Leggiero: Analog WiFi Backscatter with Payload Transparency

Xin Na
nx20@mails.tsinghua.edu.cn
Tsinghua University
Beijing, China

Xiuzhen Guo
guoxiuzhen94@gmail.com
Tsinghua University
Beijing, China

Zihao Yu
zh-yu17@mails.tsinghua.edu.cn
Tsinghua University
Beijing, China

Jia Zhang
j-zhang19@mails.tsinghua.edu.cn
Tsinghua University
Beijing, China

Yuan He*
heyuan@tsinghua.edu.cn
Tsinghua University
Beijing, China

Yunhao Liu
yunhao@tsinghua.edu.cn
Tsinghua University
Beijing, China

ABSTRACT

Backscatter is an enabling technology for battery-free sensing in today's Artificial Intelligence of Things (AIOT). Building a backscatter-based sensing system, however, is a daunting task, due to two obstacles: the unaffordable power consumption of the microprocessor and the coexistence with the ambient carrier's traffic. In order to address the above issues, in this paper, we present Leggiero, the first-of-its-kind analog WiFi backscatter with payload transparency. Leveraging a specially designed circuit with a varactor diode, this design avoids using a microprocessor to interface between the radio and the sensor, and directly converts the analog sensor signal into the phase of RF (radio frequency) signal. By carefully designing the reference circuit on the tag and precisely locating the extra long training field (LTF) section of a WiFi packet, Leggiero embeds the analog phase value into the channel state information (CSI). A commodity WiFi receiver without hardware modification can simultaneously decode the WiFi and the sensor data. We implement Leggiero design and evaluate its performance under varied settings. The results show that the power consumption of the Leggiero tag (excluding the power of the peripheral sensor module) is 30μW at a sampling rate of 400Hz, which is 4.8× and 4× lower than the state-of-the-art WiFi backscatter schemes. The uplink throughput of Leggiero is sufficient to support a variety of sensing applications, while keeping the WiFi carrier's throughput performance unaffected.

CCS CONCEPTS

• **Hardware → Wireless integrated network sensors**; • **Networks → Network protocol design**.

KEYWORDS

Backscatter; Analog; Phase; RF computing

ACM Reference Format:
Xin Na, Xiuzhen Guo, Zihao Yu, Jia Zhang, Yuan He, and Yunhao Liu. 2023. Leggiero: Analog WiFi Backscatter with Payload Transparency. In *The 21st Annual International Conference on Mobile Systems, Applications and Services (MobiSys '23), June 18–22, 2023, Helsinki, Finland.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3581791.3596835

1 INTRODUCTION

Backscatter is a crucial technology for the Internet of Things (IoT). A backscatter device (i.e., the backscatter tag) is excited by the energy from a carrier source and modulates its own data over the backscattered signals, thus enabling battery-free communication. Sensor data collection is the mainstream application of backscatter. When wired with a sensing module, a backscatter tag becomes a battery-free sensor, delivering the sensor data to the receiver with extremely low power consumption.

Research on backscatter has received broad interest. In recent years, we have witnessed significant progress in this technology with regard to the communication throughput, range, enabled applications, etc. [22, 38, 42, 45, 46]. But building a backscatter-based sensing system still appears to be a daunting task, mainly due to the following two obstacles:

• **Unaffordable power consumption of the μP**: Regarding how the sensor data is acquired and transmitted, the conventional practice is to involve a microprocessor (μP) to interface between the radio and peripheral sensor. Though the power consumption of a backscatter radio can be as low as the level of microwatts (μWs), the μP remains the bottleneck of a sensor's energy consumption. The typical energy consumption of such a μP is at the level of milliwatts (mWs), which is generally unaffordable, given the stringent energy budget of a battery-free tag [23].

• **Coexistence with the ambient carrier's traffic**: The ability to utilize an ambient carrier as the excitation source is critical to the ubiquitous deployment of backscatter, but the other side of the coin is that it is usually hard for the backscatter traffic to coexist with the carrier's traffic. The existing approaches usually need to manipulate the carrier's packets, e.g., by modifying payloads [68, 69] or corrupting entire frames [2], which damages the carrier's traffic and may lead to decoding failure at the receiver.

In order to tackle the above problems, we in this paper propose Leggiero, the first-of-its-kind analog WiFi backscatter scheme. Leggiero directly modulates the analog sensor signals in the CSI (Channel State Information) of the backscattered WiFi packets, which can be received and decoded by a commercial WiFi receiver. Fig. 1 compares the schemes of Leggiero and conventional WiFi

[*] Corresponding Author.

MobiSys '23, June 18–22, 2023, Helsinki, Finland

ACM ISBN 979-8-4007-0110-8/23/06.
https://doi.org/10.1145/3581791.3596835

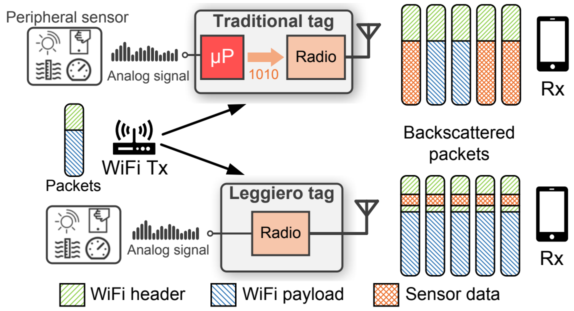


Figure 1: Leggiero eliminates the need for using microprocessors (μP) and works transparently with the WiFi carrier's traffic.

backscatter. In Leggiero, the sensor is directly interfaced with the radio. The sensor data embedded in the CSI coexist transparently with the payload of the WiFi carrier's packets. The advantages of Leggiero are attributed to the following innovative designs:

- **Low-power signal conversion in the analog domain.** The analog sensors mostly output signals in the form of voltage. Leggiero takes the sensor's analog voltage as input and directly converts it to the phase of RF signals in the analog domain. We choose the RF phase due to its stability in propagation compared with the amplitude modulation [57], as well as its compatibility with the WiFi network compared with the pulse width modulation [45]. We first show that the reflected RF phase is determined by the reflection coefficient (§2.1). Then we explore the capacitor model (§2.2) to establish the requirement of the circuit design with respect to the generality, phase range, and conversion linearity. By utilizing the varactor diode, we design a passive reflective circuit (§2.3) that meets the requirement. Leveraging the varactor diode to alter the reflection coefficient of the tag, Leggiero can control the phase of the reflected signal according to the sensor's analog voltage. In this way, Leggiero avoids using microprocessors as the interfacing media and reduces the energy consumption to an affordable level.
- **Analog modulation with payload transparency.** Leggiero exploits the "extra spatial sounding" (ESS) feature in 802.11n and utilizes CSI to carry the analog sensor signals (§3.1). Fig. 2 shows the structure of an ESS-enabled packet. The sensor signal, converted into the form of the RF signal phase, is embedded in the extra CSI of a WiFi packet. Leggiero precisely locates the extra long training field (LTF) section of a packet by using an envelope detector, and then embeds the accurate analog phase value by using a carefully designed reference circuit (§3.2). On receiving the backscattered packet, a receiver can efficiently extract the embedded sensor readings as well as cancel out the environmental influences on the CSIs by taking the phase difference of the two CSIs in the same packet (§3.3). Throughout this process, no modification is made to the payload of the WiFi packet, as is called payload transparency. Hence, the original WiFi data in the payload can also be decoded at the same time. Importantly, Leggiero does not require hardware modification to commercial WiFi transceivers.

In addition to the above key design, we also present the MAC layer design of Leggiero (§4) and the implementation details (§5). The hardware schematics are made publicly available.[1] §6 presents the comprehensive evaluation of Leggiero. The ASIC power consumption of the Leggiero tag (excluding the power of the peripheral sensor module) is 30μW at a sampling rate of 400Hz, which is 4.8× and 4× lower than the existing WiFI backscatter schemes[2, 69]. This power enables the sensor tag to work in a battery-free manner. Furthermore, due to the payload transparency of Leggiero, the WiFi carrier's data traffic is always preserved with unaffected throughput performance. Leggiero achieves 5Kbps throughput, which is sufficient to support a variety of sensing applications. At a high level, Leggiero's design incorporates an RF computing mechanism that operates passively on the RF signal during its propagation.

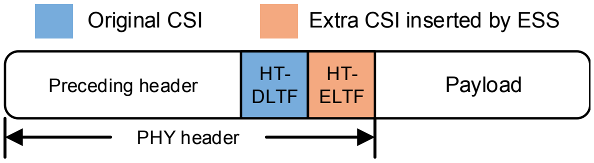


Figure 2: Extra spatial sounding featured 802.11n packet. It provides a duplicated CSI since the long-training-fields (LTF) experience the same channel.

§7 discusses practical issues of Leggiero and the potential research space. §8 briefly introduces related works. We conclude this work in §9.

2 ANALOG SIGNAL CONVERSION

This section introduces how Leggiero converts the sensor signal to the phase of the WiFi signal. For a backscatter tag, the phase of the reflected RF signal is determined by the **reflection coefficient (Γ)** of the tag. Therefore, Leggiero achieves the conversion by relating the sensor signal (usually a voltage signal) with the reflection coefficient. We build a passive RF circuit to produce different Γ according to the analog voltage, thus constructing different phases in the reflected signal.

2.1 Primer: Reflection Coefficient

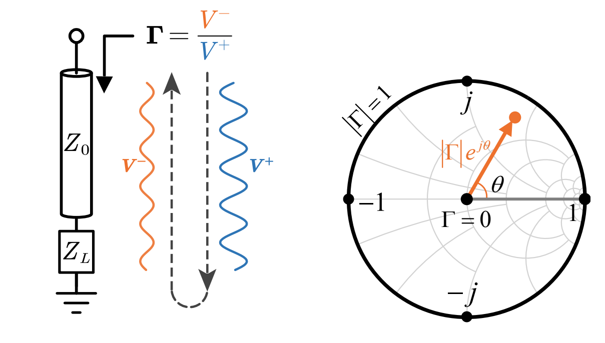
For an RF circuit, the reflection coefficient represents the ratio of the reflected voltage wave (V^-) to the incident voltage wave (V^+) at a particular port. Fig. 3(a) shows a transmission line of characteristic impedance Z_0 feeding a load with impedance Z_L. The reflection coefficient Γ is given by:

$$\Gamma = \frac{V^-}{V^+} = \frac{Z_L - Z_0}{Z_L + Z_0} = |\Gamma| e^{j\theta}, \tag{1}$$

where $|\Gamma|$ and θ represent the relative amplitude attenuation and the relative phase variation of the reflected wave compared to the incident wave, respectively. A simple understanding is that for an incident wave signal $A\sin(2\pi ft)$, the reflected signal of this circuit is $A|\Gamma|\sin(2\pi ft + \theta)$. In *S-parameter* theory [47], the reflection coefficient is also denoted by $\mathbf{S_{11}}$. In the rest of this paper, we will also use S_{11} to denote the reflection coefficient.

In the conventional backscatter design, the tag modulates bit 0 and bit 1 by providing two discrete Γ values. For example, the RFID tag provides $\Gamma_1 = 0$ as a matched state where the incident wave is completely absorbed and $|\Gamma_2| = 1$ as a reflective state where the wave is completely reflected. These two values can be shown in a Smith chart in Fig. 3(b) in polar coordinates. Other examples

[1] Open source hardware can be found at https://github.com/wonderfulnx/Leggiero.



(a) Definition of reflection coefficient Γ (b) Γ in smitch chart

Figure 3: The reflection coefficient Γ. (a) shows its definition, where Z_0 and Z_L are the impedance of the transmission line and the load, respectively. (b) shows its polar coordinates representation in a Smith chart.

are recent WiFi backscatter designs such as HitchHike [68], the two different values have the same magnitude but provide different phases, e.g., $\Gamma_1 = j$ and $\Gamma_2 = -j$. It means that the incident signal is always reflected in both states but contains a 180° phase difference between the two states.

Our insight here is that the reflection coefficient can not only be switched digitally but also be controlled in an analog form, which provides the opportunity to realize signal conversion in the analog domain. By performing an analog variation on the reflection coefficient, the reflected RF phase can be adjusted to carry the tag's sensor readings.

2.2 Exploring the Capacitor Model

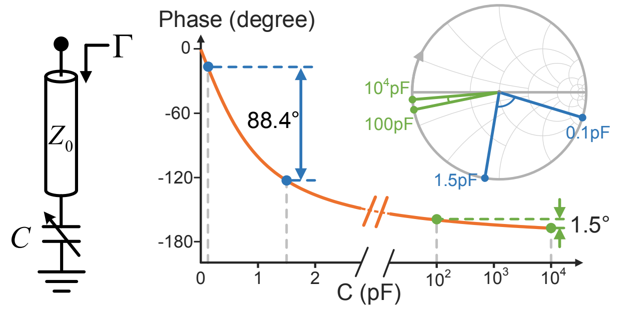
A potential method to realize the above-mentioned phase variation is to use a shorted variable capacitor, as shown in Fig. 4(a), which simply replaces the load of the circuit in Fig. 3(a) with a variable capacitor. The reflection coefficient Γ_C of such a circuit is computed by replacing the load impedance Z_L with the capacitor impedance Z_C in Eq. (1):

$$\Gamma_C = \frac{Z_C - Z_0}{Z_C + Z_0} = \frac{1 - j2\pi f C Z_0}{1 + j2\pi f C Z_0} = e^{j\theta_C} \tag{2}$$

$$\theta_C = -2\arctan(2\pi f C Z_0), \tag{3}$$

where f is the signal frequency, C represents the capacitance of the capacitor, and Z_0 is the characteristic impedance of the antenna or the transmission line, which is usually 50Ω. Eq. (2) shows that the reflection coefficient of a shorted capacitor is a complex unit, and its phase depends only on the capacitance since the signal frequency and the characteristic impedance are constant. Therefore, a shorted capacitor will completely reflect the incident signal, and its capacitance will determine the reflected signal phase.

In order to convert the sensor readings to the RF signal phase, we need to relate the capacitance with the peripheral sensor readings. An intuitive solution is to directly use a capacitive sensor as the shorted variable capacitor. For example, the external pressure on a pressure sensor is directly converted to the variable capacitor's capacitance, which corresponds to an RF signal phase. However, in practice, using a capacitor sensor is not an option due to the following reasons.



(a) Model (b) Phase range of different capacitance

Figure 4: The shorted variable capacitor model and the corresponding phase variation. Higher capacitance leads to a smaller phase range and worse linearity.

- **Generality:** Directly using a capacitive sensor limits Leggiero to only specific sensing scenarios. Such a design cannot support other types of sensor signals since capacitive sensors are a small part of all sensors' designs.
- **Phase Range and Linearity:** The capacitance range of the capacitive sensors is usually above 100pF. According to Eq. (3), higher capacitance leads to a lower phase range and worse linearity. As shown in Fig. 4(b), for 2.4GHz WiFi signals, the phase variation between capacitance 0.1pF and 1.5pF can be up to 90°, while there is only 1.5° of the phase difference between 100pF and 10^4pF. Note that $\arctan(x)$ function is close to linear when $x \in (0, \frac{\pi}{2})$. Therefore, to achieve a wider phase range and better accuracy, we prefer to control the capacitance between 0 and 2pF. Most capacitive sensors cannot satisfy this range requirement.

2.3 Designing Reflective Circuit

Since directly using capacitance as the sensor signal loses generality, we turn to consider that all types of sensor signals can be acquired as voltage signals when sampling. The signal conversion that takes voltage signals as input appears to be a better option. We then need to translate the voltage signal to a variable capacitance. As discussed above, this translation must yield very small capacitance to achieve a wider phase range and better linearity.

Leggiero introduces a varactor diode to convert the external analog voltage into a small capacitance. The varactor diode is a reverse-biased PN junction. It produces a junction capacitance that varies smoothly with the bias voltage. The junction capacitance is dependent on the reversed junction bias voltage, V, according to

$$C_j(V) = \frac{C_0}{(1 - V/V_0)^{\gamma}}, \tag{4}$$

where C_0 is the junction capacitance with no bias; V_0 and γ depend on the diode type and are constants for a specific diode. Existing commercial varactor diodes can provide the capacitance range of 0 to 2pF. For example, a typical GaAs varactor diode can have a junction capacitance that varies from about 0.1 to 2.0pF as the reversed bias voltage ranges from 0 to 20V. Specifically, in Fig. 8(a),

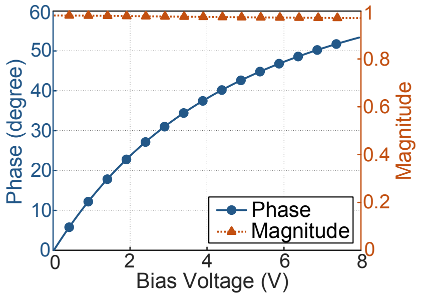


Figure 5: Simulated phase and magnitude of the reflected signal v.s. input voltage. The phase is near-linear in 0-5V with little attenuation.

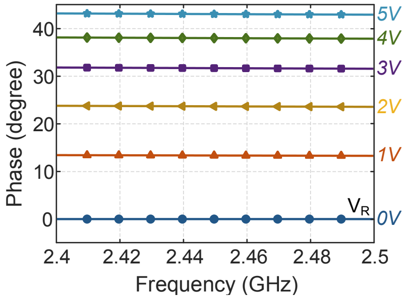


Figure 6: Simulated phase v.s. frequency with different input voltage V_R. The reflected signal phase is flat on the whole 2.4GHz band.

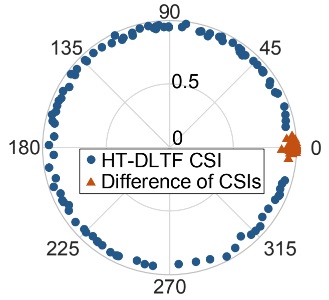
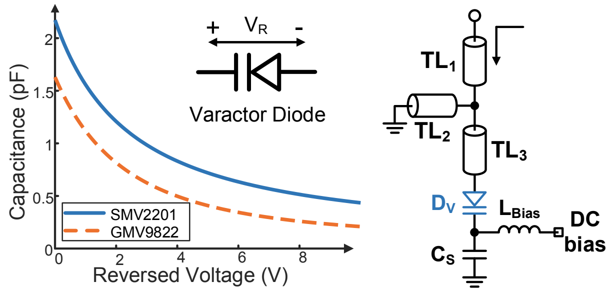


Figure 7: Verifying the consistency between the ESS and regular CSI. While their phases vary significantly, the difference remains steady.



(a) Capacitance-voltage curve of varactor

(b) Circuit design

Figure 8: Leggiero uses a varactor diode to conduct the analog signal conversion. It converts the input analog voltage to a small capacitance and then shifts the RF phase accordingly.

we show the junction capacitance versus the voltage for a silicon diode SMV2201 [54] and a GaAs diode GMV9822 [53].

By using the varactor diode, Leggiero relates external analog voltage to the small capacitance and thus the reflection coefficient of the tag. We design a passive circuit as shown in Fig. 8(b). It provides a continuously variable reflection coefficient that is used to convert the analog voltage signal into the RF phase. The circuit includes three transmission lines $\mathrm{TL}_{1,2,3}$, the varactor diode D_V, the biasing inductor L_{Bias} that works as a radio frequency choke (RFC) to isolate the DC path and the RF path, and a series capacitor C_S that blocks DC bias and the ground. The shorted to ground transmission line TL_2 works as an RF component at 2.4GHz and provides DC for the reverse-biased varactor diode D_V. The three transmission lines also offer flexibility in tuning the phase variations, which is evaluated in §6.4.3.

Note that all components used in this circuit are passive components and do not require a power source. The analog signal conversion of Leggiero consumes nearly no power since the main DC path is blocked by the capacitor C_S and the varactor diode D_V. The only DC current here is the reverse saturation current of the varactor diode, which is usually less than 0.01μA. Therefore, Leggiero conducts the analog signal conversion with negligible energy cost.

For a quick proof of the above design methodology, we build and simulate the passive conversion circuit using PathWave Advanced Design System (ADS). By tuning the impedance and the length of the transmission line, the tag provides a flat phase variation over the whole WiFi 2.4GHz frequency band. Fig. 5 shows the reflected phase versus the bias voltage when the signal frequency is 2.45GHz. We also show the relative phase variation over the whole 2.4GHz band in Fig. 6. We can see that the phases are flat and identical over the entire band for a given voltage.

Fig. 5 also shows the tag's supported input analog voltage range and its resolution (i.e., the amount of phase change corresponding to a certain voltage change). Note that by tuning the length of the three transmission lines $\mathrm{TL}_{1,2,3}$ and varying the capacitance of the series capacitor C_S, Leggiero tag can trade-off between the voltage range and the resolution. We show the evaluation result of this trade-off in §6.4.3. The resolution of Leggiero also heavily depends on the CSI reception accuracy on the receiver end since the actual sampling part of the voltage takes place in the CSI calculation process. We will assess this accuracy in §6.4.1.

Novelty of the conversion circuit. From the perspective of RF circuit design, Leggiero's reflective conversion circuit is an analog RF phase shifter, except that the circuit is reflective. Existing commercial analog phase shifting RFICs (Radio Frequency Integrated Circuit) can also vary the input RF signal phase according to an analog voltage. In general, these commercial ICs have complex circuit designs that provide wider frequency and phase-shifting ranges, with some also incorporating varactor diodes for analog-tunable phase shifting. However, we cannot use these components in Leggiero directly; instead, we design our own conversion circuit for the following reasons.

- **Power consumption and price:** Commercial ICs are designed for military radars, satellites, and beamforming phase arrays, where performance is the primary concern. For example, HMC928LP5E [7] is a 450° analog phase shifter on 2-4GHz. However, the uW-level power consumption demand and pricing constraints of backscatter tags make it impossible to use such ICs, which usually have mW-level power and cost more than \$50 each. Whereas our phase-shifting circuit consumes negligible power and only costs \$2.
- **Tag complexity:** The commercial ICs separate the input and output ports so that the signal enters from one port and exits on another. Using these ICs requires two antennas on the tag, leading to a complicated tag design.

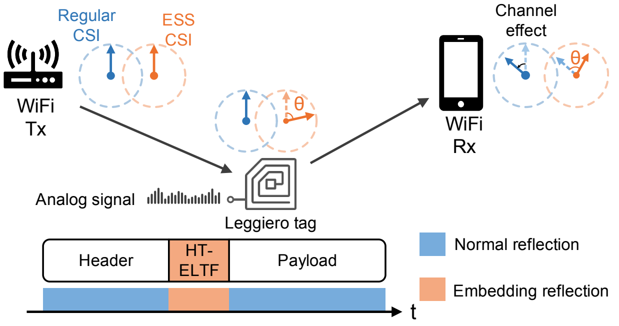


Figure 9: Transparent phase embedding of Leggiero. It finds the Extra LTF section of 802.11n packets and embeds the analog sensor reading in the RF phases. It is then extracted by calculating the phase difference.

- **Accuracy and robustness:** The robustness of our phase shifting circuit are on par with commercial ICs, as validated in the evaluation with a vector network analyzer (VNA). The result is depicted in the blue line in Fig. 21, indicating accurate and stable phase shifts conducted on the tag, with no errors.

In summary, our reflective phase shifter is a simple yet tailored solution that meets all the requirements of backscatter tags while providing accurate phase shifting at the same time.

3 TRANSPARENT PHASE EMBEDDING

We now introduce how Leggiero transparently embeds the converted RF phase information into the WiFi's packet, so that a commercial WiFi device can decode the analog sensor readings and the WiFi data simultaneously. Leggiero exploits the ESS feature of the 802.11n standard and embeds the sensor readings in WiFi's CSI. This section presents the details of the process of phase embedding.

3.1 Primer: Extra Spatial Sounding

For the WiFi transmission, CSI [41] acts as an indicator of the wireless channel from the transmitter to the receiver at certain frequencies. It characterizes the wireless channel and helps the WiFi receiver to decode the packets. In the backscatter scenario, the tag also influences the wireless channel by introducing attenuation and phase change to the RF signal. Leggiero leverages such influences and modifies the phase of the CSI according to the analog sensor readings.

As we all know, the environment dynamics (including multipath propagation) affect the state of a wireless channel [28]. The CSI changes caused by environment dynamics are likely to overwhelm the intentionally embedded phase change of CSI in Leggiero. In order to obtain the phase change correctly, it is necessary to avoid the environmental influences completely.

Leggiero exploits the extra spatial sounding (ESS) feature in 802.11n standard [1] to cancel out the environmental influences. ESS is originally used to sound extra spatial dimensions (i.e., extra channels) of the multi-input multi-output (MIMO) channel that are not utilized to transmit WiFi data. It inserts the same long training field (LTF) to the physical layer header of a WiFi packet. As shown in Fig. 2, the ESS LTF (or **HT-ELTF**, **E** for **E**xtra) follows closely after the regular HT-DLTF (**D** for **D**ata) in the 802.11n preamble, containing the same baseband signal. In a single-input single-output (SISO) scenario, these two LTFs will experience the same channel, thereby giving two identical CSI measurements. To show this consistency, we measure the CSIs in a noisy environment using two QCA9300 WiFi NICs [49], as shown in Fig. 7. As the phase of each CSI changes rapidly, the phase difference is always very close to 0.

3.2 Embedding Process

In order to embed the sensor reading into a WiFi packet, the Leggiero tag precisely embeds the converted RF phase information in the HT-ELTF section of an ESS-enabled WiFi packet. Other sections of the WiFi packet act as a reference and are reflected with a constant phase, including the original HT-DLTF. We refer to the tag's state when reflecting the HT-ELTF section as **the embedding state** and the corresponding extra CSI measurement as **the ESS CSI**. Similarly, we refer to the tag's state when reflecting other sections as **the reference state** and the CSI as **the regular CSI**. In this way, the phase difference between the ESS CSI and the regular CSI should be equal to the converted RF phase variation we introduced in §2. The environmental influences are completely canceled out when calculating the difference because both the ESS CSI and the regular CSI experience an identical wireless channel. The embedding process is shown in Fig. 9. To realize this design in practice, there are three critical problems to address.

• **Avoiding self interference.** Leggiero embeds the converted RF phase on the WiFi's CSI by changing the phase of the wireless channel. If the original link from the transmitter to the receiver persists, there exists some signal path that does not include the backscatter tag and results in a confused CSI phase difference. We solve this problem by shifting the frequency of the reflected signal by ±20MHz. The receiver will receive the WiFi packet in a secondary WiFi channel. This frequency shifting is achieved by multiplying the incident signal with a 20MHz square wave which can be generated using a ring oscillator. Existing WiFi backscatter works, such as HitchHike [68] and FreeRider [69], have used similar approaches. However, they use frequency shifting to separate the backscattered traffic from the carrier traffic's channel. Consequently, a single receiver can only receive either the carrier or the backscattered traffic at a time. To receive both simultaneously, two receivers are necessary. In contrast, Leggiero embeds the sensor signal in the extra CSI section without modifying the payload. In this way, after frequency shifting, the receiver can receive both the backscattered traffic and the carrier traffic simultaneously in the secondary channel without self-interference, improving channel utilization.

• **Locating HT-ELTF.** Since the Leggiero tag goes into the embedding state only in the HT-ELTF section of a WiFi packet, it needs to synchronize the switching time with this section. We achieve this by incorporating a commonly used packet detection circuit into the tag, as illustrated in Fig. 10. The circuit consists of an envelope detector in a cascade connection with a voltage comparator. Specifically, the signal strength output of the envelope detector is directly compared to a reference voltage using the comparator. Once the WiFi transmitter starts its transmission, a signal will be generated on the comparator, enabling the tag to identify the beginning of a

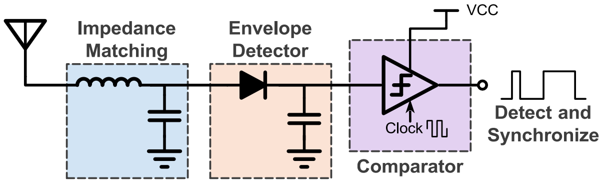


Figure 10: Packet detection and synchronization circuit of Leggiero. An envelope detector is connected to the antenna. The output signal strength is compared with a threshold to locate the beginning of a packet.

WiFi packet. Meanwhile, the tag stays in the reference state in the preceding header, which lasts for exactly 36μs. It then switches to the embedding state in the HT-ELTF section, which has the same 4μs duration as the WiFi data symbols. Finally, at the end of the HT-ELTF section, the tag switches back to the reference state. Note that the envelope detector can be passive and consumes zero power, allowing the power consumption of this circuit to be as low as a single-digit μW.

In practice, mismatches in the synchronization exist and may impact the performance of the phase embedding. For instance, the tag may experience a delay in its switching time compared to the beginning of the HT-ELTF section. In Leggiero, we find that a synchronization accuracy of 250ns between them is enough for the phase embedding process and results in negligible demodulation errors. This mismatch or tag delay tolerance is mainly attributed to the preceding guard interval (GI) inside the CSI section. The GI lasts for 0.8μs and is excluded during the CSI calculation, while the latter 3.2μs baseband signal is actually used. Small synchronization delays (less than 0.8μs) will fall into the preceding GI section so that its impact is naturally minimized during the GI removal. The 250ns synchronization requirement is met by applying a 4MHz clock to the comparator, which can be derived from the main 20MHz clock. §6.4.2 presents our validation of the synchronization error (i.e., mismatch) and its impact on backscattering. It shows that the mismatch's impact on demodulation is negligible with the 4MHz clock applied in our implementation. A Similar level of accuracy has also been achieved in state-of-the-art WiFi backscatter systems [10, 68, 69].

• **Designing reference circuit.** Leggiero uses the CSI phase difference between the embedding and the reference states to encode and decode the analog sensor readings. The phase in the reference state is also determined by the tag. Therefore, designing the reference circuit is important. Naturally, we set the tag's phase in the reference state equal to a 0V phase in the embedding state. Then, a phase difference of 0° corresponds to 0V of the tag's analog voltage. The other phase-voltage correspondences are the same as in Fig. 5.

A straightforward reference circuit design is to switch the DC bias voltage of the varactor diode between the input voltage in the embedding state and 0V in the reference state, respectively, as shown in Fig. 11(a). However, it does not work in practice. The RF choke L_{Bias} and capacitor C_S together form an LC circuit for the input voltage. This circuit has a transient process when switching from 0V to the input voltage. It causes the voltage of the varactor diode to stabilize gradually instead of changing instantaneously. This transient process may last for more than 2us long in our implementation. It seriously affects the synchronization accuracy and corrupts the embedded phase, as shown in Fig. 11(b).

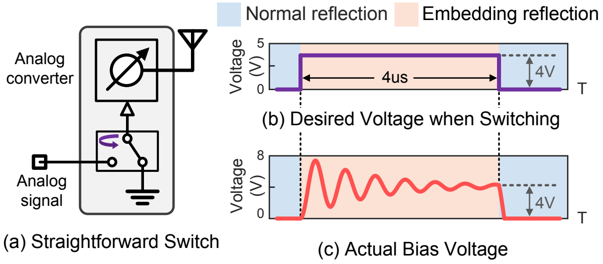


Figure 11: Problem of the straightforward approach. (a) The direct voltage switching method. (b) Due to the transient process of the LC circuit, the varactor's actual bias voltage varies in the phase embedding state.

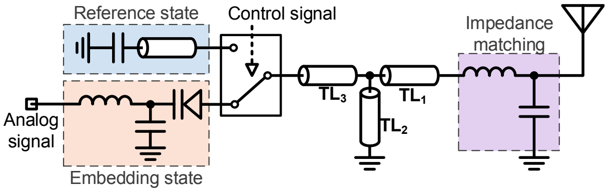


Figure 12: Phase embedding circuit schematic of Leggiero. The tag uses an RF switch for the reference circuit.

In order to avoid this transient process and reduce the switching time, Leggiero adds an RF switch in front of the varactor diode. As shown in Fig. 12, The RF switch toggles between the varactor diode branch and the constant phase branch, which correspond to the embedding state and the reference state, respectively. By carefully selecting the capacitor and length of the transmission line on the constant phase branch, the Leggiero tag sets the reference state's phase to be equal to a 0V phase of the embedding state. Compared with the straightforward approach, a common RF switch such as ADG918/919 [9] has a switching time of less than 10ns, which is more than 200 times faster than the LC transient process. Therefore, using an RF switch to toggle from two branches can easily satisfy our synchronization requirement.

3.3 Extracting Analog Readings

So far, we have explained how Leggiero embeds the analog sensor readings into a WiFi packet. We now introduce the method to extract these readings.

In the backscatter process of Leggiero, the ESS CSI and the regular CSI experience identical wireless channels except for the phase variation brought by the embedding state of the tag. We denote the phase difference between the embedding state and the reference state as θ_V. Then, the regular CSI $\mathbf{H}_{regular}$ and the ESS CSI $\mathbf{H}_{ess}$ are calculated by:

$$\mathbf{H}_{regular} = \mathbf{H}_{air} \cdot \mathbf{H}_{err}, \tag{5}$$

$$\mathbf{H}_{ess} = \mathbf{H}_{air} e^{j\theta_V} \cdot \mathbf{H}_{err}, \tag{6}$$

where $\mathbf{H}_{air}$ denotes the environmental wireless channel response, and $\mathbf{H}_{err}$ includes all phase errors induced by carrier frequency

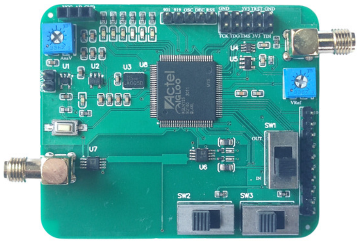


Figure 13: The prototype of Leggiero tag.

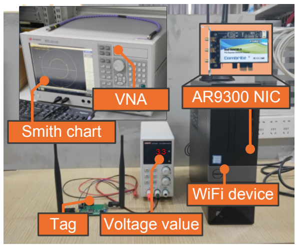


Figure 14: Experiment setup.

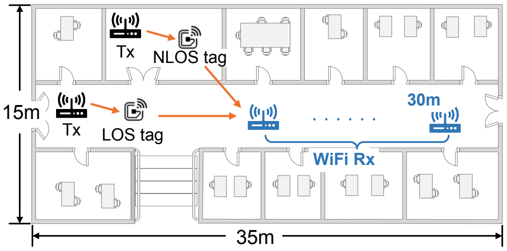


Figure 15: Experiment environment for LOS and NLOS evaluation

offset (CFO), sampling frequency offset (SFO), etc. By taking the division of these complex CSI values, we obtain the phase difference converted from the analog voltage:

$$\frac{\mathbf{H}_{ess}}{\mathbf{H}_{regular}} = e^{j\theta_V} . \tag{7}$$

After obtaining the phase difference θ_V, we should convert it back to the analog voltage according to the phase-voltage relation shown in Fig. 5. Since the conversion from voltage to phase is near-linear, in theory, the analog voltage value can be obtained by simply dividing the phase by a constant. However, random measurement error exists in the CSI phase difference in practice. To deal with this error, we split the whole possible phase range into several discrete segments to achieve digitization of the sensor voltage. The number of segments determines the resolution of this sampling process. A higher segment number means higher throughput, but more errors may be introduced to digitization. We evaluate the digitization resolution of the Leggiero tag in §6.4.4. In this way, Leggiero transfers the sensor readings completely in the analog form without using microprocessors and shifts the sampling part to the WiFi receiver.

Last but not least, according to 802.11n, the ESS CSI is only used as an extra sounding of the wireless channel and is not used to decode the WiFi data. The embedded phase change does not interfere with the decoding of the original payload. Therefore, Leggiero works transparently with WiFi networks with no impact on the WiFi's throughput.

4 THE MAC LAYER DESIGN

As described in the previous section, Leggiero interacts with two WiFi channels (20MHz apart from each other), since frequency shifting is involved. Without confusing the terms, we refer to the channel where the WiFi transmitter operates as the original channel, and the channel that the tag shifts the frequency to as the secondary channel. With regard to the design of MAC (Medium Access Control), Leggiero employs a receiver-initiated process, detailed as follows.

The reader (i.e., the receiver in Fig. 1) switches to the secondary channel when it is ready to receive backscattered sensor data from the tag. The reader first broadcasts a *CTS_TO_SELF* to reserve the channel, followed by two consecutive excitation packets with a specific interval. The tag recognizes this pattern of packets with its onboard packet detector. Then the tag wakes up and gets ready for backscatter. From then on, the packets sent by the transmitter in the original channel will excite the tag, making the latter conduct the corresponding operations including phase embedding and frequency shifting. The reader listening in the secondary channel is able to receive those packets from the tag. The reader can send ACKs back to the transmitter right in the secondary channel. According to the frequency shifting mechanism, the tag will shift the frequency of the ACKs back to the original channel, so that the transmitter can receive them.

As for the transmitter, there is not any modification to its MAC layer. A transmitter can work in a way exactly the same as that in a normal WiFi network.

5 IMPLEMENTATION

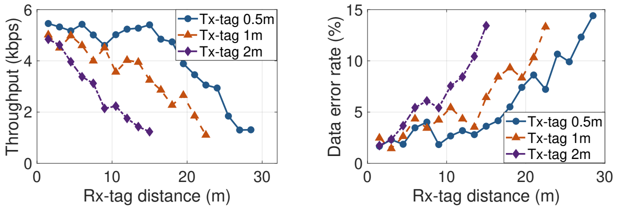
5.1 Backscatter Tag

We implement the Leggiero tag on a printed circuit board (PCB) using commercial off-the-shelf components, as shown in Fig. 13. The tag contains two RF paths: the packet detector and the backscatter circuit, each connected with a typical 2.4GHz omnidirectional antenna, at 3dBi gain.

The packet detector is implemented using an LT5534[58] envelope detector and a comparator TLV3201[20]. It identifies the arriving WiFi packet and achieves synchronization so that the tag can locate the HT-ELTF section.

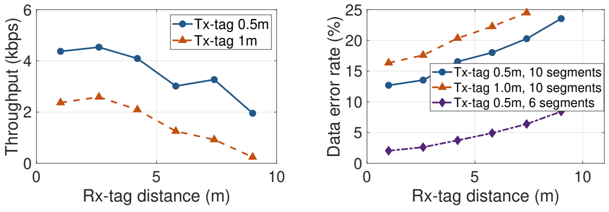
The backscatter circuit mainly consists of three modules: voltage-phase conversion, control logic, and frequency shifting. We use PathWave ADS to simulate and implement the voltage-phase conversion circuit, using a SMV2201[54] as the varactor diode and the microstrip line as the transmission line. To switch between the embedding state and the reference state, we use an ADG919[9] RF switch. The control logic of the phase embedding is implemented using a nano-low power ALGN125 FPGA[43]. Note that the FPGA included in our prototype only works as a part of the radio, providing its control logic. When delivered to production, the FPGA will be substituted by digital gate circuits, consuming a mere 1 to 2 μW power. For frequency shifting, we build a ring oscillator with 3 SN74AUP3G04[19] inverters to generate a 20MHz clock. By multiplying the incident signal with this clock signal, the backscattered WiFi signal is moved ±20MHz away on the frequency band. In our implementation, the multiplication is done by toggling an ADG901[8] RF switch at 20MHz.

As an analog backscatter interface, Leggiero tag supports connecting any peripheral analog sensors in a **plug-and-play** manner. In our implementation, we connect the tag with two types of analog



(a) Throughput (b) DER of 10 segments digitization

Figure 16: LOS throughput and data error rate.



(a) Throughput (b) DER

Figure 17: NLOS throughput and data error rate.

sensors, a light intensity sensor using a photoresistance (GL7549) and a joystick position sensor (EGN-J-O100A). Both sensors output the sensor readings as voltage signals. No MCU is used in such a tag-sensor connection. We show the proof-of-concept application using the light sensor in §6.6.

5.2 WiFi Transceiver

The WiFi transmitter and the WiFi receiver are two computers equipped with Atheros AR9300 WiFi NICs [49]. Leggiero does not modify the WiFi hardware. The transmission of ESS-featured 802.11n packets, CSI acquisition, as well as the aforementioned MAC layer design is enabled after a driver upgrade. Our receiver uses the PicoScenes CSI tool [48] to obtain CSI measurements. It records both the regular CSI and the ESS CSI so that the receiver can extract the embedded sensor readings.

6 EVALUATION

We first show the methodology in §6.1 and the overall performance in §6.2. §6.3 presents the power consumption and power benefit of Leggiero. §6.4 presents the result of ablation studies. §6.5 evaluates the impact on WiFi carrier transmissions. Finally, we show the proof-of-concept application of Leggiero in §6.6.

6.1 Methodology

To evaluate the transmission capacity and efficiency of Leggiero, we first define its throughput and data error rate. Leggiero's reader splits the possible phase range into several segments. The number of segments determines how many bits can be embedded in a packet. Therefore, the **throughput** is calculated as the product of the number of received backscatter packets and the number of bits each packet contains. Similarly, a data error occurs when the digitalized sensor voltage falls into the wrong segment. We calculate the **data error rate (DER)** by measuring the proportion of packets with data errors to the total number of received packets.

6.2 Overall Performance

We first evaluate the throughput and DER of Leggiero in the line-of-sight (LOS) and non-line-of-sight (NLOS) scenarios. We conduct our experiment in an office area, as shown in Fig. 15. The transmitter is placed at the end of the corridor and inside a meeting room for line-of-sight and non-line-of-sight scenarios, respectively. It transmits packets at a peak power of 30dBm on WiFi channel 1. The tag shifts the frequency of the WiFi signal by ±20MHz, so that the backscattered signals are in channel 5. We let the transmitter transmit 2000 packets per second for 10 seconds and receive them at different Tx-tag distances and Rx-tag distances. The experiment in each position is repeated 20 times so that the tag embeds 20 different voltages in the range of 0V to 5V into the WiFi packets. Unless otherwise posted, the following experiments use the same setting.

Upon receiving the packet, the receiver calculates the phase difference in CSIs of all 56 subcarriers. Since the Leggiero tag provides flat phase conversion on the whole frequency band, all 56 subcarriers have the same phases in theory. We take their average to be digitalized. In this experiment, we split the phase range of about 40 degrees into ten segments so that each embedded packet contains about 3.3 bits of information.

The throughput in the LOS scenario is shown in Fig. 16(a). Leggiero achieves a throughput of about 5Kbps when the tag is close to the Tx or the Rx. The throughput decreases when the distance between the tag and Tx/Rx increases due to the energy degradation of the backscattered signal. Moreover, Leggiero achieves a communication range of about 30m, which is comparable to the existing works.

The DER in the LOS scenario is shown in Fig. 16(b). We can see that Leggiero achieves a DER of less than 5% when the tag is close to the Tx or the Rx. The DER increases to about 10% when the distance increases. Although the phase difference should be fixed in theory, a few degrees of random measurement error exist in the CSI calculation. This random error will increase when the distance increases due to lower signal strength and a more complex multipath environment. To achieve a better DER, we can reduce the number of segments during the digitization, so as to have a higher tolerance of the phase error. We evaluate this method in §6.4.4.

The throughput and DER of Leggiero in the NLOS scenario are shown in Fig. 17. Leggiero achieves about 4Kbps throughput in the NLOS scenario. For the DER, we find that when using the same segment number as that in the LOS scenario, the DER degrades to around 20%. Such degradation can be compensated by using smaller segment numbers. When the segment number is 4, the DER will be less than 10%. In other words, we can trade the throughput for better error tolerance in the NLOS scenario.

The throughput of Leggiero is sufficient to meet the data collection requirement of many IoT sensing applications, but it may be argued that such throughput is not comparable to that of many digital backscatter approaches. It is worth emphasizing that Leggiero achieves such a throughput in a transparent manner, which doesn't hurt the WiFi carrier's throughput, as shown in §6.5.

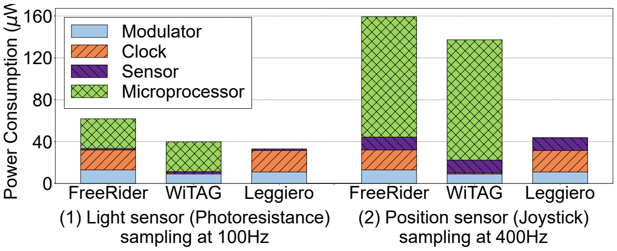


Figure 18: Comparison of the end-to-end power consumption breakdown when connecting with sensors.

6.3 Power Consumption

6.3.1 Tag Power Consumption. The Leggiero tag's power consumption mainly comes from four parts: RF switches, packet detector, control logic, and the 20MHz clock generation. Here we report the power in an ASIC solution. We use two RF switches in our implementation, one for communication state switching and one for frequency shifting. These switches consume 2μW in total according to off-the-shelf products [8]. The packet detector can work in a hierarchical mode and consumes about 7μW when implemented in 65nm CMOS technology [10]. The control logic provides the control signal and consumes 1 to 2μW power according to existing study [68]. The clock generation is the major source of power consumption. Similar to the existing WiFi backscatter works [70], we use a ring oscillator to generate the 20MHz clock, which consumes 20μW in ASIC technology. Therefore, the power consumption of a Leggiero tag in the ASIC implementation will be around 30μW. For a prototype PCB implementation, the power consumption is around 40mW.

Meanwhile, a Leggiero tag can work with existing RF energy harvesting technologies that harvest RF energy. Such an energy harvester can provide more than 30μW of power [32], which is the power consumption of the Leggiero tag. Other energy harvesters such as solar panels can also be considered to power the tag. A small solar panel of 2-3cm^2 is sufficient to provide energy for a Leggiero tag.

6.3.2 Power Benefit. To fully understand the power benefit of Leggiero, we compare it to existing WiFi backscatter systems, specifically FreeRider [69] and WiTAG [2]. These two works are representative of state-of-the-art WiFi backscatter systems [6]. We compare the end-to-end power consumption of transferring sensor data, as shown in Fig. 18. We choose power consumption under the same acquisition speed as the metric rather than the energy efficiency of data transmission (measured by bit per joule). This is because we desire to evaluate the entire sensing process of the backscatter tag, including sensor reading acquisition, sensor-radio interfacing, and transmission. Energy efficiency alone fails to take into account the power consumed during acquisition and interfacing.

In this experiment, we connect the tags with a light sensor and a position sensor, operating at 100Hz and 400Hz sampling rates, respectively. The data for WiTAG and FreeRider is acquired and fed to the radio by an external MCU MSP430FR5969 [21], which is the common solution for building digital backscatter sensors (e.g., WISP 5.0 platform). This MCU has very low standby and sleep currents (0.4μA and 0.02μA) and is put to sleep whenever possible to ensure a fair comparison. Whereas in Leggiero, the analog sensors can be directly connected. Furthermore, to ensure a fair comparison of the power of the backscatter radio, we use the optimal ASIC implementation result reported in each work [6]. We can see that Leggiero saves the energy consumption brought by the MCU, which has become the bottleneck for the digital backscatter sensor, especially in the case of a high sampling rate.

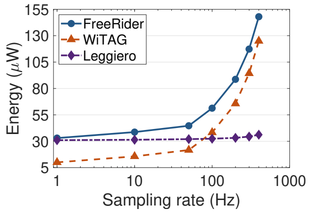


Figure 19: Power benefit of Leggiero.

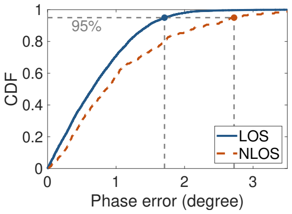


Figure 20: Phase error CDF for LOS and NLOS.

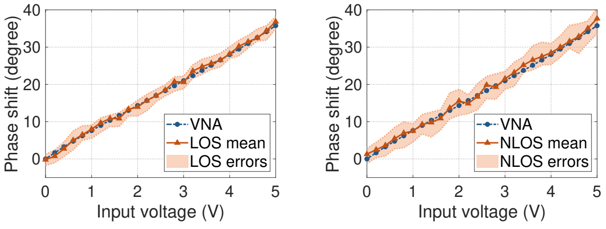
To further show the impact of sampling rates, we measure the end-to-end power consumption of the three tags when acquiring and transmitting the light sensor data at different sampling rates. Fig. 19 shows the result. Excluding the power brought by the peripheral sensor, the Leggiero tag has 4.8× and 4.0× lower power consumption at a sampling rate of 400Hz, compared with FreeRider [69] and WiTAG [2], respectively. The two existing approaches require 115μW power to interface with the sensor, which is often unaffordable for existing RF energy harvesting technologies and solar panels in indoor environments [6].

6.4 Ablation Study

To better understand the performance of Leggiero, we conduct ablation studies on the phase conversion, analog readings embedding, and readings extraction. §6.4.1 compares the phase conversion between CSI calculation and vector network analyzer (VNA) measurement. §6.4.2 presents the impact of synchronization errors of the embedding process. §6.4.3 shows the design considerations of different reflective circuit components. §6.4.4 presents the impact of the digitization resolution on the extraction of sensor readings.

6.4.1 Analog Conversion Accuracy. We measure the reflection coefficient of the tag under different input voltages to verify whether it is consistent with our simulation result. We use a Keysight E5071C VNA to measure the S_{11} parameter at an input voltage range of 0V to 5V. The result is shown in the blue line in Fig. 21. We can see that the Leggiero tag provides a linearly changing phase with respect to the voltage and the phase variation is consistent with the result of the simulation.

Next, we measure the phase-voltage relation of the embedded WiFi CSI. We calculate the phase difference between the ESS CSI and the regular CSI in LOS and NLOS scenarios. The input voltage range is also 0 to 5V with a step interval of 0.2V. Fig. 21(a) and Fig. 21(b) show the LOS result and NLOS result, respectively. We can see that the phase embedded in the WiFi CSI changes with the input voltage in a pattern that is the same as the VNA result. However, as we have mentioned, the inevitable measurement error exists in the CSI calculation, and it will result in some phase errors. Note that these phase errors are solely attributed to the CSI measurement of



(a) Line-of-sight scenario

(b) Non-line-of-sight scenario

Figure 21: Phase conversion comparison between VNA and wireless channel.

the channel, and have nothing to do with the tag's phase shifting circuit. Moreover, the phase error in the NLOS scenario is more than that in the LOS scenario, since the multipath environment is more complex.

To further study the phase error of the embedded WiFi CSI. We show the CDF of phase error in LOS and NLOS scenarios in Fig. 20. Although the maximum phase error in the NLOS scenario can be up to 4.5 degrees, more than 95% of the errors are less than 3 degrees. This means that by carefully selecting the number of segments during the digitization, Leggiero can provide a low DER in the NLOS scenario. Fig. 20 also shows that phase errors increase as the multipath becomes more severe. Nevertheless, it is important to note that successful packet decoding is a prerequisite for obtaining the CSI phase. When packets experience extreme multipath conditions, they cannot be successfully received and are naturally excluded from CSI measurement. Therefore, in general, the effect induced by multipath is limited, and the NLOS results in Fig. 20 exhibit the highest phase errors.

6.4.2 Synchronization Error of Embedding. Leggiero precisely embeds the converted phase in the HT-ELTF section of 802.11n packets. When reflecting, the tag needs to synchronize its switching time with this 4μs WiFi symbol. We now evaluate the impact of possible synchronization errors. In this experiment, we vary the switching time in a 150ns step to measure the throughput and the DER. The result is shown in Fig. 22. A negative error means that the state switching of the tag is before the actual arrival time of the HT-ELTF. A positive error means the opposite case. We find that the existence of the synchronization error degrades Leggiero's performance—the greater the error is, the worse the throughput and the DER will be. Interestingly, the degradation brought by the negative and the positive errors is different. A negative error affects the performance more seriously than a positive one with the same absolute value. The reason is that the LTF section contains a 0.8μs guard interval (GI) before the actual 3.2μs baseband signal. When calculating the CSI, the WiFi receiver only uses the latter 3.2μs signal and drops the GI. Therefore, a positive error less than 800 ns still includes the complete 3.2μs signal in its embedding state, which results in less degradation. The result shows that Leggiero can tolerate about 300ns synchronization error, which means that the switch requires a 4MHz clock to work properly. Such a clock can be acquired from our ring oscillator with a simple counter.

6.4.3 Reflective Circuit Component. In our current implementation, about 40 degrees of maximum phase shift is produced, and the phase changes linearly with the input voltage in the range of 0 to 5V. With different choices of the tag's component, these values may be different. Specifically, the length of the transmission line TL_2 in the reflective circuit design, as shown in Fig. 8(b), can greatly affect the phase-voltage relation. We adjust the length of the TL_2 and simulate the reflection coefficient of the circuit. The phase-voltage relation with different lengths is shown in Fig. 23. We find that by decreasing the length, we obtain a wider range and more fine-grained phase shift. But there are also disadvantages of using a shorter transmission line. The linear phase-voltage variation range will decrease, which means a smaller input voltage range. Moreover, a very short TL_2 may lead to a non-flat phase shift on the 2.4GHz frequency band. Given the same input voltage, the phase shift difference between 2.40GHz and 2.50GHz may be up to 10 degrees. Therefore, there is a trade-off in using different transmission lines. Here we leave the tag's component choice to users as they can flexibly select the transmission lines according to the application scenarios.

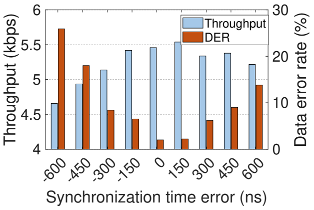


Figure 22: Impact of synchronization error.

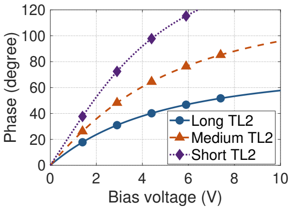


Figure 23: Different tag component choices.

6.4.4 Digitization Resolution of Extraction. When extracting the analog voltage at the tag, the receiver of Leggiero conducts a digitization process. The resolution of this process, namely the number of the split segment, is variable. In this experiment, we show the influence of setting different resolutions. We vary the number of the split segments and measure the throughput and the DER of Leggiero at a fixed distance. The result is shown in Fig. 24. With a higher segment number, Leggiero achieves higher resolution and therefore higher data throughput. At the same time, the DER goes up. There exists a trade-off in choosing the resolution, and the decision depends on the demand for high throughput or high reliability.

6.5 Impact on WiFi Carrier's Traffic

We compare Leggiero with existing works in terms of the impact on the WiFi carrier's traffic. We consider the single-reader backscatter approaches as the targets to compare. The dual-reader approaches such as HitchHike [68], FreeRider [69], and MOXScatter [71] require two readers to listen to the transmitter simultaneously and thus have low transparency in the coexistence scenario. We make a simulation to measure the reader's maximum WiFi throughput under different tag data rates. We calculate the ratio of the throughput with the backscatter tag and without the tag, as shown in Fig. 25. For *WiFi-Backscatter*[33], although it has high transparency, it only provides 400bps of data rate. For WiTAG[2], since it uses MAC layer OOK modulation, it corrupts about half of the frames to reach its maximum 4Kbps data rate. Leggiero can preserve all the packet payloads and always has high transparency regardless

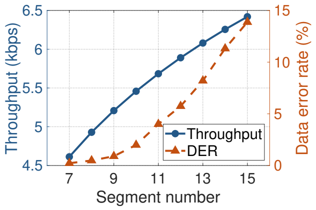


Figure 24: Impact of digitization resolution.

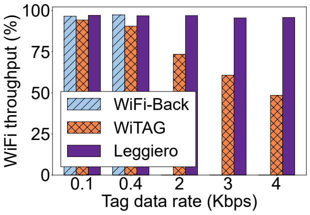
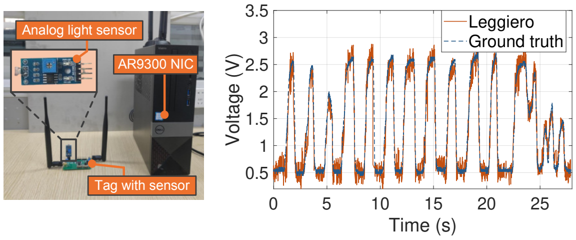


Figure 25: Tag's impact on WiFi throughput.



(a) Experiment setup (b) Light sensor voltage comparison

Figure 26: Proof-of-concept application with Leggiero.

of the tag data rate. Note that in this experiment, Leggiero's result includes the overhead of using ESS-enabled packets, while regular WiFi packets are used for existing works.

6.6 Proof-of-Concept Application

We build a real-world application of Leggiero, in which we connect the tag with the low-power light intensity sensor, as shown in Fig. 26(a). We manually modify the ambient light intensity and compare the Leggiero results with the ground truth in real-time, as shown in Fig. 26(b). The ground truth voltage is measured directly on the tag by a Tektronix MDO3000 oscilloscope, while the Leggiero voltage is calculated from the CSI phase difference according to the linear relationship shown in Fig. 21(a). This experiment is conducted in a noisy office environment to evaluate the robustness of Leggiero, with people walking around and computers and WiFi routers operating near the test site. The tag is placed 1 meter away from the WiFi transmitter and 10 meters away from the receiver.

We can see deviations in the Leggiero voltages in Fig. 26(b), which are caused by the errors in the CSI phase differences shown in Fig. 20. Since 95% of the phase errors are within 2 degrees in the LOS scenario, and 3 degrees in the NLOS scenario. That translates into voltage deviations within 0.25V and 0.375V, respectively. These deviations can be smoothed in the digitization process.

Leggiero directly transmits analog voltage signals over the air. Most types of analog sensors can be easily integrated with our tag without the need for complex interfacing or programming. We believe such a convenient plug-and-play scheme is a promising direction for future IoT systems.

7 DISCUSSION

• **Post-processing of sensor data.** The analog domain signal conversion of Leggiero is limited to producing the raw sensor signal. In reality, however, post-processing of the sensor data, such as local filtration or aggregation, is often needed in a sensing application. With the current design of Leggiero, such functionalities are offloaded from the local sensor unit to the remote WiFi receiver, which is more powerful in terms of computational capacity. We are also interested in exploring the design of low-power analog processing circuits [36] to realize such functionalities in our future work.

• **Digitization and noise.** We split the entire voltage range into several segments in the digitization process as a way of showing the bit throughput of Leggiero. However, in real-world applications, the sensor produces arbitrary analog voltage values, and no prior segmentation is possible. Instead, the collected sensor readings (i.e., arbitrary voltages) are sampled when the receiver completes reception and can be used directly. This delayed sampling is the key difference Leggiero introduces to sensing applications, as the sampled sensor readings can contain noise from the wireless communication channel. It causes jitters or deviations in the sensor readings as presented in §6.6. To mitigate these jitters, a low-pass or Kalman filter can be applied to the sensor readings, similar to the post-processing techniques used in modern IMU sensors [64]. Alternatively, one can decrease the length of the transmission line TL_2 according to §6.4.3, to achieve a more fine-grained phase shift and reduce voltage jitters for a fixed CSI phase deviation (e.g., 2 degrees in our LOS experiment).

• **Multi-sensor integration.** It is feasible to connect the Leggiero tag with multiple peripheral sensors. The design presented in this paper provides only one port for the sensor connection. It is not difficult to add a peripheral interface that interacts between the analog backscatter radio and the peripheral sensors. A simple solution is to use a multiplexer on the tag and transmit the sensor readings in a round-robin manner.

• **Multi-tag support.** When there are multiple tags in the network, access to the shared medium can be controlled by the reader. Specifically, the interval between two consecutive wake-up packets in the MAC layer design can be used to indicate the tag's ID. By altering this interval, the reader can switch the channel access from one tag to another.

• **Generalization of our approach.** Although ESS is enabled only in 802.11n, a legacy LTF field in newer standards (e.g., 802.11ac) also provides duplicate CSI for Leggiero's data embedding. As for MIMO, ESS CSI can work as duplicate channel information for a specific spatial stream to embed the tag's data. Therefore, applying Leggiero to newer WiFi standards and MIMO scenario is feasible.

8 RELATED WORKS

IoT sensing systems have experienced significant advances in recent years [16], evolving from early wireless sensor networks [3, 39, 44, 65] to emerging research areas such as wireless sensing [41, 63, 66] and battery-free sensing [25, 52]. Among the battery-free sensing solutions, backscatter technology has emerged as a promising option [12, 26, 29, 30, 40, 55, 59, 61, 62]. Traditional backscatter systems such as RFID [18, 31, 60, 74] require specialized readers to communicate with the tag. Ambient backscatter approaches utilize the existing wireless signals such as WiFi [4, 10, 34, 51, 71, 73], LoRa [13, 14, 27, 46], LTE [5], Bluetooth [11, 22, 67], and even mmWave [24, 42] as the carrier signals. Leggiero is related to two categories of backscatter works: WiFi backscatter and analog backscatter.

Technology	Through-put	Tag-Rx range	Trans-parency	Power at 400Hz sampling	Require μP
WiFi-Back.[33]	0.4Kbps	2m	High	125μW	Yes
HitchHike[68]	300Kbps	50m	Low	147μW	Yes
WiTAG[2]	4Kbps	15m	Med	125μW	Yes
Leggiero	5Kbps	30m	High	30μW	No

Table 1: Comparison with existing WiFi backscatter systems.

8.1 WiFi Backscatter

WiFi backscatter takes the ambient WiFi as the carrier signal to transmit data. Some existing WiFi backscatter approaches [68–70] propose to separate backscattered traffic from the carrier's traffic by shifting the backscattered signal's frequency. As a result, they require two receivers simultaneously listening on two channels to decode the backscattered data. Such dual-receiver designs are essentially customized and do not work in an arbitrary WiFi network.

Two existing approaches work with any WiFi transceiver pairs, namely *WiFi-Backscatter*[33] and WiTAG[2]. *WiFi-Backscatter*[33] modulates tag data on the WiFi carrier's packets by reflecting or absorbing the WiFi signals. The receiver employs an energy-based detection scheme to decode the tag data, which has gained widespread usage in heterogeneous communication [17]. It is far constrained in terms of throughput (0.4kbps) and communication range (3m). In WiTAG[2], the tag corrupts subframes in an aggregated frame from the sender, and the receiver uses the block ACK to transmit data back to the sender. Since block ACK is initially used for ACK from the receiver to the sender, the operation of WiTAG inevitably interferes with normal WiFi transmissions. For example, it assumes the ACKs are always positive in normal communications. In comparison, Leggiero's backscattered traffic is transparent to the carrier WiFi's traffic and achieves higher throughput and longer range.

We summarize the comparison between Leggiero and existing works in Table 1. Note that the power consumption values listed in the table for a sampling rate of 400Hz do not take into account any peripheral sensor modules, so as to ensure that they are not specific to any particular application. All the existing digital backscatter approaches require complicated operations and the help of MCUs to interface with sensors, which induces relatively high power consumption and often overburdens a tag's limited energy budget. In comparison, Leggiero proposes a tailored design for IoT sensors and avoids high power consumption through analog domain signal conversion.

8.2 Analog Backscatter

Existing digital backscatter designs do not include external data acquisition and require microprocessors as the interface media. In contrast, analog backscatter fits with sensor signal streaming inherently. Many sensing and streaming applications can be done in an ultra-low power manner. [57] builds a battery-free analog sensing platform by continuously varying the impedance of the antenna to achieve an amplitude modulation (AM). [56] demonstrates a battery-free audio communication system also by modulating the amplitude of the signal. There exists a frequency-modulated analog RF backscatter system [50], but the demodulation is still amplitude-based. One problem with these AM systems is that the amplitude of the analog sensor signal is weak and may be easily influenced by noise. Therefore, these approaches often require a high SNR scenario to work properly.

Recent researches begin to seek preferable analog transmission media. Video backscatter [45] proposes to use the duration of reflecting in one state to achieve pulse width modulation. It builds a video streaming backscatter link to demonstrate the high throughput of such an analog modulation mechanism. The work in [72] builds a microphone array backscatter that enables concurrent transmission based on this mechanism. Similarly, [37] presents a direct analog sensor-radio bus using duration-based analog backscatter. Moreover, the RF signal phase is also considered to convey the sensor readings directly [15, 35].

The differences between Leggiero and the existing analog backscatter approaches mainly lie in two aspects. First, Leggiero is compatible and coexists well with commodity networks. It does not require a dedicated exciter or receiver to generate sine tone excitation or decode the backscattered data. Instead, it embeds sensor readings in the extra CSI while preserving the WiFi carrier's traffic. Second, compared with existing RF phase-based designs, Leggiero provides a generic analog interface for various types of sensors at a low cost. The analog signal conversion only costs $2, without using expensive components like a circulator (more than $10) or high insertion loss components like a SAW filter (more than 3dB).

9 CONCLUSION

This paper presents Leggiero, an analog WiFi backscatter that enables ultra-low power transmission of the IoT sensor data in commodity WiFi networks. Leggiero directly embeds analog sensor readings in the ESS CSI of WiFi packets, avoiding the use of power-hungry microprocessors. At the same time, Leggiero works transparently with WiFi networks. Our evaluations show that Leggiero provides 4.8× and 4× power reduction compared to the existing approaches. It achieves a 5Kbps throughput with minimal effect on the WiFi carrier's throughput performance.

Leggiero introduces a novel passive RF computing mechanism that operates on the RF signal's phase during its propagation in the analog domain. It is low power, low latency, and high efficiency, making it suitable for ubiquitous sensing. Looking ahead, the future work on Leggiero may include incorporating analog data post-processing capabilities and improving the capacity of the passive phase embedding. Moreover, we believe that further research on similar RF computing techniques will facilitate the advancement of low-power IoT technology, and we look forward to exploring these possibilities in future studies.

ACKNOWLEDGMENTS

We sincerely thank our anonymous shepherd and all reviewers for their valuable feedback. This work is supported in part by the Joint Funds of the National Natural Science Foundation of China under grant No. U21B2007, and the Guoqiang Institute of Tsinghua University under grant No. 2021GQG1002.

REFERENCES

[1] IEEE Std 802.11n 2009. 2009. IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput. *IEEE Std 802.11n-2009* (2009), 1–565.

[2] Ali Abedi, Farzan Dehbashi, Mohammad Hossein Mazaheri, Omid Abari, and Tim Brecht. 2020. WiTAG: Seamless WiFi Backscatter Communication. In *Proceedings of the 2020 ACM SIGCOMM*. Association for Computing Machinery, New York, NY, USA, 240–252.

[3] Catalina Aranzazu-Suescun and Mihaela Cardei. 2017. Distributed algorithms for event reporting in mobile-sink WSNs for Internet of Things. *Tsinghua Science and Technology (TST)* 22, 4 (2017), 413–426.

[4] Dinesh Bharadia, Kiran Raj Joshi, Manikanta Kotaru, and Sachin Katti. 2015. BackFi: High Throughput WiFi Backscatter. In *Proceedings of the 2015 ACM SIGCOMM*. Association for Computing Machinery, New York, NY, USA, 283–296.

[5] Zicheng Chi, Xin Liu, Wei Wang, Yao Yao, and Ting Zhu. 2020. Leveraging Ambient LTE Traffic for Ubiquitous Passive Communication. In *Proceedings of the 2020 ACM SIGCOMM*. Association for Computing Machinery, New York, NY, USA, 172–185.

[6] Farzan Dehbashi, Ali Abedi, Tim Brecht, and Omid Abari. 2021. Verification: can wifi backscatter replace RFID?. In *Proceedings of the 2021 ACM Mobicom*. Association for Computing Machinery, New York, NY, USA, 97–107.

[7] Analog Devices. 2012. Analog Devices HMC928LP5E 450° analog phase shifter in 2-4GHz. https://www.analog.com/media/en/technical-documentation/data-sheets/hmc928.pdf

[8] Analog Devices. 2017. Analog Devices ADG901 wideband SPST RF switch. https://www.analog.com/media/en/technical-documentation/data-sheets/adg901_902.pdf

[9] Analog Devices. 2017. Analog Devices ADG919 wideband SPDT RF switch. https://www.analog.com/media/en/technical-documentation/data-sheets/ADG918_919.pdf

[10] Manideep Dunna, Miao Meng, Po-Han Wang, Chi Zhang, Patrick Mercier, and Dinesh Bharadia. 2021. SyncScatter: Enabling WiFi like synchronization and range for WiFi backscatter Communication. In *Proceedings of the 2021 USENIX NSDI*. USENIX Association, Virtual Event, 923–937.

[11] 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 *Proceedings of the 2015 IEEE RFID*. IEEE, Tokyo, Japan, 78–85.

[12] Xiuzhen Guo, Yuan He, Zihao Yu, Jiacheng Zhang, Yunhao Liu, and Longfei Shangguan. 2022. RF-Transformer: A Unified Backscatter Radio Hardware Abstraction. In *Proceedings of the 2022 ACM MobiCom*. Association for Computing Machinery, New York, NY, USA, 446–458.

[13] Xiuzhen Guo, Longfei Shangguan, Yuan He, Nan Jing, Jiacheng Zhang, Haotian Jiang, and Yunhao Liu. 2022. Saiyan: Design and Implementation of a Low-power Demodulator for LoRa Backscatter Systems. In *Proceedings of the 2022 USENIX NSDI*. USENIX Association, Renton, WA, 437–451.

[14] Xiuzhen Guo, Longfei Shangguan, Yuan He, Jia Zhang, Haotian Jiang, Awais Ahmad Siddiqi, and Yunhao Liu. 2020. Aloba: Rethinking ON-OFF Keying Modulation for Ambient LoRa Backscatter. In *Proceedings of the 2020 ACM Sensys*. Association for Computing Machinery, New York, NY, USA, 192–204.

[15] Agrim Gupta, Cédric Girerd, Manideep Dunna, Qiming Zhang, Raghav Subbaraman, Tania Morimoto, and Dinesh Bharadia. 2021. WiForce: Wireless Sensing and Localization of Contact Forces on a Space Continuum. In *Proceedings of the 2021 USENIX NSDI*. USENIX Association, Virtual Event, 827–844.

[16] Yuan He, Junchen Guo, and Xiaolong Zheng. 2018. From Surveillance to Digital Twin: Challenges and Recent Advances of Signal Processing for Industrial Internet of Things. *IEEE Signal Processing Magazine* 35, 5 (2018), 120–129.

[17] Yuan He, Xiuzhen Guo, Xiaolong Zheng, Zihao Yu, Jia Zhang, Haotian Jiang, Xin Na, and Jiacheng Zhang. 2022. Cross-Technology Communication for the Internet of Things: A Survey. *ACM Computing Surveys (CSUR)* 55, 5, Article 89 (dec 2022), 29 pages.

[18] Yuan He, Yilun Zheng, Meng Jin, Songzhen Yang, Xiaolong Zheng, and Yunhao Liu. 2021. RED: RFID-Based Eccentricity Detection for High-Speed Rotating Machinery. *IEEE Transactions on Mobile Computing (TMC)* 20, 4 (2021), 1590–1601.

[19] Texas Instruments. 2011. Texas Instruments SN74AUP3G04 low-power triple inverter gate. https://www.ti.com/lit/ds/symlink/sn74aup3g04.pdf

[20] Texas Instruments. 2016. Texas Instruments TLV3201 high-speed, single push-pull comparator. https://www.ti.com/product/TLV3201

[21] Texas Instruments. 2018. Texas Instruments MSP430FR5969 Mixed-Signal Microcontrollers. https://www.ti.com/product/MSP430FR5969

[22] Vikram Iyer, Vamsi Talla, Bryce Kellogg, Shyamnath Gollakota, and Joshua Smith. 2016. Inter-Technology Backscatter: Towards Internet Connectivity for Implanted Devices. In *Proceedings of the 2016 ACM SIGCOMM*. Association for Computing Machinery, New York, NY, USA, 356–369.

[23] Hrishikesh Jayakumar, Kangwoo Lee, Woo Suk Lee, Arnab Raha, Younghyun Kim, and Vijay Raghunathan. 2014. Powering the Internet of Things. In *Proceedings of the 2014 IEEE/ACM International Symposium on Low Power Electronics and Design (ISLPED)*. Association for Computing Machinery, New York, NY, USA, 375–380.

[24] Chengkun Jiang, Junchen Guo, Yuan He, Meng Jin, Shuai Li, and Yunhao Liu. 2020. MmVib: Micrometer-Level Vibration Measurement with Mmwave Radar. In *Proceedings of the 2020 ACM Mobicom*. Association for Computing Machinery, New York, NY, USA, 13 pages.

[25] Chengkun Jiang, Yuan He, Xiaolong Zheng, and Yunhao Liu. 2021. OmniTrack: Orientation-Aware RFID Tracking With Centimeter-Level Accuracy. *IEEE Transactions on Mobile Computing (TMC)* 20, 2 (2021), 634–646.

[26] Haotian Jiang, Jiacheng Zhang, Xiuzhen Guo, and Yuan He. 2021. Sense Me on the Ride: Accurate Mobile Sensing over a LoRa Backscatter Channel. In *Proceedings of the 2021 ACM Sensys*. Association for Computing Machinery, New York, NY, USA, 125–137.

[27] Jinyan Jiang, Zhenqiang Xu, Fan Dang, and Jiliang Wang. 2021. Long-range ambient LoRa backscatter with parallel decoding. In *Proceedings of the 2021 ACM Mobicom*. Association for Computing Machinery, New York, NY, USA, 684–696.

[28] Zhiping Jiang, Tom H. Luan, Xincheng Ren, Dongtao Lv, Han Hao, Jing Wang, Kun Zhao, Wei Xi, Yueshen Xu, and Rui Li. 2022. Eliminating the Barriers: Demystifying Wi-Fi Baseband Design and Introducing the PicoScenes Wi-Fi Sensing Platform. *IEEE Internet of Things Journal (IOTJ)* 9, 6 (2022), 4476–4496.

[29] Meng Jin, Yuan He, Chengkun Jiang, and Yunhao Liu. 2021. Parallel Backscatter: Channel Estimation and Beyond. *IEEE/ACM Transactions on Networking (TON)* 29, 3 (mar 2021), 1128–1140.

[30] Meng Jin, Yuan He, Xin Meng, Dingyi Fang, and Xiaojiang Chen. 2018. Parallel Backscatter in the Wild: When Burstiness and Randomness Play with You. In *Proceedings of the 2018 ACM Mobicom*. Association for Computing Machinery, New York, NY, USA, 471–485.

[31] Meng Jin, Yuan He, Songzhen Yang, Yunhao Liu, Li Yan, and Yuyi Sun. 2022. Versatile RFID-based Sensing: Model, Algorithm, and Applications. *IEEE Transactions on Mobile Computing (TMC)* (2022), 1–14.

[32] Ermeey Abd. Kadir, Aiguo Patrick Hu, Morteza Biglari-Abhari, and Kean C Aw. 2014. Indoor WiFi energy harvester with multiple antenna for low-power wireless applications. In *IEEE 23rd International Symposium on Industrial Electronics (ISIE)*. IEEE, Istanbul, Turkey, 526–530.

[33] Bryce Kellogg, Aaron Parks, Shyamnath Gollakota, Joshua R Smith, and David Wetherall. 2014. Wi-Fi backscatter: Internet connectivity for RF-powered devices. In *Proceedings of the 2014 ACM SIGCOMM*. Association for Computing Machinery, New York, NY, USA, 607–618.

[34] Bryce Kellogg, Vamsi Talla, Shyamnath Gollakota, and Joshua R. Smith. 2016. Passive Wi-Fi: Bringing Low Power to Wi-Fi Transmissions. In *Proceedings of the 2016 USENIX NSDI*. USENIX Association, Santa Clara, CA, 151–164.

[35] Nabil Khalid, Rashid Mirzavand, Hossein Saghlatoon, Mohammad Mahdi Honari, Ashwin K. Iyer, and Pedram Mousavi. 2022. A Batteryless RFID Sensor Architecture With Distance Ambiguity Resolution for Smart Home IoT Applications. *IEEE Internet of Things Journal (IOTJ)* 9, 4 (2022), 2960–2972.

[36] Fabian Khateb, S Bay Abo Dabbous, and Spyridon Vlassis. 2013. A survey of non-conventional techniques for low-voltage low-power analog circuit design. *RadioEngineering* 22, 2 (2013), 415–427.

[37] Songfan Li, Chong Zhang, Yihang Song, Hui Zheng, Lu Liu, Li Lu, and Mo Li. 2020. Internet-of-microchips: direct radio-to-bus communication with SPI backscatter. In *Proceedings of the 2020 ACM Mobicom*. Association for Computing Machinery, New York, NY, USA, Article 25, 14 pages.

[38] 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 2018 ACM Sensys*. Association for Computing Machinery, Shenzhen, China, 159–171.

[39] Zhenjiang Li, Mo Li, and Yunhao Liu. 2014. Towards Energy-Fairness in Asynchronous Duty-Cycling Sensor Networks. *ACM Transactions on Sensor Networks (TOSN)* 10, 3, Article 38 (may 2014), 26 pages.

[40] Xin Liu, Zicheng Chi, Wei Wang, Yao Yao, and Ting Zhu. 2020. VMscatter: A Versatile MIMO Backscatter. In *Proceedings of the 2020 USENIX NSDI*. USENIX Association, Santa Clara, CA, 895–909.

[41] Yongsen Ma, Gang Zhou, and Shuangquan Wang. 2019. WiFi Sensing with Channel State Information: A Survey. *ACM Computing Surveys (CSUR)* 52, 3, Article 46 (2019), 36 pages.

[42] Mohammad Hossein Mazaheri, Alex Chen, and Omid Abari. 2021. mmTag: A Millimeter Wave Backscatter Network. In *Proceedings of the 2021 ACM SIGCOMM*. Association for Computing Machinery, New York, NY, USA, 463–474.

[43] Microsemi. 2014. Microsemi AGLN125 IGLOO nano Low Power Flash FPGA. https://www.microsemi.com/product-directory/fpgas/1689-igloo#igloo-nano

[44] Lufeng Mo, Yuan He, Yunhao Liu, Jizhong Zhao, Shao-Jie Tang, Xiang-Yang Li, and Guojun Dai. 2009. Canopy Closure Estimates with GreenOrbs: Sustainable Sensing in the Forest. In *Proceedings of the 2009 ACM Sensys*. Association for Computing Machinery, New York, NY, USA, 99–112.

[45] Saman Naderiparizi, Mehrdad Hessar, Vamsi Talla, Shyamnath Gollakota, and Joshua R Smith. 2018. Towards Battery-Free HD Video Streaming. In *Proceedings of the 2018 USENIX NSDI*. USENIX Association, Renton, WA, 233–247.

[46] 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 *Proceedings of the 2018 ACM SIGCOMM*. Association for Computing Machinery, New York, NY, USA, 147–160.

[47] David M Pozar. 2011. *Microwave Engineering, 4th Edition.* John Wiley & Sons.

[48] ps.zpj.io. 2021. PicoScenes: Versatile Wi-Fi sensing platform. https://ps.zpj.io/

[49] Qualcomm. 2012. Qualcomm Atheros 9300 WiFi NIC. https://www.qualcomm.com/products/application/networking

[50] Vaishnavi Ranganathan, Sidhant Gupta, Jonathan Lester, Joshua R. Smith, and Desney Tan. 2018. RF Bandaid: A Fully-Analog and Passive Wireless Interface for Wearable Sensors. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)* 2, 2, Article 79 (2018), 21 pages.

[51] Mohammad Rostami, Karthik Sundaresan, Eugene Chai, Sampath Rangarajan, and Deepak Ganesan. 2020. Redefining Passive in Backscattering with Commodity Devices. In *Proceedings of the 2020 ACM Mobicom*. Association for Computing Machinery, New York, NY, USA, Article 3, 13 pages.

[52] Longfei Shangguan, Zimu Zhou, Xiaolong Zheng, Lei Yang, Yunhao Liu, and Jinsong Han. 2015. ShopMiner: Mining Customer Shopping Behavior in Physical Clothing Stores with COTS RFID Devices. In *Proceedings of the 2015 Sensys* (Seoul, South Korea). Association for Computing Machinery, New York, NY, USA, 113–125.

[53] Skyworks. 2012. Skyworks GMV9822 GaAs Hyperabrupt Junction Varactor Diode. https://pdf1.alldatasheet.com/datasheet-pdf/view/122619/SKYWORKS/GMV9822.html

[54] Skyworks. 2012. Skyworks SMV2201-040LF Silicon Hyperabrupt Tuning Varactor Diode. https://www.skyworksinc.com/en/Products/Diodes/SMV2201-040LF

[55] Yihang Song, Chao Song, Li Lu, Shen Yang, Songfan Li, Chong Zhang, Qianhe Meng, Xiandong Shao, and Haili Wang. 2022. Chipnet: Enabling Large-Scale Backscatter Network with Processor-Free Devices. *ACM Transactions on Sensor Networks (TOSN)* 18, 4, Article 61 (nov 2022), 26 pages.

[56] Vamsi Talla, Bryce Kellogg, Shyamnath Gollakota, and Joshua R Smith. 2017. Battery-Free Cellphone. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)* 1, 2, Article 25 (2017), 20 pages.

[57] Vamsi Talla and Joshua R Smith. 2013. Hybrid analog-digital backscatter: A new approach for battery-free sensing. In *Proceedings of the 2013 IEEE RFID*. IEEE, Orlando, Florida, USA, 74–81.

[58] Linear Technology. 2012. Linear Technology LT5534 50MHz to 3GHz RF Power Detector. https://www.analog.com/media/en/technical-documentation/data-sheets/5534fc.pdf

[59] Deepak Vasisht, Guo Zhang, Omid Abari, Hsiao-Ming Lu, Jacob Flanz, and Dina Katabi. 2018. In-Body Backscatter Communication and Localization. In *Proceedings of the 2018 ACM SIGCOMM*. Association for Computing Machinery, New York, NY, USA, 132–146.

[60] Ju Wang, Liqiong Chang, Shourya Aggarwal, Omid Abari, and Srinivasan Keshav. 2020. Soil moisture sensing with commodity RFID systems. In *Proceedings of the 2020 ACM Mobisys*. Association for Computing Machinery, New York, NY, USA, 273–285.

[61] Jue Wang, Haitham Hassanieh, Dina Katabi, and Piotr Indyk. 2012. Efficient and reliable low-power backscatter networks. In *Proceedings of the 2012 ACM SIGCOMM*. Association for Computing Machinery, New York, NY, USA, 61–72.

[62] Jingxian Wang, Junbo Zhang, Rajarshi Saha, Haojian Jin, and Swarun Kumar. 2019. Pushing the Range Limits of Commercial Passive RFIDs. In *Proceedings of the 2019 USENIX NSDI*. USENIX Association, Boston, MA, 301–316.

[63] Weiguo Wang, Luca Mottola, Yuan He, Jinming Li, Yimiao Sun, Shuai Li, Hua Jing, and Yulei Wang. 2023. MicNest: Long-Range Instant Acoustic Localization of Drones in Precise Landing. In *Proceedings of the 2022 Sensys* (Boston, Massachusetts) *(SenSys '22)*. Association for Computing Machinery, New York, NY, USA, 504–517.

[64] WHEELTEC. 2022. WHEELTEC N100/N200/N300 IMU. https://www.ebay.com/itm/284515586875

[65] Zihao Yu, Xin Na, Carlo Alberto Boano, Yuan He, Xiuzhen Guo, Pengyu Li, and Meng Jin. 2022. SmarTiSCH: An Interference-Aware Engine for IEEE 802.15.4e-based Networks. In *Proceedings of the 2022 ACM/IEEE IPSN*. IEEE, Virtual Event, 350–362.

[66] Jia Zhang, Yinian Zhou, Rui Xi, Shuai Li, Junchen Guo, and Yuan He. 2022. AmbiEar: MmWave Based Voice Recognition in NLoS Scenarios. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)* 6, 3, Article 151 (sep 2022), 25 pages.

[67] Maolin Zhang, Si Chen, Jia Zhao, and Wei Gong. 2021. Commodity-Level BLE Backscatter. In *Proceedings of the 2021 ACM Mobisys*. Association for Computing Machinery, New York, NY, USA, 402–414.

[68] Pengyu Zhang, Dinesh Bharadia, Kiran Joshi, and Sachin Katti. 2016. HitchHike: Practical Backscatter Using Commodity WiFi. In *Proceedings of the 2016 ACM Sensys*. Association for Computing Machinery, New York, NY, USA, 259–271.

[69] Pengyu Zhang, Colleen Josephson, Dinesh Bharadia, and Sachin Katti. 2017. FreeRider: Backscatter Communication Using Commodity Radios. In *Proceedings of the 2017 ACM CoNEXT*. Association for Computing Machinery, New York, NY, USA, 389–401.

[70] Pengyu Zhang, Mohammad Rostami, Pan Hu, and Deepak Ganesan. 2016. Enabling Practical Backscatter Communication for On-body Sensors. In *Proceedings of the 2016 ACM SIGCOMM*. Association for Computing Machinery, New York, NY, USA, 370–383.

[71] Jia Zhao, Wei Gong, and Jiangchuan Liu. 2018. Spatial Stream Backscatter Using Commodity WiFi. In *Proceedings of the 2018 ACM Mobisys*. Association for Computing Machinery, New York, NY, USA, 191–203.

[72] Jia Zhao, Wei Gong, and Jiangchuan Liu. 2021. Microphone Array Backscatter: An Application-Driven design for Lightweight Spatial Sound Recording over the Air. In *Proceedings of the 2021 ACM Mobicom*. Association for Computing Machinery, New York, NY, USA, 710–722.

[73] Renjie Zhao, Fengyuan Zhu, Yuda Feng, Siyuan Peng, Xiaohua Tian, Hui Yu, and Xinbing Wang. 2019. OFDMA-Enabled Wi-Fi Backscatter. In *Proceedings of the 2019 ACM Mobicom*. Association for Computing Machinery, New York, NY, USA, Article 20, 15 pages.

[74] Zimu Zhou, Longfei Shangguan, Xiaolong Zheng, Lei Yang, and Yunhao Liu. 2017. Design and Implementation of an RFID-Based Customer Shopping Behavior Mining System. *IEEE/ACM Transactions on Networking (TON)* 25, 4 (aug 2017), 2405–2418.