Leveraging Ambient LTE Traffic for Ubiquitous Passive Communication

Zicheng Chi*
zicheng1@umbc.edu
University of Maryland, Baltimore County

Xin Liu*
xinliu1@umbc.edu
University of Maryland, Baltimore County

Wei Wang
ax29092@umbc.edu
University of Maryland, Baltimore County

Yao Yao
of90379@umbc.edu
University of Maryland, Baltimore County

Ting Zhu
zt@umbc.edu
University of Maryland, Baltimore County

ABSTRACT

To support ubiquitous computing for various applications (such as smart health, smart homes, and smart cities), the communication system requires to be ubiquitously available, ultra-low-power, high throughput, and low-latency. A passive communication system such as backscatter is desirable. However, existing backscatter systems cannot achieve all of the above requirements. In this paper, we present the first LTE backscatter (LScatter) system that leverages the continuous LTE ambient traffic for ubiquitous, high throughput and low latency backscatter communication. Our design is motivated by our observation that LTE ambient traffic is continuous (v.s. bursty and intermittent WiFi/LoRa traffic), which makes LTE ambient traffic a perfect signal source of a backscatter system. Our design addresses practical issues such as time synchronization, phase modulation, as well as phase offset elimination. We extensively evaluated our design using a testbed of backscatter hardware and USRPs in multiple real-world scenarios. Results show that our LScatter's performance is consistently orders of magnitude better than WiFi backscatter in all the above scenarios. For example, LScatter's throughput is 13.63Mbps, which is 368 times higher than the latest ambient WiFi backscatter system [54]. We also demonstrate the effectiveness of our system using two real-world applications.

CCS CONCEPTS

• **Networks** → **Network architectures**; • **Hardware** → **Wireless devices**;

KEYWORDS

Backscatter, Internet of things, LTE

*Authors contributed equally to the paper

SIGCOMM '20, August 10–14, 2020, Virtual Event, NY, USA

ACM ISBN 978-1-4503-7955-7/20/08…$15.00
https://doi.org/10.1145/3387514.3405861

ACM Reference Format:
Zicheng Chi, Xin Liu, Wei Wang, Yao Yao, and Ting Zhu. 2020. Leveraging Ambient LTE Traffic for Ubiquitous Passive Communication. In *Annual conference of the ACM Special Interest Group on Data Communication on the applications, technologies, architectures, and protocols for computer communication (SIGCOMM '20), August 10–14, 2020, Virtual Event, NY, USA.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3387514.3405861

1 INTRODUCTION

As a passive communication system, backscatter provides a promising low-power method for connecting Internet-of-Thing (IoT) devices to realize ubiquitous computing. Researchers have proposed various systems by backscattering WiFi [27, 28, 51, 54, 56], Bluetooth [23], ZigBee [19, 55], or LoRa [21, 38, 42] signals.

In order to achieve ubiquitous, high throughput, and long-range backscatter communication so that the industry can easily adopt the backscatter techniques and widely deploy them, the backscatter system's excitation signal is also very important. Ideally, the excitation signal has to satisfy the following requirements:
(1) **Ambient excitation signal.** The backscatter system should leverage the ambient signals generated by existing infrastructure, instead of requiring a designated excitation signal generator (e.g., RFID reader) which continuously occupies extra radio spectrum and increases the deployment complexity and costs.
(2) **Continuous excitation signal.** In the time domain, the excitation signal should be continuous so that the backscatter system can reflect the excitation signal whenever it wants to piggyback the data to support various applications in smart health, smart homes, and smart cities.
(3) **Ubiquitous coverage.** In the spatial domain, the excitation signal that is used by the backscatter system should be ubiquitously available so that the industry developers do not need to worry about how to deploy the system that generates the ambient excitation signal to cover a specific area before deploying the backscatter system. Therefore, the backscatter system can be easily moved from one place to another place.

If the above requirements were satisfied, we could observe a faster and wider adoption of backscatter techniques by the industry to support various IoT applications in smart and connected communities with lower deployment and maintenance costs. For example, monitoring the biometrics of users for smart authentication in modern cybersecurity; detection of heart or breath failure

Table 1: Features of existing backscatters' excitation signal

Technology	Ambient	Continuous	Ubiquitous
NICScatter [51]	✓		
ReMix [45]			
PLoRa [38]	✓		
LoRa backscatter [42]		✓	
Netscatter [21]		✓	
FlipTracer [25]			
FS-Backscatter [55]	✓		
WiFi backscatter [27]	✓		
MOXcatter [56]	✓		
X-Tandem [57]	✓		
FreeRider [54]	✓		
HitchHike [53]		✓	
BackFi [16]		✓	
Passive WiFi[28]		✓	
Interscatter[23]		✓	
LScatter	✓	✓	✓

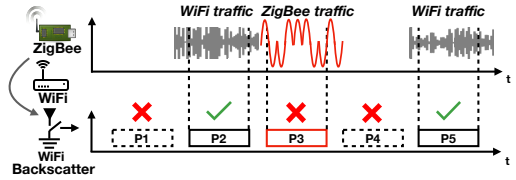


Figure 1: Limitations of Existing WiFi backscatter systems

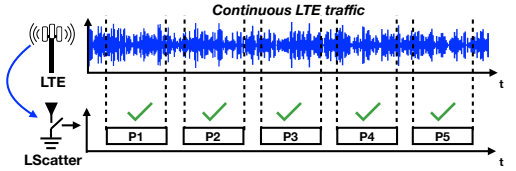


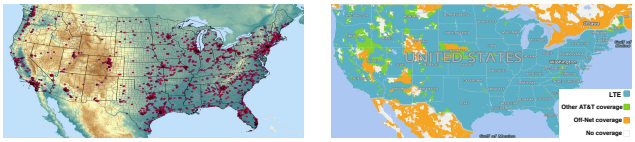
Figure 2: Our LScatter can piggyback on the continuous LTE traffic.

in smart health; and monitoring of vehicles and pedestrian levels to optimize driving and walking routes in smart cities.

However, to the best of our knowledge, as shown in Table 1, no existing backscatter systems utilize the excitation signal that satisfies the above three requirements to achieve ubiquitous, high throughput, and long-range backscatter communication. Interscatter [23], Passive WiFi [28], BackFi [16], LoRa backscatter [42], and Netscatter [21] require a dedicated continuous wave transmitter to send an excitation signal (i.e., a constant sinusoidal tone) as the carrier and the power source for their backscatter transmissions. This excitation signal continuously occupies extra spectrum in overcrowded industrial, scientific and medical (ISM) bands and increases the deployment complexity and costs.

To address this issue, researchers proposed FreeRider [54], MOXcatter [56], X-Tandem [57], FS-Backscatter [55], and PLoRa [38] that leverage the ambient WiFi or LoRa signals as the excitation signal. However, since WiFi channels share the ISM band with other devices such as ZigBee and Bluetooth, ambient WiFi signals are always bursty and intermittent. Therefore, as shown in Figure 1, existing WiFi backscatter systems have at least two limitations: i) they may not have an ambient WiFi signal to piggyback the packets $P1$ and $P4$; ii) they may piggyback their packet $P3$ on the ZigBee traffic which cannot be correctly decoded by a WiFi receiver. PLoRa backscatter also has the same limitations because LoRa channels are also shared with other devices.

In contrast to bursty and intermittent ambient WiFi and LoRa signals, ambient LTE signals are continuous. Therefore, we propose to design a backscatter that can piggyback the packets on the continuous LTE traffic. The basic idea is illustrated in Figure 2. Another advantage of using ambient LTE signals as the excitation



(a) LoRa Coverage (only red dotted areas are covered) **(b) LTE Coverage (most of the places are covered)**

Figure 3: Comparison between LoRa and LTE Coverage Maps (source: LoRaWAN [6]) and www.att.com [5]

signal is that LTE networks have been widely deployed to provide ubiquitous coverage for smartphones, while LoRaWAN networks are only deployed in very limited locations (shown in Figure 3).

Given the advantages of ambient LTE signals, in this paper, we propose LScatter, which is the first LTE backscatter design that leverages the ambient LTE traffic for ubiquitous, high throughput, and long-range backscatter communication. Specifically, our main contributions are as follows:

(i) We designed a low-power ambient LTE signal synchronization circuit on the backscatter side, which can leverage LTE's unique primary synchronization signal to synchronize the backscatter with the ambient LTE traffic without affecting the critical information (e.g., primary and secondary synchronization signals [11]) in the original LTE traffic.

(ii) We proposed a modulation method, which addressed the low throughput issue caused by the LTE signal's much longer time duration. This method modulates the backscatter data at the LTE's basic-timing unit level (i.e., the smallest time unit used for modulation). By doing this, we can significantly improve the throughput. The highest throughput in our evaluation is 13.63 Mbps, which is 3 orders of magnitude higher than the latest WiFi backscatter [54].

(iii) To utilize the entire bandwidth of an OFDM signal, we need to resolve the phase offset caused by the physical channel and asynchronization between the tag and sender. By leveraging the reference signals on different subcarriers in the original LTE physical layer, we resolved the phase offset issue, which introduces demodulation errors at the receiver side. Therefore, the receiver can demodulate the backscatter signal at the *ns* time granularity.

(iv) We build a hardware prototype of the proposed LScatter backscatter system and extensively evaluated our system in various real-world scenarios. Results show that our LScatter's performance is consistently orders of magnitude better than WiFi backscatter in all of the above scenarios.

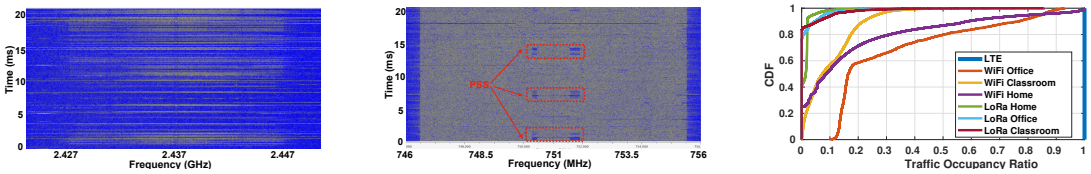
2 MOTIVATION

We argue that neither WiFi nor LoRa signal is a good carrier for backscattering because of the following observation, which serves as the foundation of this work:

Observation 1: *The frequency band of WiFi (or LoRa) shows a bursty, intermittent, and heterogenous traffic pattern while the frequency band of LTE shows continuous and homogeneous traffic pattern.*

2.1 On-site Measurements and Analysis

We measured a common WiFi channel and a typical LTE band by using a spectrum analyzer. The spectrograms for WiFi and LTE are shown in Figure 4a and Figure 4b, respectively. From Figure 4a, we can observe that the WiFi's traffic pattern is not only bursty



(a) Spectrogram of WiFi (b) Spectrogram of LTE (c) CDF of Traffic Rate

Figure 4: Traffic Comparison among LoRa, WiFi and LTE. (a) Gray color indicates higher signal strength while blue color indicates lower signal strength. (b) The highlighted part is LTE's primary synchronization signal (period=5ms) which will be used for synchronization. (c) The figure shows the data for a whole week. Note that LTE has the same curve at different places.

(the bursty traffic pattern is also observed and well studied by a few works [29, 43, 44]) but intermittent as well. On the contrary, the traffic of LTE is continuous (Figure 4b). To evaluate the traffic pattern in a larger time scale, we conducted on-site measurements in three different places (residential home, office, and classroom) throughout a few days (including rush hour and night). Figure 4c shows the CDF of the traffic rate (defined as radio of wireless signal presenting period to a certain period) for WiFi, LoRa as well as LTE. By looking at the figure, LoRa has very low traffic rate (the traffic rate is only 0.02 for most of the time) across three different places. This is because LoRa technique is rarely deployed. For WiFi, the curves vary from place to place. However, even in the heaviest traffic situation (i.e., office), the traffic rate is still less than 0.5 for 80% of the time and less than 0.7 for 90% of the time. In the contrast, the LTE shows a completely different trend that the traffic is covered all the time at three of the places.

The main reason of this huge difference is that the WiFi (or LoRa) channel is shared by other devices (e.g., Bluetooth and ZigBee). Thus, random access protocol (e.g., ALOHA or CSMA) is used for fair access. On the contrary, the LTE band is dedicated (e.g., a band is dedicated for eNodeB-to-UE transmission). Therefore, a continuous OFDM signal is used to carry data as well as the control message.

2.2 Hindrance to Backscatter

Back to the backscatter system, it is very hard for the low power backscatter tag to work with WiFi and LoRa traffic in real-world because of the following two reasons:

• **The bursty and intermittent traffic pattern makes the backscatter system unreliable.** From the backscatter's point of view, an intermittent and bursty traffic pattern means the carrier signal is unpredictable. To piggyback information on the signal, the backscatter needs to detect the signal. However, it is very difficult for a low power backscatter tag to detect the signal because there are too many factors (e.g., distance, channel fading, interference) affecting the accuracy, especially for a wide band and sophisticated modulated signals (e.g. 20 MHz OFDM signal).

• **The channel is shared with heterogeneous devices, which makes the backscattering even harder.** The WiFi (or LoRa) channel is not a dedicated channel. Different protocols (such as ZigBee and BLE) share the same frequency band. Even assuming multiple backscattering schemes (which correspond to different protocols) are integrated in the backscatter tag, since it is very hard for a low power tag to recognize the bandwidth and modulation scheme of the incoming signals, the backscatter cannot choose the right backscattering scheme to reflect data. For example, a voltage based simple signal detector is not able to accurately recognize whether the signal in the air is a WiFi, ZigBee, or BLE signal.

2.3 Opportunity and Challenges for LTE Backscatter

Based on Observation 1, we propose to entirely utilize the ambient LTE signals for resilient backscatter communication. However, none of the current backscatter techniques can apply on LTE backscatter because of the following challenges:

C1. How to ensure critical information (i.e., primary and secondary synchronization signals [11]) remains unmodified after backscattering? The continuous LTE signal periodically embeds critical information primary (PSS) [11] which can provide the starting point for Fast Fourier transform (FFT). If this key information is accidentally modified by the backscatter tag, the receiver cannot conduct FFT and demodulate the signal.

Our solution: Instead of demodulating and recognizing the LTE signal on a low power backscatter tag, our solution is to synchronize the backscatter with the LTE signal by using a low power consumption circuit. The circuit is designed according to the primary synchronization signal (PSS)'s three features i) PSS is a known Zadoff-Chu sequence [7]; ii) PSS appears every 5 ms (200 Hz); and iii) the bandwidth of PSS is narrow (0.93 MHz) and fixed (e.g., a 20 MHz LTE signal uses the same PSS as that of 1.4 MHz LTE signal). After synchronization, the backscatter tag avoids modulating when critical information is transmitting.

C2. How to modulate the LTE signal at backscatter side to achieve high throughput? Current OFDM based backscatters [54, 56] modulate at symbol level (i.e., backscatter embeds 1 bit data every two or more symbols), which yields tens of Kbps throughput. Since LTE uses a much longer symbol duration (i.e., 66.7 μs) than WiFi (i.e., 4 μs), the throughput will significantly drop if applying similar technique.

Our solution: Instead of modulating at the symbol level (i.e., 66.7 μs), we propose a new modulation method specifically for the long-symbol-duration LTE signal. In this method, we embeds 1 bit information per tens of ns. The highest throughput in our evaluation is 13.63 Mbps, which is 3 orders of magnitude higher than the latest WiFi backscatter system.

C3. How to demodulate the ns level hybrid LTE signal at the UE side? As described in challenge **C2**, backscatter embeds information at a high speed. To demodulate these ns level signals, we need to solve the phase offset introduced by not only backscatter but also the physical channel.

Our solution: Since the phase offset is varying on different subcarriers, to overcome this challenge, we utilize the reference signals on different subcarriers in the original LTE PHY layer to eliminate the phase offset. By solving this problem, the backscatter data can be demodulated correctly.

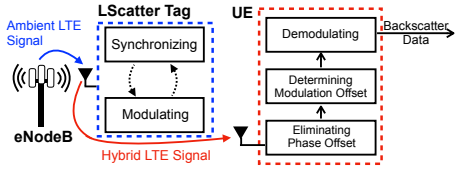


Figure 5: The system architecture of LScatter.

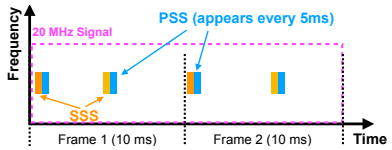


Figure 6: PSS (used for our synchronization) in LTE signal with three features: i) everyone is identical (i.e., a pre-defined Zadoff-Chu sequence [7]; ii) the signal appears every 5 ms (200 Hz); iii) the bandwidth of this signal is narrow (0.93 MHz) and fixed (e.g., a 20 MHz LTE signal uses the same PSS as that of 1.4 MHz LTE signal).)

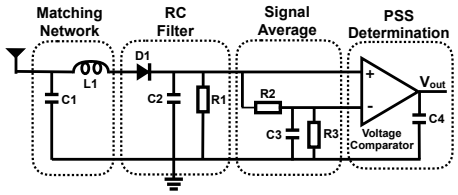


Figure 7: Ambient LTE Signal Synchronization Circuit

To utilize the ambient LTE signal for backscattering and address the above challenges , we propose LScatter. In a nutshell (shown in Figure 5), the LSscatter tag, which includes synchronizing (details introduce in Section 3.1) and modulating (details introduce in Section 3.2) modules, piggybacks its own data on ambient LTE signal from an eNodeB (Evolved NodeB is a term used for LTE base station). The User Equipment (UE) picks up the reflected hybrid LTE signal and demodulates the backscatter data (details introduce in Section 3.3).

3 DESIGN

In this section, we first explain how LScatter synchronizes with the LTE signal to avoid changes to critical information. We next introduce how LScatter piggybacks data on LTE signals using basic-timing unit modulation. We finally present how to recover backscatter data from frequency-domain subcarriers at UE side.

3.1 Synchronization

The purpose of synchronization described in this section is to avoid critical information (e.g. primary synchronization signal [11]) being modified by the backscatter tag. This signal provides the starting point for conducting FFT and demodulation at the UE. The basic idea is using a low-power circuit to coarsely synchronize (at millisecond level) with a periodical signal in LTE. We will discuss how to deal with the phase offset (at nanosecond level) between backscatter tag and LTE signal in Section 3.3.1.

A naive solution is to utilize a high power consumption module to continually calculate the correlation of the LTE signal and synchronize the tag. However, the energy-constrained tag cannot afford it. Instead, we utilize the features of the primary synchronization signal (PSS) in LTE signals for synchronization that we designed a low power circuit to detect and synchronize the tag with the LTE signal.

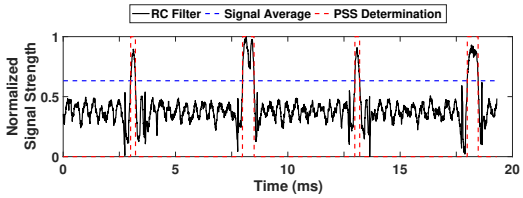


Figure 8: Outputs of Each Stage for the Sync Circuit

As shown in Figure 6, the PSS signal is periodically (period=5ms) embedded into the frame. For each PSS signal, it is a pre-defined Zadoff-Chu sequence [7]. Regardless of the bandwidth of LTE signal, the bandwidth of the PSS keeps the same (0.93 MHz). Based on these features, a low power circuit as shown in Figure 7 is designed to detect and synchronize the tag with LTE signal. Specifically, after the RF signal is picked up by the antenna, an impedance matching network ($C1$ and $L1$) is used to maximize the incoming signal. Then, the signal goes through the RC filter ($D1$, $C2$, and $R1$) which outputs the envelop of the high frequency signal.

To detect the PSS in LTE, the main parameter (i.e., time constant $\tau = R_1C_2$) needs to satisfy: $1/f_{pss} < \tau < 1/f_c$, where f_{pss} is the appearing frequency of PSS which equals to 200 Hz. f_c is the carry wave's frequency (e.g., LTE usually uses hundreds of MHz carry wave). Since f_{pss} is far less than f_c. τ can be easily chosen. The black curve in Figure 8 shows a sample output of the RC filter. We can observe that, the PSS (appearing every 5 ms) is outstanding. To capture the PSS signal by FPGA, instead of using an ADC (which is energy-consuming to the low power tag) to sample the signal, we use a voltage comparator to determine whether the PSS signal is coming. The first input of the comparator is fed by the output of the RC filter. The second input is connected to a simple averaging circuit ($R2$, $C3$, and $R3$) which averages the output of the RC filter. The comparator outputs a logical high when the PSS signal is appearing. In Figure 8, the blue dashed line shows the reference signal from the averaging circuit. And the red dashed line shows the output of the comparator, which is fed into the FPGA.

After detecting the PSS signals, the backscatter tag can avoid the PSS and SSS (as shown in Figure 6, the locations of PSS and SSS signals are fixed in a frame) by transmitting square waves (without phase change for modulation backscatter data). In this way, the PSS and SSS can be ensured passing to UE without modification.

Though this low-power circuit is not capable of providing precise synchronization performance, ms level (we will show the experimental results in the evaluation section) is enough to avoid the critical information. The reason is that the useful modulation occupies 54.6% of a symbol duration, and the rest is filled by continuous square waves (details provided in Section 3.2.3). This redundancy leaves plenty of space for synchronization inaccuracy.

We note that the synchronization does not need to be very precise (for keeping low energy consumption) because around 54% of the time during a symbol can be modulated by backscatter (details provide in Section 3.2.3), which means the remaining 46% of the time need to transmit square waves.

3.2 Backscatter Modulation

In this section, we first explain why we cannot adopt the existing backscatter modulation techniques. We then provide our solution that embeds the backscatter data in every basic-timing unit of the

LTE signal. At last, we give a practical design to show how to avoid embedding backscatter data into the cyclic prefix.

3.2.1 The limitation of existing techniques. Existing backscatter modulation techniques can be divided into three categories and they are not suitable for LTE backscatter.

Category 1. Some backscatter techniques like Interscatter [23] and Passive WiFi [28] are used to generate a single tone carrier for backscattering by one backscatter tag but they cannot be used for multi-subcarrier LTE signals. This is because LTE requires a high power consuming inverse fast Fourier transform (IFFT) module to create multiple subcarriers. Due to the low power budget, it is difficult to run an IFFT on a backscatter tag.

Category 2. Recent work [58] proposed to use 48 backscatter tags to generate 48 subcarriers for OFDM based WiFi backscattering. However, the 20MHz LTE has 1200 subcarriers and it is very hard to cooperate 1200 tags to generate a LTE signal. Besides, if each tag generates a subcarrier at a specific frequency bin, 1200 slightly different oscillators need to be implemented, which is impractical.

Category 3. The techniques like X-Tandem [56, 57] modulate two WiFi symbols to convey a backscatter bit in time domain, which yields tens of Kbps throughput. However, the throughput will significantly drop if applying similar technique to LTE backscatter. This is because LTE uses a much longer symbol (i.e., 66.7 μs) than WiFi (i.e., 4 μs).

3.2.2 Modulation for LTE backscatter. We present the first LTE backscatter modulation scheme that embeds backscatter data by *changing the phases of the LTE signals in different basic-timing units.* The key insight is that without the need of a higher frequency oscillator (which introduces higher power consumption), the basic-timing units scheme uses a much higher granularity (i.e., at the level of ns) than a symbol duration (i.e., at the level of μs), which can achieve significantly higher performance. Before presenting the modulation method, we first explain how the basic-timing units construct the LTE signal in time-domain.

One LTE frame (in the period of 10 ms) is divided into 20 equally sized slots. Each slot consists of a number of OFDM symbols. The OFDM symbol consists of two major components: the useful symbol and the cyclic prefix (CP). We will discuss how to deal with CP in Section 3.2.3. As shown in Figure 9, the useful symbol can be represented by multiplication of the baseband signal and the carrier wave. The baseband signal is generated by OFDM module as follows:

$$x_n = \frac{1}{K}\sum_{k=0}^{K-1} X_k e^{j2\pi kn/K} \quad , \quad n = 0, ..., K-1 \tag{1}$$

where X_k is the value of each subcarrier and K is the FFT size. Equation 1 shows that the baseband signal is broken into K units. Since K units construct a useful symbol, each unit is a basic-timing unit in the time-domain and has a duration of $T_s = \frac{66.7\mu s}{K}$, where $66.7\mu s$ is the useful symbol duration. In the nth unit, the baseband signal x_n is a constant value. When x_n is up converted to a carrier frequency f_c, the LTE signal in this unit can be expressed as:

$$S_{lte}(n) = x_n e^{j2\pi f_c t} \tag{2}$$

By using Equation 2, the ambient LTE signal is expressed as the combination of signals in different basic-timing units. Therefore, we can embed backscatter data into the LTE signal by changing the phases of the signals in different units while still preserving the hybrid signal compatible with the LTE standard.

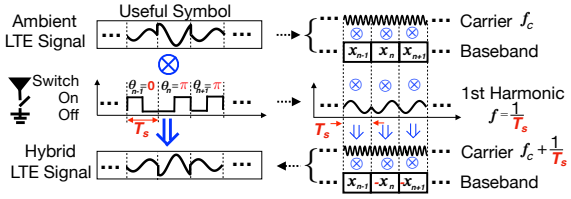


Figure 9: LScatter's modulation. When the tag modulates the ambient LTE signal at the basic-timing unit level, the phase of the ambient signal in each timing unit T_s is changed to embed the backscatter data. To minimize interference with original LTE signals, the carrier frequency is shifted to $f_c + \frac{1}{T_s}$ which is out of original LTE band.

To modulate the phases in different units, the key is to set the backscatter switching cycle the same as the timing unit T_s and simultaneously change the initial phase (i.e., either 0 or π) of each switch action according to the backscatter data. We define that if the transmitted data is '1' or '0', the initial phase is 0 or π, respectively. Figure 9 shows an example, the backscatter is transmitting data $'100'$, the initial phases of three switch actions are $[0, \pi, \pi]$. Since the switch is controlled by square waves, the switch actions are a serial of square waves which are used to modulate the phase of the LTE signals. The square wave can be presented by Fourier series:

$$S_{tag}(n) = 0.5 + \frac{2}{\pi}\sum_{m=1,2,3,..}^{\infty} \frac{sin(\frac{\pi}{2}m)}{m} cos(2\pi m \frac{t}{T_s} + \theta_n) \tag{3}$$

where m is the order number of the harmonic, n is the square wave number and $\theta_n \in \{0, \pi\}$ is the initial phase of the nth square wave. We observed that the even order harmonics (i.e., $m = 2, 4, 6, ...$) are all zeros. The third and fifth order harmonics (i.e., $m = 3, 5$) can be canceled by using multi-level signal quantification (introduced in [42] and [58]). The higher odd order harmonics (i.e., $m = 5, 7, ..$) attenuate quickly along with the increasing of the order number. Therefore, the first order harmonic ($m = 1$) cosine wave (used to carry backscatter data) in the Fourier series is given by:

$$S_{tag}(n) = cos(2\pi \frac{t}{T_s} + \theta_n)$$

From the ambient signal $S_{lte}(n)$ and the first harmonic $S_{tag}(n)$, the hybrid signal can be calculated by using the following equation:

$$S_{lte} \times S_{tag}(n) = \frac{1}{2} x_n (e^{j\theta_n} e^{j2\pi(f_c + \frac{1}{T_s})t} + e^{-j\theta_n} e^{j2\pi(f_c - \frac{1}{T_s})t}) \tag{4}$$

Equation 4 shows that the phase of the ambient baseband signal x_n is changed according to $e^{j\theta_n}$ and the carrier frequency is shifted by $\frac{1}{T_s}$ away from the original band to minimize the mutual interference with original LTE signal. From Figure 9, we can observe that the hybrid signal modulated by phase 0 has the same phase as the ambient signal, and the hybrid signal modulated by π rotates 180 degrees. We note that $\frac{1}{T_s}$ is greater than the ambient LTE bandwidth. Thus, the strong interference from the original LTE signal can be minimized.

The modulation produces two sidebands ($f_c + \frac{1}{T_s}$ and $f_c - \frac{1}{T_s}$), one is the desired whereas the other one is unwanted as shown in Equation 4. The unwanted sideband can be easily eliminated by

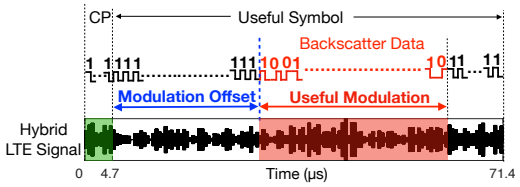


Figure 10: Prevent backscatter data from falling into CP.

making the signal have a negative copy on the unwanted sideband and have the same copy on the desired sideband, which has been introduced in HitchHike [53].

3.2.3 Dealing with CP and ISI. At the UE side, OFDM removes the cyclic prefix (CP) to prevent inter symbol interference (ISI). If the backscatter data falls into the CP, it will be removed as well, which causes demodulation failure. Thus, we need to ensure that all the data falls into the useful symbols. This is non-trivial because we cannot use a high-power circuit to synchronize the backscatter tag with the LTE signal (as described in Section 3.1) to locate the CP. To solve this problem, we utilize the redundancy in LTE system. As shown in Figure 10, for a 20MHz LTE signal, the total number of the basic-timing units in a single symbol (the symbol duration is 71.4 μs) is 2196 which include the CP of 144 units (green shaded part). Since there are only 1,200 subcarriers carrying the LTE data and 1,200 subcarriers are less than 2196 basic-timing units, there is a redundancy. To ensure compatibility with the LTE protocol, the number of basic-timing units used to carry backscatter data should be equal to the number of subcarriers in LTE signal. Therefore, the number of useful basic-timing units is 1200 (the red shaded part in Figure 10) during one LTE symbol. That means the useful modulation occupies $\frac{1200}{2196} \approx 54.6\%$ of a symbol duration. Since the CP occupies $\frac{144}{2196} \approx 6.6\%$, we have the remaining 1-54.6%-6.6% = 38.8% of a symbol duration, i.e., 27.7 μs, to tolerate the modulation offset (which is highlighted in blue color) caused by the low power circuit for coarse synchronization. We will introduce how to deal with the modulation offset at the UE in Section 3.3.2. Other than the useful modulation period, LScatter transmits continuous square waves (i.e., data '1'). It is worth noting that since the useful modulation occupies 54.6% of a symbol duration, and the rest is filled by continuous square waves (i.e., data '1'), there are time gaps among symbols to minimize the ISI.

3.3 Backscatter Demodulation

In this section, we explain how to demodulate the backscatter data from the hybrid LTE signal. In contrast to the existing demodulation techniques which sequentially demodulate the backscatter data at time-domain, our demodulation method is to parallelly demodulate the backscatter data from LTE signal's subcarriers at frequency-domain. The challenge is how to eliminate the phase offset (i.e., the offset within one basic-timing unit) and determine modulation offset (i.e., the offset within one symbol).

3.3.1 Eliminating phase offset. In this section, we first analyze the root cause of the phase offset. Then, we present the corresponding elimination technique.

The delay response of the synchronization signal and physical channel between backscatter tag and UE cause a synthesized phase offset, which affects the demodulation. Ideally, each square wave

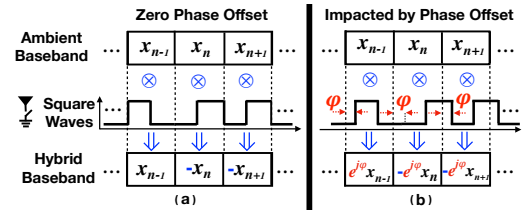
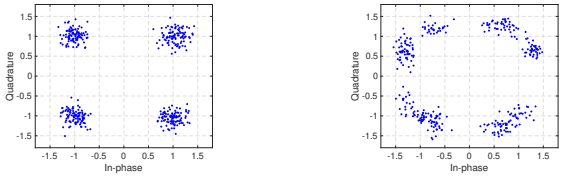


Figure 11: Due to the delay response of the synchronization, a phase offset between the square wave and the corresponding ambient baseband signal occurs.



(a) The ideal constellation **(b) Phase offset impacted**

Figure 12: The constellation impacted by the phase offset rotates certain degrees compared with the idea one.

should be edge aligned with an existing ambient LTE signal in LScatter's modulation (shown in Figure 11a). However, due to the delay response of the synchronization signal and physical channel, a phase offset φ occurs (as shown in Figure 11b). Since each cycle of square waves equals the basic-timing unit T_s (described in Section 3.2.2), the phase offset φ is the same for different basic-timing units. Therefore, the hybrid baseband signal impacted by the phase offset can be represented by multiplying the ideal hybrid baseband signal ($x_n e^{j\theta_n}$) and the phase offset ($e^{j\varphi}$) as $x_n e^{j(\theta_n+\varphi)}$.

After the impacted hybrid baseband signals $x_n e^{j(\theta_n+\varphi)}$ ($n \in \{0, ..., K-1\}$) are fed into the OFDM module at the UE side, the demodulated subcarrier values can be represented as:

$$Y_k = e^{j\varphi} \sum_{n=0}^{K-1} x_n e^{j\theta_n} e^{-j2\pi nk/K} \quad , \quad k = 0, ..., K-1 \tag{5}$$

Equation 5 shows that the backscatter information θ_n has been reflected in the demodulated subcarrier values Y_k, but the phase offset φ also exists. Figure 12 shows two snapshots of the demodulated constellations at the UE side. We can observe that the constellation impacted by the phase offset rotates certain degrees compared with the ideal one.

To eliminate the impact of the phase offset, LScatter utilizes the reference signal Y_r (which are a few pre-defined bits spread on different subcarriers) in the original LTE PHY layer to compensate the phase offset. We take the conjugate of reference signal Y_r^* and multiply the data subcarriers:

$$Y_k Y_r^* = (\cancel{e^{j\varphi}} \sum_{n=0}^{K-1} x_n e^{j\theta_n} e^{\frac{-j2\pi nk}{K}})(\cancel{e^{-j\varphi}} \sum_{n=0}^{K-1} x_n^* e^{-j\theta_n} e^{\frac{j2\pi nr}{K}}) \tag{6}$$

where x_n^* is the conjugate of x_n, $k \in \{0, ..., K-1\}$ and $k \neq r$.

Equation 6 demonstrates that the phase offset φ is eliminated by the reference signal. Moreover, Equation 6 provides the model that captures the UE OFDM demodulation of the received backscatter information θ_n.

3.3.2 Determining modulation offset. To conduct demodulation, the UE should know the exact location of the starting point of backscatter data. As shown in Figure 13, the starting point of

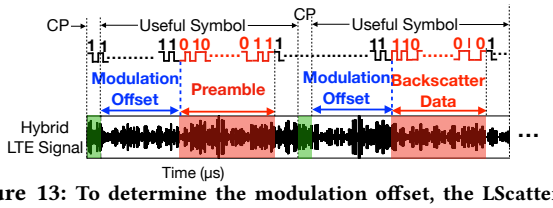


Figure 13: To determine the modulation offset, the LScatter tag sends a preamble prior to the backscatter data.

backscatter data is uncertain due to the incapability of precise time synchronization at the backscatter tag (as described in Section 3.1), which introduces the modulation offset. To determine the modulation offset, the backscatter tag sends a pre-defined preamble ahead of real data. After the preamble is recognized by the UE, it obtains the modulation offset and then starts to demodulate the backscatter data. We rewrite Equation 6 below to calculate the modulation offset:

$$\Theta = \underset{\theta_n \in \{0,\pi\}}{\operatorname{argmin}} \sum_{\substack{k=0 \\ k \neq r}}^{K-1} ||Y_k Y_r^* - (\sum_{n=0}^{K-1} x_n e^{j(\theta_n - \frac{2\pi nk}{K})})(\sum_{n=0}^{K-1} x_n^* e^{j(\frac{2\pi nr}{K} - \theta_n)})|| \tag{7}$$

where $\Theta = [1, ..., 1, \theta_p, ..., \theta_{p+N-1}, 1, ..., 1]$ and N is the number of subcarriers carrying the LTE data. p is the index of the first basic-timing unit of the useful modulation and $p + N - 1$ is the index of the last basic-timing unit of the useful modulation. We note that the length of the preamble equals to the length of backscatter data in a symbol. Therefore, we can use Equation 7 to calculate the modulation offset and decode the backscatter data.

3.3.3 Demodulating backscatter data. In contrast to the existing demodulation techniques which demodulate the backscatter data serially in time-domain, our novelty is parallel demodulation of the backscatter data from subcarriers in frequency-domain as presented in Equation 7. After we obtain the modulation offset p, we make $[\theta_p, ..., \theta_{p+N-1}]$ sequentially go through all the possible values. The minimum value in Equation 7 corresponds to the most likely backscatter data. We note that the left side and the right side of Equation 7 have the same size of N, which means Equation 7 is full row-rank and has a unique solution. Since each backscatter data θ_n ($n \in \{p, p + N - 1\}$) only has two values (i.e., either 0 or π), the process requires minimum computation resource at the UE side, which can be applied to the real world scenario.

4 EVALUATION

In this section, we first introduce the implementation of LScatter. Then we provide the details of the experimental setup. Finally, we show the experimental results of our extensive evaluation.

4.1 Implementation

The LScatter tag (shown in Figure 14) is implemented on a customized PCB board. The main components are as follows: A Microsemi Igloo Nano AGLN250 low power FPGA is used as the micro controller for synchronizing (as we described in Section 3.1) and modulating (as we described in Section 3.2). An ADG902 RF switch is used as the modulator to embed backscatter bits on to the ambient LTE signal and form the hybrid LTE signal. A voltage comparator as well as a few resistors, capacitors and inductors are used for the synchronization circuit.

We used two USRP B210 to implement the eNodeB (with the default transmission power of 10 dBm) and UE. Since the transmission power of USRP is far smaller than the base station, we extensively evaluate the communication distance of LScatter by connecting our eNodeB with an RF5110 RF power amplifier [40] that boosts the transmission power to 40 dBm. The USRP ran an open source LTE stack library srsLTE [8] which is compatible with LTE eNodeB and UE. To avoid emitting signals on licensed band, we used the 680 MHz white space which is very close to the major US cellular carriers (Chorus [20] also uses this methodology to evaluate a LTE related system).

To compare with and illustrate the benefit of LScatter, we also implemented a WiFi backscatter using ambient WiFi signals and a LoRa backscatter using ambient LoRa signals. The main modulation techniques are adopted from FreeRider [54] and PLoRa [38]. Since the ambient signal detection modules in FreeRider and PLoRa are very weak and cannot correctly detect the starting and ending points of ambient traffic, we enhanced these modules as follows:

WiFi Backscatter: As we introduced in the motivation section, since the WiFi traffic is bursty and intermittent, FreeRider cannot correctly detect the starting and ending points of ambient WiFi traffic. To help WiFi backscatter accurately detect the existence of ambient WiFi traffic, we connect the WiFi backscatter tag to a powerful USRP X300. The USRP X300 seeks the ambient WiFi traffic in real-time (i.e., by continuously calculating the correlation with the pre-defined WiFi packet preamble). After the WiFi traffic is found, the USRP X300 immediately sends a trigger signal to the WiFi backscatter tag so that the WiFi backscatter tag can fully utilize the WiFi traffic in the air.

LoRa Backscatter: In PLoRa [38], a low-resolution ADC (to save energy consumption) based correlation circuit is proposed to search for the LoRa signal. To have a better performance for LoRa backscatter, we used the ADC (which has much higher resolution than on the PLoRa tag) on USRP X300 to correlate the LoRa signal.

It is worth noting that the power consumption is very high for the above enhanced ambient signal detection modules in WiFi and LoRa backscatters. Therefore, FreeRider and PLoRa cannot use these modules.

4.2 Experimental Setup

To extensively evaluate the performance of LScatter, we conducted the experiments in three different setups. The first one is a mutipath rich environment **smart home** where the communication distances among eNodeB, LScatter tag, and UE are approximately 3 feet. The second setup is a large indoor **shopping mall**. We evaluated the traffic impact in a large area. We also conducted experiments at different communication distances from 10 feet to 180 feet between the LScatter tag and UE. The third setup is in an **outdoor** environment. In this setup, we evaluate how LScatter performs at street level in an outdoor environment. We also conducted the experiments for different distances between eNodeB and LScatter tag (up to 40 feet) as well as between LScatter tag and UE (up to 320 feet). To prevent emitting signals to the commercial licensed band, we used a recording and playback method (which can mimic the traffic pattern of LTE signals) to move the same baseband signals from

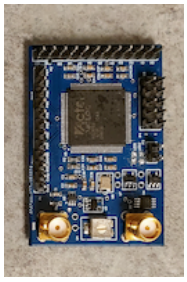


Figure 14: LScatter Tag

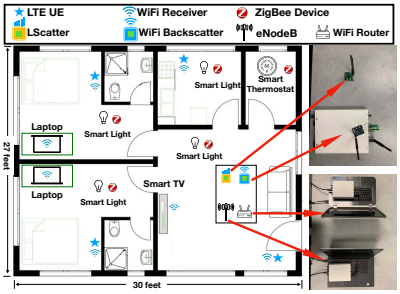


Figure 15: Smart Home Experimental Field

licensed band to the white space for our experiments. To ensure the representative, multiple pieces of traffic data were recorded for one hour. The recording was conducted every hour in a whole day and 7 days in a whole week (including weekday and weekend).

To obtain stable evaluation results, we let the receiver obtain more than 10,000 values on each data point. The total number of values we obtained is 1,020,000. The following two metrics are used to asses the system performance:

Bit error rate (BER): The Bit error rate is defined as the number of bit errors divided by the total number of transferred bits.

Throughput: The throughput is defined as correctly demodulated data bits.

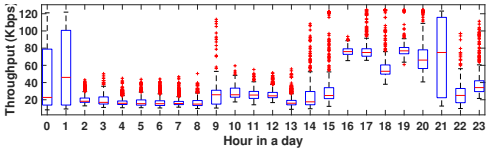
Since the LoRa traffic occupancy ratio is so low in our experimental sites, the backscatter does not have sufficient ambient LoRa traffic to piggyback its data. Thus, the throughput of LoRa backscatter is always 0 in our experiments. For clarity purpose, we do not plot the throughput of LoRa in the following evaluation results.

4.3 Smart Home

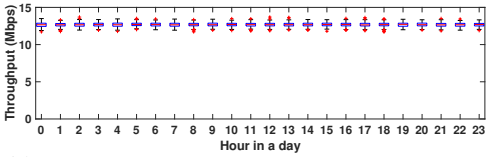
In this section, we evaluate LScatter in a two bedroom 800 ft^2 apartment (the layout is shown in Figure 15). There are many walls and objects in the home to create a multipath rich environment.

4.3.1 Throughput in A Whole Day. Figure 16a shows the throughput of WiFi backscatter over 24 hours in a typical day. From the result, we observe that the throughput is fluctuating. The highest median value is around 80 Kbps during 4pm to 9pm while the lowest (less than 20 Kbps) occurs before dawn. Another interesting observation is that there are a number of outliers on multiple box plots. This suggests that the throughput of WiFi backscatter is not stable even during one hour period. The main reason is that the traffic pattern is bursty which may yield relatively high throughput during a short period. But the intermittent traffic makes the overall throughput low and unstable.

It is worth noting that as we described in Section 4.1, the WiFi backscatter tag is triggered by an USRP based WiFi signal detector. Thus, even very short packet (such as beacon) can be used for transmitting backscatter data. In reality, a low power detector (such as an envelope detector) is not accurate to detect the beginning of a packet. Furthermore, the low power detector cannot distinguish traffic from heterogeneous devices (e.g., ZigBee or BLE). Thus, the performance will be even lower.



(a) Smart Home: WiFi Backscatter Throughput in 24 Hours



(b) Smart Home: LScatter Throughput in 24 Hours

Figure 16: Comparison between LTE and WiFi in Smart Home Setup: Overall, LScatter shows a resilient performance during a day while WiFi backscatter's performance fluctuates. Furthermore, LScatter's throughput is 368 times higher than WiFi throughput.

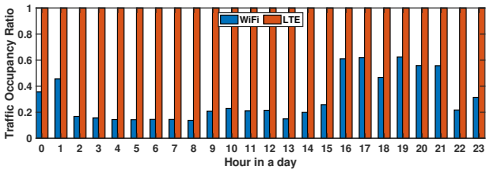
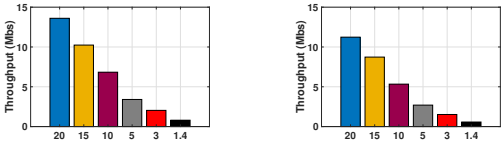


Figure 17: Smart Home: traffic occupancy ratio of WiFi and LTE Signals in 24 Hours



(a) Los **(b) NLoS**

Figure 18: Throughput under Different LTE Bandwidth

Figure 16b shows the throughput of LScatter over 24 hours. The box plot is comparatively short. This suggests that the throughput of LScatter is stable even during night time. The average throughput is 13.63 Mbps which is 368 times higher than WiFi backscatter's average throughput (around 37 Kbps).

The main reason LScatter has a resilient performance is that the traffic is continuous while the WiFi traffic is bursty and intermittent (we have discussed this in the motivation section). Figure 17 shows the corresponding traffic occupancy ratio of WiFi and LTE signals in the same day. We observe that the LTE's traffic occupancy ratio is 100% even during night. However, the WiFi has a high traffic hour during noon and evening but low traffic in the night. Thus, the performance of WiFi backscatter varies from hour to hour.

4.3.2 Throughput under Different Bandwidth. LTE has multiple possible bandwidths (i.e., 1.4 MHz, 3 MHz, 5 MHz, 10 MHz, 15 MHz and 20 MHz). With different bandwidth, the LTE signal itself carries different amount of data. In this section, we show the throughput results for LScatter under different LTE bandwidth. Figure 18a and Figure 18b show the results in direct line-of-sight (LoS) and none-line-of-sight (NLoS), respectively. From the results, we observe that the throughput of LScatter is directly proportional to the bandwidth, which means the modulation scheme of LScatter is efficient. We also observe that the throughput drops less than 10% in NLoS comparing with that in LoS. This means the modulation scheme of LScatter is stable and resilient to multipath effects.

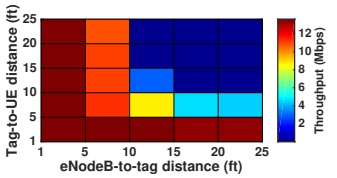


Figure 19: Throughput v.s. Distance

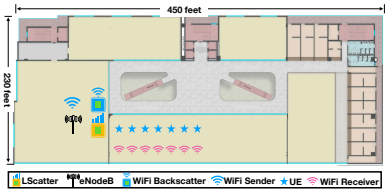
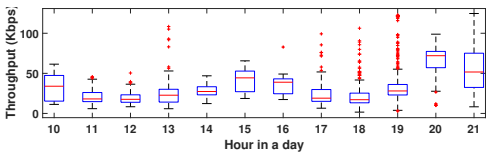
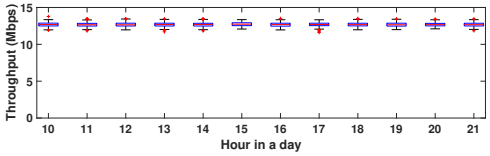


Figure 20: Shopping Mall Experimental Field



(a) Shopping Mall: WiFi Backscatter Throughput, 10am-9pm



(b) Shopping Mall: LScatter Throughput, 10am-9pm

Figure 21: Comparison in Shopping Mall Setup

4.3.3 Throughput v.s. Distance. A matrix in Figure 19 shows the throughput with distributed LScatter tags in the home setup. We can observe that as long as the tag is within 15 feet of either eNodeB or UE, we can get a 4-13 Mbps throughput. If the tag is too far away from both the eNodeB and UE, the throughput drops quickly. This is because the property of passive communication. However, it is worth noting that we only used 10 dBm transmission power which is much lower than a cellular tower. We show the results with an RF power amplifier of 40 dBm in an outdoor setting in Section 4.5.4.

4.4 Shopping Mall

In this section, we evaluate LScatter in a large shopping mall (103,500 ft^2). Figure 20 shows the layout of the shopping mall.

4.4.1 Throughput from 10am to 9pm. Figure 21a shows the throughput of WiFi backscatter. By comparing with the traffic occupancy ratio (shown in Figure 22), we learned that when the traffic occupancy ratio is about 0.5 (at 8pm), the throughput is the highest. The median value of the highest throughput is about 55 Kbps. However, there are multiple outliers above and below the box. This suggests that the throughput is unstable. The reason is that the WiFi traffic is bursty. Therefore, during some period, the throughput is higher but maybe lower during another period.

Figure 21b shows the throughput of LScatter. Since there is no obvious difference among boxes and all the boxes are flat, we can conclude that the throughput of LScatter is stable from 10am to 9pm. The 100% traffic occupancy ratio of LTE in Figure 22 confirmed that LTE is a good carrier for ubiquitous backscatter communication.

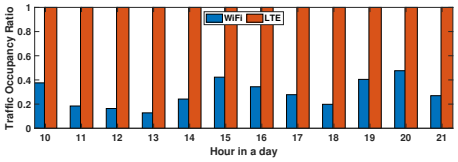


Figure 22: Shopping Mall: traffic occupancy ratio of WiFi and LTE Signals from 10am to 9pm

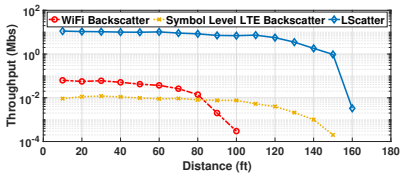


Figure 23: Shopping Mall: Throughput v.s. Distance (the y-axis is in log scale): The throughput of LScatter is two orders of magnitude higher than that of WiFi backscatter.

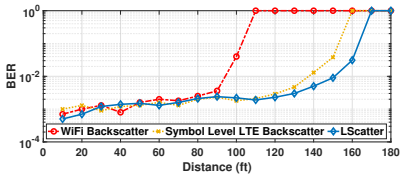


Figure 24: Shopping Mall: BER v.s. Distance (the y-axis is in log scale)

4.4.2 Throughput v.s. Distance. In this section, we show how LScatter performs under different communication distances. To illustrate the benefit of LScatter, we implemented a WiFi backscatter (FreeRider [54]). For a fair comparison, we also implemented a symbol level LTE backscatter which adopts the symbol level modulation technique from existed WiFi backscatters. Figure 23 shows the comparison among WiFi backscatter, symbol level LTE backscatter and our LScatter. We can observe that when the distance is less than 80 feet, symbol level LTE backscatter performs worse than WiFi backscatter because LTE has a much longer symbol duration than WiFi (as we discussed in the motivation section). After 80 feet, symbol level LTE backscatter's performance is better than WiFi backscatter because a 600MHz signal has range advantage compared to a 2.4GHz signal. By looking at our LScatter, it shows better performance across all distances than WiFi backscatter and symbol level LTE backscatter. The reason is that LScatter assigns different values on square waves during a symbol period (i.e., embed more data into a symbol) while the symbol level scheme assigns the same value (i.e., embed only a bit data into a symbol).

4.4.3 BER v.s. Distance. Figure 24 shows the BER of WiFi backscatter, symbol level LTE backscatter and our LScatter under different distances. We observed that the BER is similar among three backscatter systems when the distance is within 90 feet. Specifically, the BER for LScatter is less than 0.1% within 40 feet and less than 1% within 150 feet.

4.5 Outdoor

In this section, we evaluate the performance of LScatter in an outdoor environment (Figure 25).

4.5.1 Throughput in A Whole Day. Figure 26a shows the the throughput distribution in 24 hours of a day. Since the coverage

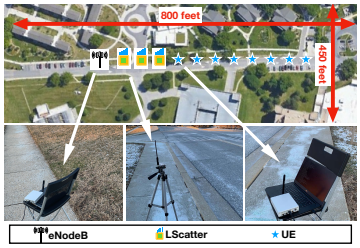
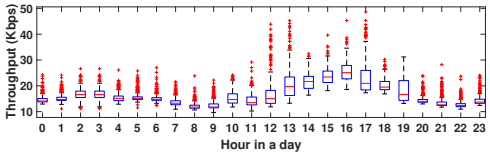
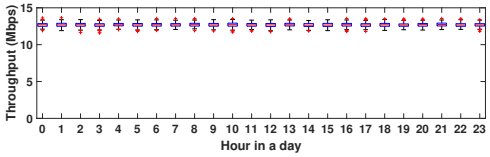


Figure 25: Outdoor Experimental Field



(a) Outdoor: WiFi Backscatter Throughput in 24 Hours



(b) Outdoor: LScatter Throughput in 24 Hours

Figure 26: Comparison between LTE and WiFi in outdoor setup with the same 10 dBm transmission power

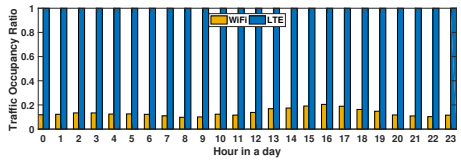


Figure 27: Outdoor with 10 dBm transmission power: traffic occupancy ratio of WiFi and LTE Signals in 24 Hours

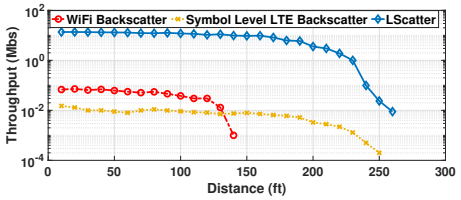


Figure 28: Outdoor with 10 dBm transmission power: Throughput v.s. Distance (the y-axis is in log scale)

of WiFi signal is worse than the indoor environment, there is less traffic (shown in Figure 27). Under this traffic pattern, the average throughput drops to 16.9 kbps. On the contrary, LScatter still has a high and stable throughput (shown in Figure 26b) across different times due to the traffic occupancy ratio is still 100%.

4.5.2 Throughput v.s. Distance. The results of throughput under different distances in an outdoor environment are shown in Figure 28. Overall, the throughput is higher at the same distance when compared with the indoor environment (Figure 23) because the signal suffers less multipath effect in the open space. With less degradation when distance increases, LScatter gains longer distance.

4.5.3 BER v.s. Distance. Figure 29 shows the Bit error rate (BER) in the outdoor environment. When the distance is within 120 feet,

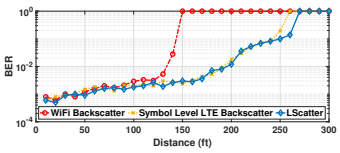


Figure 29: BER v.s. Distance (the y-axis is in log scale), 10 dBm transmission power

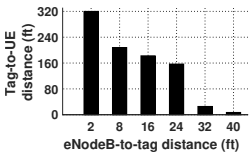


Figure 30: eNodeB-to-tag distance v.s. tag-to-UE distance, 40 dBm transmission power

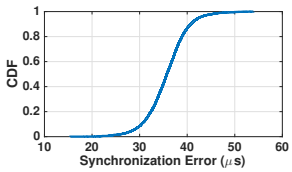


Figure 31: Synchronization Accuracy

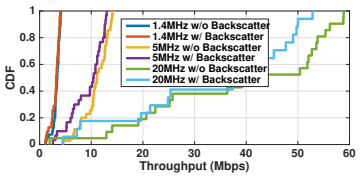


Figure 32: Impact to LTE

WiFi backscatter, symbol level LTE backscatter, and LScatter have a similar trend. However, when the distance exceeds 120 feet, the BER of WiFi backscatter increases sharply. The BER of the two LTE backscatter systems is still under 1% when the distance is shorter than 200 feet. This is because we could eliminate the phase offset introduced by backscattering and physical channel. Thus, the backscatter data can be correctly demodulated.

4.5.4 eNodeB-to-tag & tag-to-UE Distance. Since the transmission power of USRP is far lower than the base station, we extensively evaluate the communication distance of LScatter by connecting our eNodeB (USRP B210) with an RF5110 RF power amplifier [40] that boosts the transmission power from 10 dBm to 40 dBm. In the experiment, we fixed the eNodeB and moved the LScatter tag and the UE separately. We logged the two maximum distances i) between the tag and eNodeB; and ii) between the tag and UE. Figure 30 shows the results. We can observe that when the eNodeB-to-tag distance is 2 feet, the receiver can be 320 feet away from the tag. Along with the eNodeB-to-tag distance increasing to 24 feet, we can still get 160 feet tag-to-UE distance. Though the transmission power of RF5110 is still lower than that of base station, we can see the potential long range communication of LScatter. We also note that the future of cellular networks will be formed by plenty of small cell base stations. This concept has been defined in 3GPP Release-12 [1] and will help network operators launch home, enterprise, metro, and rural small cells [4]. These small cells will facilitate the wide deployment of LTE backscatters.

4.6 Synchronization Accuracy

In this section, we evaluate the synchronization circuit described in Section 3.1. To determine the synchronization accuracy, we measure the synchronization error which is defined as the time difference between the reception of PSS signal by LTE receiver (implemented on USPR) and by our synchronization circuit. By using LTE receiver as baseline, we can get rid of the wireless signal propagation delay. The result is shown in Figure 31. We can observe that majority of errors (~90%) are within the range of 30μs-40μs and follow the normal distribution. This synchronization accuracy is sufficient to avoid the PSS signals as described in Section 3.1.

4.7 Impact to Existing LTE

Figure 32 shows the LTE throughput (under different bandwidth setups) without or with the impact of backscatter. Overall, backscatter has negligible impact on original LTE transmission. The reason is that the backscattered signal is shifted to white space (out of original LTE band). Furthermore, the backscattered signal strength is usually much lower than the signal strength of the original LTE transmission. Therefore, backscatter communication does not impact too much on original LTE transmission.

4.8 Power Consumption

In this section, we analyze the energy consumption of our hardware tag which includes four parts:

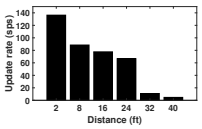
Synchronization Module. As shown in Figure 7, a low power circuit is designed to detect and synchronize the tag with LTE signal. In the circuit, the voltage comparator is the main power consuming component. Although the COTS low-power comparators usually have long propagation delay (orders of μs), the cycle of the synchronization signal is long enough ($200Hz = 5ms$) to tolerate the propagation delay. Therefore, a low-power comparator [35] with $12\mu s$ propagation delay is used. According to the data sheet, it consumes around $10\mu W$ of power.

RF Front. Since the backscatter is a passive radio, the RF front is simple and only has a low-power reflective RF switch (ADG902 [13]) and an passive antenna. The power consumption of the RF switch is linearly related to the channel bandwidth [55]. LTE has different channel bandwidths, the power consumption of the RF switch for the maximum channel width (20MHz) is around $57\mu W$.

Baseband Processor. Since the modulation technique introduced by LScatter is lightweight and requires neither complex computation nor bandwidth expansion, 80% flash can be frozen (by using the Flash Freeze technology provided by Igloo Nano AGLN250 FPGA) to support the reliable backscatter communication. Then, the power consumption can be reduced to $82\mu W$.

Clock. Both our basic time unit modulation and the symbol level modulation proposed in previous works need to shift the incoming signals to the adjacent channel to minimize the interference. Thus, the minimum clock rate depends on the bandwidth of the incoming signal. The reason our LScatter can get a higher throughput than prior work is because when LScatter shifts the incoming signal to the adjacent channel, it assigns different values on square waves during a symbol period (i.e., embeds multiple bits of data into one symbol) instead of taking the symbol level modulation approach (i.e., embed only one bit data into one symbol). Therefore, our basic time unit modulation can achieve a higher throughput than symbol level modulation, while its energy consumption is similar to symbol level modulation when we apply our basic time unit modulation method on WiFi backscatters. On the other hand, LTE signals have a special property which requires a higher clock rate than bandwidth to contain redundancy. For example, a 1.4MHz bandwidth LScatter tag uses a 1.92MHz clock with 588 μW power consumption [10]. We note that even with 1.4MHz configuration, LScatter can still achieve 800 Kbps throughput which is several times higher than that of FreeRider [54] and MOXcatter [56] (shown in Figure 18). To achieve the maximum throughput (13.63Mbps), a 20MHz LScatter tag uses a 30.72MHz clock with 4.5 mW power consumption [9]. In IC design, we can also significantly reduce the power consumption by using a ring oscillator which is used in HitchHike[53] and Interscatter [23] to generate 30MHz and 35.75MHz clocks with 4 μW and 9.69 μW of power consumption, respectively.

(a) Enabled by using Lscatter with EMG pad



(b) Update rate v.s. tag-to-source distance

Figure 33: Continuous Authentication

5 APPLICATION

In this section, we show an application that could be enabled by our backscatter. Continuous authentication is one of the important technologies that changes authentication from an event to a process. With continuous authentication, instead of a log in or out event, the applications continually monitor and authenticate users based on some biometrics. For example, an online banking application can log out immediately if an user change is detected. A great continuous authentication candidate is wearable devices which continuously monitor the biometrics (e.g., heartbeat pattern or electromyography) of the user and wirelessly transmit the measurements to devices (e.g., a laptop or smartphone) with authentication needs. However, the large amount of wireless transmissions cost much more energy (tens to hundreds of mW) on a traditional wearable device (which uses WiFi, BLE, or ZigBee protocol) that the tiny device cannot afford.

Thus, we use LScatter for continuous authentication because LScatter features: i) ultra low power wireless communication (only tens of μW); ii) ubiquitous coverage of LTE signals; and iii) continuous excitation signals.

In our prototype (shown in Figure 33a), an electromyography sensor is continuously measuring the electromyography and the measurements are transmitted via the LScatter tag. A laptop receives measurements from an LScatter tag and analyzes the data to determine whether the legitimate user is present or not. Figure 33b shows that the update rate (i.e., the amount of electromyography data is successfully received in one second) is as high as 136 samples per second (sps) when the distance between tag and source is 2 feet. Even when the distance is increased to 40 feet, the update rate can still reach 5 sps. This means the application running on the laptop can be authenticated five times in one second, which is sufficient for continuous authentication.

6 DISCUSSION AND OPPORTUNITIES

This paper presents LScatter, the first technology that explores how to leverage ambient LTE signals for ubiquitous passive communication. The modulation scheme, phase offset elimination technique, and demodulation scheme introduced in this paper are generic. Potentially, these techniques can be applied to any other OFDM signal based protocols (e.g, IEEE 802.11 a/g/n/ac/ax and 5G) to support the ubiquitous sensing and communication in smart cities. In this section, we discuss the potential development and research opportunities that can leverage our LScatter technology.

Implementation in cell phones: Our LScatter design strictly follows the LTE standard. The eNodeB we used in experiments ran the

open-source LTE stacks srsLTE [8], which is available under both commercial and open-source licenses, and is trusted by a lot of companies such as NOKIA, NEC, NI and etc. Thus, the emitted LTE signal is fully compatible with commercial LTE devices (e.g., cell phone). Therefore, it is very possible to use an off-the-shelf smartphone to decode the backscattered signals. We plan to use a smartphone to test our backscattered signal. Specifically, we plan to follow the detailed instruction (described in [3]) to program a blank USIM with the parameters aligning with the USRP-based base station.

Interference Minimization and Spectrum Sharing: The goal of our LScatter system is to reuse the continuous ambient LTE traffic for ultra-low power wireless communication with negligible interference introduced to the original LTE system. In Section 3.2.2, we described that the carrier frequency of the backscattered signal is shifted away from the original LTE band to minimize mutual interference between original LTE signal and backscattered signal. Besides shifting the backscattered signal from the original LTE band, the backscatter is a passive device which does not generate active signals. Thus, the power level of backscattered signals is as low as the signal reflected by a moving object (e.g., a car). On the other hand, we note that based on the LTE band allocation [2], LTE usually does not have back-to-back bands. Thus, by shifting the backscattered signal to the white space, it does not impact a neighboring LTE band. In an extreme scenario, the adjacent bands may be owned by different companies, because LTE networks have strong spectrum ownership boundaries. In this case, spectrum sharing technique is needed among these companies when they want to adopt our LScatter technology. Given the increasingly expensive and scarcity of wireless spectrum, we believe that spectrum sharing will become popular among cellular carriers.

7 RELATED WORK

Our work mainly lies in the intersection of two important subtopics of Wireless Networks:

Backscatter Techniques. Backscatter provides a promising direction to support low cost and energy-efficient communication [37, 45]. The first ambient backscatter [33] achieves communication between two backscatter devices that are up to 2.5 feet away from each other with 1 kbps information rate. After that, researchers have proposed various systems by backscattering WiFi [27, 51], Bluetooth [23], ZigBee [19, 32, 55], LoRa [21, 38, 42] or visible light signals [50]. [34] piggybacks on MIMO signals to reduce bit error rate. The approaches that are most related to LScatter are WiFi backscatter techniques. WiFi Backscatter [27] is the first work of backscattering WiFi signals. It utilizes CSI/RSSI for demodulation. Based on this work, NICScatter [51] uses a WiFi NIC to reflect the WiFi signals. Since these two approaches are suffering strong self-interference, the throughput is limited. To suppress the interference, Passive WiFi [28] transmits a tone by using the outside WiFi channel frequency, which improves the performance of throughput and energy consumption. However, all these pioneer works cannot support the OFDM scheme. To overcome this problem, FreeRider [54] and MOXcatter [56] change an OFDM symbol to another valid OFDM symbol by changing the phase of the signal. Since these approaches mainly modulate the backscatter data at the symbol level, the throughput still remains a problem. In addition, they are not compatible with existing WiFi networks. To solve this problem, WiTAG [12] combines several MAC layer subframes to enable communication while X-Tandem [57] decodes backscattered WiFi data from a clean receive channel. To support OFDMA, the latest work [58] leverages the frequency shift method in both time and frequency domain. Although this work preforms good in its scenario, due to the inconstancy of the WiFi traffic, the performance will be hampered in real world settings.

Different from the above approaches, LScatter is the first ambient LTE backscatter. It can provide ubiquitous communication under various real-world settings. In addition, our system not only significantly increases the throughput but also improves the communication range. By leveraging continuous ambient LTE traffic, LScatter can support various IoT applications.

Cellular Networks. Researchers have introduced lots of excellent work with focusing on cellular networks, including new Network Architectures [26, 48] and Protocols [31, 47, 52], increasing Coverage Range [17, 59], reducing Operating Cost [39] and improving User Experience [22, 24, 49], etc. For example, CellFi proposes [14] a LTE compatible architecture for outdoor coverage in TV white spaces. [17] utilizes drones to extend the Cell Tower coverage range in LTE networks. To reduce the operating cost and improve the user experience, [46] provides a new pattern extraction and modeling methodology while [15] investigates how radio network characteristics affect the user experience. Researchers have also studied the complement between cellular networks and other types of networks [30, 36, 41]. For example, iDEAL [18] leverages third-party network resource owners to offload cellular traffic. Win-coupon [60] uses WiFi to help cellular networks offload the data.

Different from these advanced techniques in cellular networks, LScatter leverages the ambient cellular signal for ubiquitous and high throughput backscatter communication.

8 CONCLUSION

We present the first LTE backscatter system by leveraging the unique features of the ambient LTE signal (i.e., continuous signal in time domain and ubiquitous coverage in spatial domain). We designed the low-power ambient LTE signal synchronization circuit to avoid affecting the critical information in the LTE signal. We proposed a new modulation scheme, which can significantly increase the throughput even under the fact that LTE uses a much longer symbol duration than WiFi. Moreover, we also addressed the practical issues such as phase offset by leveraging the reference signals on different subcarriers in original LTE physical layer. Finally, we extensively evaluated our system in various real-world scenarios to demonstrate the orders of magnitude performance improvement of our LScatter compared to the latest ambient WiFi backscatter system [54]. This work does not raise ethical issues.

ACKNOWLEDGMENTS

This work is supported in part by NSF grants CNS-1824491 and CNS-1652669. We also thank anonymous shepherd and reviewers for their valuable comments.

REFERENCES

[1] 2015. 3GPP Release 12. https://www.3gpp.org/specifications/releases/68-release-12.
[2] 2017. LTE Frequency Bands. https://www.everythingrf.com/community/lte-frequency-bands.
[3] 2018. Build a LTE Network with srsLTE and Program Your Own USIM Card. https://cyberloginit.com/2018/05/03/build-a-lte-network-with-srslte-and-program-your-own-usim-card.html.
[4] 2018. Small Cell Forum. https://www.3gpp.org/news-events/partners-news/1463-small-cell-forum-release-one.
[5] 2019. AT&T LTE Coverage. https://www.att.com/maps/wireless-coverage.html?kbid=121192&partner=LinkShare&siteId=je6NUbpObpQ-tqiwovJYjaUbhNyY7pcOnQ&source=ECay0000000CEL00O.
[6] 2019. LoRaWAN LPWAN for America. http://penteon.io/page-4/index.html.
[7] 2019. https://en.wikipedia.org/wiki/Zadoff-Chu_sequence.
[8] 2019. https://github.com/srsLTE/srsLTE.
[9] 2020. CSX-252F. http://cfd.citizen.co.jp/english/prod-tech/product/pdf/datasheet_Oscillator/CSX-252F.pdf.
[10] 2020. LTC6990. https://www.analog.com/media/en/technical-documentation/data-sheets/LTC6990.pdf.
[11] 3GPP. 2009. 3GPP TS 36.211 V8.9.0 (2009-12). Technical Report.
[12] Ali Abedi, Mohammad Hossein Mazaheri, Omid Abari, and Tim Brecht. 2018. WiTAG: Rethinking Backscatter Communication for WiFi Networks. In HotNets, 2018.
[13] Analog Devices 2019. ADG901/ADG902: Wideband, 40 dB Isolation at 1 GHz, CMOS 1.65 V to 2.75 V, SPST Switches Data Sheet. Analog Devices. Rev. D.
[14] Ghufran Baig, Dan Alistarh, Thomas Karagiannis, Bozidar Radunovic, Matthew Balkwill, and Lili Qiu. 2017. Towards unlicensed cellular networks in TV white spaces. In CoNEXT, 2017.
[15] Athula Balachandran, Vaneet Aggarwal, Emir Halepovic, Jeffrey Pang, Srinivasan Seshan, Shobha Venkataraman, and He Yan. 2014. Modeling web quality-of-experience on cellular networks. In MobiCom, 2014.
[16] Dinesh Bharadia, Kiran Raj Joshi, Manikanta Kotaru, and Sachin Katti. 2015. Backfi: High throughput wifi backscatter. In SIGCOMM, 2015.
[17] Ashutosh Dhekne, Mahanth Gowda, and Romit Roy Choudhury. 2017. Extending cell tower coverage through drones. In HotMobile, 2017.
[18] Wei Dong, Swati Rallapalli, Rittwik Jana, Lili Qiu, KK Ramakrishnan, Leo Razoumov, Yin Zhang, and Tae Won Cho. 2014. iDEAL: Incentivized dynamic cellular offloading via auctions. In TON, 2014.
[19] Joshua F Ensworth and Matthew S Reynolds. 2015. Every smart phone is a backscatter reader: Modulated backscatter compatibility with bluetooth 4.0 low energy (ble) devices. In RFID, 2015.
[20] Ezzeldin Hamed, Hariharan Rahul, and Bahar Partov. 2018. Chorus: Truly Distributed distributed-MIMO. In Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication (SIGCOMM '18). ACM, New York, NY, USA, 461–475. https://doi.org/10.1145/3230543.3230578
[21] Mehrdad Hessar, Ali Najafi, and Shyamnath Gollakota. 2018. Netscatter: Enabling large-scale backscatter networks. In arXiv preprint, 2018.
[22] Jonghwan Hyun, Youngjoon Won, Kenjiro Cho, Romain Fontugne, Jaeyoon Chung, and James Won-Ki Hong. 2017. High-end LTE service evolution in Korea: 4 years of nationwide mobile network measurements. In CNSM, 2017.
[23] Vikram Iyer, Vamsi Talla, Bryce Kellogg, Shyamnath Gollakota, and Joshua Smith. 2016. Inter-Technology Backscatter: Towards Internet Connectivity for Implanted Devices. In SIGCOMM, 2016.
[24] Junchen Jiang, Xi Liu, Vyas Sekar, Ion Stoica, and Hui Zhang. 2014. Eona: Experience-oriented network architecture. In HotNets, 2014.
[25] Meng Jin, Yuan He, Xin Meng, Yilun Zheng, Dingyi Fang, and Xiaojiang Chen. 2017. FlipTracer: Practical Parallel Decoding for Backscatter Communication. In MobiCom, 2017.
[26] Morteza Karimzadeh, Hans van den Berg, Ricardo de O Schmidt, and Aiko Pras. 2017. Quantitative Comparison of the Efficiency and Scalability of the Current and Future LTE Network Architectures. In Wireless Communications and Mobile Computing, 2017.
[27] Bryce Kellogg, Aaron Parks, Shyamnath Gollakota, Joshua R Smith, and David Wetherall. 2014. Wi-Fi backscatter: Internet connectivity for RF-powered devices. In SIGCOMM, 2014.
[28] Bryce Kellogg, Vamsi Talla, Shyamnath Gollakota, and Joshua R Smith. 2016. Passive Wi-Fi: Bringing Low Power to Wi-Fi Transmissions.. In NSDI, 2016.
[29] David Kotz and Kobby Essien. 2002. Analysis of a Campus-wide Wireless Network. In Proceedings of the 8th Annual International Conference on Mobile Computing and Networking (MobiCom '02). ACM, New York, NY, USA, 107–118. https://doi.org/10.1145/570645.570659
[30] Kyunghan Lee, Joohyun Lee, Yung Yi, Injong Rhee, and Song Chong. 2010. Mobile data offloading: How much can WiFi deliver?. In CoNEXT, 2010.
[31] Li Li, Ke Xu, Tong Li, Kai Zheng, Chunyi Peng, Dan Wang, Xiangxiang Wang, Meng Shen, and Rashid Mijumbi. 2018. A measurement study on multi-path TCP with multiple cellular carriers on high speed rails. In SIGCOMM, 2018.
[32] Yan Li, Zicheng Chi, Xin Liu, and Ting Zhu. 2018. Passive-ZigBee: Enabling ZigBee Communication in IoT Networks with 1000X+ Less Power Consumption. In Proceedings of the 16th ACM Conference on Embedded Networked Sensor Systems (SenSys '18). ACM, New York, NY, USA, 159–171.
[33] Vincent Liu, Aaron Parks, Vamsi Talla, Shyamnath Gollakota, David Wetherall, and Joshua R. Smith. 2013. Ambient Backscatter: Wireless Communication out of Thin Air. In Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM (SIGCOMM). ACM, New York, NY, USA, 39–50. https://doi.org/10.1145/2486001.2486015
[34] Xin Liu, Zicheng Chi, Wei Wang, , Yao Yao, and Ting Zhu. 2020. VMscatter: A Versatile MIMO Backscatter. In 17th USENIX Symposium on Networked Systems Design and Implementation (NSDI 20). USENIX Association, Santa Clara, CA, 895–909. https://www.usenix.org/conference/nsdi20/presentation/liu-xin
[35] MAXIM 2019. MAX931-MAX934 Ultra Low-Power, Low-Cost Comparators. MAXIM. Rev. 1.
[36] Morteza Mehrnoush, Sumit Roy, Vanlin Sathya, and Monisha Ghosh. 2018. On the Fairness of Wi-Fi and LTE-LAA Coexistence. In TCCN, 2018.
[37] Saman Naderiparizi, Mehrdad Hessar, Vamsi Talla, Shyamnath Gollakota, and Joshua R Smith. 2018. Towards battery-free HD video streaming. In NSDI, 2018.
[38] Yao Peng, Longfei Shangguan, Yue Hu, Yujie Qian, Xianshang Lin, Xiaojiang Chen, Dingyi Fang, and Kyle Jamieson. 2018. Plora: A passive long-range data network from ambient lora transmissions. In SIGCOMM, 2018.
[39] Zafar Ayyub Qazi, Vyas Sekar, and Samir Das. 2014. A framework to quantify the benefits of network functions virtualization in cellular networks. In arXiv preprint, 2014.
[40] RF5110G 2018. RF5110G 3V General Purpose/GSM Power Amplifier. RF5110G. Rev. 1.
[41] Joel Sommers and Paul Barford. 2012. Cell vs. WiFi: on the performance of metro area mobile connections. In IMC, 2012.
[42] Vamsi Talla, Mehrdad Hessar, Bryce Kellogg, Ali Najafi, Joshua R Smith, and Shyamnath Gollakota. 2017. Lora backscatter: Enabling the vision of ubiquitous connectivity. IMWUT, 2017.
[43] Diane Tang and Mary Baker. 1999. Analysis of a Metropolitan-area Wireless Network. In Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom '99). ACM, New York, NY, USA, 13–23. https://doi.org/10.1145/313451.313460
[44] Diane Tang and Mary Baker. 2000. Analysis of a Local-area Wireless Network. In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom '00). ACM, New York, NY, USA, 1–10. https://doi.org/10.1145/345910.345912
[45] Deepak Vasisht, Guo Zhang, Omid Abari, Hsiao-Ming Lu, Jacob Flanz, and Dina Katabi. 2018. In-body backscatter communication and localization. In SIGCOMM, 2018.
[46] Huandong Wang, Fengli Xu, Yong Li, Pengyu Zhang, and Depeng Jin. 2015. Understanding mobile traffic patterns of large scale cellular towers in urban environment. In IMC, 2015.
[47] Keith Winstein, Anirudh Sivaraman, Hari Balakrishnan, et al. 2013. Stochastic Forecasts Achieve High Throughput and Low Delay over Cellular Networks.. In NSDI, 2013.
[48] Wenfei Wu, Li Erran Li, Aurojit Panda, and Scott Shenker. 2014. PRAN: Programmable radio access networks. In HotNets, 2014.
[49] Xing Xu, Yurong Jiang, Tobias Flach, Ethan Katz-Bassett, David Choffnes, and Ramesh Govindan. 2015. Investigating transparent web proxies in cellular networks. In PAM, 2015.
[50] Xieyang Xu, Yang Shen, Junrui Yang, Chenren Xu, Guobin Shen, Guojun Chen, and Yunzhe Ni. 2017. PassiveVLC: Enabling Practical Visible Light Backscatter Communication for Battery-free IoT Applications. In MobiCom, 2017.
[51] Zhice Yang, Qianyi Huang, and Qian Zhang. 2017. NICScatter: Backscatter as a Covert Channel in Mobile Devices. In MobiCom, 2017.
[52] Zengwen Yuan, Qianru Li, Yuanjie Li, Songwu Lu, Chunyi Peng, and George Varghese. 2018. Resolving Policy Conflicts in Multi-Carrier Cellular Access. In Cell, 2018.
[53] Pengyu Zhang, Dinesh Bharadia, Kiran Joshi, and Sachin Katti. 2016. HitchHike: Practical Backscatter Using Commodity WiFi. In SenSys, 2016.
[54] Pengyu Zhang, Colleen Josephson, Dinesh Bharadia, and Sachin Katti. 2017. FreeRider: Backscatter Communication Using Commodity Radios. In CoNEXT, 2017.
[55] Pengyu Zhang, Mohammad Rostami, Pan Hu, and Deepak Ganesan. 2016. Enabling practical backscatter communication for on-body sensors. In SIGCOMM, 2016.
[56] Jia Zhao, Wei Gong, and Jiangchuan Liu. 2018. Spatial Stream Backscatter Using Commodity WiFi. In MobiSys, 2018.
[57] Jia Zhao, Wei Gong, and Jiangchuan Liu. 2018. X-Tandem: Towards Multi-hop Backscatter Communication with Commodity WiFi. In MobiCom, 2018.
[58] R Zhao, F Zhu, Y Feng, S Peng, X Tian, H Yu, and X Wang. 2019. OFDMA-Enabled Wi-Fi backscatter. In Mobicom 2019.
[59] Yibo Zhu, Zengbin Zhang, Zhinus Marzi, Chris Nelson, Upamanyu Madhow, Ben Y Zhao, and Haitao Zheng. 2014. Demystifying 60GHz outdoor picocells. In

MobiCom, 2014.
[60] Xuejun Zhuo, Wei Gao, Guohong Cao, and Yiqi Dai. 2011. Win-Coupon: An incentive framework for 3G traffic offloading. In ICNP, 2011.