Enable Autonomous Backscatter in Everyday Devices

Si Liao*‡§, Fengxu Yang*, Huangxun Chen†, Zhice Yang*¶
*School of Information Science and Technology, ShanghaiTech University, China
†IoT Thrust, Information Hub, Hong Kong University of Science and Technology (Guangzhou), China
Email: liaosi, yangfx, yangzhc@shanghaitech.edu.cn, huangxunchen@hkust-gz.edu.cn

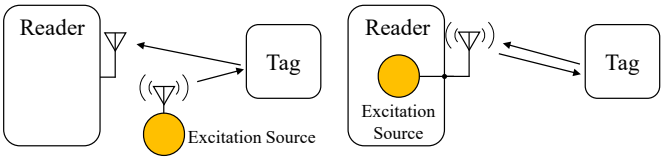
***Abstract*—Recent research has integrated backscatter mechanisms into existing wireless networks, aiming to enable backscatter transmitters to communicate directly using conventional wireless protocols. This would allow for low-power wireless communication within today's network infrastructure. However, the lack of native support poses a challenge in seamlessly accommodating backscatter transmitters within legacy infrastructure. This paper introduces EMScatter, a backscatter system designed for commodity mobile devices. It eliminates the need for an external excitation source separate from the transceiver peers. The proposed approach utilizes the inherent electromagnetic radiation (EMR) signals emitted by the device as the excitation signal, effectively transforming commodity mobile devices into backscatter readers. Users can utilize their mobile devices to directly communicate with backscatter tags anytime and anywhere.**

I. Introduction

Backscatter has been highly expected in the field of low-power wireless communication. It transmits information through reflection rather than active emission of radio frequency (RF) signals. This working mechanism, distinct from traditional RF front-ends, offers the potential to significantly reduce transmission energy consumption.

Recent research has attempted to integrate the backscatter mechanism into popular protocols like Wi-Fi [11], [27], [35], Bluetooth [34], LTE [16], *etc.* This would make it possible to achieve low-power communication in today's wireless infrastructure. However, backscatter systems rely on a component that is out of conventional communication setup: the source of excitation signals. This excitation source generates RF signals in place of a traditional transmitter, making it an integral part of backscatter systems. Accommodating the excitation source smoothly within the existing network architecture has been a long-standing design challenge.

Many studies have proposed utilizing ambient RF signals as the source of excitation [29], [35]. However, an issue associated with this approach is its inability to provide service when there is no "effective" coverage. As pointed by recent research [16], the coverage of signals like Wi-Fi, LoRa, *etc.*, remains limited, and even LTE coverage in suburban and underdeveloped regions is uncertain [2]. Moreover, even in areas with coverage, it is not entirely sure whether these signals can be eventually utilized. These methods often rely on infrastructure support, including authenticated network connections [11], collaborative decoding capabilities [35], and dedicated hardware and software components. Another approach is to always carry and maintain an external excitation source specifically for backscatter, *e.g.*, a single-tone emitter [28], or a Bluetooth transceiver [24], [34].



(a) Helper-based Systems (b) Autonomous Systems

Fig. 1: **Excitation Source in Backscatter Systems.**

We refer to the above-mentioned methods as the "Helper-based" backscatter systems as shown in Figure 1 (a). Despite many advances in these systems, a research question naturally arises: **can we integrate the excitation source within the reader to enable "autonomous" systems**? (Figure 1 (b)). This integration would make the transceiver peers self-contained and would greatly benefit scenarios that demand high availability at any time and place. For example, an in-body backscatter implant needs to transmit health alerts spontaneously.

Enabling autonomous systems to communicate with tags is non-trivial. RFID readers achieve autonomy at the cost of being bulky and expensive [5], [7]. Although many mobile devices have multiple RF transceivers, they either operate in different frequency bands or, like Wi-Fi and Bluetooth, function in a time-division manner to prevent inter-protocol interference [10]. Thus, making one RF chain to provide excitation for another is challenging, if not impossible, and would require substantial hardware upgrades or replacements.

In this paper, we aim to **explore the potential of using inherent electromagnetic radiation (EMR) signals from the device's circuitry, as the excitation signal**. The resultant system, EMScatter, is depicted in Figure 2. EMScatter seeks to enable mobile devices to function as autonomous backscatter readers, eliminating the need for an external excitation source and providing a plug-and-play solution for tag communication.

The advantage of EMR lies in its high availability in mobile devices, while the challenge in leveraging it primarily stems from the fact that it is not a conventional RF signal and requires adaption to successfully serve as an excitation signal. (i) USB interface as EMR amplifier@Reader: Tags prefer a strong and sharp RF tone for excitation, whereas the original EMR spectrum is decentralized and dispersed. Here, our key

‡Also with Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences.
§Also with University of Chinese Academy of Sciences.
¶Corresponding Author.

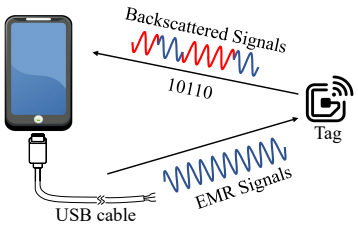


Fig. 2: **EMScatter Overview.**

insight is to leverage the universal serial bus (USB) interface as the EMR emission source. Specifically, we output alternating bits 0 and 1 on the USB interface to generate a continuous square wave at 2.5 GHz, concentrating the EMR spectrum near the 2.4 GHz ISM band. Moreover, we have developed an extremely low-cost method to repurpose USB charging cables into antennas to further amplify EMR radiation.

(i) De-Spread Spectrum@Tag: The 2.5 GHz EMR signal transmitted through the USB interface is subject to the effects of Spread Spectrum Clocking (SSC), which smooths out the peak spectral power of EMR by rapidly varying the clock frequency of digital signals. Consequently, the EMR frequency exhibits significant jitter, rendering it less than ideal as an excitation source. To overcome this issue, we implement a De-Spread Spectrum (DSS) scheme at the tag end. DSS enables the tag to backscatter and shift the EMR frequency influenced by SSC to a stable desired value, functioning like signal cancellation in the frequency domain. On top of the single tone generated by DSS, the tag can apply any data modulation scheme as shown in Figure 2.

Our main contributions are as follows:

- We take the first step to explore using inherent SSC-modulated EMR signals as excitation signals for backscatter communication, freeing the system from the need for an external excitation source.
- We successfully leverage the USB interface and associated USB cable to concentrate the EMR spectrum and amplify the radiation power up to -40 dBm for data transmissions in 2.4 GHz ISM.
- We formulate the impact of SSC and designed an effective DSS method on the tag to stabilize the USB EMR into a pure tone signal for durations ranging from several milliseconds to several seconds for communication.
- Based on evaluations on commodity mobile platforms, EMScatter can enable backscatter transmissions at distances of up to 40 cm with throughputs of up to 1 kbps, sufficient to support critical spontaneous tag communications, such as in-body implants transmitting health alerts.

II. Related Work

EMScatter is an autonomous backscatter system that does not require external excitation source for communication. It allows commodity mobile devices to act as tag readers. We compare EMScatter with existing work in Table I.

Helper-based Backscatter Systems rely on one or more devices other than the reader to generate the excitation signal. One way is to directly utilize a dedicated device to generate a pure-tone excitation signal, *i.e.*, a continuous sinusoidal signal. This signal offers the advantage of providing high flexibility in backscatter modulation design. With it, Passive Wi-Fi [28] and RF-Transformer [19] successfully synthesized standard transmissions of current wireless protocols. Alternatively, the tone can also be generated by existing wireless modules [24], [33], [34], [39], [40]. Compared to EMScatter, their users have to carry and manage an additional RF device, which adds complexity to the interaction.

Work	External Excitation Source	COTS Reader
[24], [28], [34]	• (single tone)	•
[19], [33], [39]	• (single tone)	○
[17], [30], [35], [36]	• (Wi-Fi)	•
[29]	• (TV)	○
[20], [21], [32]	• (LoRa)	○
[16]	• (LTE)	○
[11], [27], [37]	• (Wi-Fi)	•
[13], [26]	○	○
EMScatter	○	•

TABLE I: **Comparison of Backscatter Systems.**

Another branch of work attempted to leverage existing wireless infrastructure as the excitation signal source. Ambient transmissions from various sources such as TV broadcasts [29], Wi-Fi [11], [17], [27], [30], [35]–[38], LoRa [20], [21], [32], and LTE [16] packets have been investigated for their feasibility in backscattering information. Recently, LeakageScatter [31] exploites ambient leaked RF signals from modulated LiFi systems as the excitation source. As ambient signals have been modulated, achieving high-throughput backscatter over them necessitates the use of dedicated hardware like software-defined radios, or assisting devices, *e.g.*, multiple access points, to enable cooperative reception [35], [36]. This echos the issue highlighted by Passive LTE [16]: the effective coverage of ambient signals matters. These approaches are more suitable for scenarios indoors, in urban areas, or for devices with relatively fixed positions.

Autonomous Backscatter Systems. The aforementioned issues arise from the dependence on the separate helper, which complicates the practical deployment and use of the communication systems [13]. As such, EMScatter and some other works seek to let the reader emit the excitation signal to make the communication peers self-contained. One challenge in such a design is that the reader has to be able to withstand interference from its own transmitted excitation signal. Traditional RFID readers achieve this using full-duplex radio [14], but this comes with higher implementation costs [22] and does not seamlessly integrate with existing wireless infrastructure. BackFi [13] and Full-duplex LoRa [26] designed new readers to allow for backscattering Wi-Fi and LoRa signals. EMScatter enables commodity mobile devices to function as readers.

III. Preliminaries on USB

The Universal Serial Bus (USB) is a widely-used protocol for wired data transfer. In mobile devices, the USB interface is also used for charging purpose. The USB charging

interface will be mandated in the European Union starting from 2024 [1]. USB3.x is the mainstream USB version in the current market. It specifies the transfer protocols, connectors, and transmission cables. The 3.2 version [9] specifies three physical layers (PHY): Gen1, Gen2, and Dual-Lan Operation. This paper focuses on the USB 3.2 Gen1 physical layer that the raw speed is 5 Gbps, as others are all backward compatible.

Two USB interfaces transfer data by connecting via cables, regardless of the connector types A, B or C. There are wires inside the cable for power supply, USB 2.0's Tx/Rx, and USB 3.0's Tx/Rx. There are several metal shielding layers aground the wires. The physical layer of USB 3.0 maps digital bits to binary voltage levels (high and low) at every clock edge to drive the signals in the transmission (Tx) lines. As the raw data rate is 5 Gbps, the corresponding EMR is near 2.5 GHz, overlapping with the 2.4 GHz ISM band.

USB uses various electromagnetic compatibility (EMC) designs to minimize the interference from EMR. Spread spectrum clocking (SSC) is an active EMC approach, widely adopted in modern high-speed data connections, including PCIe, memory bus, USB, HDMI, and many more, to conform to the EMC regulations. SSC reduces the peak power of the EMR signals by spreading their spectrum over a wide range of frequencies in a short period. To do this, it deliberately jitters the clock frequency of the source signals, *e.g.*, USB Tx signal.

IV. EMScatter Reader Design

This section describes the method to generate continuous and strong EMR signals on commercial mobile devices through their USB interface.

A. Harnessing USB Signals

EMScatter reader needs to bypass above EMC mechanisms to leverage USB EMR for excitation. USB EMR is mainly generated by its Tx signals. To concentrate EMR into a single-tone signal, the Tx signals must be driven by periodic bits. One way is to reverse engineer USB PHY's scrambling and line code to derive the link-layer data that produces the desired bit stream, and then feed the data in as payload to generate the desired Tx signal. However, the Tx signal generated by this method contains large noise. This is because the Tx signal cannot be fully determined by the upper layer data.

To avoid the above issues, EMScatter reader leverages the *compliance mode* of the USB controller. Compliance mode is a standard working mode defined by the USB specification. Its purpose is to allow manufacturers to perform compatibility tests on their products to conform the specification.

The USB controller enters the compliance mode with proper configuration commands. Then, its PHY transmits one of the predefined pattern sequences (CP0-CP16) [9]. Among them, CP1 forces the PHY continuously transmitting '01' sequence at 5 Gbps. The corresponding Tx signal is close to an ideal square (clock) wave with cycle frequency at f_0=2.5 GHz. The EMR, $w_{\text{EMR}}(t)$ mirrors the Tx signal:

$$w_{\text{EMR}}(t) = A \cdot \text{sgn}(\sin(2\pi f_0 t)) = \sum_{n=1}^{+\infty} A_n \sin(2\pi n f_0 t), \quad (1)$$

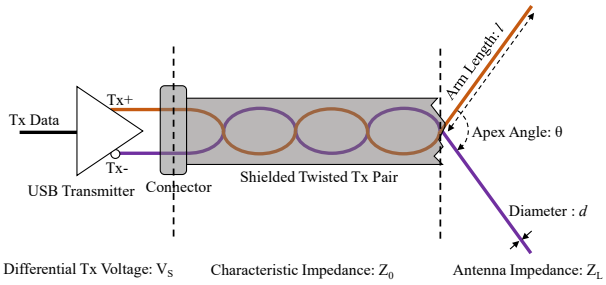
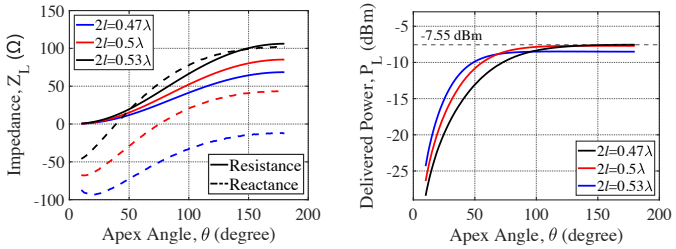


Fig. 3: **Using USB Cable as Antenna.**



(a) Antenna Impedance v.s. Arm Length and Apex Angle.

(b) Power Delivered to the Antenna from the USB Transmitter.

Fig. 4: **Tuning USB Antenna Parameters to Maximize EMR Radiation Power.**

where $A \cdot \text{sgn}(\sin(2\pi f_0 t))$ defines a square wave with amplitude A, frequency f_0, and 50% duty cycle. According to its Fourier expansion, $w_{\text{EMR}}(t)$ concentrates its power in its first harmonic component, *i.e.*, $w_{\text{EMR}}(t) \approx w_1(t) = A_1 \sin(2\pi f_0 t)$, which is just a 2.5 GHz single-tone wave.

B. Using Cable as Antenna

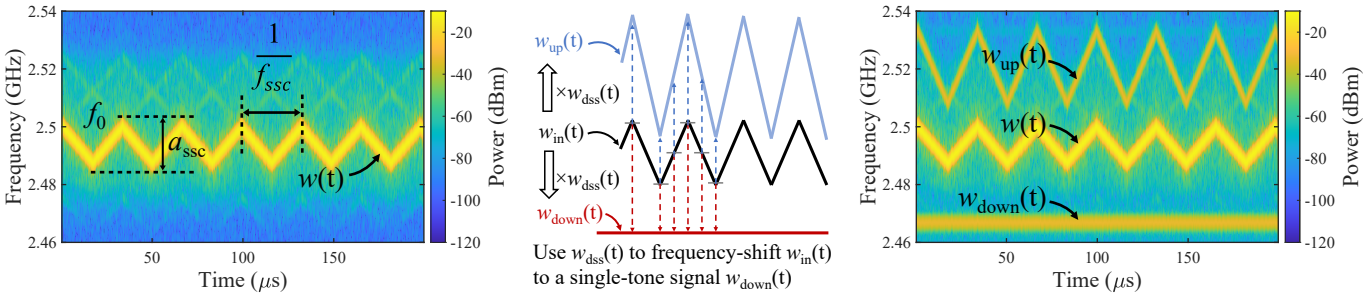
$w_1(t)$ can serve as an excitation signal, but due to EMC designs, the radiation is almost within the device and around the USB connector, with very limited far-field power. Our idea is to directly use the USB cable as the antenna, which is intuitive, convenient and extremely low-cost. As shown in Figure 3, the USB transmitter drives a differential signal pair, Tx+ and Tx-, with equal amplitude but opposite signs. This implies that after unwrapping the shielding layers and untwisting the Tx+/Tx- lines, *the exposed portion of the Tx+/Tx- lines is just a center-fed dipole antenna.*

As the driving power of the USB transmitter is almost fixed, the efficiency of the cable antenna solely determines the radiation power. Since the USB transmitter and cable are impedance-matched, the delivered power at the antenna is determined by [18]:

$$P_L = \frac{(\frac{V_S}{4})^2}{2Z_0} \left(1 - \left|\frac{Z_L - Z_0}{Z_L + Z_0}\right|^2\right), \quad (2)$$

where Z_0 is determined by the characteristic impedance Z_0 of the cable and Z_L is the antenna impedance Z_L. The power delivered to the antenna is maximum when $Z_0 = Z_L$, but Z_L is (likely) not equal to Z_0.

The impedance of the cable dipole, Z_L is determined by the arm length l, the bearing angle of the arms, *i.e.*, the apex angle θ, and the diameter of the arm d. We model the antenna as a half-wavelength dipole, *i.e.*, $2l \approx 0.5\lambda$, to choose



(a) EMR Spectrogram when Transmitting 01 at 5 Gbps (b) Effect of DSS Operations (c) EMR Spectrogram when Backscattering with DSS

Fig. 5: **Using De-spread Spectrum Scattering (DSS) to Counter Against Spread Spectrum Clocking (SSC).**

appropriate parameters to maximize the transmission power[1]. Figure 4a shows the real (resistance) and imaginary (reactance) parts of Z_L versus angles θ and arm lengths l at 2.5 GHz, with normative USB parameters (line diameter d=0.02 mm, Z_0=90 Ω, V_S=800 mV).

Figure 4b jointly considers Equation 2 and Figure 4a to show the power delivered to the antenna versus different antenna parameters[2]. The maximum power (-7.55 dBm) in Figure 4b is reached when θ=169° and l=2.81 cm. The curve is relatively flat, meaning that it is flexible to choose antenna parameters to achieve radiation power close to the optimum.

The above results lead to the following steps turning a USB cable into the antenna to radiate USB EMR signals: cut the USB cable in half, remove the shielding layers of the open end to expose the lines for about 3 cm, then untwist and spread out the Tx lines. When the opened cable is plugged into the device's USB connector, it radiates out Tx signals efficiently.

V. EMScatter Tag Design

A. Impact of Spread Spectrum Clocking

We measured the EMR signal generated by the EMScatter reader with a spectrum analyzer. The emission power of $w_1(t)$ is about -15 dBm, close to the theoretical value, but its peak at 2.5 GHz is not as sharp as a single-tone signal. Figure 5a is its spectrogram for time-frequency analysis. The spectrogram visually shows the spectrum of frequencies (y-axis) of a signal as it varies over time (x-axis). The main frequency peak of the EMR signal shifts slightly around 2.5 GHz.

This is due to the SSC mechanism specified in USB 3.0 [9] employed by the USB transmitter. SSC uses frequency-modulation to linearly decrease and increase the frequency of the data clock, which introduces a frequency deviation of up to $2a_{ssc}$=0.5%f_0=12.5 MHz with a modulation rate of up to f_{ssc}=31.5 kHz. SSC causes the frequency of $w_1(t)$ to vary between f_0 and $f_0 - 2a_{ssc}$ with a period of $1/f_{ssc}$. Hence, at time t, the instantaneous frequency of the EMR signal becomes:

$$f(t) = f_0 + a_{ssc}\left(\text{tri}\left(2\pi f_{ssc} t + \phi_{ssc}\right) - 1\right), \tag{3}$$

where tri(x) is the standard triangular wave with amplitude of 1 and period of 2π.

Since the phase of the EMR signal is the integral of the angular frequency, $2\pi f(t)$. Due to SSC, the EMR signal of the 01 Tx sequence becomes:

$$w(t) = A_1 \sin\left(2\pi \int_0^t f(x)dx\right) \tag{4}$$

From the tag's perspective, it is not possible to directly utilize such frequency-varying signals for backscatter communication. This is particularly true when aiming to integrate the backscattered signals into the modulation of existing wireless protocols, as their fine structure differs significantly from that of $w(t)$. $w(t)$ varies its frequency by 5000 ppm, or 12.5 MHz at 2.5 GHz, in 15 μs. As for a comparison, a single 802.11 symbol lasts for several μs, and the standard-compliant tolerance of the carrier frequency offset is 40 ppm.

B. De-spread Spectrum Scattering

To make use of the EMR signal governed by SSC, we introduce the De-spread Spectrum Scattering (DSS) scheme in the backscatter tag to convert the SSC-modulated signal into a single-tone carrier.

Primer on using backscatter to frequency-shift signals: We consider a representative backscatter transmitter whose antenna impedance is controlled by a digital switch. Due to reflection properties, the backscattered signal is phase aligned and phase inverted to the incident signal, when the switch is toggled to the short and open circuit, respectively. This implies that the backscattered signal is just the product of the incident signal and the signal that controls the antenna switch. In particular, when the control signal is a square wave of frequency f_{dss}, *i.e.*, $\text{sgn}(\sin(2\pi f_{dss} t))$, and the incident signal is $\sin(2\pi f t)$, the backscattered signal is :

$$\text{sgn}(\sin(2\pi f_{dss} t))\sin(2\pi f t) \approx \frac{\cos 2\pi(f+f_{dss})t + \cos 2\pi(f-f_{dss})t}{2}.$$

Note that the above is a signal frequency-shifted from the incident signal by $\pm f_{dss}$. This implies that backscatter modulation can be used to frequency-shift the incident signal [28].

DSS is to frequency-shift the SSC-modulated signal to right frequencies: DSS is based on the above property. Generally, suppose the tag receives a portion of the radiation power of the USB EMR signal, *i.e.*, $w_{in}(t) = \frac{A_{in}}{A_1} w(t)$. The tag then applies $w_{dss}(t)$ to backscatter $w_{in}(t)$. The instantaneous

[1]Dipole antennas have high efficiency at lengths near odd half-wavelengths, but only the impedance at the half-wavelength is the closest to Z_0=90 Ω, so we only need to consider half-wavelength dipoles.

[2]We focus on the power of the first harmonic. For ideal square wave, $A_1/A = 4/\pi$ in Equation 1, leading to a 0.9 dB loss in the total power.

frequency of $w_{\text{dss}}(t)$ is $f_{\text{dss}}(t)$. Similar to Equation 4, $w_{\text{dss}}(t)$ can be written as

$$w_{\text{dss}}(t) = \text{sgn}\left(\sin\left(2\pi\int_0^t f_{\text{dss}}(x)dx\right)\right). \quad (5)$$

Therefore, the backscattered signal is

$$w_{\text{in}}(t)\cdot w_{\text{dss}}(t) \approx \frac{A_{\text{in}}}{2}\cos\left(2\pi\int_0^t f(x)+f_{\text{dss}}(x)dx\right) + \frac{A_{\text{in}}}{2}\cos\left(2\pi\int_0^t f(x)-f_{\text{dss}}(x)dx\right) = w_{\text{up}}(t)+w_{\text{down}}(t), \quad (6)$$

where $w_{\text{in}}(t)$ is frequency-shifted by $w_{\text{dss}}(t)$ into two signals, $w_{\text{up}}(t)$ and $w_{\text{down}}(t)$, respectively.

Note that $f_{\text{dss}}(t)$ is not necessarily time-invariant. In particular, considering Equation 3 and $w_{\text{down}}(t)$, when $f_{\text{dss}}(t)$ equals $f(t)$ except for an content offset of F_{ch}, *i.e.*,

$$f_{\text{dss}}(t) = f_0 - F_{\text{ch}} + a_{\text{ssc}}\left(\text{tri}\left(2\pi f_{\text{ssc}}t+\phi_{\text{ssc}}\right)-1\right), \quad (7)$$

then $w_{\text{down}}(t)$ becomes $\frac{A_{\text{in}}}{2}\cos(2\pi F_{\text{ch}}t)$, *i.e.*, a desired single-tone signal at frequency F_{ch}.

Figure 5b illustrates the DSS operations. The tag uses modulation signal $w_{\text{dss}}(t)$ to frequency-shift $w_{\text{in}}(t)$ to compensate for the shifts introduced by SSC. $w_{\text{up}}(t)$ and $w_{\text{down}}(t)$ are the up-shifted and down-shifted portion of $w_{\text{in}}(t)$, respectively. $w_{\text{up}}(t)$ is an SSC-modulated sinusoidal wave with a frequency deviation twice of the original SSC modulation, while $w_{\text{down}}(t)$ is a single tone at F_{ch}. Figure 5c shows the spectrogram of the backscattered USB EMR signals under the presence of a nearby DSS backscatter tag.

C. Uplink: Loading Wi-Fi Transmissions

The single-tone sinusoidal wave $w_{\text{down}}(t)$ can be further modulated to generate transmissions compatible with mainstream wireless protocols, *e.g.*, Wi-Fi, Bluetooth, Zigbee, Lora, *etc.* We choose Wi-Fi as an example.

We first synthesize the frequency of $w_{\text{down}}(t)$ to the center frequency of a Wi-Fi channel, *e.g.*, in channel 12 (2467), by setting F_{ch}=2.467 GHz. Existing work provides a detailed description of 802.11b [28], we only describe the essential part here for brevity. The 802.11b PHY manipulates the phase of the carrier wave to convey information. Its baseband signal $X(t)$ can modulate the single-tone signal at F_{ch} by multiplying with $w_{\text{down}}(t)$. Note that $X(t)$ takes values from $+1, -1, j$, and $-j$, so it can be combined with $w_{\text{dss}}(t)$ to synthesize the overall modulation to drive the antenna switch:

$$w_{\text{in}}(t)\cdot \underbrace{[w_{\text{dss}}(t)\cdot X(t)]}_{\text{backscatter modulation}} \approx w_{\text{up}}(t)\cdot X(t) + w_{\text{down}}(t)\cdot X(t),$$

where $w_{\text{down}}(t)\cdot X(t)$ is a 802.11b-compatible signal with its centre frequency at F_{ch}.

D. Downlink

EMScatter reader delivers messages to tags by sending Wi-Fi packets. Similar to existing work [27], the reader encodes bits into the duration of its outgoing Wi-Fi packets. It controls the duration by varying the payload size at a fixed PHY rate. The tag uses a power detector and a comparator to detect the envelope of the received Wi-Fi packets. It counts the duration to obtain the encoded bits.

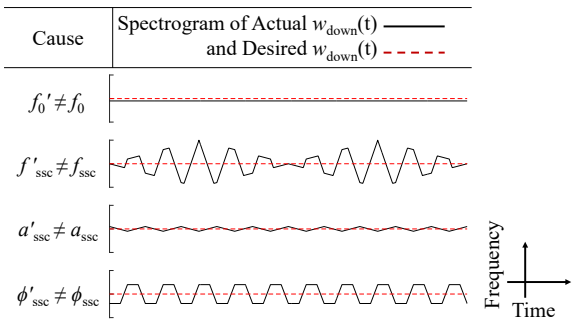


Fig. 6: **Spectrogram of the Backscattered Signal.**

VI. Synchronization

From the previous section, DSS operates like signal cancellation in the frequency domain. Hence, to achieve a clean and stable single-tone signal, it is critical for the frequency offset generated by DSS to precisely match the frequency offset generated by SSC. However, in practice, the parameters describing SSC, *i.e.*, f_0, f_{ssc}, a_{ssc}, and ϕ_{ssc} in Equation 3 often have only approximate normative values or are even unknown. This will lead to differences between the actual $w_{\text{down}}(t)$ and the desired one, as shown in Figure 6.

To understand the impact of these errors, we assume the tag uses inaccurate f_0', a'_{ssc}, f'_{ssc}, and ϕ'_{ssc} to calculate $w_{\text{dss}}(t)$ in Equation 7 and 5, the frequency of $w_{\text{down}}(t)$ will become:

$$\begin{aligned} f_{\text{down}}(t) &= f(t) - f'_{\text{dss}}(t) \\ &= F_{\text{ch}} + (f_0 - f_0') - (a_{\text{ssc}} - a'_{\text{ssc}}) + \\ &\quad a_{\text{ssc}}\text{tri}(2\pi f_{\text{ssc}}t + \phi_{\text{ssc}}) - a'_{\text{ssc}}\text{tri}(2\pi f'_{\text{ssc}}t + \phi'_{\text{ssc}}). \end{aligned} \quad (8)$$

The time-invariant parts result in a constant offset in the desired frequency F_{ch}. The remaining parts cause frequency variations in the backscattered signal, which is expected to be a single-tone signal with a fixed frequency.

However, in practice, the error tolerance of USB 3.0 data clock is $\pm$300 ppm [9], while the requirement of 802.11b is $\pm$20 ppm. This means that using f_0'=2.5 GHz to estimate f_0, the obtained F_{ch} may contain a carrier frequency offset exceeding the tolerance. Further, our experiments (latter in §VIII-B) show that the network interface card (NIC)'s tolerance for $|f_{\text{ssc}} - f'_{\text{ssc}}|$ is only at the Hz level, while different USB devices may have a difference of up to 1 kHz. Again, there may be a difference between a_{ssc} and a'_{ssc} of up to 1000 ppm.

Similar but less prominent issues exist widely in asynchronous communication systems. A common practice is that the receiver synchronizes to the transmitter's profile through measurements, but low-power tags do not have complete receiving chains to process SSC signals. Therefore, our approach is to let the reader measure its own USB profile first, and then inform the tag before transmissions.

A. Measuring SSC with Wi-Fi Spectral Scan

To accurately determine these parameters, we still face two main problems: First, there is no suitable RF sampling module working at 2.5 GHz on commodity mobile devices. Second, effective measurement of these parameters requires very high frequency resolution.

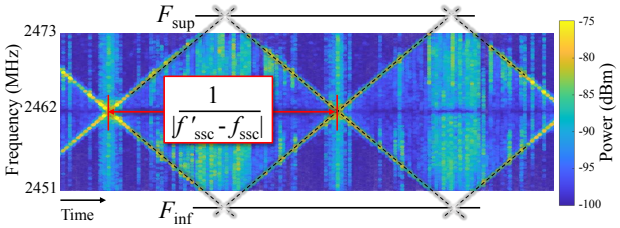


Fig. 7: **Using Wi-Fi NIC to Measure SSC Parameters.**

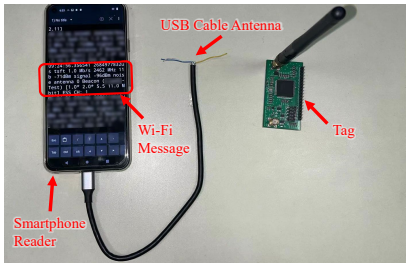


Fig. 8: **EMScatter Reader and Tag.**

Our solution is to leverage a helper tag to shift the 2.5 GHz USB EMR signal $w_{\text{in}}(t)$ down to the 2.4 GHz ISM band without loading 802.11b modulation. Then, we make use of the spectral scan function of Wi-Fi NICs [6], [15] to observe the frequency domain of $w_{\text{down}}(t)$. Spectral scan performs FFT, a basic operation of modern OFDM-based NICs, on the received RF signals and reports the power of each frequency bin, but it only provides coarse-grained spectral information, which is not enough to directly determine these parameters.

We amplify the information of a single measurement by accumulating the results of spectral scans over time. The frequency-time domain reveals highly relevant features:

- As the range of the triangular function in Equation 8 is $[-1,1]$, $f_{\text{down}}(t)$ varies between F_{sup} and F_{inf}, where
$$F_{\text{sup}} = F_{\text{ch}} + (f_0 - f'_0) + 2a'_{\text{ssc}} \quad (9)$$
$$F_{\text{inf}} = F_{\text{ch}} + (f_0 - f'_0) - 2a_{\text{ssc}} \quad (10)$$
This implies that the frequency range of $w_{\text{down}}(t)$ in the spectrogram is bounded by F_{sup} and F_{inf} over time.
- Using sine functions to approximate the triangular functions[3] in Equation 8 gives
$$f_{\text{down}}(t) \approx (F_{\text{sup}} + F_{\text{inf}})/2 + \quad (11)$$
$$\frac{16}{\pi^2} a_{\text{ssc}} \cos\left(2\pi \frac{(f + f'_{\text{ssc}})}{2} t + \phi_a\right) \sin\left(2\pi \frac{(f - f'_{\text{ssc}})}{2} t + \phi_b\right).$$
$\sin(2\pi \frac{(f-f'_{\text{ssc}})}{2} t)$ goes from zero to its peaks once for each half cycle. It shapes the envelope of the $\cos(2\pi \frac{(f+f'_{\text{ssc}})}{2} t)$ part. This implies that the frequency range of $w_{\text{down}}(t)$ fluctuates in the spectrogram at a rate of $|f'_{\text{ssc}} - f_{\text{ssc}}|$.

The above implications are depicted in the spectrogram in Figure 7, which is formed by accumulating consecutive spectral scans captured by the reader's Wi-Fi NIC.

According to the above observations, we measure the SSC parameters by first commanding the helper tag to modify its f'_{ssc} value until obvious frequency peaks increasing and decreasing over time appear in the spectrogram. This is the indicator that f'_{ssc} has been close to f_{ssc}. We use Hough transform [23] to determine the line patterns in the spectrogram. Then, we measure the upper and lower bounds of the spectrum as F_{sup} and F_{inf}, and calculate f_0 and a_{ssc} according to Equation 9 and 10.

As the frequency resolution of spectral scan is about 80 kHz (256-point FFT on 20 MHz), this method allows for precise measurement for f_{ssc}, f_0, and a_{ssc}. To account for potential small error residues, the reader guides the tag to perform an active search around nearby values based on un-/successful transmissions. Our experience also suggests that this measurement only needs to be performed once for a device, as the SSC parameters seem to be relatively stable.

However, because the phase offset is random after power-on reset and oscillator frequency is affected by factors such as temperature, keeping a stable phase offset is almost impossible. To this end, we propose to let the two asynchronous signals to synchronize themselves. We refer to such periods that can be used for backscatter transmissions as the *crossing periods*, corresponding to the area around the point where the lines intersect in Figure 7. Additionally, we deliberately introduce an offset in f'_{ssc} to let the occurrence of crossing periods predictable. As such, the tag only wakes up to transmit in these periods. Our tests show that when f_{ssc} is selected properly, the crossing period can last tens of milliseconds.

VII. Implementation

Figure 8 shows the EMScatter tag and commodity reader.

A. Reader Implementation

We use two COTS mobile devices as EMScatter readers: a Pixel 5 smartphone from Google and ODROID XU 3 running Ubuntu 16.04 LTS. As ODROID lacks on-board Wi-Fi NIC, it uses a USB 2.0 NIC with Atheros 9271 Wi-Fi chip. The USB 3.0 connectors of the two devices are different, ODROID's is Type-A and Pixel's is Type-C. The cable antennas can be made in 2 minutes with household scissors.

It seems most of the USB controllers integrated in ARM SoCs on the market use Synopsys's USB3.0 IP core [3], which is used with the `dwc3` driver [8]. Hence, the ways to enter the compliance mode in different mobile devices are similar, and are to set the relevant registers through the driver. We use COMPEX WLE1216VX NIC to obtain the channel spectral scan information through the `debugfs` of the `ath10k` driver [6]. Pixel smartphone also provides a similar function. Its integrated Wi-Fi module is very similar to Qualcomm's independent Wi-Fi NICs, but its driver is `QCACLD` [4]. Since there is no public interface to access `QCACLD`'s spectral scan functions, we implement a native app similar to `ath10k` to query the spectral scan data. Then we put the Wi-Fi NICs into the monitor mode and use `tcpdump` to receive the packets from the tag. We use `scapy` to send raw MAC-layer packets to the tag.

B. Tag Implementation

To demonstrate that the DSS design is compatible with general tag implementation. We implement the representative

[3] $\text{tri}(2\pi ft) = \frac{8}{\pi^2} \sum_{i=0}^{+\infty} \frac{(-1)^i}{(2i+1)^2} \sin(2\pi(2i+1)ft) \approx \frac{8}{\pi^2} \sin(2\pi ft)$

backscatter tag from HitchHike [35]. The tag uses a low-power FPGA to drive an RF switch to change the antenna impedance. We fabricated the hardware and reused their 802.11b modulation logic. We use lookup tables to store the ideal triangular and the device-specific waveform template. To measure the latter, we use USRP X310 to collect the waveform of the USB EMR, *i.e.*, $w(t)$, at a sampling rate of 50MHz. In order to obtain the frequency of $w(t)$, we first calculate the instantaneous phase of $w(t)$ through I/Q samples, and then differentiate it with respect to time, which is just $f(t)$. We extract 100 cycles and resample them to ensure that they are precisely aligned in the time domain. We then average them into a one-cycle waveform, which is normalized and stored as the template of the SSC modulated EMR signal of this specific device. After obtaining w_{dss}(t) according to Equation 5, we use its sign bit as the DSS modulation signal, and synthesize it with the 802.11b modulation signal by `XOR`ing them.

VIII. Evaluation

A. Cable Antenna Performance

To evaluate factors affecting the antenna efficiency, we set the reader's USB controller to the compliance mode to transmit '01' sequence. Using an SMA cable to connect a 2 dBi omnidirectional antenna and a Keysight N9030A PXA signal analyzer, we measure the radiation power received at different locations. Since the output power of the USB transmitter is almost constant, the received power reflects the antenna efficiency. We use the ODROID board in this measurement, and similar results were observed with antennas made from different cables.

The cable antenna is set to the optimal parameters as calculated in Figure 4b. The received power at different distances is shown in dashed lines in Figure 9a. As expected, the power decays with the distance. The received power at 0.5 m is about -45 dBm, inferring the transmitted power at antenna is about -15 dBm (consider the antenna gain and free space attenuation). For comparison, we plot the theoretical received power when the transmitting power is -7.55 dBm. The 8 dB difference is due to the imperfectness of handcrafting and modeling, *e.g.*, impedance mismatches in the USB cable or transmitter.

To investigate the power distribution of the actual backscatter situation, we put together the USB antenna and the receiving antenna side by side, and use a tag to frequency-shift the EMR signal to 38 MHz away. We then use the spectrum analyzer to measure the power that the reader is expected to receive during actual backscatter transmissions. We put the backscatter tag to different distances from the two antennas, and plot the measured and theoretical curves in solid lines in Figure 9a. The transmitting power of the theoretical model [28] is set to -15 dBm. There is a 10 dB difference between the measured and theoretical values in [28], which is likely due to our imperfect replication of the tag. However, this also implies that further improvements in tag implementation can increase the communication range of the system.

The efficiency of the USB cable antenna mainly depends on the length and apex angle between the antenna arms. Since the half-wave dipole is used, the arm length is fixed. We measure the received power at different apex angles at a distance of 40 cm from the antenna. Figure 9b shows the received power decreases as the apex angle decreases. This is because the two antenna arms become a combined differential pair at 0 degrees, canceling most of their radiation. Further, the theoretical value of the delivered power is plotted according to Figure 4b, closely matches the measured trend (dashed line).

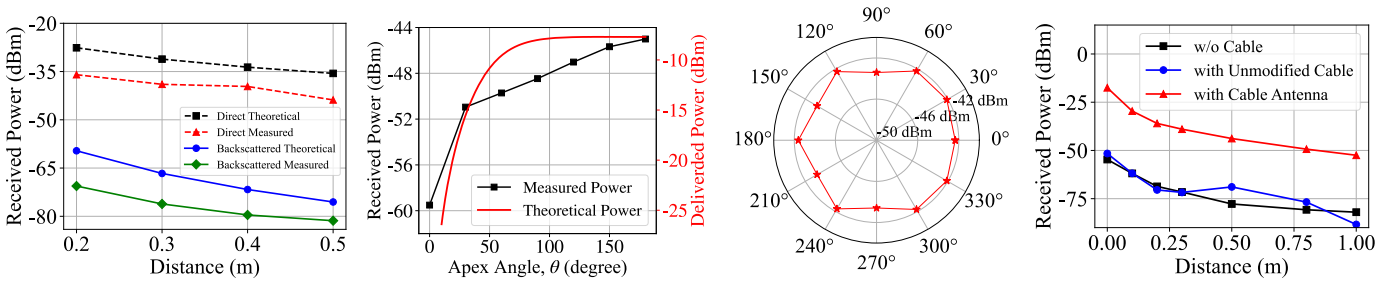
Figure 9c shows the received power at different horizontal directions at the same distance in an open environment. It shows that the received radiation power at different angles are similar. This is because the dipole antenna made by the USB cable is an omnidirectional antenna in the horizontal direction. This feature implies that the antenna cannot intensively concentrate radiation power to a certain direction, that is, a low antenna gain, but it also avoids the problem of antenna direction alignment between the tag and the reader.

Figure 9d compares the cases of using or not using USB cable antennas. The received power is similar when the reader is not connected to the USB cable and when it is connected to an unmodified USB cable (with the other end floating). Their curve shows a 30 dB EMR isolation compared with the cable antenna case. From the absolute values, we can infer that without using the cable antenna, the reader can hardly generate EMR signals with sufficient power for backscatter.

B. DSS Performance

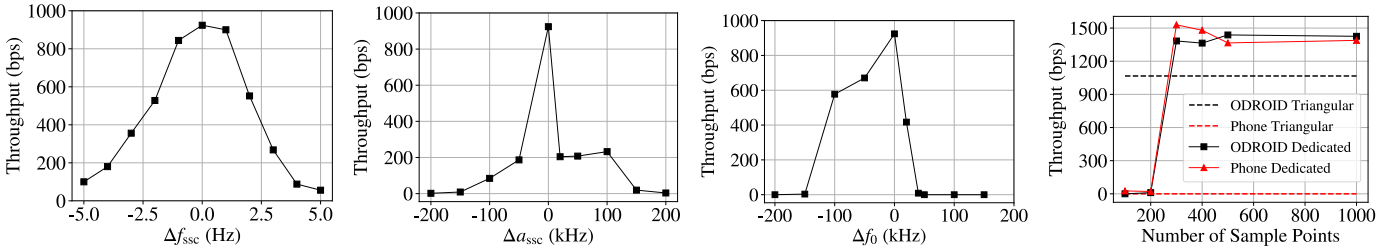
DSS compensates the frequency offset caused by SSC. As shown in Figure 6, imperfect DSS operations lead to frequency noise in the single-tone signal used for synthesizing data frames. This frequency noise is different from the well-studied carrier frequency offset (CFO) in communication systems. In the 802.11 standards, the CFO tolerance is 40 ppm, or 100 kHz at 2.5 GHz, but it represents a stable frequency offset caused by temperature or the aging of the oscillator. In contrast, SSC varies the carrier frequency by up to 12.5 MHz and at a rate of 30 kHz. After applying DSS, there will still be similar high-frequency frequency variations in the produced signal. This type of frequency noise does not exist in the convectional communication systems, we next evaluate its impact on transmissions through experiments.

The frequency of the produced "single-tone" signal in Equation 8 is affected by four error sources: the SSC frequency error $\Delta f_{\text{ssc}} = f_{\text{ssc}} - f'_{\text{ssc}}$, the SSC amplitude error $\Delta a_{\text{ssc}} = a_{\text{ssc}} - a'_{\text{ssc}}$, the SSC phase error, and the error of the USB clock frequency $\Delta f_0 = f_0 - f'_0$. In this experiment, we first use a USRP to accurately measure the actual parameters of the reader device, *i.e.*, obtain f_{ssc}, a_{ssc}, and f_0, and then modify the values that are used by DSS modulation, *i.e.*, f'_{ssc}, a'_{ssc}, and f'_0, to deliberately introduce errors to inspect their impact. Due to the *lazy waiting* mechanism, we cannot analyze phase errors separately. The experiments use ODROID and the tag transmits 1000-bit 802.11b packets with antenna placed close to the reader. The throughput is defined as the received correct bits over the measurement period, *i.e.*, 10 mins.



(a) Received Power v.s. Distance (b) Received Power v.s. Apex Angle (c) Received Power v.s.Direction (d) Open and Closed Cable

Fig. 9: **Performance of USB Cable Antenna.**



(a) Throughput v.s. Δf_{ssc} (b) Throughput v.s. Δa_{ssc} (c) Throughput v.s. Δf_0 (d) Throughput v.s. Template

Fig. 10: **Performance of DSS.**

Figure 10a shows the impact of Δf_{ssc} when fixing other parameters. According to Equation 8, Δf_{ssc} determines the frequency and duration of crossing periods. As Δf_{ssc} increases, the throughput decreases slowly. This is because although the increase of Δf_{ssc} leads to a decrease in the absolute time of a single crossing period, it will also lead to an increase in their occurrence frequency, so the proportional decrease is not obvious. However, throughput decreases after a stable period. This is because the reduced crossing period brings more noise and also becomes tighter to contain a complete packet. From Figure 10a we can conclude that 11b transmissions are reasonably supported only if $|\Delta f_{\text{ssc}}| < 2$ Hz.

Figure 10b shows the impact Δa_{ssc}. According to Equation 8, Δa_{ssc} turns into the an "oscillating" frequency offset. This is illustrated in Figure 6. $|\Delta a_{\text{ssc}}|$ determines the oscillating amplitude, so then it increases, its impact also increases. When $|\Delta a_{\text{ssc}}|$ reaches the order of 100 kHz, it corrupts most transmissions. Therefore, to support 11b transmissions, $|\Delta f_0|$ should be $\leq$ 50 kHz. Figure 10c shows the impact of Δf_0. According to Equation 8, Δf_0 primarily creates a constant frequency offset similar to CFO. The tolerance of CFO is 100 kHz in 802.11b standard, and Figure 10c confirms this. To support 11b transmissions, $|\Delta f_0|$ should be $\leq$ 50 kHz.

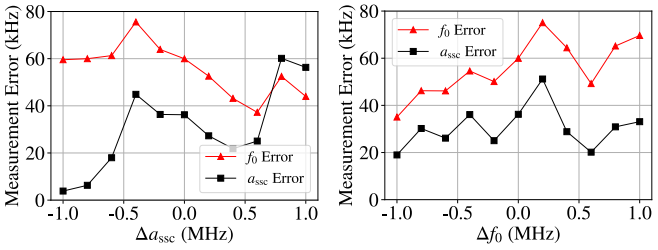
Figure 10d shows the throughput using different templates to implement DSS. We compare the template generated with an ideal triangular waveform (Triangular) and the dedicated template obtained through measurements (Dedicated). As the SSC modulation signal of the ODROID board closely matches ideal triangular waveform, both templates can be used to transmit data successfully. However, using the dedicated template resulted in higher rates, as it captures more detailed signal features. This difference is more pronounced in the phone test bed, where the triangular waveform results in no reception due to slight signal differences. We also investigate the impact of using different numbers of sampling points to describe the template. Figure 10d shows no significant difference beyond 500 points. We use a conservative value of 1000 points in our implementation to store the template.

C. Accuracy of Parameter Measurement

The above evaluation indicates that the communication performance of EMScatter highly depends on the accuracy of the SSC parameters used by the tag. It also empirically gives the error tolerance of these parameters. In this subsection, we evaluate our parameter measurement method that is based on Wi-Fi spectral scan.

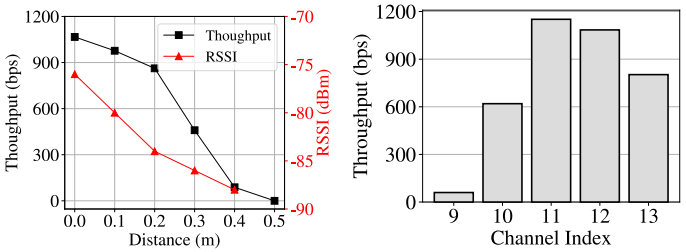
For f_{ssc}, our method identifies the line patterns in the spectrogram (Figure 7). The false positive rate of the detection method (§VI-A) is very low. This is because we restrict the period of these line patterns, and only when $|\Delta f_{\text{ssc}}| < 2$ Hz can they satisfy the criteria. At this scale, the period of these line patterns lasts for hundreds of milliseconds, making misclassification unlikely. We choose 1 Hz as the step size to tune f'_{ssc}. As a result, the algorithm can reduce $|\Delta f_{\text{ssc}}|$ to Hz-level, which meets the measured tolerance.

For a_{ssc} and f_0, we first use the USRP to measure their ground truth. Since they are device-dependent and fixed, we choose to change a'_{ssc} and f'_0 in the tag, as if the ground truth is unknown, to estimate the ground truth with our method. By comparing the estimated values with the ground truth, we evaluate the accuracy of the measurement method. Figure 11a and Figure 11b show the errors of the measured SSC parameters when changing a'_{ssc} and f'_0 to different values (from the ground truth). The four curves show that the measurement errors of a_{ssc} and f_0 at different situations are all within 80 kHz. This



(a) Δa_{ssc} v.s. Measurement Error (b) Δf_0 v.s. Measurement Error

Fig. 11: **Performance of Parameter Measurement.**



(a) Throughput v.s. Distance (b) Throughput v.s. Channel

Fig. 12: **Overall Performance.**

accuracy is reasonable, since the resolution of the spectral scan that it based on is also about 80 kHz. Although these values are slightly larger than the tolerances indicated by previous measurements, they have little effect on practical usage. This is because, with the measured parameters as reference, a rapid search around them can be made to find right values according to the feedback of the achievable throughput.

D. Overall Performance

We evaluate EMScatter performance in practical settings.

Throughput v.s. Distance. We use the ODROID board as the reader and place the tag at different distances from the reader. We make sure the tag's distances to the reader's antenna and the USB antenna are equal. The tag keeps sending 802.11b packets with a length of 1000 bits at Wi-Fi channel 12. The reader also records the RSSI of the received packets. Figure 12a shows the throughput decreases when the distance increases. This is because the power of the backscattered signal decreases, which is reflected in the RSSI values. When the tag is close to the reader, the achieved throughput is around 1000 kbps. The reader can hardly receive packets when the distance increases to 0.5 m, where the RSSI is about -90 dBm, being close to the NIC's decoding limit.

Throughput v.s. Channel. We move the tag close to the reader and investigate impact of channels. Figure 12b shows the throughput varies across different channels. Since Channel 13 is closer to the EMR's spectrum around 2.5 GHz, the backscattered signal is adversely affected by the high-power EMR signal, resulting in a decrease in throughput. Except for Channel 13, the EMR signal does not significantly interfere with nearby Channels, *e.g.*, 12 and 13. This is because the NIC's front-end has a bandpass filter that can filter out most of the interference outside the desired channel range. Additionally, being farther away from the EMR signal does not necessarily guarantee better throughput performance, *e.g.*, Channel 9. Farther frequency channel requires a higher switching frequency, which leads to more power loss in reflection.

Power Analysis. We adapt full logic of EMScatter tag into Synopsis Design Complier toolkits, and estimate its power consumption based on HLMC-40 nm typical NMOS and typical PMOS fabrication process. Table II shows EMScatter tag IC consumes a total power of 106.91 μW for Wi-Fi transmissions. The logic for generating 1 Mbps 802.11b signal consumes 19.96 μW, which is close to the result of Passive Wi-Fi [28]. However, the tag only needs to wake up and transmit before crossing periods start, as transmissions at other times cannot be received. Note that a crossing period lasts for about a dozen milliseconds. Setting a reasonable duty cycle for the tag, such as 1:1000, can effectively improve its transmission power efficiency.

Triangle	Frequency Shift	Wi-Fi Modulation	**Total Power**
42.76μW	44.19μW	19.96μW	106.91μW

TABLE II: **Power of EMScatter Tag IC.**

Practical Applications. The capability of EMScatter can effectively support many critical applications that require anytime and anywhere phone-tag communication without external excitation source. For example, an in-body insulin pump could utilize EMScatter to provide glucose monitoring and alerts to mobile phones [12]; a subminiature capsule could utilize EMScatter to report drug delivery and absorption status [25], which generally need a few hundred kbps data rate and a few centimeter transmission range. These implanted applications usually require low power consumption because it is inconvenient to change batteries frequently.

IX. Conclusion

This paper presents EMScatter, a system designed to enable backscatter communication on mobile devices without the need for external excitation sources, offering a plug-and-play solution. The key idea of our system is the utilization of inherent EMR signals from mobile devices for excitation. We introduce delicate design modules, including the use of the USB interface as an EMR amplifier on the reader side and a DSS scheme at the tag side, to successfully adapt EMR—an unconventional RF source—as an excitation source. We conduct comprehensive evaluations on commodity mobile platforms to demonstrate the potential of EMScatter to support critical spontaneous tag communications.

X. Acknowledgement

We sincerely thank the anonymous reviewers for their valuable comments. We also thank Dr. Xin Lou and Kangjie Long from the PMICC at Shanghaitech University for their assistance with power analysis. This work is supported by the Guangdong Provincial Key Lab of Integrated Communication, Sensing and Computation for Ubiquitous Internet of Things (No.2023B1212010007) and NSFC 62002224.

REFERENCES

[1] EU ministers give final approval to one-size-fits-all charging port. https://ec.europa.eu/newsroom/representations/items/763031/en.

[2] Improving Wireless Coverage in Rural America. https://www.fcc.gov/news-events/blog/2016/10/27/improving-wireless-coverage-rural-america.

[3] Popular USB DWC3 Linux Driver Likely To "Never Be Finished" With Continued Adaptations. https://www.phoronix.com/news/USB-Thunderbolt-Linux-5.19.

[4] Qcacld. https://github.com/EssentialOpenSource/qcacld-3.0/tree/master.

[5] RFID Reader Store. https://www.atlasrfidstore.com/rfid-readers/.

[6] Spectral Scan. https://wireless.wiki.kernel.org/en/users/drivers/ath10k/spectral.

[7] ST RFID Reader Chip. https://www.st.com/en/nfc/st25ru3993.html.

[8] Synopsys DesignWare Core SuperSpeed USB 3.0 Controller. https://www.kernel.org/doc/html/v6.1/driver-api/usb/dwc3.html.

[9] USB 3.2 Revision 1.1 - June 2022. https://www.usb.org/document-library/usb-32-revision-11-june-2022.

[10] Wi-Fi Coexistence. https://www.silabs.com/wireless/wi-fi/wi-fi-coexistence.

[11] Ali Abedi, Farzan Dehbashi, Mohammad Hossein Mazaheri, Omid Abari, and Tim Brecht. WiTAG: Seamless WiFi Backscatter Communication. In *Proceedings of the Annual Conference of the ACM Special Interest Group on Data Communication on the Applications, Technologies, Architectures, and Protocols for Computer Communication*, SIGCOMM '20, page 240–252, 2020.

[12] Tadej Battelino and Thomas Danne. Clinical Targets for Continuous Glucose Monitoring Data Interpretation: Recommendations From the International Consensus on Time in Range. *Diabetes Care*, 42(8):1593–1603, 06 2019.

[13] Dinesh Bharadia, Kiran Raj Joshi, Manikanta Kotaru, and Sachin Katti. BackFi: High Throughput WiFi Backscatter. In *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, SIGCOMM '15, page 283–296, 2015.

[14] Dinesh Bharadia, Emily McMilin, and Sachin Katti. Full duplex radios. In *Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM*, SIGCOMM '13, page 375–386, 2013.

[15] Ruirong Chen and Wei Gao. TransFi: emulating custom wireless physical layer from commodity WiFi. In *Proceedings of the 20th Annual International Conference on Mobile Systems, Applications and Services*, MobiSys '22, page 357–370, 2022.

[16] Zicheng Chi, Xin Liu, Wei Wang, Yao Yao, and Ting Zhu. Leveraging Ambient LTE Traffic for Ubiquitous Passive Communication. In *Proceedings of the Annual Conference of the ACM Special Interest Group on Data Communication on the Applications, Technologies, Architectures, and Protocols for Computer Communication*, SIGCOMM '20, page 172–185, 2020.

[17] Manideep Dunna, Miao Meng, Po-Han Wang, Chi Zhang, Patrick Mercier, and Dinesh Bharadia. SyncScatter: Enabling WiFi like synchronization and range for WiFi backscatter Communication. In *18th USENIX Symposium on Networked Systems Design and Implementation (NSDI 21)*, pages 923–937, 2021.

[18] Steven W Ellingson. *Electromagnetics, Volume 1*. VT Publishing, 2018.

[19] Xiuzhen Guo, Yuan He, Zihao Yu, Jiacheng Zhang, Yunhao Liu, and Longfei Shangguan. RF-Transformer: A Unified Backscatter Radio Hardware Abstraction. In *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking*, MobiCom '22, page 446–458, 2022.

[20] Xiuzhen Guo, Longfei Shangguan, Yuan He, Nan Jing, Jiacheng Zhang, Haotian Jiang, and Yunhao Liu. Saiyan: Design and Implementation of a Low-power Demodulator for LoRa Backscatter Systems. In *19th USENIX Symposium on Networked Systems Design and Implementation (NSDI 22)*, pages 437–451, 2022.

[21] Xiuzhen Guo, Longfei Shangguan, Yuan He, Jia Zhang, Haotian Jiang, Awais Ahmad Siddiqi, and Yunhao Liu. Aloba: Rethinking ON-OFF Keying Modulation for Ambient LoRa Backscatter. In *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*, SenSys '20, page 192–204, 2020.

[22] Jennifer Halstead. A Breakdown Of 7 RFID Costs, From Hardware To Implementation. https://www.airfinder.com/blog/rfid-cost. 2020.

[23] John Illingworth and Josef Kittler. A survey of the Hough Transform. *Computer vision, graphics, and image processing*, 44(1):87–116, 1988.

[24] Vikram Iyer, Vamsi Talla, Bryce Kellogg, Shyamnath Gollakota, and Joshua Smith. Inter-Technology Backscatter: Towards Internet Connectivity for Implanted Devices. In *Proceedings of the 2016 ACM SIGCOMM Conference*, SIGCOMM '16, page 356–369, 2016.

[25] Abhinanda Kar, Nadim Ahamad, Mahima Dewani, Lisha Awasthi, Runali Patil, and Rinti Banerjee. Wearable and implantable devices for drug delivery: Applications and challenges. *Biomaterials*, 283:121435, 2022.

[26] Mohamad Katanbaf, Anthony Weinand, and Vamsi Talla. Simplifying Backscatter Deployment: Full-Duplex LoRa Backscatter. In *18th USENIX Symposium on Networked Systems Design and Implementation (NSDI 21)*, pages 955–972, 2021.

[27] Bryce Kellogg, Aaron Parks, Shyamnath Gollakota, Joshua R. Smith, and David Wetherall. Wi-Fi Backscatter: Internet Connectivity for RF-Powered Devices. In *Proceedings of the 2014 ACM Conference on SIGCOMM*, SIGCOMM '14, page 607–618, 2014.

[28] Bryce Kellogg, Vamsi Talla, Shyamnath Gollakota, and Joshua R Smith. Passive Wi-Fi: Bringing Low Power to Wi-Fi Transmissions. In *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*, pages 151–164, 2016.

[29] Vincent Liu, Aaron Parks, Vamsi Talla, Shyamnath Gollakota, David Wetherall, and Joshua R. Smith. Ambient Backscatter: Wireless Communication out of Thin Air. In *Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM*, SIGCOMM '13, page 39–50, 2013.

[30] Xin Liu, Zicheng Chi, Wei Wang, Yao Yao, Pei Hao, and Ting Zhu. Verification and Redesign of OFDM Backscatter. In *18th USENIX Symposium on Networked Systems Design and Implementation (NSDI 21)*, pages 939–953, 2021.

[31] Muhammad Sarmad Mir, Minhao Cui, Borja Genoves Guzman, Qing Wang, Jie Xiong, and Domenico Giustiniano. LeakageScatter: Backscattering LiFi-leaked RF Signals. In *Proceedings of the Twenty-Fourth International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing*, MobiHoc '23, page 290–299, 2023.

[32] Yao Peng, Longfei Shangguan, Yue Hu, Yujie Qian, Xianshang Lin, Xiaojiang Chen, Dingyi Fang, and Kyle Jamieson. PLoRa: a passive long-range data network from ambient LoRa transmissions. In *Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication*, SIGCOMM '18, page 147–160, 2018.

[33] Yifan Yang, Longzhi Yuan, Jia Zhao, and Wei Gong. Content-Agnostic Backscatter from Thin Air. In *Proceedings of the 20th Annual International Conference on Mobile Systems, Applications and Services*, MobiSys '22, page 343–356, 2022.

[34] Maolin Zhang, Si Chen, Jia Zhao, and Wei Gong. Commodity-level BLE backscatter. In *Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services*, MobiSys '21, page 402–414, 2021.

[35] Pengyu Zhang, Dinesh Bharadia, Kiran Joshi, and Sachin Katti. HitchHike: Practical Backscatter Using Commodity WiFi. SenSys '16, page 259–271, 2016.

[36] Pengyu Zhang, Colleen Josephson, Dinesh Bharadia, and Sachin Katti. FreeRider: Backscatter Communication Using Commodity Radios. In *Proceedings of the 13th International Conference on Emerging Networking EXperiments and Technologies*, CoNEXT '17, page 389–401, 2017.

[37] Pengyu Zhang, Mohammad Rostami, Pan Hu, and Deepak Ganesan. Enabling Practical Backscatter Communication for On-body Sensors. In *Proceedings of the 2016 ACM SIGCOMM Conference*, pages 370–383, 2016.

[38] Jia Zhao, Wei Gong, and Jiangchuan Liu. X-Tandem: Towards Multi-hop Backscatter Communication with Commodity WiFi. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*, MobiCom '18, page 497–511, 2018.

[39] Renjie Zhao, Fengyuan Zhu, Yuda Feng, Siyuan Peng, Xiaohua Tian, Hui Yu, and Xinbing Wang. OFDMA-Enabled Wi-Fi Backscatter. In *The 25th Annual International Conference on Mobile Computing and Networking*, MobiCom '19, 2019.

[40] Fengyuan Zhu, Yuda Feng, Qianru Li, Xiaohua Tian, and Xinbing Wang. DigiScatter: Efficiently Prototyping Large-Scale OFDMA Backscatter Networks. In *Proceedings of the 18th International Conference on Mobile Systems, Applications, and Services*, MobiSys '20, page 42–53, 2020.