Analog Backscatter for Commodity WiFi with Payload Transparency

Xin Na, *Student Member, IEEE,* Yuan He*, *Senior Member, IEEE,* Xiuzhen Guo, *Member, IEEE,* Jia Zhang, *Student Member, IEEE,* Yang Zou, *Student Member, IEEE,* Zihao Yu, Yunhao Liu, *Fellow, IEEE/ACM*

***Abstract*—Backscatter is an enabling technology for battery-free sensing in today's Artificial Intelligence of Things (AIOT). Building a backscatter 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 issues, we present Leggiero, the first-of-its-kind analog WiFi backscatter with payload transparency, and its enhanced version, Leggiero+. A specially designed circuit based on the varactor diode directly converts fast-varying analog sensor signals into the RF (radio frequency) signal phase, eliminating the need for a microprocessor to interface between the radio and the sensor. By precisely locating the WiFi packet's extra long training field (LTF) section and carefully designing the reference circuit, Leggiero embeds the analog phase into the channel state information (CSI). A commodity WiFi receiver without hardware modification can simultaneously decode the WiFi and the sensor data. We implement and evaluate Leggiero and Leggiero+ under varied settings. Results show the tag's power consumption (excluding the power of the peripheral sensor module) is 30μW at a 400Hz sampling rate, 4.8× and 4× lower than the state-of-the-art WiFi backscatter schemes. Leggiero+ demonstrates enhanced throughput, communication range, and analog signal reproduction accuracy. Our design supports a variety of sensing applications, while maintaining the WiFi carrier's throughput performance.**

***Index Terms*—Backscatter, Analog, Phase, RF computing.**

I. 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. [1]–[4]. 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 [5].

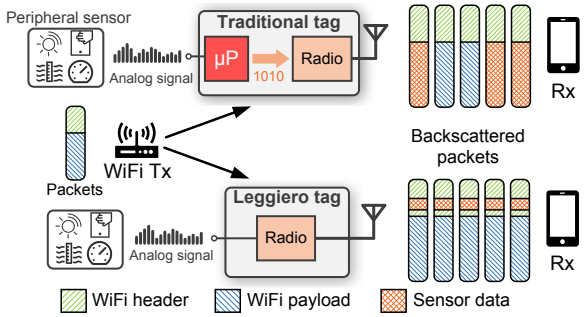


Fig. 1. Leggiero eliminates the need for using microprocessors (μP) and works transparently with the WiFi carrier's traffic.

• **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 [6], [7] or corrupting entire frames [8], 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, and its enhanced version, Leggiero+. 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 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 design is further analyzed and enhanced to produce Leggiero+. The advantages of our design 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 [9], as well as its compatibility with the WiFi network compared with the pulse width [4]. The conversion relies on altering the reflection coefficient (§II-A), and is theoretically achievable with a variable capacitor model that satisfies requirements for generality, phase range, and

Xin Na, Yuan He, Jia Zhang, Yang Zou, Zihao Yu and Yunhao Liu are with Tsinghua University, P.R. China. Xiuzhen Guo is with Zhejiang University, P.R. China.

Email: {nx20, j-zhang19, zouy23, zh-yu17}@mails.tsinghua.edu.cn, heyuan@tsinghua.edu.cn, guoxz@zju.edu.cn and yunhao@tsinghua.edu.cn.

Yuan He* is the corresponding author.

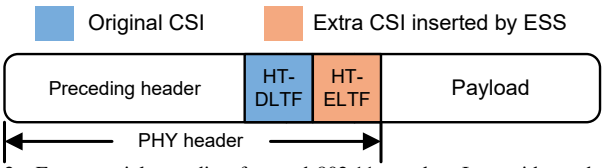


Fig. 2. Extra spatial sounding featured 802.11n packet. It provides a duplicated CSI since the long-training-fields (LTF) experience the same channel.

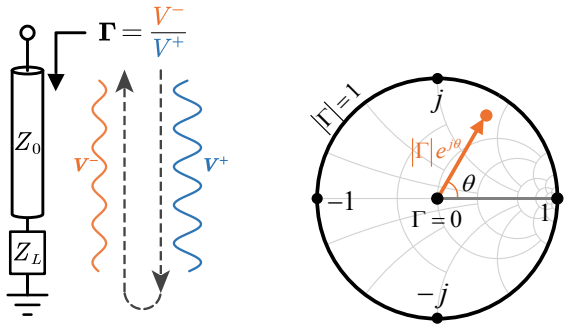
linearity (§II-B). By utilizing two types of varactor diodes, we first design Leggiero's passive reflective circuit to accomplish this and then introduce optimized enhancement with Leggiero+ (§II-C). Additional analysis (§II-D) reveals Leggiero's capability to convert the instantaneous analog voltage of fast-varying sensor signals (up to a hundred kilohertz). In this way, Leggiero avoids using microprocessors as the interfacing media and reduces 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 (§III-A). 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 through an envelope detector, and then embeds the phase by using a carefully designed reference circuit (§III-B). With a deeper analysis of the reference circuit, Leggiero+ introduces a more fundamental solution to improve performance. Upon receiving the backscattered packet, a receiver can efficiently extract the sensor readings without environmental influences by taking the phase difference of the two CSIs (§III-C). Throughout this process, no modification is made to the WiFi packet payload, as is called payload transparency. The original WiFi payload can also be decoded simultaneously. 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 (§IV) and the implementation details (§V). The hardware schematics are made publicly available.[1] §VI presents the comprehensive evaluation. The ASIC power consumption of the 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 [7], [8]. This power enables the sensor tag to work in a battery-free manner. Furthermore, due to the payload transparency, the WiFi carrier's data traffic is always preserved with unaffected throughput performance. The enhanced Leggiero+ improves throughput, communication range, and signal reproduction accuracy. It achieves 7Kbps 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.

§VII discusses practical issues of Leggiero and the potential research space. §VIII briefly introduces related works. We conclude this work in §IX. Compared to the published MobiSys version [10], we generalize the RF choke network design in Leggiero's conversion circuit, offering multiple options, as shown in Fig. 5 and 12. We enhance the hardware performance by optimizing the circuit with a GaAs-based varactor to develop Leggiero+ in §II-C. We also analyze and reveal Leggiero+'s capability to convert fast-varying sensor signals in §II-D. Additionally, we conduct a deeper analysis of the reference circuit and refine its design in §III-B to address the remaining drawbacks of the original Leggiero design. To evaluate Leggiero+, we perform experiments comparing its performance with Leggiero. First, we demonstrate improvements in overall throughput and data error rate in §VI-A. We then conduct experiments specifically to evaluate Leggiero+'s critical transient characteristics in §VI-C1. We also perform a real-world ECG signal capture task to visually demonstrate the improvements of Leggiero+ when applying fast-varying sensor signals in §VI-E.

[1]https://github.com/wonderfulnx/Leggiero.



(a) Reflection coefficient Γ (b) Γ in smitch chart

Fig. 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.

II. 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. We design a passive RF circuit to produce different Γ according to the analog voltage, thus constructing different phases in the reflected signal. The instantaneous response of this circuit to a time-varying sensor signal is analyzed to verify its usability under high speed sensor inputs.

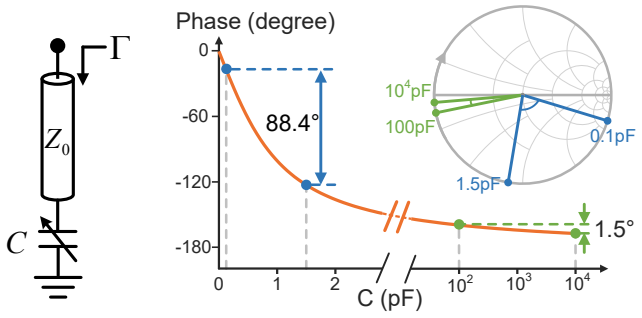
A. Primer: Reflection Coefficient

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 phase variation of the reflected wave compared to the incident wave, respectively.

Conventional backscatter design modulates bit 0 and bit 1 by providing two discrete Γ values. RFID tag provides $\Gamma_1 = 0$ as a matched state to completely absorbe RF signal and



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

Fig. 4. The shorted variable capacitor model. Higher capacitance leads to a smaller phase range and worse linearity.

$|\Gamma_2| = 1$ as a reflective state to reflect. These two values can be shown in a Smith chart in Fig. 3(b) in polar coordinates. Other designs leverages $\Gamma_1 = j$ and $\Gamma_2 = -j$ to embed a $180°$ phase difference between 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.

B. 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):

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

$$\theta_C = -2\arctan(2\pi f C Z_0), \quad (3)$$

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 completely reflects the incident signal, and its capacitance determines 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.

• **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.

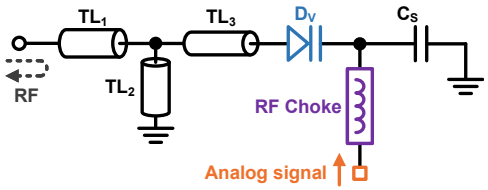


Fig. 5. Leggiero's analog conversion circuit design. It converts the input analog voltage to a small capacitance and then shifts the RF phase accordingly.

• **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.

C. Designing Conversion Circuit

We 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 bias voltage V:

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

where C_0 is the junction capacitance with no bias; V_0 and M depend on the diode type and are constants for a specific diode. Commercial varactor diodes can offer a capacitance range from 0 to 2pF, usually with the reverse bias voltage ranging from 0 to $20V$. We consider two varactor diodes: a silicon-based SMV2201 used in Leggiero and a gallium arsenide-based (GaAs) MAVR000120 used in Leggiero+. Fig. 6 illustrates their junction capacitance as a function of the applied voltage.

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. 5. 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 $TL_{1,2,3}$, the varactor diode D_V, a radio frequency choke network (RFC) to isolate the RF path from the DC 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.

Note that all components used in this circuit are passive components and do not require a power source. The analog

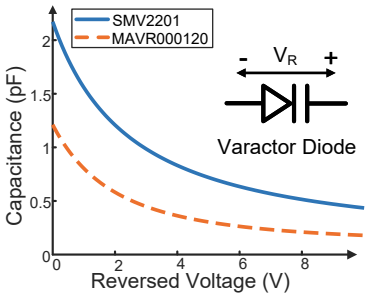


Fig. 6. Leggiero uses a varactor diode to conduct the analog signal conversion, whose capacitance varies with reverse-biased voltage.

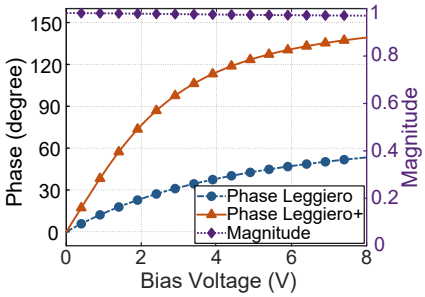


Fig. 7. Simulated phase and magnitude of the reflected signal v.s. input voltage. The phase is near-linear in 0-5V with little attenuation.

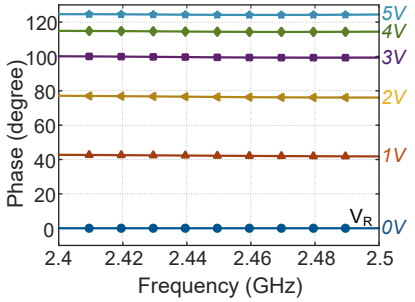


Fig. 8. Simulated phase v.s. frequency with different input voltage V_R. The reflected signal phase is flat on the whole 2.4GHz band.

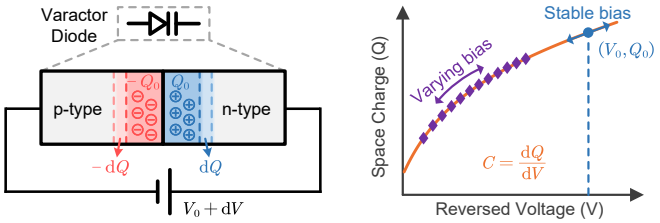
signal conversion of Leggiero consumes nearly no power since the main DC path is blocked by the capacitor C_S and the varactor diode D_V. The only DC current here is the reverse saturation current of the varactor diode, which is much less than 0.01μA. Therefore, Leggiero conducts the analog signal conversion with no energy cost.

For a quick validation of the above design methodology, we construct the Leggiero circuit using the SMV2201 varactor in the MobiSys version. Building on this, we enhance the original circuit to create the Leggiero+ circuit by incorporating the GaAs-based MAVR000120 varactor and optimizing the three transmission lines $TL_{1,2,3}$ using PathWave Advanced Design System (ADS) to further increase the phase variation range. Fig. 7 compares the ADS-simulated RF phase variation versus the bias voltage of the two versions (at 2.45GHz frequency). We also present the phase variation of Leggiero+ across the entire 2.4 GHz band in Fig. 8. Similar to Leggiero, Leggiero+ maintains a consistent phase variation for a given voltage over the entire band. The results of the original Leggiero circuit can be found in the MobiSys version.

Fig. 7 also shows the tag's supported input analog voltage range and its resolution, defined as the amount of phase change corresponding to a specific voltage change. For the standard 0 to 3.3V range of sensor inputs, Leggiero+ enhances the phase variation range (i.e., resolution) by threefold, reaching up to 105 degrees. Apart from the circuit design, the conversion accuracy also heavily depends on the CSI reception at the receiver end and can be affected by channel noise since the actual sampling part of the voltage takes place in the CSI calculation process. Therefore, the increase in resolution provided by Leggiero+ improves resistance to channel noises. We will assess this in §VI-E.

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. However, we cannot use these components in Leggiero directly for the following reasons.

• **Power consumption and price:** Commercial ICs target at military radars, satellites, and beamforming phase arrays, where performance is the primary concern. They usually have



(a) Space-charge of PN junction (b) Q-V curve defines capacitance

Fig. 9. A varactor's capacitance originates from its space-charge region. Its operating point should locate on the charge-voltage curve in both stable and time-varying inputs.

mW-level power and cost more than $50 each. In comparison, our phase-shifting circuit consumes negligible power and only costs $2, satisfying backscatter's demands.

• **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.

• **Accuracy and robustness:** The robustness of our phase shifting circuit are on par with commercial ICs, as validated in §VI-C1 where transient phase shifts are highly accurate.

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.

D. Converting Varying Signal

So far, we have focused on how Leggiero converts an analog voltage value into RF phase, assuming the analog input in Fig. 5 is stable overtime (i.e., DC bias). However, in reality, the sensor's analog input is a time-varying voltage signal. We now analyze the reflective circuit's instantaneous response to time-varying inputs.

We begin by analyzing the varactor diode, which is the main contributor to the analog conversion. The capacitance of the varactor diode originates from the space-charge region formed within a PN junction, as illustrated in Fig. 9(a). When P-type and N-type semiconductors are joined, carriers diffuse across the junction and accumulate space charges in the contact area. These charges create an electric field that prevents electrons from passing through, behaving like a capacitor [11]. An increase in the reverse bias voltage (e.g., $\mathrm{d}V$) increases the space charge quantity (e.g., by $\mathrm{d}Q$), forming a junction capacitance that varies with the voltage. Fig. 9(b) shows the space charge quantity at different reverse voltages.

Stable voltage input. At a stable bias voltage V_0, the stored charge is Q_0, as illustrated in Fig. 9(b). When an incident RF signal is applied, it induces a small voltage oscillation at the ends of the varactor, causing slight variations in the PN junction's voltage and charge. Given that the oscillation is minimal (e.g., 0.06V for typical -20dBm RF power in the backscatter scenario), the varactor can be approximated as operating at the point (V_0, Q_0) and oscillating along the tangent of the curve. This results in a constant capacitance of $C_0 = \frac{\mathrm{d}Q}{\mathrm{d}V}\Big|_{V=V_0}$ [12]. This equation derives the capacitance in Eq. 4 and results in a stable phase shift given by Eq. 2.

Varying voltage input. For a varying voltage input, the instantaneous capacitance at any moment is calculated using a similar equation: $C(t) = \frac{\mathrm{d}Q(t)}{\mathrm{d}V(t)}$. Ideally, we expect the instantaneous capacitance $C(t)$ to be determined solely by the instantaneous voltage $V(t)$, consistent with the stable input case. This means that $C(t) = \frac{C_0}{(1-V(t)/V_0)^M}$ should hold at any moment. Consequently, for a varying sensor voltage signal input, the operating point of the varactor should always lie on the charge-voltage (Q-V) curve in Fig. 9(b), moving along the curve as the voltage varies.

To quickly verify the above analysis, we perform a transient simulation on both Leggiero and Leggiero+ circuits in ADS. We apply sinusoidal analog inputs to the circuits to compare the instantaneous Q-V operating point and capacitance with the time-invariant results. The instantaneous charge is obtained by integrating the current over time. The results indicate that, regardless of the RF choke network chosen, Leggiero's reflective circuit ensures correct instantaneous capacitance up to a 100 kHz voltage signal input, meeting the needs of almost all high-speed sensing tasks. This simulation analysis is made publically available along with the hardware schema. In conclusion, for time-varying analog sensor signal inputs, the instantaneous voltage-phase conversion of the reflective circuit is consistent with the time-invariant case.

III. 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 phase embedding.

A. Primer: Extra Spatial Sounding

Leggiero modifies the phase of WiFi CSI to transmit its analog sensor readings. However, environmental dynamics (including multipath propagation) can affect the state of the wireless channel. The CSI changes caused by these dynamics are likely to overwhelm the intentionally embedded phase in Leggiero. To obtain the phase correctly, it is essential to avoid these environmental influences completely.

Leggiero exploits the extra spatial sounding (ESS) feature in 802.11n standard [13] to cancel out the 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 almost the same channel, thereby giving two nearly identical CSI measurements. In practice, the difference between them is usually smaller than ± 3 degrees, even in multipath rich environments [10].

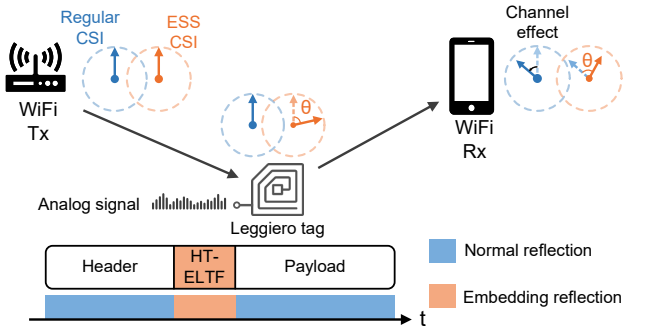


Fig. 10. Transparent phase embedding of Leggiero. It finds the Extra LTF section of 802.11n packets and embeds the analog sensor reading in the RF phases. It is then extracted by calculating the phase difference.

B. Embedding Process

The Leggiero tag precisely embeds the converted RF phase information in the HT-ELTF section of an ESS-enabled WiFi packet. Other sections act as 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. The embedding process is shown in Fig. 10. To realize this design in practice, there are three critical problems to address.

- **Avoiding self interference.** Existence of the original link from the transmitter to the receiver inevitably includes signal path excluding the backscatter tag and confuses the CSI phase. We solve this problem by shifting the frequency of the reflected signal by $\pm$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 [6] and FreeRider [7], have used similar approaches.
- **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. 11. 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

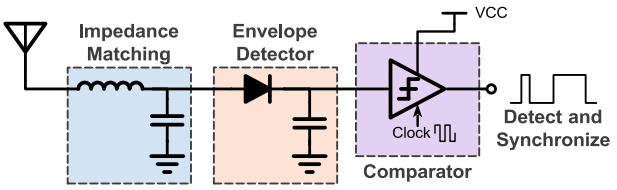
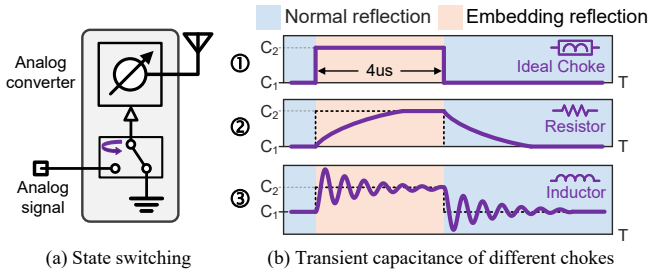
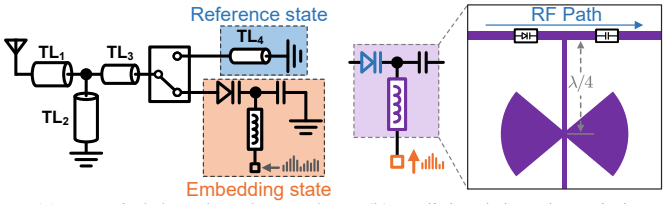


Fig. 11. Packet detection and synchronization circuit of Leggiero. An envelope detector is connected to the antenna. The output signal strength is compared with a threshold to locate the beginning of a packet.



(a) State switching (b) Transient capacitance of different chokes

Fig. 12. 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.



(a) RF switch-based workaround (b) Radial stub-based RF choke

Fig. 13. Phase embedding circuit schematic of Leggiero. The tag uses an RF switch for the reference circuit.

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 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. We find that the preceding guard interval (GI) inside the CSI section help tolerant synchronization error. §VI-C3 presents our validation of the synchronization error (i.e., mismatch) and its impact on backscattering. It shows that a synchronization accuracy of 250ns is enough for the phase embedding process and results in negligible demodulation errors. The requirement is met by applying a 4MHz clock to the comparator, which can be derived from the main 20MHz clock.

• **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. 7.

An ideal and straightforward reference circuit design would be to switch the analog input signal between the sensor input in the embedding state and 0V in the reference state, as illustrated in Fig. 12(a). However, the effectiveness of this approach relies heavily on the design of the RF choke network, highlighted in purple in Fig. 5. The RF choke's objective is to prevent the DC (or low-frequency) analog signal input from affecting the upper RF path. It blocks the RF signal (at GHz-level) from entering the voltage input part while allowing the sensor signal (at kHz-level) to pass. Ideally, when the input voltage switches between 0V and the analog input, the instantaneous capacitance should switch rapidly and stably, as shown in Fig. 12(b)①. In practice, the common choices for an RF choke network are either a large *resistor* or a large *inductor*. Unfortunately, neither achieves the ideal performance. The resistor-based choke, along with varactor D_V and capacitor C_S in Fig. 5, forms an RC circuit for the input voltage. This circuit undergoes a transient process when switching voltages, causing the instantaneous capacitance of the varactor to stabilize gradually rather than change rapidly, as depicted in Fig. 12(b)②. Similarly, the inductor-based choke forms an LC circuit with a different transient process, as shown in Fig. 12(b)③. Both transient processes can last for more than $2us$, seriously damaging the synchronization accuracy and corrupting the embedded phase.

To address this problem, our original approach in Leggiero involves adding an RF switch in front of the varactor diode, as shown in Fig. 13(a). This switch is used instead of a voltage switch to toggles between the embedding and the reference states. The RF switch usually has a switching time of less than $10ns$, which is adequate for our synchronization requirement. However, this design has two drawbacks: (1) the insertion loss from the additional RF switch reduces the power of the backscattered signal (by up to 3dB in Leggiero's implementation), and (2) precise fine-tuning of the reference state's phase is required to match the 0V phase of the embedding state. The imperfections during hardware production make it challenging to achieve an exact phase match.

In Leggiero+, we focus on addressing the root cause of transient processes. We find that the issue stems from the high resistance or inductance of the RF choke, leading to significant transition times. To mitigate this, Leggiero+ retains the original straightforward switching approach but introduces a radial-stub-based RF choke network, as illustrated in Fig. 13(b). This choke, constructed entirely from transmission lines, employs a unique structure that includes a quarter wavelength line and a butterfly stub to block RF signals. It offers superior RF performance compared to traditional resistors and inductors, while significantly reducing the transition time to the tens of nanoseconds range. Consequently, Leggiero+ overcomes the drawbacks of Leggiero and easily meets synchronization requirements.

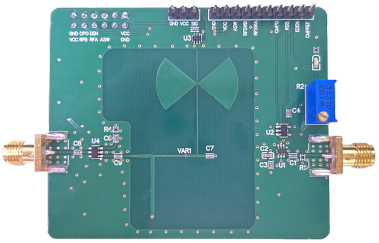


Fig. 14. The prototype of Leggiero tag.

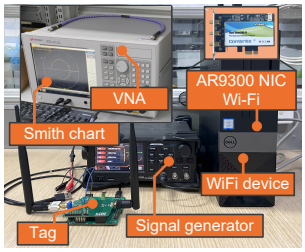


Fig. 15. Experiment setup.

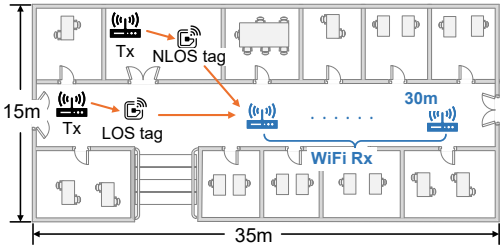


Fig. 16. Experiment environment for evaluation

C. Extracting Analog Readings

In 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:

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

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

where $\mathbf{H}_{air}$ denotes the environmental wireless channel response, and $\mathbf{H}_{err}$ includes all phase errors induced by carrier frequency offset (CFO), sampling frequency offset (SFO), etc. By calculating the phase difference of these complex CSI values, we obtain θ_V.

Then we convert it back to the analog voltage according to the phase-voltage relation shown in Fig. 7. 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. Given the fact that Leggiero+ enhances its resolution, the impact of such random noise is significantly less than that of the original Leggiero. To deal with this error, wavelet denoising techniques on the converted analog signal are applied in the receiver end similar to commonly seen sensor signal processing. We also 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. 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.

IV. 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.

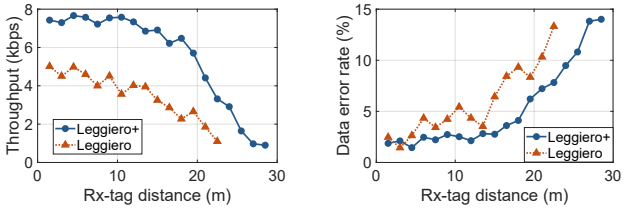
The reader (i.e., the receiver in Fig. 1) switches to the secondary channel when it is ready to receive backscattered sensor data from the tag. The reader first broadcasts a *CTS_TO_SELF* packet to reserve the channel, followed by two consecutive excitation packets with a specific interval. The tag recognizes 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.

V. Implementation

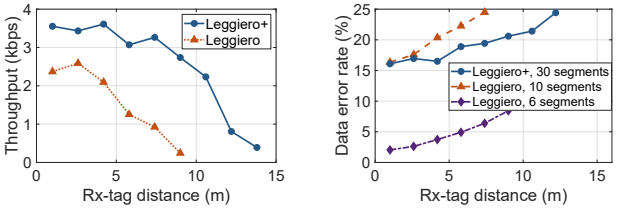
Backscatter Tag. We implement both the Leggiero and Leggiero+ tag on printed circuit boards (PCB) using commercial off-the-shelf components. The latter is shown in Fig. 14 while the former can be found in the MobiSys version. Both tags contain two RF paths: the packet detector and the backscatter circuit, each connected with a typical 2.4GHz omnidirectional antenna, at 3dBi gain.

The packet detector on both tags is implemented using an envelope detector LT5534 and a comparator TLV3201, and continuously listens to WiFi packets. For the backscatter circuit, we use PathWave ADS to simulate and implement the voltage-phase conversion circuit, using a SMV2201 and a MAVR000120 for Leggiero and Leggiero+, respectively. To switch between the embedding and the reference state, we use an ADG919 RF switch for Leggiero and an XS3A1T5157 analog switch for Leggiero+. The control logic for switching the phase embedding states is implemented using a low power ALGN125 FPGA. Note that this FPGA is used exclusively for the switching control logic, which is part of the radio. When delivered to production, the logic will be integrated into the ASIC and consume only 1 to 2 μW of power [6]. To provide the frequency shift signal, we build a ring oscillator with three SN74AUP3G04 inverters to generate a 20MHz clock. The frequency shift is achieved by toggling an ADG901 [14]



(a) Throughput (b) DER

Fig. 17. LOS throughput and data error rate with Leggiero split phase range to 10 segments and Leggiero+ split to 30.



(a) Throughput (b) DER

Fig. 18. NLOS throughput and data error rate with Leggiero split phase range to 10 segments and Leggiero+ split to 30.

RF switch for Leggiero and an HMC221B [15] for Leggiero+ using this clock.

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 to a waveform generator and several types of analog sensors for evaluation, all without the use of MCUs.

WiFi Transceiver. The WiFi transmitter and the WiFi receiver are two computers equipped with Atheros AR9300 WiFi NICs. 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 [16] to obtain CSI measurements. It records both the regular CSI and the ESS CSI so that the receiver can extract the embedded sensor readings.

VI. Evaluation

We first show the overall performance of Leggiero and Leggiero+ in §VI-A. §VI-B presents the power consumption and power benefit. §VI-C presents the result of ablation studies. §VI-D evaluates the impact on WiFi carrier transmissions. Finally, we compare the performance of Leggiero and Leggiero+ in a real-world application in §VI-E.

Methodology. Although the Leggiero tag embeds and transmits continuous analog values, inevitable errors caused by channel noises exist during the extraction of sensor readings. To quantitatively evaluate the capacity and efficiency of the overall end-to-end transmission, we define and measure the equivalent throughput and data error rate. The 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.

A. Overall Performance

We first compare the throughput and DER of Leggiero and Leggiero+ in both the line-of-sight (LOS) and non-line-of-sight (NLOS) scenarios, with their phase ranges divided into **10** and **30** segments, respectively. This is because Leggiero+ has about threefold improvement on the phase variation range. Therefore, each embedded packet in Leggiero contains about 3.3 bits of information while Leggiero+ contains about 4.9 bits. We conduct the experiment in an office area, as shown in Fig. 16. 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 tags shift the frequency of the WiFi signal by $\pm$20MHz, so that the backscattered signals are in channel 5. The transmitter is placed 1 meter away from the tag and transmit 2000 packets per second for 10 seconds. Evaluation results for other Tx-tag distances can be found in the MobiSys version. The experiment in each Rx-tag distance is repeated multiple times to embed different voltages in the range of 0V to 5V. Unless otherwise posted, the following experiments use the same setting.

The throughput in the LOS scenario is shown in Fig. 17(a). Leggiero achieves a throughput of about 5Kbps when the tag is close to the Rx, while Leggiero+ achieves 7Kbps since more segments are introduced. As the tag-Rx distance increases, the throughput of Leggiero+ decreases more slowly compared to Leggiero. This is because Leggiero+'s RF choke network design avoids the unnecessary energy loss present in Leggiero, as discussed in §III-B. Leggiero+ achieves a communication range of about 30m, comparable to existing works.

The DER in the LOS scenario is shown in Fig. 17(b). We can see that a DER of less than 5% is achieved when the tag is close to the Rx. The DER increases 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. The DER of Leggiero+ also increases more slowly compared to Leggiero, benefiting from the improved RF choke network design.

The throughput and DER comparison in the NLOS scenario are shown in Fig. 18. Leggiero+ improves the throughput from approximately 2.5Kbps with Leggiero to about 3.5Kbps when the distance is short. For the DER, we find that using the same segment number as that in the LOS scenario leads to significant increase for both Leggiero and Leggiero+. This increase can be mitigated by using smaller segment numbers. For instance, as in Fig. 18(b), the DER is reduced to less than 10% when the segment number is decreased to 6 for Leggiero. This indicates that we can trade throughput for better error tolerance in the NLOS scenario.

The throughput is sufficient to meet the data collection requirement of many IoT sensing applications, but it may be

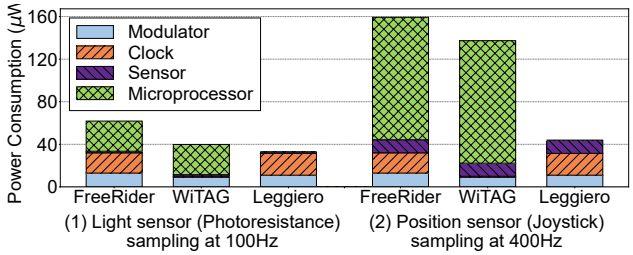


Fig. 19. Comparison of the end-to-end power consumption breakdown when connecting with sensors.

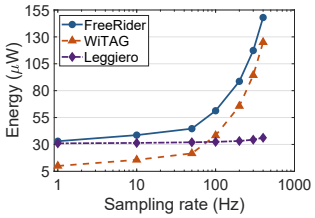


Fig. 20. Power benefit of Leggiero.

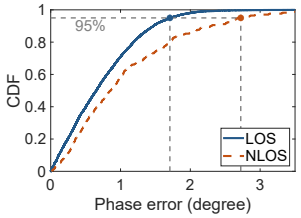


Fig. 21. Phase error CDF.

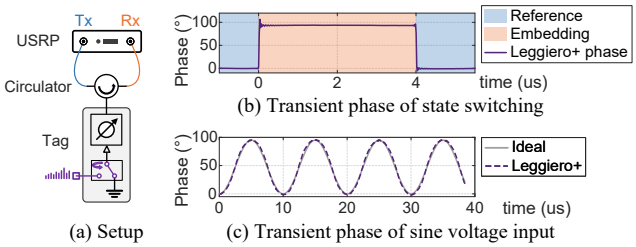


Fig. 22. Transient characteristics of the Leggiero+ tag.

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 §VI-D.

B. Power Consumption

1) Tag Power Consumption: The Leggiero and Leggiero+ tag's power consumption mainly comes from four parts: RF and analog switches, packet detector, control logic, and the 20MHz clock generation. Here we report the power in an ASIC solution. The RF and analog switches consume 2μW in total according to their datasheets. The packet detector can work in a hierarchical mode and consumes about 7μW when implemented in CMOS technology [17]. The control logic generates the phase embedding state switching signal and consumes 0.991μW of power in a digital IC simulation using TSMC 28nm CMOS technology. The clock generation is the major source of power consumption and consumes 20μW in ASIC when using a ring oscillator [18]. In short, the power consumption in the ASIC implementation will be around 30μW. For a prototype PCB implementation, the power consumption is around 40mW.

A Leggiero tag can operate in a battery-free manner using energy harvesters such as solar panels. A small solar panel of 2-3cm^2 is sufficient to provide the 30μW of power required by a Leggiero tag [19]. When considering typical peripheral analog sensors, such as temperature, photosensitive, and noise sensors, which consume the same level of power as the tag, the entire sensor node can still operate battery-free.

2) Power Benefit: To fully understand the power benefit of Leggiero, we compare the end-to-end power consumption of transferring sensor data with representative WiFi backscatter systems, as shown in Fig. 19. We connect the tags with a light sensor and a position sensor, operating at 100Hz and 400Hz sampling rates, respectively. The data for WiTAG [8] and FreeRider [7] is acquired and fed to the radio by an commonly used MCU MSP430FR5969. 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. The analog sensors in Leggiero 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 [20]. 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.

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. 20 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 [7] and WiTAG [8], 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 [20].

C. Ablation Study

To better understand the performance of Leggiero, we conduct ablation studies. §VI-C1 evaluates the tag's transient characteristics regrading switching and varying input. §VI-C2 evaluates errors of Leggiero's analog transmissions. §VI-C3 presents the impact of synchronization errors of the embedding process. Other ablation studies about Leggiero's design considerations can be found in the MobiSys version.

1) Transient Characteristics: We evaluate the transient performance of the analog signal conversion, particularly for the Leggiero+ tag, which retains the straightforward switching approach and may be affected by the transient process. To measure the tag's reflected RF signal, we connect it to a USRP N310 using a circulator, as shown in Fig. 22(a). The USRP transmits carrier at 2.45GHz and demodulates the tag's embedded phase. We measure the transient phase during the CSI embedding process to observe its switching characteristic, as illustrated in Fig. 22(b). We can see that the Leggiero+ tag transitions from the reference state to the embedding state rapidly, completing in less than 100 ns.

Next, we verify the varying signal conversion capability of the conversion circuit, as discussed in §II-D. We provide a 100 kHz cosine voltage signal as the input and compare the real-time recorded phase with the ideally calculated one. We find that the transient converted phase closely matches the ideal value, suggesting that the Leggiero+ tag can accurately convert varying signals up to 100 kHz. However, Leggiero's

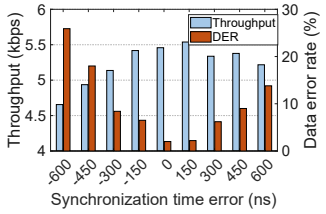


Fig. 23. Impact of synchronization error.

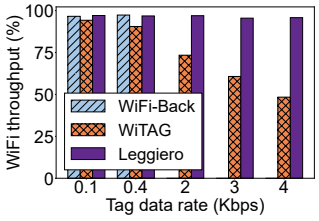
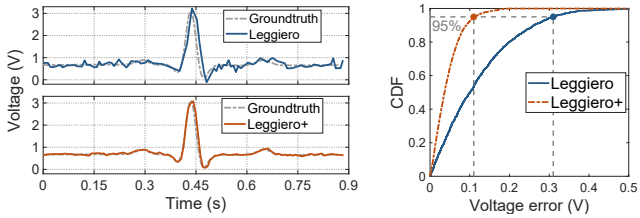


Fig. 24. Tag's impact on WiFi throughput.



(a) An example ECG signal comparison (b) Volatage error CDF

Fig. 25. Comparison between Leggiero and Leggiero+ in a ECG capture application.

practical capability is mainly limited by the Wi-Fi protocol, where the actual sampling rate of the analog sensor equals the number of packets transmitted per second. Enhancement regarding this aspect is left as future work.

2) Analog transmission errors: In real-world deployments, analog sensor voltages are directly fed into the tag and embedded into the WiFi CSI. While the tag itself introduces no error during the conversion, inevitable measurement errors arise during extraction, due to channel noise and environmental variations. To study this error, we show the the phase error CDF in LOS and NLOS scenarios in Fig. 21. Although the maximum phase error in the NLOS scenario can be up to 4.5°, more than 95% of the errors are less than 3°.

Next, we derive the voltage transmission errors caused by CSI measurement inaccuracies. Considering a standard sensor input voltage range of 0 to 3.3V, Leggiero and Leggiero+ convert this range to 0-35° and 0-105° ranges, respectively, as shown in Fig. 7. The 3-degree phase error then translates to absolute voltage errors of 0.3V and 0.1V for Leggiero and Leggiero+, respectively. In conclusion, Leggiero+ achieves an accuracy of about 3% and a resolution of approximately 5 bits.

Leggiero avoids most environmental influences using the ESS feature, but residual variations can still introduce errors. Fig. 21 also shows an increase of the phase errors 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. 21 exhibit the highest phase errors.

3) 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 $4\mu s$ 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. 23. 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 $0.8\mu s$ guard interval (GI) before the actual $3.2\mu s$ baseband signal. When calculating the CSI, the WiFi receiver only uses the latter $3.2\mu s$ signal and drops the GI. Therefore, a positive error less than 800 ns still includes the complete $3.2\mu s$ 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.

D. 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 [6], FreeRider [7], and MOXScatter [21] 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. 24. For *WiFi-Backscatter* [22], although it has high transparency, it only provides 400bps of data rate. For WiTAG [8], 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 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.

E. Real-world Application

To demonstrate the improvement of Leggiero+ in real-world applications involving fast-varying voltage signals, we connect analog ECG sensors to the tags and compare the results. 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 extract the Leggiero and Leggiero+ voltage signals from the CSI phase differences and compare them with the ground truth measured by an oscilloscope. Fig. 25(a) shows an example result. We can see that Leggiero+ reproduces the ECG signal more accurately than Leggiero, particularly in rapidly changing parts. This is due to Leggiero+'s higher resolution, which provides better resistance to noise. Additionally, its

Technology	Through-put	Tag-Rx range	Trans-parency	Power at 400Hz sampling	Require μP
WiFi-Back. [22]	0.4Kbps	2m	High	125μW	Yes
HitchHike [6]	300Kbps	50m	Low	147μW	Yes
WiTAG [8]	4Kbps	15m	Med	125μW	Yes
Leggiero+	7Kbps	30m	High	30μW	No

TABLE I
COMPARISON WITH EXISTING WIFI BACKSCATTER.

longer communication distance reduces packet loss at 10-meter Rx-tag distance, improving the sampling rate for rapidly changing signals.

To further illustrate the resolution improvement, we plot the CDF of voltage errors for the extracted ECG signals over a 30-second duration. As shown in Fig. 25(b), Leggiero+ demonstrates significant improvement, with 95% of the voltage errors within around 0.1V compared to 0.3V for Leggiero. This is consistent with Leggiero+'s threefold improvement in the phase variation range, as well as our error analysis in §VI-C2.

VII. DISCUSSION

• **Post-processing of sensor data.** The analog domain signal conversion of Leggiero produces the raw sensor signal. In reality, post-processing of the sensor data, such as local filtration or aggregation, is often needed in a sensing application. Leggiero offload these functionalities from the local sensor unit to the remote WiFi receiver, which is more powerful in terms of computational capacity.

• **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.

VIII. RELATED WORKS

Backscatter technology has emerged as a promising option for IoT sensing systems [23]–[28]. Traditional backscatter systems such as RFID [29]–[31] require specialized readers to communicate with the tag. Ambient backscatter approaches utilize the existing wireless signals such as WiFi [17], [21], [32]–[34], LoRa [2], [35]–[37], mmWave [1], [38], [39], and etc., as the carrier signals. Leggiero is related to two categories of backscatter works: WiFi backscatter and analog backscatter.

A. WiFi Backscatter

WiFi backscatter takes the ambient WiFi as the carrier signal to transmit data. Some existing approaches [6], [7], [18] separate backscatter traffic from the carrier by introducing frequency shifting. As a result, they require two receivers listening on two channels to decode the data. These 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* [22] and WiTAG [8]. *WiFi-Backscatter* modulates tag data by reflecting or absorbing WiFi packets. The receiver employs an energy-based detection scheme to decode the tag data, far constrained in terms of throughput (0.4kbps) and communication range (3m). In WiTAG [8], 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, WiTAG's operation inevitably interferes with normal transmissions. Further, it assumes the ACKs to be always positive. In comparison, Leggiero's backscatter traffic is transparent to the carrier traffic and achieves higher throughput and longer range.

We summarize the comparison between Leggiero and existing works in Table I. The power consumption values listed 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 backscatters require complicated operations and the help of MCUs to interface with sensors, which induces high power consumption and overburdens a tag's limited energy budget. In comparison, Leggiero's tailored design for IoT sensors reduces power through analog domain signal conversion.

B. Analog Backscatter

Existing digital backscatters do not include external data acquisition and require microprocessors as the interface media. In contrast, analog backscatter fits with sensor signal streaming inherently and in an ultra-low power manner. [9] and [40] develop a sensing platform and a communication system, respectively, varying the tag's impedance to achieve amplitude modulation (AM). There exists a frequency-modulated system [41], but the demodulation is still amplitude-based. The problem with these AM systems is that the amplitude of the analog sensor signal is weak and may be easily influenced by noise. They often require a high SNR scenario to work properly.

Recently, researches begin to seek preferable analog transmission media. [4] proposes to use the duration in one state to achieve pulse width modulation (PWM). It builds a video streaming backscatter link to demonstrate its high throughput. Other works [42], [43] also leverage the duration-based mechanism to build analog backscatter. Moreover, the RF signal phase is also considered to convey the sensor readings directly [44], [45].

The differences between Leggiero and the existing approaches lie in two aspects. First, Leggiero is compatible and coexists well with commodity networks. It does not require a dedicated exciter or receiver. 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).

IX. Conclusion

This paper presents Leggiero (and its enhanced version 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. The enhanced Leggiero+ achieves a 7Kbps throughput with minimal effect on the WiFi carrier's throughput performance.

Acknowledgments

This work is supported in part by the National Natural Science Foundation of China under grant No. 62425207 and No. U21B2007.

References

[1] M. H. Mazaheri, A. Chen, and O. Abari, "mmtag: A millimeter wave backscatter network," in *Proceedings of the 2021 ACM SIGCOMM*, 2021.

[2] Y. Peng, L. Shangguan, Y. Hu, Y. Qian, X. Lin, X. Chen, D. Fang, and K. Jamieson, "Plora: a passive long-range data network from ambient lora transmissions," in *Proceedings of the 2018 ACM SIGCOMM*, 2018.

[3] V. Iyer, V. Talla, B. Kellogg, S. Gollakota, and J. Smith, "Inter-technology backscatter: Towards internet connectivity for implanted devices," in *Proceedings of the 2016 ACM SIGCOMM*, 2016.

[4] S. Naderiparizi, M. Hessar, V. Talla, S. Gollakota, and J. R. Smith, "Towards battery-free hd video streaming," in *Proceedings of the 2018 USENIX NSDI*, 2018.

[5] H. Jayakumar, K. Lee, W. S. Lee, A. Raha, Y. Kim, and V. Raghunathan, "Powering the internet of things," in *Proceedings of the 2014 IEEE/ACM International Symposium on Low Power Electronics and Design (ISLPED)*, 2014.

[6] P. Zhang, D. Bharadia, K. Joshi, and S. Katti, "Hitchhike: Practical backscatter using commodity wifi," in *Proceedings of the 2016 ACM Sensys*, 2016.

[7] P. Zhang, C. Josephson, D. Bharadia, and S. Katti, "Freerider: Backscatter communication using commodity radios," in *Proceedings of the 2017 ACM CoNEXT*, 2017.

[8] A. Abedi, F. Dehbashi, M. H. Mazaheri, O. Abari, and T. Brecht, "Witag: Seamless wifi backscatter communication," in *Proceedings of the 2020 ACM SIGCOMM*, 2020.

[9] V. Talla and J. R. Smith, "Hybrid analog-digital backscatter: A new approach for battery-free sensing," in *Proceedings of the 2013 IEEE RFID*, 2013.

[10] X. Na, X. Guo, Z. Yu, J. Zhang, Y. He, and Y. Liu, "Leggiero: Analog wifi backscatter with payload transparency," in *Proceedings of the 2023 ACM MobiSys*, 2023.

[11] S. M. Sze, *Semiconductor devices: physics and technology*. John wiley & sons, 2008.

[12] B. Streetman and S. Banerjee, *Solid State Electronic Devices, Global Edition*. Pearson Deutschland, 2015. [Online]. Available: https://elibrary.pearson.de/book/99.150005/9781292060767

[13] I. S. 802.11n 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.

[14] A. Devices, "Analog devices adg901 wideband spst rf switch," 2017. [Online]. Available: https://www.analog.com/media/en/technical-documentation/data-sheets/adg901_902.pdf

[15] ——, "Analog devices hmc221b gaas mmic spdt switch," 2015. [Online]. Available: https://www.analog.com/en/products/hmc221bg.html

[16] Z. Jiang, T. H. Luan, X. Ren, D. Lv, H. Hao, J. Wang, K. Zhao, W. Xi, Y. Xu, and R. Li, "Eliminating the barriers: Demystifying wi-fi baseband design and introducing the picoscenes wi-fi sensing platform," *IEEE Internet of Things Journal (IOTJ)*, 2022.

[17] M. Dunna, M. Meng, P.-H. Wang, C. Zhang, P. Mercier, and D. Bharadia, "Syncscatter: Enabling WiFi like synchronization and range for WiFi backscatter communication," in *Proceedings of the 2021 USENIX NSDI*, 2021.

[18] P. Zhang, M. Rostami, P. Hu, and D. Ganesan, "Enabling practical backscatter communication for on-body sensors," in *Proceedings of the 2016 ACM SIGCOMM*, 2016.

[19] A. Chakraborty, G. Lucarelli, J. Xu, Z. Skafi, S. Castro-Hermosa, A. Kaveramma, R. G. Balakrishna, and T. M. Brown, "Photovoltaics for indoor energy harvesting," *Nano Energy*, 2024.

[20] F. Dehbashi, A. Abedi, T. Brecht, and O. Abari, "Verification: can wifi backscatter replace rfid?" in *Proceedings of the 2021 ACM Mobicom*, 2021.

[21] J. Zhao, W. Gong, and J. Liu, "Spatial stream backscatter using commodity wifi," in *Proceedings of the 2018 ACM Mobisys*, 2018.

[22] B. Kellogg, A. Parks, S. Gollakota, J. R. Smith, and D. Wetherall, "Wi-fi backscatter: Internet connectivity for rf-powered devices," in *Proceedings of the 2014 ACM SIGCOMM*, 2014.

[23] J. Wang, H. Hassanieh, D. Katabi, and P. Indyk, "Efficient and reliable low-power backscatter networks," in *Proceedings of the 2012 ACM SIGCOMM*, 2012.

[24] H. Jiang, J. Zhang, X. Guo, and Y. He, "Sense me on the ride: Accurate mobile sensing over a lora backscatter channel," in *Proceedings of the 2021 ACM Sensys*, 2021.

[25] Y. Song, C. Song, L. Lu, S. Yang, S. Li, C. Zhang, Q. Meng, X. Shao, and H. Wang, "Chipnet: Enabling large-scale backscatter network with processor-free devices," *ACM Transactions on Sensor Networks (TOSN)*, 2022.

[26] J. Wang, J. Zhang, R. Saha, H. Jin, and S. Kumar, "Pushing the range limits of commercial passive rfids," in *Proceedings of the 2019 USENIX NSDI*, 2019.

[27] X. Liu, Z. Chi, W. Wang, Y. Yao, and T. Zhu, "Vmscatter: A versatile mimo backscatter," in *Proceedings of the 2020 USENIX NSDI*, 2020.

[28] X. Guo, Y. He, Z. Yu, J. Zhang, Y. Liu, and L. Shangguan, "Rf-transformer: A unified backscatter radio hardware abstraction," in *Proceedings of the 2022 ACM MobiCom*, 2022.

[29] J. Wang, L. Chang, S. Aggarwal, O. Abari, and S. Keshav, "Soil moisture sensing with commodity rfid systems," in *Proceedings of the 2020 ACM Mobisys*, 2020.

[30] Y. He, Y. Zheng, M. Jin, S. Yang, X. Zheng, and Y. Liu, "Red: Rfid-based eccentricity detection for high-speed rotating machinery," *IEEE Transactions on Mobile Computing (TMC)*, 2021.

[31] Z. Zhou, L. Shangguan, X. Zheng, L. Yang, and Y. Liu, "Design and implementation of an rfid-based customer shopping behavior mining system," *IEEE/ACM Transactions on Networking (TON)*, 2017.

[32] R. Zhao, F. Zhu, Y. Feng, S. Peng, X. Tian, H. Yu, and X. Wang, "Ofdma-enabled wi-fi backscatter," in *Proceedings of the 2019 ACM Mobicom*, 2019.

[33] M. Rostami, K. Sundaresan, E. Chai, S. Rangarajan, and D. Ganesan, "Redefining passive in backscattering with commodity devices," in *Proceedings of the 2020 ACM Mobicom*, 2020.

[34] Y. Chae, Z. Lin, K. M. Bae, S. M. Kim, and P. Pathak, "mmComb: High-speed mmWave commodity WiFi backscatter," in *Proceedings of the 2024 USENIX NSDI*, 2024.

[35] X. Guo, L. Shangguan, Y. He, N. Jing, J. Zhang, H. Jiang, and Y. Liu, "Saiyan: Design and implementation of a low-power demodulator for lora backscatter systems," in *Proceedings of the 2022 USENIX NSDI*, 2022.

[36] J. Jiang, Z. Xu, F. Dang, and J. Wang, "Long-range ambient lora backscatter with parallel decoding," in *Proceedings of the 2021 ACM Mobicom*, 2021.

[37] X. Guo, L. Shangguan, Y. He, J. Zhang, H. Jiang, A. A. Siddiqi, and Y. Liu, "Aloba: Rethinking on-off keying modulation for ambient lora backscatter," in *Proceedings of the 2020 ACM Sensys*, 2020.

[38] K. M. Bae, H. Moon, S.-M. Sohn, and S. M. Kim, "Hawkeye: Hectometer-range subcentimeter localization for large-scale mmwave backscatter," in *Proceedings of the 2023 ACM MobiSys*, 2023.

[39] K. M. Bae, N. Ahn, Y. Chae, P. Pathak, S.-M. Sohn, and S. M. Kim, "Omniscatter: extreme sensitivity mmwave backscattering using commodity fmcw radar," in *Proceedings of the 2022 ACM MobiSys*, 2022.

[40] V. Talla, B. Kellogg, S. Gollakota, and J. R. Smith, "Battery-free cellphone," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, 2017.
[41] V. Ranganathan, S. Gupta, J. Lester, J. R. Smith, and D. Tan, "Rf bandaid: A fully-analog and passive wireless interface for wearable sensors," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, 2018.
[42] J. Zhao, W. Gong, and J. Liu, "Microphone array backscatter: An application-driven design for lightweight spatial sound recording over the air," in *Proceedings of the 2021 ACM Mobicom*, 2021.
[43] S. Li, C. Zhang, Y. Song, H. Zheng, L. Liu, L. Lu, and M. Li, "Internet-of-microchips: direct radio-to-bus communication with spi backscatter," in *Proceedings of the 2020 ACM Mobicom*, 2020.
[44] N. Khalid, R. Mirzavand, H. Saghlatoon, M. M. Honari, A. K. Iyer, and P. Mousavi, "A batteryless rfid sensor architecture with distance ambiguity resolution for smart home iot applications," *IEEE Internet of Things Journal (IOTJ)*, 2022.
[45] A. Gupta, C. Girerd, M. Dunna, Q. Zhang, R. Subbaraman, T. Morimoto, and D. Bharadia, "Wiforce: Wireless sensing and localization of contact forces on a space continuum," in *Proceedings of the 2021 USENIX NSDI*, 2021.

Xin Na is currently a Ph.D. student at Tsinghua University. He received his B.E. degree from Tsinghua University. His research interests include wireless networking and low-power IoT.

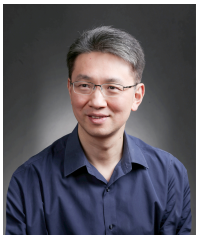
Yuan He is a professor in the School of Software and BNRist at Tsinghua University. He received his B.E. degree in the University of Science and Technology of China, his M.E. degree in the Institute of Software, Chinese Academy of Sciences, and his Ph.D. degree in Hong Kong University of Science and Technology. His research interests include wireless networks, Internet of Things, pervasive and mobile computing. He is a senior member of IEEE and a member of ACM.

Xiuzhen Guo is an assistant professor with the College of Control Science and Engineering, Zhejiang University. She received her B.E. degree from Southwest University, and her Ph.D. degree from Tsinghua University. Her research interests include wireless networks, Internet of Things, and mobile computing. She is a member of IEEE and a member of ACM.

Jia Zhang received his B.E. degree from Tsinghua University in 2019 and his Ph.D. degree from Tsinghua University in 2024. His research interests include Internet of things and wireless sensing.

Yang Zou is currently a Ph.D. student at Tsinghua University. He received his B.E. degree from the Beijing University of Aeronautics and Astronautics (BUAA). His research interests include wireless networking and communication.

Zihao Yu received his B.E. degree from the University of Science and Technology of China in 2017, and his Ph.D. degree from Tsinghua University in 2023. His research interests are in the field of network protocols of IoT and network infrastructure for AI systems.



Yunhao Liu is a professor in the Department of Automation and dean of the Global Innovation Exchange (GIX) at Tsinghua University. He received his B.S. degree in the Department of Automation from Tsinghua University. He received his M.S. and Ph.D. degree in the Department of Computer Science and Engineering at Michigan State University. His research interests include sensor network and pervasive computing, peer-to-peer computing, IOT and supply chain. Yunhao is a Fellow of IEEE and ACM.