit such a leaked RF channel to achieve backscattering. In Section 3, we will present how to modify the LiFi transmitter to achieve a 18 m backscattering communication distance.

Backscatter tag. The battery-free IoT tags are capable of receiving not only the LiFi signals (i.e., visible light signals) through a small and passive solar cell but also the leaked RF signals through our customized coil antenna. *In the downlink LiFi communication*, the received visible light signals are split into low-frequency and high-frequency components. The tags decode information from high-frequency ones and harvest energy from low-frequency ones, both using a solar cell as receiver and energy harvester, respectively. *In the uplink backscattering communication*, the tag provides wanted information and backscatters it through the received leaked RF signals to the backscatter receiver. The tag is battery-free and totally powered by the energy harvested from the LiFi signals using solar cell. Besides, the proposed backscatter part can be extended to any other tags which aims at utilizing the leaked signals from LiFi system as the carrier signals.

RF backscatter receiver. It has the coil antenna matched with the frequency of the leaked signals to receive the backscattered leaked RF signals. After capturing the signals, the receiver uses an envelope detector to decode the backscattered information.

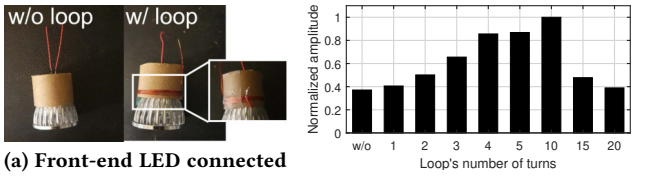
3 TRANSMITTER DESIGN

In this section, we present an effective way to increase the power of LiFi-leaked RF signals without affecting LiFi communication. We also tune the frequency of backscattering communication to an ISM band to avoid interfering with communications in licensed bands.

3.1 Increasing the Leaked RF Signal's Strength

The RF signals we exploit for backscattering are leaked from the LiFi transmitter while it is modulating LEDs for transmitting data. It is a "by-product", and its signal strength is too weak to support backscattering communication. For example, in our measurement, the signal strength of leaked RF signals at the backscatter receiver is only about -100 dBm,[1] and thus, cannot support backscattering communication. To achieve backscattering communication, the first step is to increase the signal strength of the leaked RF signals.

3.1.1 Can we simply increase the length of the power line at the LiFi transmitter? According to the physical model of the LiFi-leaked RF signals [3], the leaked signals are created by the current change in the power line of the LiFi transmitter, which connects the LiFi bulb to the power supply. The longer the power line, the larger



(a) Front-end LED connected without loops and with loops at transmitter side

(b) Measured amplitude of the LiFi leaked signals

Figure 2: Validation experiment for using the loop connected with LED to increase the LiFi leaked signal's amplitude.

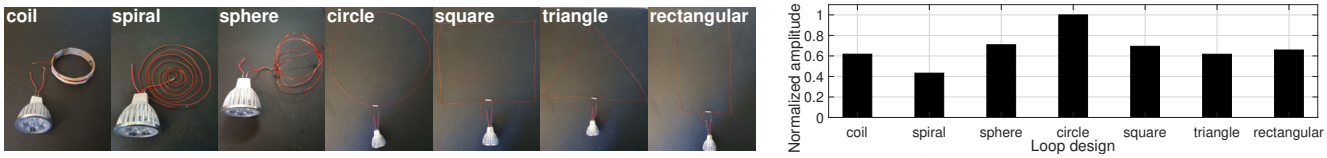
the amplitude of the leaked RF signals. To obtain stronger leaked RF signals, one solution is to manually increase the length of the power line at the LiFi transmitter by connecting a wire loop to the front-end LED. To test this solution, we wind a 22 AWG copper wire around 4cm-diameter cardboard, as shown in Figure 2a. We vary the number of turns from 1 to 20 to have different power line lengths. To detect the leaked RF signals, we use a 15-turn 1cm-diameter coil which has a flat frequency response. The experimental results are shown in Figure 2b. We can observe that by connecting the extra loop with the front-end LED could increase the leaked RF signals' amplitude. Besides, more turns of the loop will result in larger signal strength within five-turn loops. However, when the number of turns goes above 10, the signal strength starts to drop. This means that it is not always true that a more number of turns of the loop will provide a larger leaked RF signal.

The reason behind this is that when the number of turns in the loop increases, it will introduce more inductance into the transmitter circuit. More circuit inductance will slow the current change in the transmitter circuit, leading to smaller amplitudes of the leaked RF signals. Furthermore, such a large extra inductance will unavoidably affect the original LiFi performance, which is unacceptable.

3.1.2 Loop design in LeakageScatter. The above analysis raises the question in the loop design for LeakageScatter: how to design a loop with longer copper wire length (to increase the amplitude of the leaked RF signals) but with smaller inductance (to alleviate the influence on both leaked RF signals and LiFi signals)? The key is to study the effectiveness of different loop shape designs, which affects the loop's inductance. Note that we cannot simply borrow the coil design from the previous work [5], which is aimed at the receiver side. Different from the receiver coil design, designing the additional loop at the transmitter needs to balance the performance of both LiFi channel and leaked RF channel. What is more important is that we cannot modify other LiFi transmitter circuit designs and components but only add a loop coil to achieve this goal. We use seven copper wires with the same length and thickness to build seven loops with different two-dimensional and three-dimensional shapes, i.e., coil, sphere, spiral, circle, square, triangle, and rectangular. They are shown in Figure 3a. The 15-turn 1cm-diameter coil is still used to receive the leaked RF signals sent out from these LEDs with different loop designs. The results are shown in Figure 3b. We can see that the circle has the best performance among the seven loop designs with the same wire length.

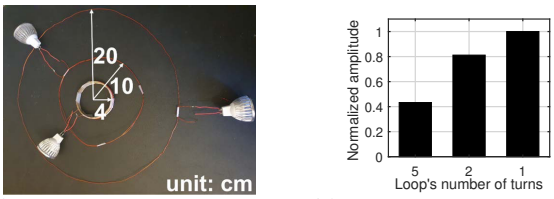
The underlying reason why the circle has the best performance compared to other loop designs is the *proximity effect* [30]. This effect mainly occurs when the copper wire is carrying high-frequency signals (the frequency of leaked RF signal is around tens of MHz).

[1]The measurement is done when the backscatter receiver co-locates with the backscatter tag, both placed one meter away from the LiFi transmitter.



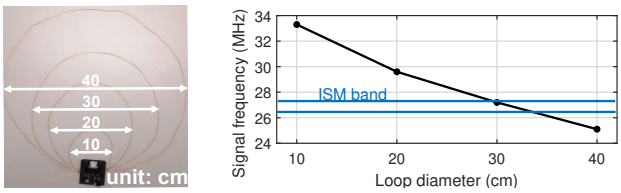
(a) Different loop designs (b) Leaked signals' amplitude

Figure 3: Validation experiment for the loop design's influence on the leaked RF signal.



(a) Different turns of the loops (b) Leaked signal's amplitude

Figure 4: Impact of the number of turns on leaked RF signal.



(a) Different loop sizes (b) Leaked signal's frequency

Figure 5: Tuning the frequency of the leaked RF signal.

When the alternating current flows through one or more other nearby conductors, the distribution of current within each conductor will be constrained to smaller regions, resulting in larger inductance. The larger inductance will not only slow down the current change but also result in smaller current flows through the powerline, which finally leads to smaller leaked RF signals. Since the circle design has the largest inter-distance among the copper wire compared with other loop designs, the circle loop has the largest leaked RF amplitude.

To further validate the proximity effect, we conduct an experiment with coils having a different number of turns. But, they are made of four same-length copper wires as shown in Figure 4a. The inductance of a coil is calculated as [21]:

$$L_{\text{coil}} = \mu_r \mu_0 N^2 \pi r^2 / l, \tag{1}$$

where L_{coil} denotes the inductance of the coil, μ_r is the relative permeability of the core material, μ_0 is the permeability of free space, N is the number of turns, r is the coil radius, and l is the coil length. The same total wire length should result in the same inductance value according to Equation (1). When the total lengths, i.e., $N \times 2\pi r$ for all these coils, are the same, the term $N^2 r^2$ in Equation (1) also gets the same values for these coils. The same inductance value of these three coils should mean that they will provide the same power gain for leaked RF signals. However, the results shown in Figure 4b present us that the one-turn circle has the best performance. The less number of turns gets better performance due to the proximity effect.

3.2 Tuning the Frequency to the ISM Band

In our work [4, 5], we showed that the pulse-liked leaked RF signals do not cause interference on other RF channels. In LeakageScatter, with extra conductive loop as designed in Section 3.1, the LiFi transmitter leaks larger RF signals for better backscattering. Such leaked RF signals could interfere with licensed RF communications in the corresponding frequency band and can not be ignored.

To address the RF interference issue, we propose to operate the LiFi leaked RF backscattering in the low-frequency ISM band available worldwide and centered at 27.12 MHz. The frequency of leaked RF signals mainly depends on the transmitting hardware circuit [3]. However, it is difficult to model the relationship between the hardware design (including LEDs, hardware components, and hardware circuit) and the frequency of leaked RF signals. Generally, the LiFi transmitter consisting of circuit components with faster response time leaks RF signals with higher frequency than modulation frequency. We use and customize the OpenVLC1.3 LiFi transmitter [9] according to the experiments discussed in the evaluation section. Thus, we need a precise method to shift the frequency of leaked RF signals to the nearest ISM band centered at 27.12 MHz.

Fortunately, we find that the extra loop which is designed for enlarging the leaked RF signals could also influence the frequency of the leaked RF signals. The reason lies in the fact that the extra conductive loop connecting to the transmitter circuit will bring more inductance into it and the extra inductance in the circuit will make the frequency of the leaked RF signals lower according to the LC circuit equation. The inductor in parallel to the capacitor is called a tank circuit. The resonant frequency f of the tank circuit with inductance L and capacitance C is given by following equation:

$$f = 1/(2\pi\sqrt{LC}), \tag{2}$$

where f is the resonant frequency of the tank circuit, which is also the frequency of the leaked RF signals.

Preliminary evaluation. To validate this approach, as shown in Figure 5a, we conduct the experiment by using four same LEDs connected with loops of different sizes, i.e., the loops' diameters are 10, 20, 30 and 40 cm, to evaluate the frequency of the leaked RF signals. We use a 15-turn 1 cm diameter coil, which has flat frequency response, to receive the leaked RF signals. The corresponding frequency results are shown in Figure 5b. The leaked RF frequency decreases with the increase in diameter due to the inductance introduced by the circular loop that we design, where a larger diameter will introduce a larger inductance value. The experiment validates that our approach can give us precise control over leaked RF frequency selection and make it operate in the ISM band by simply using a proper diameter of the circle at LiFi transmitter, assisted by a variable inductor for dynamic configuration of the frequency of the leaked RF signal. The solution is also compatible with commercial LEDs and can be easily deployed on them.

LeakageScatter may interfere with co-located systems operating in the same ISM band. Fortunately, the leaked signals are pulsed-based in the time domain, making it barely influence others [4]. In a multi-tag network, each tag will be allocated with a different

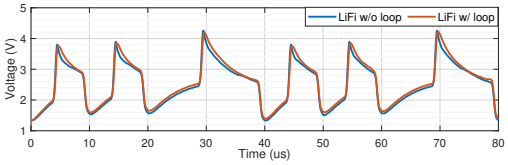


Figure 6: Validation of loop's influence on LiFi signals.

oscillator frequency, as shown later in Section 6.5, then operating at different frequencies and avoiding the inter-tag interference.

3.3 Impact on the LiFi Channel

According to the above preliminary experiments, we conclude that the one-turn circle as the extra loop connected to the LiFi transmitter can produce the best performance for the LiFi leaked RF signals. However, besides enlarging the leaked RF signals, we also need to make sure that such an extra conductive loop at the transmitter will not influence much the original LiFi channel. To evaluate it, we use OpenVLC1.3 [9] as the visible light receiver and connect it to the oscilloscope to sample the light signals at a sampling rate of 100 MHz. Two identical commercial LEDs are utilized at the transmitter to send light signals, where the only difference is that one LED is without any extra loop and the other one is connected with a 30 cm diameter circle loop. The modulation scheme we use is On-Off-Keying (OOK).

The received visible light signals are presented in Figure 6. We can observe that the extra loop has a negligible impact on the maximum amplitude of the received visible light signals. It slightly slows the changing of the amplitude. Such influence on the LiFi channel is expected because the extra loop adds more inductance to the transmitting circuit and slows the current change in the power line, resulting in slower amplitude change of the visible light signals. Overall, it is validated that connecting an extra conductive loop to the current LiFi transmitter does not influence much the performance of the original LiFi channel. This conclusion also applies to other modulation schemes commonly used in LiFi, such as Pulse Position Modulation (PPM), Variable Pulse Position Modulation (VPPM), and Color-Shift-Keying (CSK) [13].

4 TAG DESIGN

4.1 Hardware Design

The block diagram of our designed tag is shown in Figure 7. The tag hardware consists of two parts: 1) a solar cell array for LiFi signal reception and energy harvesting; 2) a coil antenna for backscattering the leaked RF signals. The first part is built upon a state-of-the-art work [19][2]; in LeakageScatter, we mainly focus on the second part: backscattering design. Note that the solar cell array is not necessary for our tag to conduct the proposed backscattering communication. Our backscattering design can be extended to any other tags which aim to utilize the leaked signals from LiFi for backscattering.

To enable backscattering communication with RF signals leaked from the LiFi transmitter, the antenna design for the tag is an important step. Specialized coil antennas for 27-30 MHz are very

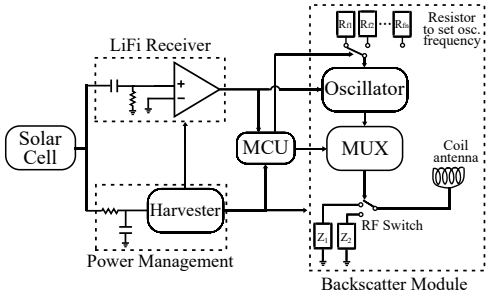


Figure 7: Block diagram of LeakageScatter battery-free tag.

costly (around a hundred dollars) and oversized (around one meter height) for IoT applications. A custom antenna design is the proposed solution to this problem. A coil antenna, as used in the state-of-the-art work [3, 5] for detecting LiFi-leaked RF signals, could be leveraged for the backscattering in LeakageScatter. However, they are not optimized for backscattering because 1) they are not tuned at the desired frequency, which leads to important receiver losses; 2) they are not matched with the input impedance of the circuitry, which is key to maximize the backscatter signal power. Besides, traditional antennas detect the *electric field*, which creates a voltage difference at its edges. Instead, coil antennas are based on the principle that the detected *magnetic field* generates a current in the receiver circuitry, and we aim to use them for backscattering.

According to electromagnetic theory, in the near field, the ratio of the electric and magnetic fields is not constant. Instead, this ratio will be constant in the far field [27]. In particular, larger currents at the transmitter result in larger magnetic fields than electric fields (reduced impedance) in the near field of the LiFi transmitter.[3] As described in Section 3.1, the selected choice at the LiFi transmitter results in largest current, and the magnetic fields around the LiFi transmitter is larger and better to be received. Therefore, a coil antenna at the tag (also at the backscatter receiver) is desired, as it would allow having the best performance in the near field, without affecting the sensitivity in the far field.

Besides the coil antenna, the backscattering part of our designed tag also includes an oscillator, an RF switch, and a multiplexer. For the coil antenna, a coil with 4 cm diameter is made with 20 AWG laminated copper wire with N=15, without core and a coil length l = 4.8 cm. The oscillator controls the speed to which the RF switch must change between the impedances Z_1 and Z_2 (cf. Figure 7), to modulate the reflection coefficient of the tag's antenna when transmitting bit '1' (*reflection state*). This produces a backscatter signal at a frequency of the RF leaked signal plus the oscillator frequency. Differently, when transmitting bit '0' all power of the RF leaked signal is absorbed in the tag's antenna thanks to maintaining the RF switch in the matched load Z_2 (*absorption state*). Bits are transmitted by the MCU and multiplexed with an oscillator signal to control the RF switch. Deriving the values of Z_1 and Z_2 is based on the principle of maximizing the difference in their reflection coefficients [28]; the details are omitted due to space limit.

In LeakageScatter, when transmitting a bit '1' (*reflection state*), we change between impedances Z_1 and Z_2 at the oscillator frequency, leading to a reflection coefficient of 3.7 dB when the system is

[2]The incoming LiFi signals are AC signals. In [19], these signals are filtered by a high-pass filter and demodulated by a low-power comparator and MCU for downlink LiFi. The remaining signals are filtered with a low-pass filter for energy harvesting. A harvester chip in the tag manages the filtered energy and stores it in a super-capacitor, which powers all the circuitry components of the tag with a voltage regulator.

[3]The leaked signal's frequency is 27 MHz with wavelength of 11.1 m, so communication happening within 11.1 m from LiFi transmitter is all considered near field.

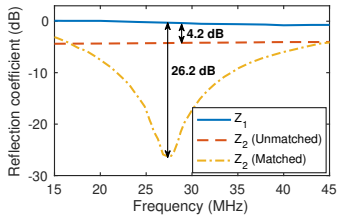


Figure 8: Reflection coefficient of backscatter module.

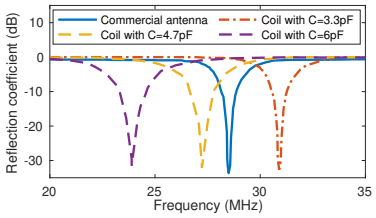


Figure 9: Reflection coefficient for commercial antenna and coil antennas.

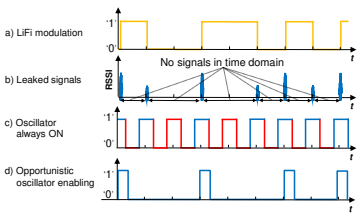


Figure 10: The occurrences of leaked pulses affect backscatter modulation.

unmatched, and 25.7 dB when the system is matched, as shown in Figure 8. This enhances the backscattering of the leaked RF signal by around 160× when employing a matched system.

4.2 Frequency Tuning to the 27 MHz ISM band

As we aim to make our system work in the ISM band and have already tuned the frequency of leaked signals to it, we also need to tune the frequency of tag to the ISM band. In the coil antenna design, the inductance L_{coil} is provided by the coil according to Equation (1). Frequency is tuned with a small capacitance according to Eq. (2) and the real part of the impedance is set to nearly 50 Ω by a series resistor.

Besides, the oscillator frequency determines the frequency shift in the uplink backscatter signal with respect to the *carrier* (RF leaked signal). Note that, to avoid interfering with neighbouring wireless services, the maximum frequency shift must be such that the backscatter signal is within the 26.957–27.283 MHz ISM band. If the RF leaked signal is at the center frequency of the ISM band (27.12 MHz), a maximum oscillator frequency of 163 kHz is allowed.

4.3 Protocol Design

In the above two subsections, we have solved the problem of *"how to backscatter the leaked RF signals"* with carefully designed hardware for reflecting/absorbing the leaked RF signals. Another challenge we must tackle is *"when and how often to reflect/absorb the leaked RF signals"*. This is essential to guarantee extremely low-power consumption at the tag.

The leaked RF signals backscattered in LeakageScatter are *pulse-liked* signals as illustrated in Figure 10, which are different from the continuous RF signals transmitted in other backscattering systems, such as RFID and NFC. In other words, the leaked RF signals are *sparse in time domain* and only exist in the particular time windows, as shown in Figure 10b. Thus, we must accurately control the timing of reflecting/absorbing at the tag. Otherwise, even if the tag switches impedance for backscattering, there might be no leaked RF signals at that time window to carry the backscattering data, as shown in Figure 10c, where the impedance switching process highlighted in red color is invalid.

To only enable the backscattering on the presence of the leaked RF signals, we exploit the coupling of LiFi signals and its leaked RF signals, which means the leaked RF signal only occurs when LiFi signal transits from "ON" to "OFF", or from "OFF" to "ON". The reason lies in the fact that LiFi signal's transition means the current in the power line of the transmitter circuit changes, which generates the leaked RF signal as detailed in Section 3.1. As our tag receives LiFi signals in downlink by using a solar cell, it perfectly knows when there are LiFi transitions, and accordingly, the leaked RF signals. This is different from traditional RF backscatter systems where the tag relies on unstable/unreliable RF triggers [10].

Another problem is that the leaked RF signals only appear for an extremely short time following the LiFi transition at the transmitter. Thus, for successfully backscattering the leaked signals, we need to enable the oscillator in backscatter module for that short time window with fastest response time. To achieve this goal, the proposed backscatter module utilizes a comparator and directly connects it with the oscillator as shown in Figure 7. The comparator is used to monitor the LiFi transition received by the solar cell. Once noticing a LiFi transition, it bypasses the MCU and directly enables the oscillator such that the corresponding leaked RF signal is backscattered. Such a design not only minimizes the time between detecting the LiFi transition and enabling backscatter, but also reduces energy cost in the MCU. Besides, as the oscillator is the most power-hungry component for backscattering, with our approach, we save up to 75% of the oscillator's power consumption (7.5 μW vs. 30 μW in our measurements) comparing with the traditional approach where the oscillator is always enabled.

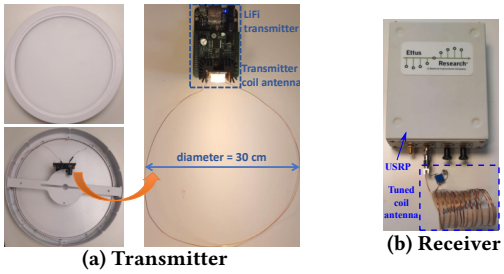
Another question is *"how can we guarantee the existence of the leaked signals during each LiFi downlink transmission?"* Fortunately, we find that there always exists at least one leaked RF signal pulse in a fixed time window, no matter what data the LiFi transmitter is sending. This is due to the coding schemes adopted in most LiFi systems, which breaks continuous '0' or '1' data chunks to avoid flickering [13]. Thus, such coding schemes require current change must happen in a fixed time window, which guarantees the existence of leaked signals. For example, if the LiFi transmitter adopts Manchester coding, where data bit '1' is coded by "OFF-ON" and data bit '0' by "ON-OFF", then the time window where there is at least one leaked RF signal pulse is two LiFi modulation cycles.

4.4 Networking Multiple Tags

In a network with multiple tags, each tag is allocated with a different oscillator frequency that can be changed on the fly by the MCU upon orders received through the downlink LiFi channel. This is done by a switch connected to multiple loads, each of them modifying the oscillator frequency as represented in Figure 7. Multi-tag scheduling is done in a Frequency Division Multiple Access (FDMA) fashion, where each tag transmits data through the uplink at different frequency shifts with respect to the carrier wave coming from the leaked RF signal.

5 IMPLEMENTATION

LiFi transmitter. We use a switching regulator based LiFi transmitter, same as in PassiveLiFi [19]. To strengthen the leaked RF signals and to operate in the 27 MHz ISM band, we include an additional



(a) Transmitter (b) Receiver

Figure 11: Hardware of LiFi bulb and RF backscatter receiver with corresponding designed antennas.

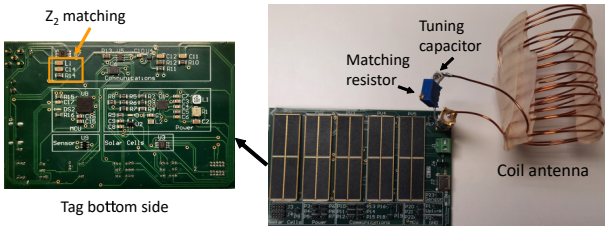


Figure 12: Backscatter tag including tag circuit, impedance matching network and coil antenna.

wire to the power line of the front-end LED with the design parameters decided in Section 3 and Section 4: a 30 cm diameter circular wire loop, which only costs around 10 cents. The loop is twined into a circular LED cover (whose diameter is also 30 cm) commonly seen in our daily life, as shown in Figure 11a. For the modulation of the LiFi signals, we use OOK with Manchester Coding, and we adopt BeagleBone Black as the embedded processor for modulating the LED, same as in OpenVLC [9].

Tag. We use a battery-free IoT tag as in [19] for LiFi reception while modifying the RF backscatter module. The matching circuit in absorption state of backscatter communication and homemade antenna design on tag enables the uplink with LiFi-leaked RF signals. We show our tag hardware in Figure 12. The size of the tag is 9.4 cm× 5.9 cm, and it is limited by the 5 solar cells connected in parallel to collect as much light energy as possible. More tag details can be found in Section 4.

Receiver design. The implemented backscatter receiver is shown in Figure 11b. We implement the receiver using a software-defined radio device. We use USRP B210 and program an envelope detector in GNU Radio at the backscatter frequency. Note that an RF envelope detector can also be implemented with COTS electronics, then reducing the receiver size and increasing the sensitivity. The antenna has been designed to be tuned at the 26.957 MHz - 27.283 MHz ISM band, to match with the frequency of the backscattered RF signal. It is a coil antenna with 15 turns and 4 cm of diameter (similar to the one in the tag), whose band has been tuned by using a capacitor and a resistor to the backscattered frequency (carrier plus the frequency shift included by oscillator in the tag). We downsample the received signal from the carrier plus shift frequency to the baseband. Then, we compute the square Root of the Mean Square (RMS) of received samples, and finally, by using a threshold we decode the bits transmitted by the tag.

6 PERFORMANCE EVALUATION

We evaluate the performance of LeakageScatter under different scenarios. The metrics we use are Received Signal Strength Indicator (RSSI), Bit Error Rate (BER), backscattering distance (tag–receiver distance), and system data rate. We use spectrum analyzer FPC1000 to analyze RSSI values and software defined radio USRP B210 with GNU radio software for processing backscatter signals.

6.1 Preliminary Evaluation

We first measure the power of the leaked RF signal at the LiFi transmitter and the power consumption of the tag. In our measurements, with the additional loop at the transmitter, the power of the LiFi-leaked RF signal is below 0 dBm. Concretely, placing receiver and

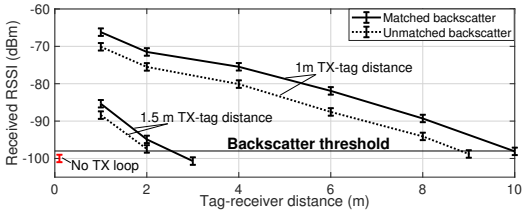


Figure 13: Backscattering distance in indoor scenarios.

transmitter very close (sub-centimeter) we receive an RF leaked power of -18 dBm. This is much lower than the maximum radiated power permitted in the ISM band 26.957-27.282 MHz which is 10 dBm [14]. The front-end of the battery-free tag, including an oscillator, multiplexer, and RF switch, consumes 35 μW of power. With OpenVLC as a transmitter, receiving 500 lux of illuminance (measured with Extech SDL400 lux meter) we harvest 244.79 μW, which is much larger than the power consumed by tag for uplink transmission, then being self-sustainable.

Maximal backscattering distance. We then evaluate backscattering range of LeakageScatter in indoor Line of Sight (LoS) scenarios. The experiments are performed indoor in the office. The LiFi transmitter, with 1 MHz ON/OFF modulation rate, is placed at a fixed position. The backscatter tag is placed at 1 m from the LiFi transmitter. We evaluate the performance when we have both matched and unmatched absorption impedance in backscatter, as explained in Section 4.1. The evaluation results are shown in Figure 13. First, we observe that without our designed loop at the LiFi transmitter, the backscattered signal is very weak (about -100 dBm in 10 cm tag-receiver distance). On the contrary, with our circular loop connected to the LED front-end of the LiFi transmitter, the leaked signal strength is significantly increased and the maximal backscattering distance can reach up to about nine meters, even under the unmatched absorption impedance in backscatter. Furthermore, when there is matching in the backscatter absorption impedance, we observe 5 dB improvement in the received signal strength and the backscattering distance is further extended to ten meters. We also evaluate the scenario when the tag is placed a bit further, i.e., at 1.5 m from the LiFi transmitter. The result is also shown in Figure 13. Still, we achieve a backscatter distance of about 2.5 m under the matched absorption impedance for the tag. Note that these results can be further improved with dedicated circuitry in this band as a receiver, which will minimize the noise floor. Besides, 1.5 m is a common distance from the ceiling to objects in the room, including tags which need backscatter communication. Thus we believe LeakageScatter can work well in practical scenarios.

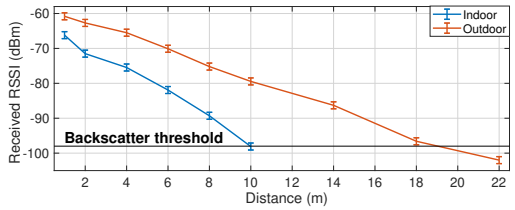
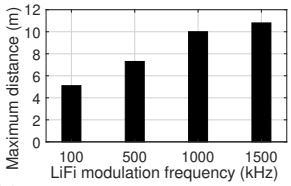
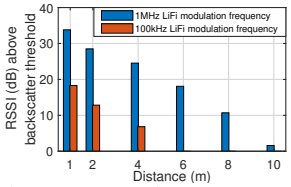


Figure 14: Backscattering distance in outdoor scenario.



(a) Backscattering distance vs. LiFi modulation frequency



(b) Relative RSSI (above decoding threshold) vs. distance

Figure 15: Backscatter performance under different LiFi modulation frequencies.

Outdoor backscattering. We have also evaluated the performance of our LeakageScatter in an outdoor LoS scenario, since LiFi may be deployed in outdoor Vehicle to Vehicle network [22] and greenhouse sensor network [15]. The distance between the LiFi transmitter and the backscatter tag is set to one meter. We move the backscatter receiver to measure the supported maximal backscattering distance. The result is given in Figure 14. We can observe that at the same distance, the RSSI in outdoor scenario is much higher than that in indoor scenarios. The difference between them also increases with the distance between the backscatter tag and receiver. At the distance of 10 m, the RSSI in the outdoor scenario is about -80 dBm, which is still much higher than the required RSSI (about -98 dBm) to decode the backscatter signal; while at the same distance, the indoor backscattering nearly has reached the upper-bound communication distance. In summary, LeakageScatter can achieve a maximal backscattering distance of 18 m outdoors, which almost doubles the achieved maximal distance in indoor scenarios.

Impact of LED's ON/OFF rate. We continue to evaluate the impact of the LED's ON/OFF rate, i.e., used modulation frequency at the LiFi transmitter, on the backscattering performance. We vary the modulation frequency from 100 kHz to 1.5 MHz (that is the 3-dB bandwidth of the LED) and plot the corresponding maximal backscattering distance in Figure 15a. We can observe that lower LiFi modulation frequencies result in shorter backscattering distances. To be more specific, we also measure the RSSI of the backscattered signals with different distances under 1 MHz and 100 kHz LiFi modulation frequency as shown in Figure 15b. The reason lies in the fact that lower LiFi modulation frequency means less ON/OFF changes happening in a fixed time window and less RF energy will be leaked from the LiFi transmitter. Thus, smaller average strength of the leaked RF signals limits the backscattering range. However, when the LiFi modulation frequency is higher than 1.5 MHz, the power of the leaked RF signal degrades. Because the modulation frequency has exceeded the 3-dB bandwidth of the low-cost LED we use, which causes the capacitance effect. Such an effect will slower the current change in the circuit and result in smaller leaked signals.

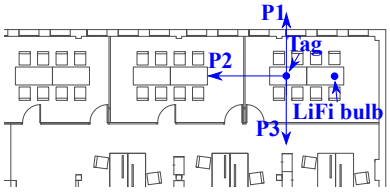


Figure 16: Map of the place for the non-LoS experiment.

Table 1: Backscattering through different walls.

Index	Wall type	Wall thickness	Distance
P1, outdoor	Concrete	25 cm	4.0 m
P2, indoor	Wooden	8 cm	5.0 m
P3, indoor	Plastic/Glass	3 cm	5.4 m

Table 2: Evaluation of LeakageScatter in dimming conditions.

Duty cycle	Illuminance at 1m	V_H across LED	P_{av} at TX	RSSI at 1m
50%	577 lux	10.75 V	1.92 W	-68 dBm
10%	314 lux	10.75 V	1.09 W	-68 dBm
1%	12 lux	10.75 V	0.21 W	-68 dBm

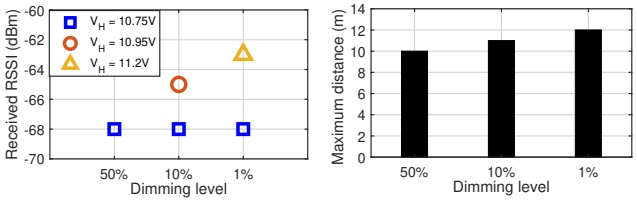
6.2 Backscattering Through the Wall

The backscattering performance of LeakageScatter is further evaluated in Non-LoS (NLoS) scenarios by placing the LiFi transmitter and the tag in the same room at a distance of 1 m, and by moving the backscatter receiver through three different directions as highlighted by labels P1, P2, and P3 in Figure 16. Our aim is to evaluate the maximum achieved distance when different types of walls are placed between the tag and the receiver. The results are summarized in Table 1. We can observe that in LeakageScatter the tag can communicate with the receiver through backscattered signals at a maximum distance of 4 m, 5 m, and 5.4 m, when concrete, wooden, and plastic/glass walls, respectively, are placed in between the tag and the receiver. The results demonstrate that LeakageScatter can leverage the LiFi-leaked RF signal to perform backscattering at meaningful distances even through the walls, breaking the limitation of light-based LiFi backscattering systems that only work in LoS scenarios[11].

6.3 Backscattering During the Day

Artificial illumination changes over 24 hours. For this reason, we evaluate the backscattering performance of LeakageScatter under different dimming conditions by operating the LED of the LiFi transmitter at 50%, 10% and 1% duty cycle. The results are presented in Table 2, where V_H is the voltage across the LED when it is ON and P_{av} is the average power consumption of the LiFi transmitter. V_H is independent of the LED's duty cycle and is set to 10.75 V. The RSSI of the backscatter signal is measured at a 1 m distance from the tag. We can see that the illuminance reduces with a decrease in the duty cycle. The amplitude of leaked RF signals depends on the ON/OFF transition speed at the LiFi transmitter [3]. Therefore, we get the same RSSI of -68 dBm independent of the LED's duty cycle with the same value of V_H. This demonstrates that our LeakageScatter can work throughout the whole day, even when the LED is turned *'off'* (not completely off, but the duty cycle is very low so for human's eyes the LED is 'off') to save energy during daytime or at midnight.

On the other hand, when the LED dims with lower duty cycles, we can increase the forward voltage V_H without heating up the LED. With a 10% duty cycle, the forward voltage can be increased



(a) RSSI of backscatter signal at a 1 m distance from the tag at different dimming levels

(b) Improvement in backscattering distance with reduced dimming levels

Figure 17: The backscattering performance improves when LED operates at higher V_H in lower duty cycles.

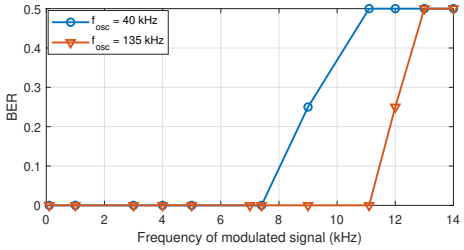


Figure 18: Uplink rate versus BER. Our system shows a throughput of up to 22.2 kb/s (11.1 kHz) with LiFi leaked RF signals as a carrier for RF backscatter.

from 10.75 V to 10.95 V; with a 1% duty cycle, the forward voltage can be increased to 11.20 V. By doing this, we can enhance the strength of the leaked RF signals by 3 dB and 5 dB, respectively, as shown in Figure 17a, allowing us to reach a longer backscattering distance (can reach 11 m and 12 m, respectively; see Figure 17b). The improvement comes from the fact that the transition speed of the transmitter increases by maintaining the same frequency (1 MHz) but operating the LED at higher V_H. The increase in consumption when operating at higher V_H is catered by reducing the duty cycle and hence the LiFi transmitter consumption is still reduced to the order of milli-Watts (mW).

6.4 Backscattering Data Rate

Our system is evaluated by placing the LiFi transmitter and backscatter receiver at a distance of 1 m and placing the tag in the middle. The uplink data rate is varied and the corresponding BER is noted with on-tag oscillator frequency set at 40 kHz and 135 kHz. The results are presented in Figure 18. Our system can achieve a transmission frequency of 7.4 kHz corresponding to 14.8 kb/s with a 40 kHz oscillator in the tag (representing the frequency shift for backscatter) and 11.1 kHz corresponding to 22.2 kb/s with a 135 kHz oscillator using OOK modulation. By using the higher frequency oscillator, the number of switching cycles per time unit between Z_1 and Z_2 in RF switch increases when transmitting bit '1', which results in a more robust uplink backscatter signal and, as a consequence, in a larger achieved throughput.

6.5 Multi-tag Backscattering

Finally, we evaluate the performance of LeakageScatter in multi-tag scenarios. We carry out experiments with two different tags, Tag 1 and Tag 2, with oscillator frequencies of 60 kHz and 90 kHz, respectively. We consider two scenarios as shown in Figure 19a: (1) a *homogeneous* scenario where Tag 1 and Tag 2 are located symmetrically to the LiFi transmitter and RF backscatter receiver; and (2) a *heterogeneous* scenario where Tag 1 and Tag 2 are located asymmetrically to the LiFi transmitter, and the receiver is moved off-center with respect to the tags. Experiments are done in an indoor environment and both tags are transmitting simultaneously.

The results for these two scenarios are shown in Figure 19b and Figure 19c, respectively. We observe that in both scenarios, the maximum achieved distance is about 9 m, which is only slightly shorter than the one obtained in the single-tag scenario as presented in Section 6.1. The RSSI values also demonstrate that decoding simultaneous multiple backscattering transmissions in LeakageScatter is possible. In the heterogeneous scenario, Tag 1 is closer to the LiFi transmitter and thus it backscatters a signal with larger power than Tag 2. From Figure 19c we know that the position with respect to the receiver is also important. That is, the more aligned the transmitter-tag-receiver are, the better the signal is received.

7 DISCUSSIONS

Potential applications. LeakageScatter can be employed in *Smart homes*, *Industry 4.0*, and *precision farming* to achieve energy-efficient bi-directional communications. In these scenarios, multiple sensors are deployed to monitor the target status, i.e., equipment and crops, and environmental parameters. In these scenarios, LeakageScatter can not only provide downlink LiFi communication but also enable uplink backscattering communication with leaked signals.

Larger transmitter-tag distance. The current system works at a 1.5 m transmitter-tag distance, which can already cover some indoor scenarios where the LiFi transmitters are placed in the ceiling and the tags are deployed on walls, cabinets, etc. One potential solution to further increase the distance is to attach the tags to surrounding objects, such as electric appliances and even the human body. These conductive objects can increase the received signals [6].

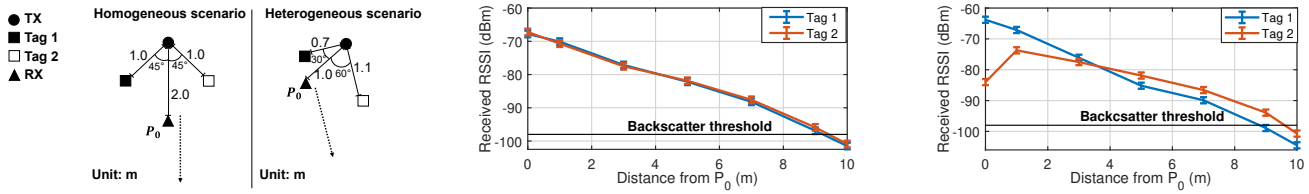
Other LiFi systems. The proposed LiFi-leaked signals backscattering can also work for LiFi systems that use various modulation schemes. This is because the leaked signals are unavoidably created by the current change at the transmitter, no matter what modulation scheme the LiFi transmitter adopts.

Higher data rate. The current backscattering data rate of LeakageScatter is limited by the narrow ISM band. We observe that the higher oscillating frequency in the tag can achieve a higher data rate from the experiments, but it could not be too high to shift the backscatter signals' frequency out of the ISM band. Without the limitation of the ISM band, LeakageScatter could easily achieve a higher data rate.

LiFi sniffing attack. Adding an extra loop to the LiFi transmitter makes the leaked signals large enough for backscattering, but also increases LiFi's risk of being sniffed through these leaked signals [3]. Potential solutions to combat sniffing attack from the LiFi-leaked RF signal are to manually decrease some leaked pulses' amplitudes by connecting an extra resistor into the transmitter circuit to corrupt the information copy carried in the leaked channel [5].

8 RELATED WORK

RF backscatter communication. With the aim of building zero-power communication systems, researchers have recently invested much effort in RF backscatter systems, some of them being compliant with standards such as WiFi [32], BLE [8] or LoRa [12]. Recent



(a) Setup for the multi-tag scenarios (b) Received RSSI in the *homogeneous* scenario (c) Received RSSI in the *heterogeneous* scenario

Figure 19: Performance evaluation of LeakageScatter in multi-tag homogeneous and heterogeneous scenarios.

work also exploits the magnetic resonance effect to increase the backscattering range of NFC [34], and another backscatters through the power line by modulating its parasitic impedance [31]. Recently, researchers have suggested the generation of carrier wave signals by using low-power tunnel diodes installed in the tag [20, 26]. Our work leverages the pervasive deployment of LEDs with LiFi capabilities and its leaked RF signals to be backscattered in uplink.

Leaked RF signals from LiFi. The LiFi leaked signals have been first found and modeled in [3]. Then, it is exploited to conduct physical level sniffing attack [3], to increase the LiFi system's robustness to the environment interference [4], and to increase the data rate [5]. The authors of these works exploit these leaked signals for downlink communication. Besides, researchers also consider such leaked RF signals as energy leakage and harvest them for powering [6]. In LeakageScatter, it is the first time to successfully achieve uplink backscattering using these leaked RF signals.

Hybrid light-RF networks. There are research works that combine VLC with RF communications [19, 24] to improve the performance of VLC, regarding the network throughput and coverage. For these systems, the transmitter needs more than one front-end circuit and separated signal sources. Even in LiFi-based (downlink) battery-free tags that employ RF backscatter as a power-efficient uplink technique, a second device is required for generating the RF carrier wave signal [10, 19]. Our LeakageScatter leverages the already existing leaked RF signals from LiFi for backscattering.

9 CONCLUSION

We have presented LeakageScatter that exploits the leaked RF signals in LiFi to enable battery-free RF backscatter systems without the need of dedicated and power-hungry carrier generators. We have optimized the designs to maximize both the RF-leaked and backscattered signals strength without affecting the LiFi channel, and to emit in ISM band, then not interfering with licensed communications. We have evaluated LeakageScatter in a number of scenarios and it shows promising results, achieving a maximum distance of 18 m and 10 m in outdoor and indoor scenarios, respectively. We envision LeakageScatter will open the door to build efficient RF backscatter systems without dedicated RF carrier generators.

Acknowledgements - This work has been partially funded by the project RISC-6G, reference TSI-063000-2021-59, granted by the Ministry of Economic Affairs and Digital Transformation and the European Union NextGenerationEU through the UNICO-5G R&D Program of the Spanish Recovery, Transformation and Resilience Plan.

REFERENCES

[1] 2022. What is the Internet of Things? What IoT means and how it works. https://www.insiderintelligence.com/insights/internet-of-things-definition/.
[2] Dinesh Bharadia, Kiran R. Joshi, Manikanta Kotaru, and Sachin Katti. 2015. BackFi: High Throughput WiFi Backscatter. *SIGCOMM Comput. Commun. Rev.* (2015).
[3] Minhao Cui, Yuda Feng, Qing Wang, and Jie Xiong. 2020. Sniffing visible light communication through walls. In *MobiCom*.
[4] Minhao Cui, Qing Wang, and Jie Xiong. 2020. Breaking the limitations of visible light communication through its side channel. In *SenSys*.
[5] Minhao Cui, Qing Wang, and Jie Xiong. 2021. RadioInLight: doubling the data rate of VLC systems. In *MobiCom*.
[6] Minhao Cui, Qing Wang, and Jie Xiong. 2022. Bracelet+: Harvesting the leaked RF energy in VLC with wearable bracelet antenna. In *SenSys*.
[7] Jasper de Winkel, Vito Kortbeek, Josiah Hester, and Przemysław Pawełczak. 2020. Battery-Free Game Boy. *In IMWUT* (2020).
[8] Joshua F Ensworth and et al. 2015. Every smart phone is a backscatter reader: Modulated backscatter compatibility with BLE devices. In *RFID*.
[9] Ander Galisteo, Diego Juara, and Domenico Giustiniano. 2019. Research in visible light communication systems with OpenVLC1.3. In *In Proceedings of IEEE WF-IoT*.
[10] Ander Galisteo, Ambuj Varshney, and Domenico Giustiniano. 2020. Two to Tango: Hybrid Light and Backscatter Networks for next Billion Devices. In *MobiSys*.
[11] Seyed Keyarash Ghiasi, Marco A. Zúñiga Zamalloa, and Koen Langendoen. 2021. A Principled Design for Passive Light Communication. In *MobiCom*.
[12] Xiuzhen Guo and et al. 2022. Saiyan: Design and Implementation of a Low-power Demodulator for LoRa Backscatter Systems. In *NSDI*.
[13] IEEE. 2018. IEEE Standard for Local and metropolitan area networks–Part 15.7: Short-Range Optical Wireless Communications. (2018).
[14] ITU-R. 2011. SM.2153-2: Technical and operating parameters and spectrum use for short-range radiocommunication devices. (2011).
[15] Krishna Kadam and et al. 2018. Smart and precision polyhouse farming using visible light communication and internet of things. *ICICC* (2018).
[16] Mohamad Katanbaf, Ali Saffari, and Joshua R. Smith. 2021. MultiScatter: Multistatic Backscatter Networking for Battery-Free Sensors. In *SenSys*.
[17] Bryce Kellogg and et al. 2014. Wi-Fi Backscatter: Internet Connectivity for RF-Powered Devices. In *SIGCOMM*.
[18] Vincent Liu and et al. 2014. Ambient Backscatter: Wireless Communication out of Thin Air. In *SIGCOMM*.
[19] Muhammad Sarmad Mir and et al. 2021. PassiveLiFi: Rethinking LiFi for Low-Power and Long Range RF Backscatter. In *MobiCom*.
[20] Muhammad Sarmad Mir and et al. 2023. TunnelLiFi: Bringing LiFi to Commodity Internet of Things Devices. In *HotMobile*.
[21] Hantaro Nagaoka. 1909. The inductance coefficients of solenoids. *The journal of the College of Science, Imperial University of Tokyo, Japan* (1909).
[22] Muhammad Amir Panhwar and et al. 2020. Li-Net: towards a smart Li-Fi vehicle network. *Indian Journal of Science and Technology* (2020).
[23] Aaron N. Parks and et al. 2014. Turbocharging Ambient Backscatter Communication. *SIGCOMM Comput. Commun. Rev.* (2014).
[24] Michael B Rahaim, Anna Maria Vegni, and Thomas DC Little. 2011. A hybrid radio frequency and broadcast visible light communication system. In *GLOBECOM*.
[25] Vamsi Talla, Bryce Kellogg, Shyamnath Gollakota, and Joshua R Smith. 2017. Battery-free cellphone. *IMWUT* (2017).
[26] Ambuj Varshney and Lorenzo Corneo. 2020. *Tunnel Emitter: Tunnel Diode Based Low-Power Carrier Emitters for Backscatter Tags.*
[27] Roald K Wangsness and Ronald K Wangsness. 1979. *Electromagnetic fields.*
[28] Chenren Xu, Lei Yang, and Pengyu Zhang. 2018. Practical backscatter communication systems for battery-free Internet of Things: A tutorial and survey of recent research. *IEEE Signal Processing Magazine* 35, 5 (2018), 16–27. https://doi.org/10.1109/MSP.2018.2848361
[29] Xieyang Xu and et al. 2017. PassiveVLC: Enabling practical visible light backscatter communication for battery-free IoT applications. In *MobiCom*.
[30] C Patrick Yue and S Simon Wong. 2000. Physical modeling of spiral inductors on silicon. *IEEE Transactions on electron devices* (2000).
[31] Junbo Zhang, Elahe Soltanaghai, Artur Balanuta, and Reese Grimsley. 2022. PLatter: On the Feasibility of Building-scale Power Line Backscatter. In *NSDI*.
[32] Pengyu Zhang, Dinesh Bharadia, Kiran Joshi, and Sachin Katti. 2016. HitchHike: Practical Backscatter Using Commodity WiFi. In *SenSys*.
[33] Pengyu Zhang, Colleen Josephson, Dinesh Bharadia, and Sachin Katti. 2017. FreeRider: Backscatter Communication Using Commodity Radios. In *CoNEXT*.
[34] Renjie Zhao, Purui Wang, Yunfei Ma, and et. al. 2020. NFC+ breaking NFC networking limits through resonance engineering. In *SIGCOMM*.