

Towards Programmable Backscatter Radio Design for Heterogeneous Wireless Networks

Xiuzhen Guo, *Member, IEEE*, Yuan He*, *Senior Member, IEEE*, Jiacheng Zhang, *Student Member, IEEE*, Yunhao Liu, *Fellow, IEEE/ACM*, and Longfei Shangguan, *Member, IEEE*

Abstract—This paper presents RF-Transformer, a unified backscatter radio hardware abstraction that allows a low-power IoT device to directly communicate with heterogeneous wireless receivers. Unlike existing backscatter systems that are tailored to a specific wireless communication protocol, RF-Transformer provides a programmable interface to the micro-controller, allowing IoT devices to synthesize different types of protocol-compliant backscatter signals in the PHY layer. By leveraging the nonlinear characteristics of the negative impedance, RF-Transformer also achieves a cross-frequency backscatter design that enables IoT devices in harmonic frequency bands to communicate with each other. We implement a PCB prototype of RF-Transformer on 2.4 GHz ISM band and conduct extensive experiments. We leverage the software defined platform USRP to transmit the carrier signal and receive the backscatter signal to verify the efficacy of our design. Our extensive field studies show that RF-Transformer achieves 23.8 Mbps, 247.1 Kbps, 986.5 Kbps, and 27.3 Kbps throughput when generating standard Wi-Fi, ZigBee, Bluetooth, and LoRa signals.

Index Terms—Wireless Communication, Internet of Things (IoT), Backscatter technology, PHY layer design

I. INTRODUCTION

The last decade has witnessed remarkable advances in backscatter technology [1], [2], [3], [4]. To save power, the backscatter radio (*a.k.a.*, passive radio) does not generate the carrier signal; it instead modulates data on top of an incident carrier signal emanating from another wireless device called the carrier signal generator. As the power consumption of communication is dominated by the carrier signal generation [5], [6], the backscatter radio thus consumes orders of magnitude lower power than the active radio, making it an appealing solution to low-power IoT devices.

The proliferation of Internet of Things (IoT) applications brings about the increasingly dense deployments of various wireless devices (*e.g.* Wi-Fi, ZigBee, Bluetooth, LoRa, etc.) [7], [8], [9], [10], [11]. The coexistence of heterogeneous wireless devices puts forward more stringent requirements for adaptability and flexibility of the backscatter design. In order to integrate seamlessly into heterogeneous wireless networks, the backscatter radio should be able to interplay directly with different technologies while maintaining ultra-low power consumption.

Xiuzhen Guo is with Zhejiang University, P.R. China. Yuan He, Jiacheng Zhang, and Yunhao Liu are with Tsinghua University, P.R. China. Longfei Shangguan is with University of Pittsburgh, USA.

E-mail: guoxz@zju.edu.cn, heyuan@mail.tsinghua.edu.cn, lefsc.zhang@gmail.com, yunhaoliu@gmail.com, shanggdldk@gmail.com

*Yuan He is the corresponding author.

However, most of the existing backscatter systems are *tailored to* a specific wireless technology operating on a predefined frequency band, but lack *flexibility* and *adaptability*. For instance, Wi-Fi backscatter [2], [12] exclusively supports the reflection of Wi-Fi signals in the 2.4 GHz frequency band, while LoRa backscatter [1], [13] is designed solely for generating LoRa signals in the 900 MHz frequency band. Such tailored backscatter designs limit their adaptability and hinder their practical deployment in diverse and heterogeneous wireless networks.

In this paper, we ask the following question: *Is it possible to build a programmable backscatter radio that can generate different types of protocol-compliant wireless signals in the PHY-layer, while retaining ultra-low power consumption?* We give an affirmative answer by presenting RF-Transformer, a programmable backscatter radio hardware abstraction. As shown in Figure 1, RF-Transformer offers support for a unified backscatter design, enabling the synthesis of various protocol-compliant wireless signals. It also incorporates cross-frequency backscatter that allows the reflection of backscatter signals in a frequency band distinct from the carrier, and cross-technology backscatter that facilitates signal modulation on alternative carrier sources. RF-Transformer would pave the way to the practical deployment of backscatter systems in heterogeneous wireless networks.

Unified backscatter design. Our design is based on an observation that the change of reflection coefficient of a backscatter radio will alter both the phase and amplitude of reflected signals. Both phase and amplitude of backscatter signals can be programmed by altering the amplitude of their In-phase part and Quadrature part, respectively (§III-A). Specifically, we leverage a passive RF splitter coupled with a delay line to build In-phase path (I-path) and Quadrature path (Q-path) on backscatter radio and terminate each path with an ultra-low power MOSFET transistor. The resistive load of a MOSFET transistor changes with its bias voltage. As the amplitude of the signal propagating along each path changes with its resistive load, we can program the bias voltage of these two MOSFET transistors to alter the amplitude of In-phase and Quadrature parts of backscatter signals, thereby generating different types of backscatter signal.

Cross-frequency & cross-technology backscatter design. We exploit the nonlinear characteristic of the negative resistance to generate backscatter signals at the harmonic frequency band (2^{nd} and 3^{rd}) of the carrier signals, making it possible to achieve cross-frequency backscatter design (§IV). Fur-

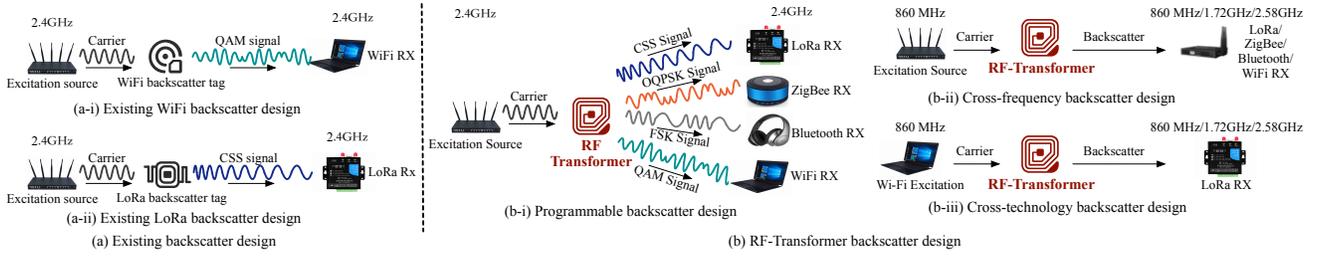


Fig. 1. Comparison of (a) existing backscatter systems and (b) RF-Transformer. RF-Transformer can not only (b-i) synthesize different types of backscatter signals based on a unified radio hardware, but also (b-ii) support cross-frequency backscatter and (b-iii) cross-technology backscatter.

thermore, RF-Transformer also supports the cross-technology backscatter design, such as WiFi-to-LoRa, ZigBee-to-LoRa, LoRa-to-WiFi, and more, by controlling the bias voltage of the transistors adaptively (§V). As shown in Figure 1(b-iii), taking the excitation signal of WiFi in 860 MHz¹ as an example, RF-Transformer generates different types of backscatter signals in 1.72 GHz and 2.58 GHz².

Implementation. We prototype RF-Transformer on printed circuit board (PCB) hardware and experiment with software defined platform USRP in various scenarios. Using the USRP platforms as the carrier transmitter and the receiver, our evaluation shows that RF-Transformer can generate 23.8 Mbps Wi-Fi signals, 247.1 Kbps ZigBee signals, 986.5 Kbps Bluetooth signals, and 27.3 Kbps LoRa signals with the communication range of 23.6 m, 45.6 m, 35.9 m, and 938.2 m.

Contributions. *i)* We propose a unified backscatter radio hardware abstraction that can synthesize different types of backscatter signals. To the best of our knowledge, RF-Transformer is the first-of-its-kind backscatter radio design that achieves both low power and high flexibility. *ii)* We further demonstrate RF-Transformer can support both cross-frequency backscatter and cross-technology backscatter design. *iii)* We address both the design and implementation challenges of RF-Transformer and demonstrate its efficacy through comprehensive experiments and long-term case studies. RF-Transformer is a significant step in a line of works that will scale out backscatter technologies to heterogeneous wireless networks.

II. RELATED WORKS

From the perspective of the modulation approach, existing backscatter systems can be divided into three groups: ON-OFF Keying, phase shifting, and frequency modulation, based backscatter designs. A comprehensive comparison of existing backscatter systems is shown in Table I.

Difference with existing backscatter systems. Our design differs from existing works in the following four aspects. First, they adopt different modulation technology. RF-Transformer is a flexible and programmable backscatter design, but most of the existing works [5], [8], [2], [17], [23], [3], [25] are

TABLE I
SUMMARY OF EXISTING BACKSCATTER SYSTEMS.

System Name	Supported Modulation	Supported Protocol	Technology
Passive RFID [5], [6]	OOK	RFID	Modulate signal amplitude by varying resistive impedance
Amb. Backscatter [8]	OOK	N/A	
Turbocharging [16]	OOK	N/A	
WiFi Backscatter [2]	OOK	N/A	
mmTag [17]	OOK	N/A	
Passive WiFi [18]	BPSK	WiFi 802.11b	Phase shifting using delay lines (Interscatter changes phase by switching between four impedance states)
Interscatter [19]	DBPSK/DQPSK/OQPSK	ZigBee	
HitchHike [20]	BPSK	WiFi 802.11b	
BackFi [21]	BPSK/16PSK	WiFi 802.11b/g	
FreeRider [22]	BPSK/16PSK/OQPSK	WiFi 802.11g/n ZigBee	
WITAG [23]	BPSK	WiFi 802.11n/ac	Frequency shifting using RF reflectors
FS-Backscatter [9]	OOK	N/A	
FM-Backscatter [24]	FSK	FM Radio	
BLE-Backscatter [25]	FSK	Bluetooth	
PLoRa [3]	CSS	LoRa	
LoRa Backscatter [1]	CSS	LoRa	Frequency synthesis
RF-Transformer	CSS BPSK/16QAM/OQPSK/ FSK	LoRa WiFi 802.11b/g/n/ac ZigBee Bluetooth	Modulate signal amplitude and phase by varying both resistive and reactive impedance

tailored to a specific wireless communication protocol. Second, the backscatter signals generated by our design and other works have different compatibility with standard protocols. RF-Transformer can generate protocol-compliant backscatter signals that are readily decodable on commodity wireless devices. Other works based on codeword translation [16], [20], [22] require either extra hardware or modification to firmware (for PHY-layer information retrieval). Third, the achievable throughput of these works is different. RF-Transformer supports chip-level modulation and can achieve a throughput of up to 23.8 Mbps. Whereas, most of the other works [23], [3], [21] modulate data at the symbol-level and thus suffer from low throughput. Fourth, existing works [1], [26], [3], [24], [18], [27] only allow the excitation source, tag, and receiver to work at the same frequency band, such as 900 MHz or 2.4 GHz, but the tag cannot reflect the carrier signal at 900 MHz to the receiver at 2.4 GHz.

In addition, the following three topics are also relevant to RF-Transformer.

Frequency shifting. Some works [9], [24], [25], [3], [1], [28] propose a method known as frequency shifting, which shifts the backscatter signal to a non-overlapping frequency band with the carrier signal. Typically, the frequency difference between the backscatter signal and the carrier signal ranges from 5 MHz to 20 MHz to avoid interference from the carrier signal on the backscatter signal. In this approach, both the backscatter signal and carrier signal operate on different channels but within the same frequency band. In contrast, cross-frequency backscatter operates with a substantial frequency difference between the backscatter signal and the carrier signal, often spanning several hundred megahertz. For

¹ IEEE 802.11ah in Europe [14], [15] supports the frequency band of 860MHz.

² We clarify that this scenario is only to assess the feasibility of tunnel diodes in generating harmonic signals. In practical experiments, we use the USRP to emulate the physical-layer protocols of Wi-Fi, ZigBee, Bluetooth, and LoRa, then evaluate RF-Transformer's performance for cross-frequency and cross-technology backscatter.

example, the carrier signal may operate at 900 MHz, while the backscatter signal operates at 1.8 GHz. This places them in completely different frequency bands. In essence, the goal of cross-frequency backscatter is to reflect the backscatter signal into a frequency band entirely distinct from that of the carrier signal. Hence, the novelty of our work lies in exploiting the non-linear impedance characteristics of the tunnel diode to achieve a cross-frequency backscatter system with ultra-low power consumption. The frequency shifting method relies on power-intensive oscillators to generate frequency offsets. For example, generating a 20 MHz frequency shift with an LTC6900 oscillator consumes around 10 mW. Moreover, power consumption increases significantly as the required frequency shift grows. It's conceivable that generating a 900MHz frequency shift with an ADF9010 would demand a substantial 1.2 W of energy, surpassing the constraints of the limited power budget for the backscatter tag. Differing from existing frequency shifting approaches, our work leverages the non-linear impedance characteristics of the tunnel diode to generate backscatter signals in the harmonic frequency band with the power consumption of only several microwatts.

Cross-Technology Communication (CTC). CTC enables direct communication among heterogeneous devices that follow different wireless standards [29], [30], [31], [32], [33]. Existing CTC techniques can be divided into the packet-level CTC and the physical-level CTC. The packet-level CTC [29] utilizes the packet transmission as the carrier to convey messages to the receiver of another technology. The physical-level CTC [31], [34], [32] leverages the fine-grained waveform, frequency, or phase information in the physical layer to achieve high-throughput CTC. The Physical-level CTC is one of the most relevant works with RF-Transformer. For example, WE-Bee [31] achieves CTC from WiFi to ZigBee via emulating the ZigBee time-domain waveform by manipulating the payload of WiFi frames. Wi-Lo [35] proposes an emulation-based CTC approach, which allows a WiFi device to generate a valid LoRa waveform. Different from CTC techniques, the backscatter technology leverages the low-power tag to bridge the communication between different wireless devices. For instance, GateScatter [36] serves as a backscatter-based gateway that bridges ZigBee devices with Wi-Fi hotspots. Similarly, RF-Transformer enables cross-technology backscatter, allowing low-power tags to reflect WiFi signals to LoRa receivers.

Intelligent Reflecting Surface (IRS). The introduction of IRS into wireless communication systems enables precise control of RF signal propagation through electronically controlled smart beamforming techniques [37]. An IRS consists of an array of reflection units [38] to change the amplitude, phase, frequency, and polarization of the incident signal. This programmable approach offers various benefits for wireless performance, such as changing signal propagation direction, compensating channel fading, eliminating interference, and enhancing signal quality [39], [40], [41]. The backscatter tag modulates signals by changing the reflection coefficient of the incident signals, and it can be regarded as a reflection unit in the IRS system.

Tunnel diode. In recent years, researchers have explored the

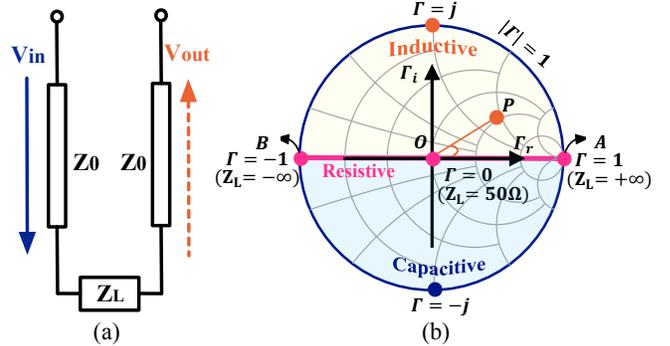


Fig. 2. Illustration of reflection coefficient. (a) Transmission line diagram. (b) Smith chart shows system's impedance.

use of tunnel diodes in backscatter systems. However, most of these works leverage the negative impedance characteristic of the tunnel diode to amplify or generate backscatter signals. TunnelScatter [42] designs a reflection amplifier based on the tunnel diode that improves the backscatter communication. Tunnel Emitter [43] further extends TunnelScatter and uses the tunnel diode oscillator to generate the backscatter signal when there is no ambient carrier source. JUDO [44] uses the injection-locking phenomenon to stabilize the tunnel diode oscillator and further proposes a radio transmitter for addressing energy asymmetry in wireless embedded systems. Different from the above works, our paper stands out by utilizing the nonlinearity of tunnel diodes to support the generation of backscatter signals with harmonic frequencies. This unique feature enables RF-Transformer to support cross-frequency backscatters, setting it apart from prior works.

III. A UNIFIED BACKSCATTER RADIO HARDWARE ABSTRACTION

In this section, we first introduce RF-Transformer's design principle (§III-A). We then describe technical challenges (§III-B) and our proposed solutions (§III-C).

A. Basic Idea

RF-Transformer is inspired by ON-OFF Keying (OOK) modulation [45] in RFID systems. To transmit data from the tag to the reader, a load resistor connected in parallel with the RFID's antenna is switched on and off in time to change the amplitude (*i.e.*, power) of reflected signals. This process can be better explained using transmission-line theory [46]. As shown in Figure 2(a), a proportion of incident voltage V_{in} is reflected by the transmission-line and returned as V_{out} . We further define Γ as the *reflection coefficient* of this power line, which is determined by the degree of mismatch between the source impedance Z_0 ³ and the load impedance Z_L [47].

$$\Gamma = \frac{V_{out}}{V_{in}} = \frac{Z_L - Z_0}{Z_L + Z_0} = \Gamma_r + j\Gamma_i \quad (1)$$

Based on the above equation, RFID varies its load impedance Z_L to alter the reflection coefficient, thereby influencing the power of reflected signals. For instance, it alternates between two states: reflecting ($|\Gamma| = 1$) or absorbing

³ Any source of power comes with an impedance, denoted as Z_0 .

($|\Gamma| = 0$) to encode a bit "1" or "0", respectively. In practice, however, the reflection coefficient Γ is a complex value⁴ because RF systems use both resistive (*e.g.*, resistors) and reactive components (*e.g.*, capacitors and inductors) to balance their load impedance. As a result, both the *amplitude* and *phase* of reflected signals will be influenced by the reflection coefficient. It is understandable that any type of wireless signal can be uniquely characterized by its amplitude, phase, and frequency. Considering that the frequency variation can be derived by the phase variation since that phase is the integral of frequency, it is thus possible to generate different backscatter signals by altering the load impedance Z_L connected to the backscatter radio's antenna.

B. Load Impedance Modulation and Technical Challenges

Smith chart [49] shown in Figure 2(b) is an effective tool to analyze the reflection coefficient of an RF system. It characterizes how the load impedance affects reflected signals in terms of phase and amplitude. For instance, when source impedance Z_0 perfectly matches load impedance Z_L , *i.e.*, $Z_L = Z_0$, the reflection coefficient Γ becomes zero, indicating the incident signal gets absorbed by the antenna without reflection (*i.e.*, the center point "O" in the Smith chart). In contrast, when the source impedance Z_0 and the load impedance Z_L are totally mismatched, *i.e.*, $Z_L = +\infty$, the reflection coefficient Γ becomes "+1". In this case, the incident signal will be totally reflected by the radio antenna (*i.e.*, the point "A" in Smith chart)⁵. Z_0 and Z_L are not strictly matched in all remaining cases. For instance, suppose Z_L and Z_0 are $(100 + j50)\Omega$ and 50Ω , respectively. The reflection coefficient Γ thus equals "0.4+0.2j". In this case, the amplitude of reflected signals will drop to $|\Gamma| = \sqrt{0.4^2 + 0.2^2} = 0.45 \times$ of the incident signal. Likewise, the phase will shift by $\angle\Gamma = \arctan(0.2/0.4) = 26.6^\circ$ with respect to the incident signal (the point "P" in Smith chart).

While the idea of load impedance modulation is compelling, practicing this idea is still challenging. Using switched resistors and capacitors is a method to achieve an impedance coverage map. However, this method has its inherent limitations as clarified in [50]. For example, combining 64 settings for the switched-resistor bank with 64 settings for the switched-capacitor bank results in 4,096 possible impedance combinations, which is still restricted. In order to reduce the out-of-band signal emissions and signal distortion caused by limited impedance combinations, this method also requires additional pulse shape filters and proper digital signal processor (DSP) management, leading to increased power consumption. The key idea of RF-Transformer lies in the programmable impedance modulation. Compared to the method of combination of resistors/capacitors/inductors or switched resistors/capacitors, our method offers more precise control of impedance by adjusting the bias voltage of transistors, resulting in a more efficient and fine-grained control mechanism.

C. Programming the Load Impedance

To program the load impedance flexibly, we leverage the insight that any RF signal can be represented as a complex value on a constellation diagram based on Euler's formula.

$$\begin{aligned} s(t) &= A(t)e^{j\phi(t)} \\ &= A(t)[\cos(\phi(t)) + j\sin(\phi(t))] = I(t) + jQ(t) \end{aligned} \quad (2)$$

where $A(t)$ is the signal amplitude; $\phi(t)$ is the signal phase. $I(t)$ and $Q(t)$ are in-phase and quadrature components, respectively. The signal amplitude and phase can be further represented by:

$$\begin{cases} A(t) &= \sqrt{I^2(t) + Q^2(t)} \\ \phi(t) &= \arctan\left(\frac{Q(t)}{I(t)}\right) = \arctan\left(\frac{|Q(t)|}{|I(t)|}\right) + \theta(t) \end{cases} \quad (3)$$

where $\theta(t)$ is the phase of the carrier signal. The above equation indicates that one can generate any backscatter waveforms by altering only the *amplitude* of their in-phase and quadrature components. Accordingly, we now transform the sophisticated resistive and reactive dual-load control into resistive-only load control.

Build the circuit. Based on the above observation, we build an ultra-low power circuit to program the amplitude of in-phase $I(t)$ and quadrature component $Q(t)$ individually by changing the resistive load connected to each part.

Figure 3(a) shows the schematic of this circuit. The incident signal (*i.e.*, carrier signal) first goes through an impedance matching circuit to ensure most of their energy gets absorbed by the antenna. We get two copies of the incident signal by passing it through a passive Wilkinson power splitter [51]. These two signal copies propagate along two separate paths. We add a delay line to one of the paths to shift the phase of the signal propagating along this path by $\frac{\pi}{4}$. When this signal goes in and then out from the same delay line, it will experience $\frac{\pi}{2}$ delay with respect to the signal propagation along another path. Consequently, these two signals form the in-phase $I(t)$ and quadrature $Q(t)$ component of backscatter signals. We optimize the length, width, and material of the microstrip line through simulation to ensure that the signal power on two paths is symmetric and of equal strength (Figure 3(b)).

To modulate the signal power along these two paths, we connect each path to a MOSFET transistor consisting of a gate (G), a source (S), and a drain (D). The resistive load impedance of this transistor can be altered by varying its bias voltage (V_{GS}). Figure 3(c) shows the resistive load impedance of this transistor (ATF-54143 [48]) as a function of bias voltage. Evidently, as we increase the bias voltage, the resistive load impedance of this transistor drops gradually, which further changes the amplitude of reflected signal. It thus allows the backscatter radio to generate different waveforms by changing the amplitude of in-phase $I(t)$ and quadratic component $Q(t)$.

Although RF-Transformer shares the same design principle with the traditional QAM transceiver [52], they separate and modulate in-phase and quadrature components in different ways. The traditional QAM transceiver uses high-precision oscillator and DAC to generate baseband in-phase and quadrature components, respectively. In contrast, RF-Transformer neither

⁴ Where Γ_r and Γ_i represent the real and imaginary part.

⁵ When $Z_L = -\infty$, the amplitude of reflected signals is the same as that of the carrier signal but opposites in phase (denoted as "B" in Smith chart).

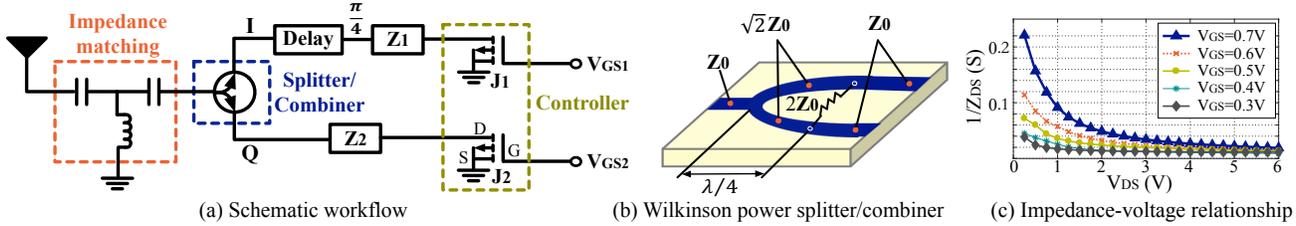


Fig. 3. The circuit design of RF-Transformer. (a) Schematic workflow. (b) Wilkinson power splitter/combiner. (c) Impedance-voltage relationship of a typical transistor ATF-54143 [48].

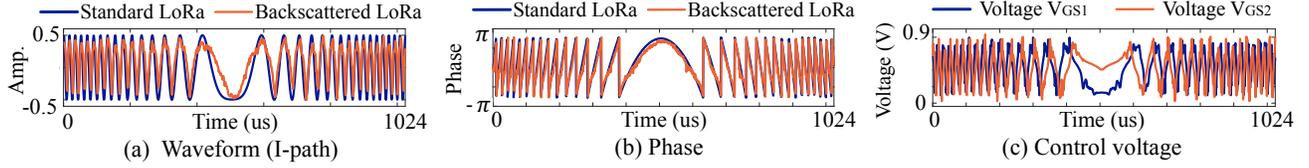


Fig. 4. LoRa symbol synthesis. (a) Standard LoRa signal and backscattered LoRa signal. (b) Standard LoRa phase and backscattered LoRa phase. (c) Control voltage V_{GS1} and V_{GS2} to synthesize the desired LoRa backscatter symbol.

generates baseband nor RF carrier signals. It instead modulates the in-phase and quadrature components of an ambient carrier signal by altering the reflection coefficient.

Modulation space. We sweep the bias voltage of both two transistors from 0 V to 0.9 V with a step of 1 mV. In each bias voltage setting, we plot the equivalent impedance of the backscatter radio in the Smith chart, shown in Figure 5. These impedance points form two borderlines, corresponding to two cases explained below:

- Varying the bias voltage of the I path while fixing the bias voltage of Q path to 0 V (dark green line).
- Varying the bias voltage of the Q path while fixing the bias voltage of I path to 0 V (light green line).

The dashed points in blue represent a set of load impedance that can be generated through the change of two transistors connected to the I-Q paths. To facilitate the presentation, we term the coverage area of these dashed points as the *modulation space of this backscatter radio*. The input impedance at the antenna port is 50Ω , which locates in the center of the Smith chart. The load impedance is situated in the modulation space, as illustrated in Figure 5(a). Notably, the radius of the modulation space is 45% of the Smith chart's radius, indicating a backscatter loss of 55% for RF-Transformer.

The modulation space (impedance coverage area on the Smith chart) varies across different hardware samples. This variation is primarily due to imperfections in the hardware, leading to differences in the initial impedance positions, as shown in Figure 5(b). To address this, the calibration of the impedance coverage area for each individual device is necessary. To correct the impedance coverage area, we further design a matching circuit by shunt inductance/capacitance or series inductance/capacitance, and then add it between the antenna and the transistor. The design principle is as follows. (1) Adding inductors in series to the circuit will rotate the modulation space clockwise with respect to the impedance circle while adding capacitors in series to the circuit will rotate the modulation space counterclockwise; (2) Adding shunt capacitors to the circuit will rotate the modulation space clockwise with respect to the admittance circle, whereas adding shunt inductors will rotate the modulation space coun-

terclockwise. Comparing Figure 5(b) with Figure 5(a), it's evident that the impedance coverage area can be corrected by adding capacitance in series.

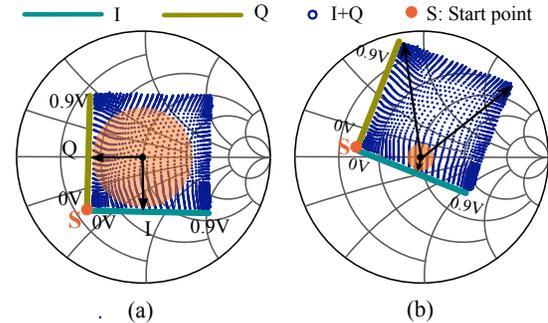


Fig. 5. Modulation space of RF-Transformer. (a): Standard modulation space. (b): Distort modulation space due to the imperfection of hardware.

D. Extending to Frequency Modulation

The above load impedance modulation circuit allows RF-Transformer to synthesize any type of amplitude-modulated signals or phase-modulated signals, or both. We next explain synthesizing frequency-modulated signals using this design.

We take LoRa as an example. LoRa adopts Chirp Spread Spectrum (CSS) to modulate data [53], [54], [55]. Each LoRa symbol is represented by a chirp whose frequency changes linearly over time, represented by $f(t) = F_0 + kt$, where F_0 is the initial frequency offset; k is the frequency changing rate, which is known in advance. It is understandable that the instantaneous frequency $f(t)$ of a LoRa symbol can be derived by the phase changing rate using the equation $f(t) = \frac{1}{2\pi} \frac{d\Phi(t)}{dt}$. Accordingly, one can emulate the frequency variation of a LoRa symbol by manipulating its phase variation. The instant phase of a LoRa symbol at time t can be derived by:

$$\begin{aligned} \Phi(t) &= 2\pi \int_0^t f(\tau) d\tau = 2\pi \int_0^t (F_0 + k\tau) d\tau \\ &= 2\pi(F_0 t + \frac{1}{2}kt^2) = \Phi_0 + \pi kt^2 \end{aligned} \quad (4)$$

where Φ_0 is the initial phase of this chirp symbol. Based on Eq. 4, RF-Transformer can derive the phase value at each

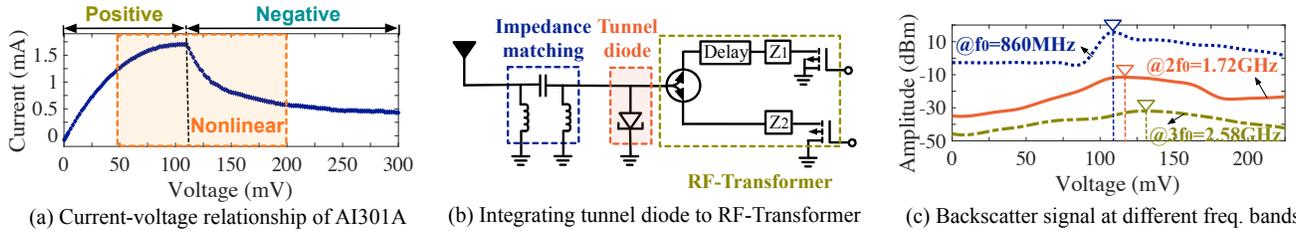


Fig. 6. Illustration of the cross-frequency backscatter design. (a): Current-voltage relationship of tunnel diode AI301A. (b): Integrating tunnel diode to RF-Transformer. (c): Backscatter signal at different frequency bands.

time point, and further leverage load impedance modulation to synthesize the desired chirp symbols.

We experimentally demonstrate the feasibility of such frequency modulation. Specifically, we use a USRP N210 software-defined radio to generate a sinusoidal carrier signal with 1 MHz bandwidth in the 2.45 GHz frequency band. The backscatter radio modulates this carrier signal into a standard LoRa symbol "100011". The bandwidth and spreading factor of this LoRa symbol are set to 125 KHz and 7, respectively. Another USRP N210 is employed to receive this backscatter signal. The receiver's sampling rate is set to 250 KHz.

Figure 4(a) shows the received backscatter waveform. We extract the phase readings and plot them in Figure 4(b). The bias voltage applied to V_{GS1} and V_{GS2} at each time point is shown in Figure 4(c). We observe that the synthesized LoRa symbol resembles the standard LoRa symbol in terms of both waveform and phase pattern. The receiver can successfully demodulate this backscattered LoRa signal through dechirping, confirming our analysis. We further evaluate backscattered LoRa signal in various SNR conditions in Section VII-A.

IV. CROSS FREQUENCY BACKSCATTER

RF-Transformer supports the cross-frequency backscatter by leveraging the nonlinear behavior of the negative resistance to generate harmonic signals.

A. Generating Harmonic Signals

Tunnel diode. A tunnel diode is a type of semiconductor diode that has effectively "negative resistance", *i.e.* as we increase the voltage beyond the peak voltage, the current through the device decreases, due to the quantum tunneling effect. The characteristic of negative resistance makes it possible to generate harmonic signals and amplify them.

How to choose a suitable tunnel diode? There are many types of tunnel diodes can be chosen, such as AI301A [56], AI201A [57], MBD5057 [58], 2 μ m resonant tunnel diode [59], and Inp 0.9 μ m resonant tunnel diode [60]. Table II compares AI301A with other tunnel diodes in terms of the operation frequency, power consumption, and amplification gain. Different with MBD5057, 2 μ m resonant, and Inp 0.9 μ m resonant, AI301A and AI201A operate at the frequency of <1 GHz. In addition, the amplification gain of AI301A is $2.3\times$ higher than that of AI201A. Hence, RF-Transformer chooses AI301A to generate and amplify the backscatter signals.

Results. Figure 6(a) shows the current-voltage ($I-V$) characteristic of the tunnel diode AI301A [61]. We have two observations. First, the tunnel diode AI301A exhibits the *negative*

TABLE II
COMPARISON OF DIFFERENT TUNNEL DIODES

	AI301A	AI201A	MBD5057	2 μ m resonant	Int 0.9 μ m resonant
Operation frequency (GHz)	0.45/0.86	0.915	5.8	5.8	5.8
Power consumption (uW)	144	178	45	420	125
Amplification gain (dB)	30	13	35	34	10

impedance characteristic when the bias voltage changes from 100 mV to 300 mV. In this case, the backscatter signal will be amplified since the denominator of the reflection coefficient shown in Eq. 1 decreases. Second, the tunnel diode AI301A exhibits the *nonlinear impedance characteristic* when the bias voltage changes from 50 mV to 200 mV. In this case, the current can be fitted as a polynomial function of voltage, *i.e.* $I(v) = \sum_{i=0}^{i=N} a_i v^i$. Due to the existence of harmonic components (v^2, v^3, \dots), frequency multiplication can be obtained. In other words, when the frequency of the incident signal is f_0 , the reflected signals with the frequencies of $2f_0$ and $3f_0$ can be generated by the tunnel diode.

B. Integrating Tunnel Diode into RF-Transformer

We integrate the tunnel diode into the design of RF-Transformer and the circuit diagram is shown in Figure 6(b). Given the carrier frequency of 860 MHz, we measure the strength of backscatter signals at the fundamental frequency (860 MHz), the 2nd harmonic frequency (1.72 GHz), and the 3rd harmonic frequency (2.58 GHz), respectively. The result is shown in Figure 6(c). Obviously, RF-Transformer can support the cross-frequency backscatter. When the bias voltage is 110 mV, 116 mV, and 131 mV, the maximum backscatter signal can be obtained at the 860 MHz, 1.72 GHz and 2.58 GHz frequency bands, respectively.

C. Comparison with Other Methods

Many other works leverage the nonlinearity of electric components to generate harmonic signals. For instance, TiFi [62] utilizes the nonlinearity of rectennas to generate harmonic signals, achieving the identification of UHF RFID at 820 MHz with WiFi at 2.46 GHz. DolphinAttack [63] exploits microphone circuit nonlinearity to modulate voice commands on ultrasonic carriers, ensuring inaudibility. HeartwormAttack [64] utilizes amplifier nonlinearity in microphones to downconvert charging frequency into an audible spectrum. In comparison, tunnel diodes offer a distinct advantage due to their significantly lower power consumption at the uW level, making them more suitable for low-power backscatter systems when compared to electric amplifiers.

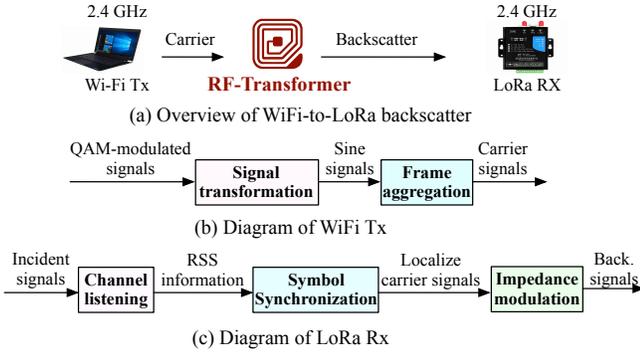


Fig. 7. Illustration of WiFi-to-LoRa backscatter.

D. Discussion on the cross-frequency backscatter

In our cross-frequency backscatter system, the tag can generate a backscatter signal with a frequency that is multiple times the frequency of the carrier signal. Generally, the cross-frequency backscatter refers to the backscatter system where the backscatter signal and the carrier signal are not in the same frequency band. In order to achieve the general cross-frequency backscatter communication, the tag should be able to generate the backscatter signal at any frequency, which is our future work.

V. RF-TRANSFORMER: CROSS TECHNOLOGY BACKSCATTER

In theory, RF-Transformer has the capability to generate a wide array of backscatter signals atop various carrier signals. This includes but is not limited to cross-technology backscatter scenarios such as WiFi-to-LoRa, ZigBee-to-LoRa, LoRa-to-WiFi, and more. The basic idea and technical implementation of cross-technology backscatter are outlined below. Basic idea.

Basic idea. Generally, we suppose the carrier signal is S_c , the target backscatter signal is S_b , and the modulation signal on the tag can be calculated by:

$$S_m = \frac{S_b}{S_c} = \frac{A_b e^{j\phi_b t}}{A_c e^{j\phi_c t}} = \frac{A_b}{A_c} e^{j(\phi_b - \phi_c)t} = A_m e^{j\phi_m t} \quad (5)$$

where (A_b, ϕ_b) and (A_c, ϕ_c) are the amplitude and phase of the backscatter and carrier signals, respectively. According to Eq. 5, we can calculate the amplitude A_m and phase ϕ_m of the modulation signal on the tag. Based on the modulation space illustrated in Figure 5(a), we can further obtain the bias voltage required to generate the modulation signal.

WiFi-to-LoRa backscatter. As a proof of concept, we introduce the WiFi-to-LoRa backscatter. The RF-Transformer tag takes the WiFi signals as the excitation source, then modulates the WiFi transmission into the LoRa signals and reflects the LoRa Rx. The specific process of WiFi-to-LoRa backscatter is shown in Figure 7.

• **WiFi Tx.** (1) *Signal transformation.* Borrowing the idea from CTC works such as WEBe [31] and WiRa [32], the WiFi Tx converts QAM-modulated signals into sine signals by selectively manipulating WiFi payload bits. (2) *Frame aggregation.* Considering the difference in frame length between Wi-Fi (200 μ s) and LoRa (1 ms), we further combine multiple Wi-Fi

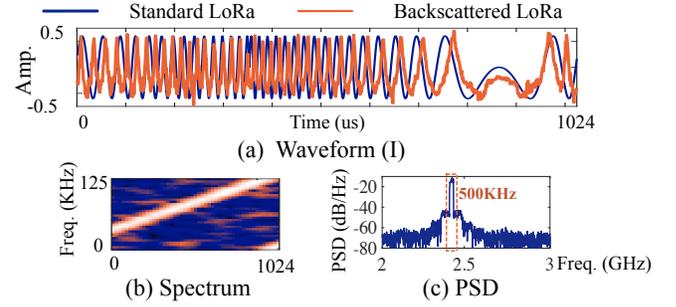


Fig. 8. RF-Transformer synthesizes LoRa backscatter signal by taking the ambient WiFi signal as the carrier. (a) Standard LoRa signal and backscattered LoRa signal. (b) The spectrum of backscattered LoRa signal. (c) PSD of backscattered LoRa signal.

frames into a single transmission unit (*i.e.*, MAC Protocol Data Unit Aggregation, A-MPDU) with a single physical header to improve the WiFi packet length. The aggregated frame length of A-MPDU (64 KB) can reach up to 72 ms, which is enough to modulate 72 LoRa symbols.

• **Tag.** To generate LoRa signals using the carrier signals transmitted by the WiFi Tx, the tag undergoes the following steps. (1) *Channel listening.* Unlike continuous sinusoidal tone, WiFi traffic is intermittent and it coexists with other types of wireless traffic (*e.g.* Bluetooth, ZigBee) on the same unlicensed band. Consequently, the tag first listens to the channel and samples the received signal strength (RSS) to detect the coming of carrier signals. (2) *Symbol synchronization.* Emulating signals through CTC techniques can only transform WiFi payload into sine signals, leaving WiFi preamble unaltered. To accurately localize WiFi payload and synchronize with its symbols for precise modulation, the tag distinguishes WiFi signals from coexisting signals and performs cross-correlation with the pre-stored Short Training Field (STF) of the WiFi packet. (3) *Impedance modulation.* Finally, the tag changes the bias voltage of two transistors to generate the desired LoRa symbols. It is worth noting that the WiFi transmitter is only the excitation source to provide the carrier sine signals for the tag. The tag modulates the data on the top of the carrier signal to generate the desired backscatter payload.

• **LoRa Rx.** The LoRa Rx decodes the backscatter signal according to the standard process of LoRa radios.

Figure 8(a) compares the waveform of a standard LoRa chirp symbol "1111100" and our synthesized LoRa symbol on top of Wi-Fi signals. Evidently, these two waveforms share very similar patterns. We further plot the spectrum of this backscatter symbol in Figure 8(b). The frequency of this chirp symbol changes continuously over time, resembling the standard LoRa chirp. Figure 8(c) shows the power spectral density (PSD) over a broader frequency range from 2-3 GHz. Notably, PSD of the backscattered LoRa signals remains concentrated within the 2.4 GHz to 2.45 GHz bandwidth of 500 KHz, ensuring the successful decoding of backscattered LoRa signals. The RF-Transformer tag can employ a bandwidth filter to mitigate out-of-band emissions, providing enhanced compatibility with coexisting wireless technologies.

VI. IMPLEMENTATION

We describe system implementation in this section.

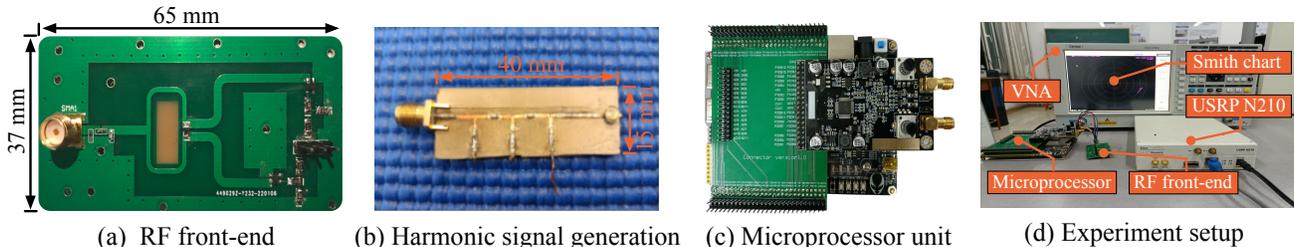


Fig. 9. RF-Transformer prototype and experiment setups.

A. Backscatter Tag

The RF-Transformer tag consists of an RF front-end and a microprocessor unit.

- RF front-end.** We implement the RF front-end on a $65\text{ mm} \times 37\text{ mm}$ one-layer PCB using commercial off-the-shelf analog components. Figure 9(a) and Figure 9(b) show the hardware prototype. The RF front-end is completely passive. We connect it to an omnidirectional antenna [65] with 3 dBi gain. The impedance matching circuit consists of two inductors connected in parallel and two capacitors connected in series. Two RF MOSFETs ATF-54143 [48] terminate the I-path and Q-path. We change the impedance of the MOSFET transistor by controlling the bias voltage, so as to synthesize the desired backscatter signal. The switching rate of the MOSFET transistor is equal to the data rate of the backscatter signal. Since the impedance of the MOSFET transistor varies non-linearly with the input voltage as shown in Figure 3(c), we need to conduct additional tuning and calibration before controlling the MOSFET's impedance. In order to generate harmonic signals, we also implement another plug-and-play circuit on a $40\text{ mm} \times 15\text{ mm}$ one-layer PCB using Rogers RO3010 substrate. This circuit consists of an impedance matching circuit and a tunnel diode AI301A [61]. By changing the bias voltage of the tunnel diode, the harmonic frequency and its corresponding signal strength can be adjusted. We further integrate AI301A into RF-Transformer according to the method shown in Section IV-B.

- Microprocessor unit.** The microprocessor unit shown in Figure 9(c) consists of a low-power Xilinx Artix-7 FPGA [66] and a 14-bit DAC AD9767 [67]. They work together to control two MOSFET transistors. The Artix-7 FPGA has an oscillator of 50 MHz that enables the maximum modulation rate of Wi-Fi 20 MHz. The 14-bit DAC AD9767 achieves the voltage accuracy of 0.3 mV given the reference voltage 5 V. We use a Vector Network Analyser (VNA) CEYEAR 3672A [68] to measure the voltage-impedance response of the transistor and store the results in FPGA. Figure 9(d) shows the setup.

B. Transmitter and Receiver

- Transmitter.** We use a Software-Defined Radio (SDR) platform USRP N210 to transmit continuous sinusoidal signals. A Mini-Circuits RF amplifier [69] is used to boost the signal power up to 30 dBm⁶. The amplified carrier signals are sent out using an omnidirectional antenna with 3 dBi

gain. Besides SDR platform, there are other two methods that can provide low-cost carrier. The first method is to build a low-cost transceiver that generates the sinusoidal carrier using Direct Digital Synthesis (DDS) [71]. The second method uses commercial devices such as a smartphone to generate the sinusoidal carrier by manipulating the payload of their transmitted Bluetooth or Wi-Fi packet [19].

- Receiver.** We use a USRP N210 equipped with the same type of antenna as the receiver. The receiver runs open-sourced gr-ieee802-11, gr-ieee802-15-4, gr-bluetooth, and gr-lora to receive and decode the backscattered Wi-Fi, ZigBee, Bluetooth, and LoRa signals.

C. Downlink and Node Coordination

The carrier transmitter leverages an OOK-modulated query message to inform the RF-Transformer tag when to backscatter, what type of excitation carrier, what type of signal to synthesize, and what frequency band to backscatter signal. The RF-Transformer tag listens to the channel and down-converts the OOK-modulated carrier signal to the baseband by using an envelope detector. Then the low-power FPGA decodes the query message. The tag will determine the received signal as a normal signal packet rather than the carrier signal if there is no query message detected. In this condition, the tag will discard this incoming frame, continue to listen to the channel, and wait for the desired carrier signal. According to the decoded query message, the tag sets the bias voltage of the tunnel diode to the corresponding value and generates the standard-compliant packet signals. The tags can also leverage slotted ALOHA protocol to coordinate multiple tags and minimize collisions. The envelope detector is a passive component (including *i.e.* inductance, capacitors, and diodes), hence the energy consumption of this downlink demodulation circuit mainly comes from the FPGA. Our FPGA works on the low sampling rate mode and the detection algorithm is simple. The total power consumption of the downlink demodulation circuit is around $85\ \mu\text{W}$. When a network consists of multiple RF-Transformer tags, the carrier transmitter allocates different time slots to different RF-Transformer tags through query messages. The RF-Transformer tags abide by the Time Division Multiple Access (TDMA) protocol to transmit backscatter signals.

VII. EVALUATION

In this section, we conduct experiments with the USRP platforms as the the carrier transmitter and the receiver to evaluate RF-Transformer's performance. We first present the

⁶ According to Federal Communications Commission (FCC) regulation, the transmission power of a frequency radio should be below 32 dBm [70].

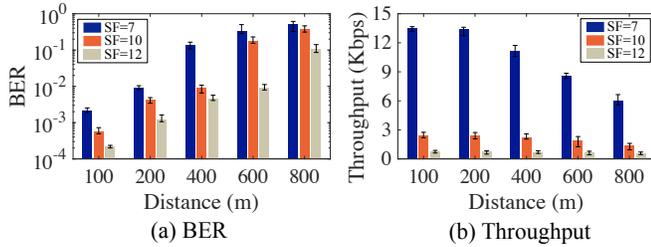


Fig. 10. Performance of LoRa backscatter link in different SF settings.

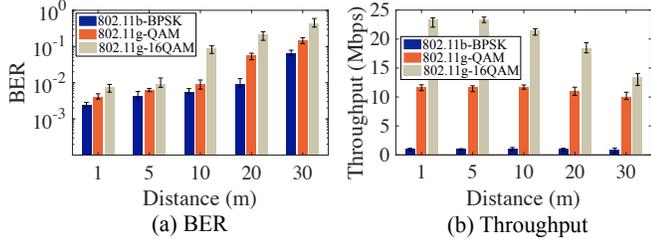


Fig. 12. Performance of Wi-Fi backscatter link.

field studies on synthesizing different types of backscatter signals (§VII-A). We then conduct micro-benchmarks to understand the key factors impacting the system performance (§VII-B). Finally, we measure the power consumption of RF-Transformer tag (§VII-C) on generating different wireless signals. The compatibility of RF-Transformer with commodity receivers is also verified (§VII-E).

Metric. We adopt *BER*, *throughput*, and *backscatter range* as the key metrics to assess RF-Transformer’s performance.

- **BER** refers to the ratio of error bits to the total number of bits received by RF-Transformer.
- **Throughput** measures the amount of received data correctly decoded by RF-Transformer within one second.
- **Backscatter distance** refers to the maximum distance between the tag and the receiver when the BER is maintained below 1%.

A. Field Studies

We control the RF-Transformer tag to synthesize multiple protocol-compliant backscatter signals, including LoRa, Wi-Fi 802.11b, Wi-Fi 802.11g/n/ac, ZigBee, and Bluetooth. We conduct end-to-end studies to assess RF-Transformer’s performance for different backscatter links.

LoRa backscatter link. We vary the spreading factor (SF) and bandwidth (BW) to assess the LoRa backscatter link’s performance. First, we observe that the BER declines with the increasing SF shown in Figure 10. This is expected since a higher SF enhances the anti-noise capability of LoRa signals, and thus the backscatter distance grows. On the other hand, the throughput grows $10.1\text{--}18.6\times$ across all tag-to-receiver distances. Second, the BER and the throughput both grow with the BW shown in Figure 11.

Wi-Fi backscatter link. The evaluation result is shown in Figure 12. First, we observe that the BER and the throughput both grow with the increase of modulation complexity. When the Wi-Fi backscatter link varies from 802.11b BPSK to 802.11g/n/ac 16QAM, the BER grows $2.3\text{--}24.5\times$, and

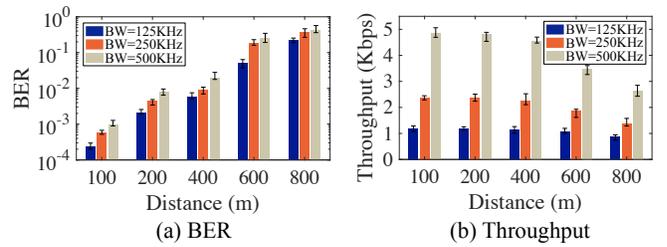


Fig. 11. Performance of LoRa backscatter link in different BW settings.

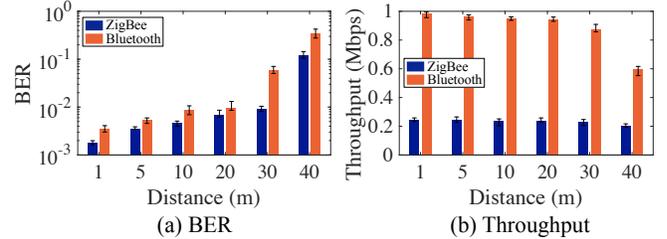


Fig. 13. Performance of ZigBee and Bluetooth backscatter links.

the throughput grows $14.7\text{--}23.9\times$ across all tag-to-receiver distances. Second, the BER grows but throughput declines with the increase of tag-to-receiver distances.

ZigBee and Bluetooth backscatter links. We have three observations based on Figure 13. First, the BER of ZigBee backscatter link and Bluetooth link grows with the increase of tag-to-receiver distance. Second, the throughput of ZigBee backscatter link and Bluetooth link drops with the increase of tag-to-receiver distance due to the deteriorating SNR. Third, the BER of ZigBee backscatter link is $1.35\text{--}6.32\times$ lower than Bluetooth backscatter link, the throughput of ZigBee backscatter link is $2.95\text{--}3.98\times$ lower than Bluetooth backscatter link.

B. Impact of Tunnel Diode

We integrate the tunnel diode into the RF-Transformer to generate and amplify the harmonic backscatter signals. In this section, we assess the impact of tunnel diode on the RF-Transformer. We control the USRP device to transmit the carrier signal at 860 MHz. We set the bias voltage of the tunnel diode is 110 mV, 116 mV, and 131 mV, respectively to excite the backscatter link at 860 MHz, 1.72 GHz, and 2.58 GHz. Then we change the impedance of RF-Transformer to generate LoRa, Wi-Fi 802.11b, Wi-Fi 802.11g/n/ac, ZigBee, and Bluetooth signals, respectively.

Backscatter link at the fundamental frequency (860 MHz).

We observe the backscatter distance grows significantly across all backscatter links as shown in Figure 14(a): the LoRa backscatter range grows by $2.27\times$ from 412.5 m to 938.2 m, the Wi-Fi 802.11b backscatter range grows by $1.56\times$ from 22.8 m to 35.6 m, the Wi-Fi 802.11g/n/ac backscatter range grows by $1.51\times$ from 15.6 m to 23.6 m, the ZigBee backscatter range grows by $1.24\times$ from 34.3 m to 45.6 m, and the Bluetooth backscatter range grows by $1.39\times$ from 25.7 m to 35.9 m.

Backscatter link at the 2^{nd} harmonic frequency (1.72 GHz). Owing to the nonlinear negative impedance characteristic of the diode, RF-Transformer can generate the harmonic backscatter signals. As shown in Figure 14(b), the

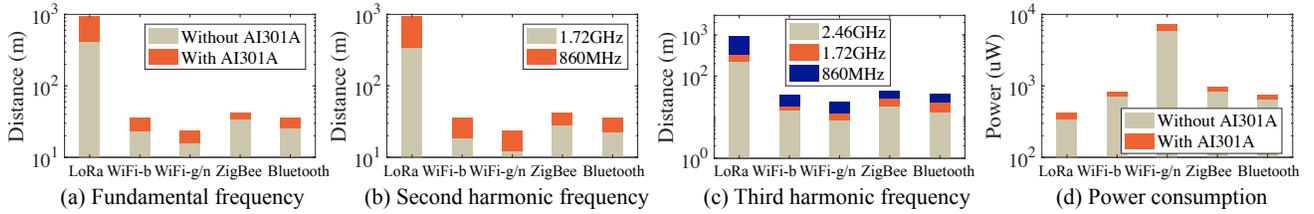


Fig. 14. Impact of the tunnel diode AI301A on the performance of RF-Transformer.

 TABLE III
 ENERGY CONSUMPTION OF EACH COMPONENT.

	Backscatter tag				Backscatter network	
	Oscillator+FPGA	DAC	RF-Transistor	Tunnel diode	Excitation source	Total
LoRa	216.2uW	268.7uW	28.6uW	82.3uW	595.8uW	10.6mW
Bluetooth	385.6uW	538.6uW	42.5uW	125.5uW	1092.2uW	11.1mW
ZigBee	428.5uW	562.5uW	58.5uW	127.4uW	1176.9uW	11.2mW
WiFi 802.11b	395.8uW	554.6uW	47.2uW	118.9uW	1116.5uW	11.1mW
WiFi 802.11g/n/ac	1845.2uW	5332.6uW	315.4uW	579.2uW	8072.4uW	18.1mW

 TABLE IV
 ENERGY CONSUMPTION OF ACTIVE RADIO (LoS)

	LoRa [72]	Bluetooth [73]	ZigBee [74]	WiFi 802.11b [75]	WiFi 802.11g/n/ac [75]
Transmission energy	10mW	10mW	10mW	10mW	10mW
Hardware power	1500m	80m	100m	60m	40m

backscatter range of the 2nd harmonic backscatter signals of LoRa, Wi-Fi 802.11b, Wi-Fi 802.11g/n/ac, ZigBee, and Bluetooth signals is 340.6 m, 18.5 m, 12.3 m, 28.4 m, and 22.6 m, respectively. Compared with the backscatter range at the fundamental frequency (Figure 14(a)), the backscatter range at the 2nd harmonic frequency drops by 1.52–2.75 \times across all the backscatter links.

Backscatter link at the 3rd harmonic frequency (2.58 GHz).

As shown in Figure 14, the backscatter range of the 3rd harmonic backscatter signals of LoRa, Wi-Fi 802.11b, Wi-Fi 802.11g/n/ac, ZigBee, and Bluetooth signals is 220.5 m, 14.6 m, 8.5 m, 18.4 m, and 13.6 m, respectively. Compared with the backscatter range at the fundamental frequency, the backscatter range at the 3rd harmonic frequency drops by 2.31–4.25 \times across all the backscatter links. Compared with the backscatter range at the 2nd harmonic frequency, the backscatter range at the 3rd harmonic frequency drops by 1.26–1.67 \times across all the backscatter links.

C. Power Consumption

Backscatter tag. As summarized in Table III, the backscatter tag consumes 595.8 μW ⁷, 1092.2 μW , 1176.9 μW , 1116.5 μW , and 8072.4 μW to synthesize LoRa, Bluetooth, ZigBee, Wi-Fi 802.11b, and Wi-Fi 802.11g/n/ac signal, respectively. Among these hardware components, the most power-hungry parts are FPGA and DAC, which account for 22.9%–36.3% and 45.2%–66.1% of the total power consumption across all synthesized signals. Tunnel diode consumes the power of 82.3 μW , 125.5 μW , 127.4 μW , 118.9 μW , and 579.2 μW for generating LoRa, Bluetooth, ZigBee, Wi-Fi 802.11b, and Wi-Fi 802.11g/n/ac, respectively. In addition, it is worth noting that the power consumption of FPGA and DAC listed in Table III is lower than that provided in the datasheet. Our analysis is as follows.

(1) *FPGA*. According to the datasheet [76], [77], the current of FPGA's Core, VCCx, logic cells, DSP slices, and I/O pins

 TABLE V
 UNIT POWER CONSUMPTION COMPARISON.

Backscatter network	Tag (energy/range)	LoRa	Bluetooth	ZigBee	WiFi 802.11b	WiFi 802.11g/n/ac
		(energy/range)	0.6uW/m (595.8uW/938.2m)	30.4uW/m (1092.2uW/35.9m)	27.6uW/m (1176.9uW/45.6m)	31.3uW/m (1116.5uW/35.6m)
Active radio (energy/range)	6.67uW/m (10mW/1500m)	125uW/m (10mW/80m)	100uW/m (10mW/100m)	166.67uW/m (10mW/60m)	250uW/m (10mW/40m)	
Active radio (energy/range)	6.67uW/m (10mW/1500m)	125uW/m (10mW/80m)	100uW/m (10mW/100m)	166.67uW/m (10mW/60m)	250uW/m (10mW/40m)	

add up to 12 mA, amounting to a total power of 18 mW with a voltage of 1.5 V. However, the tag does not consume all FPGA resources during the operation. Specifically, the Xilinx Artix-7 FPGA has 215K logic cells, 740 DSP slices, and 500 I/O pins. Taking LoRa signal generation as an example, during the operation, only 1.6K logic cells, 2 DSP slices, and 36 I/O pins are utilized by the tag, accounting for 1.2% of the total resource. The actual power consumption of FPGA is reduced to 216.2 μW .

(1) *DAC*. The theoretical power consumption of a 14-bit DAC AD9767 [67] is 40 mW based on the datasheet. This DAC chip supports dual sampling with the highest sampling rate up to 150 Mbps. However, the transmission rate of the wireless signal is much lower than 150 Mbps. For example, the actual power consumption of DAC for LoRa generation is 268.7 μW given the sampling rate of 1 Mbps.

Backscatter network. In our system, the excitation source transmits the sine signal as the carrier, then the tag modulates data on top of the carrier signal to generate different types of the backscatter signals. Given the transmission power of 10 dBm, the corresponding power consumption of the excitation source is about 10 mW. As shown in Table III, the backscatter network consumes 10.6 mW, 11.1 mW, 11.2 mW, 11.1 mW, and 18.1 mW for LoRa, Bluetooth, ZigBee, Wi-Fi 802.11b, and Wi-Fi 802.11g/n/ac backscatter link.

Comparison with active radios. We define a new metric of *unit power consumption (uPC)* to characterize the power efficiency of the backscatter radio and the active radio at the same communication distance. *uPC* calculates the unit power consumption of the backscatter or the active radio under the communication distance of 1 m. In this way, we can leverage this metric to analyze the tradeoff between the power consumption and the communication distance. Table V shows the evaluation results.

(1) *uPC* of the backscatter network. The backscatter network includes the backscatter tag and the active radios. (a) For the backscatter tag, when generating LoRa, Bluetooth, ZigBee, Wi-Fi 802.11b, and Wi-Fi 802.11g/n/ac signal, the power consumption is 595.8 μW , 1092.2 μW , 1176.9 μW , 1116.5 μW , and 8072.4 μW , and the communication range is 938.2 m, 35.9 m, 45.6 m, 35.6 m, and 23.6 m. Hence, the uPC of the backscatter tag is 0.6 $\mu\text{W}/\text{m}$, 30.4 $\mu\text{W}/\text{m}$,

⁷ μW refers to the microwatts

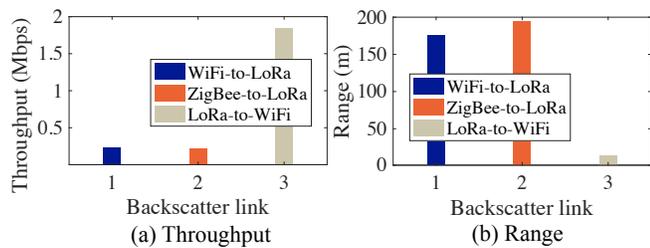


Fig. 15. RF-Transformer’s performance for cross-technology backscatter.

27.6 $\mu\text{W}/\text{m}$, 31.3 $\mu\text{W}/\text{m}$, and 342.1 $\mu\text{W}/\text{m}$ to generate LoRa, Bluetooth, ZigBee, Wi-Fi 802.11b, and Wi-Fi 802.11g/n/ac signal, respectively. (b) On the other hand, the backscatter tag takes the active radio as the excitation source to piggy back its messages, while the performance of the active radio is not affected by the tag. Including the excitation source, the uPC of the active radio is 6.67 $\mu\text{W}/\text{m}$, 125 $\mu\text{W}/\text{m}$, 100 $\mu\text{W}/\text{m}$, 166.67 $\mu\text{W}/\text{m}$, and 250 $\mu\text{W}/\text{m}$ to generate LoRa, Bluetooth, ZigBee, Wi-Fi 802.11b, and Wi-Fi 802.11g/n/ac signal, respectively.

(2) uPC of the active radio. Table IV shows the power consumption and communication range of the active radio. When given the transmission power of 10 mW, the communication range is 1500 m, 80 m, 100 m, 60 m, 40 m for active LoRa, Bluetooth, ZigBee, WiFi 802.11b, WiFi 802.11 g/n/ac. Hence, the uPC of the active radio is 6.67 $\mu\text{W}/\text{m}$, 125 $\mu\text{W}/\text{m}$, 100 $\mu\text{W}/\text{m}$, 166.67 $\mu\text{W}/\text{m}$, and 250 $\mu\text{W}/\text{m}$ to generate LoRa, Bluetooth, ZigBee, Wi-Fi 802.11b, and Wi-Fi 802.11g/n/ac signal, respectively.

D. Performance of Cross-Technology Backscatter

We conduct experiments to evaluate the performance of cross-technology backscatter, including WiFi-to-LoRa backscatter, ZigBee-to-LoRa backscatter, and LoRa-to-WiFi backscatter. The results is shown in Figure 15. We observe that the throughput of the cross-technology backscatter link for WiFi-to-LoRa, ZigBee-to-LoRa, and LoRa-to-WiFi is 231.2 Kbps, 225.7 Kbps, and 1.84 Mbps, respectively. The communication distance of the cross-technology backscatter link for WiFi-to-LoRa, ZigBee-to-LoRa, and LoRa-to-WiFi is 175.5 m, 194.6 m, and 14.3 m, respectively. The experimental results demonstrate that RF-Transformer can effectively support cross technology backscatter communication.

E. Compatibility with Commodity Receivers

In order to verify the compatibility of RF-Transformer with commodity receivers, we deploy a commercial LoRa node SX1280, a DELL laptop, an iPhone XS Max smartphone, and a commercial TelosB node to receive the LoRa, Wi-Fi, Bluetooth, and ZigBee signals generated by RF-Transformer, respectively. We measure the throughput and backscatter range of these commercial devices. Due to the limited indoor space, we report the outdoor experimental results of the LoRa node.

Results. Figure 16(b) and Figure 16(c) show the result. We observe that these commercial devices achieve comparable throughput and backscatter range with the software-defined radio platform USRP. The throughput of the LoRa,

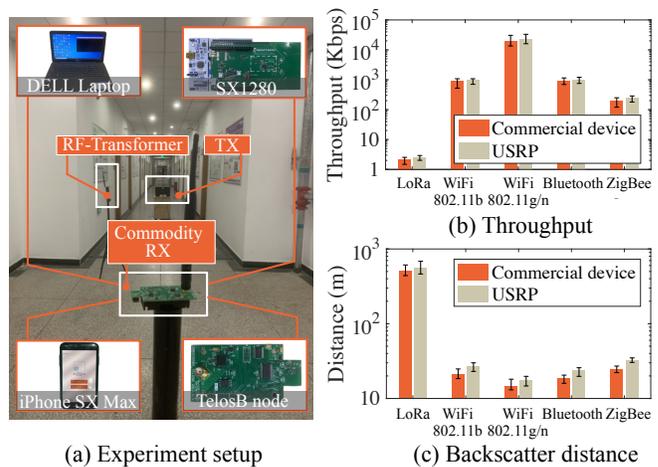


Fig. 16. RF-Transformer’s performance with commercial receivers. (a) Experiment setup. (b) Throughput. (c) Backscatter range.

Wi-Fi 802.11b, Wi-Fi 802.11g/n/ac, Bluetooth, and ZigBee are 2.4 Kbps, 922.4 Kbps, 20.2 Mbps, 935.6 Kbps, and 201.5 Kbps, respectively. The backscatter range of the LoRa, Wi-Fi 802.11b, Wi-Fi 802.11g/n/ac, Bluetooth, and ZigBee are 516.5 m, 21.5 m, 14.8 m, 18.5 m, and 24.5 m, respectively. Compared with the USRP platform, the throughput drops by 1.12–1.35 \times and the backscatter range drops by 1.06–1.43 \times across all backscatter links. The reason of performance gap between the commercial device and the USRP mainly comes from the difference of hardware receiving sensitivity.

VIII. CONCLUSION

We have presented the design, implementation, and evaluation of RF-Transformer, a unified backscatter radio hardware abstraction. RF-Transformer provides a programmable interface to the micro-controller and allows IoT devices to synthesize different types of protocol-compliant backscatter signals in the PHY layer, reflecting the idea of radio frequency (RF) computing. RF-Transformer also supports cross-frequency and cross-technology backscatter. We believe RF-Transformer is a significant step in a line of works that will scale out backscatter technologies to heterogeneous wireless networks.

ACKNOWLEDGMENT

This work is supported in part by National Science Fund of China under grant No. 62425207, No. U21B2007, No. 62202264, No. 62394341, No. 62394344. Longfei Shanguan is supported by Amateur Radio Digital Communications.

REFERENCES

- [1] V. Talla, M. Hesar, B. Kellogg, A. Najafi, J. R. Smith, and S. Gollakota, “LoRa backscatter: Enabling the vision of ubiquitous connectivity,” in *Proceedings of ACM UbiComp*, 2017.
- [2] B. Kellogg, A. Parks, S. Gollakota, J. R. Smith, and D. Wetherall, “WiFi backscatter: Internet connectivity for RF-powered devices,” in *Proceedings of ACM SIGCOMM*, 2014.
- [3] Y. Peng, L. Shanguan, 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 ACM SIGCOMM*, 2018.
- [4] X. Guo, L. Shanguan, 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 ACM SenSys, Virtual Event Japan, November 16-19, 2020*.

- [5] J. Wang, H. Hassanieh, D. Katabi, and P. Indyk, "Efficient and reliable low-power backscatter networks," in *Proceedings of ACM SIGCOMM*, 2012.
- [6] P. Hu, P. Zhang, and D. Ganesan, "Laissez-faire: Fully asymmetric backscatter communication," in *Proceedings of ACM SIGCOMM*, 2015.
- [7] H. Jiang, J. Zhang, X. Guo, and Y. He, "LoPhy: A resilient and fast covert channel over LoRa PHY," in *Proceedings of ACM IPSN, San Antonio, TX, USA, May 9-12, 2023*.
- [8] V. Liu, A. Parks, V. Talla, S. Gollakota, D. Wetherall, and J. R. Smith, "Ambient backscatter: Wireless communication out of thin air," in *Proceedings of ACM SIGCOMM*, 2013.
- [9] P. Zhang, M. Rostami, P. Hu, and D. Ganesan, "Enabling practical backscatter communication for on-body sensors," in *Proceedings of ACM SIGCOMM*, 2016.
- [10] X. Guo, L. Shanguan, 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 USENIX NSDI*, 2022.
- [11] F. Zhu, M. Ouyang, L. Feng, Y. Liu, X. Tian, M. Jin, D. Chen, and X. Wang, "Enabling software-defined PHY for backscatter networks," in *Proceedings of ACM MobiSys*, 2022.
- [12] X. Na, X. Guo, Z. Yu, J. Zhang, Y. He, and Y. Liu, "Leggiero: Analog WiFi backscatter with payload transparency," in *Proceedings of ACM MobiSys, Helsinki, Finland, June 18-22, 2023*.
- [13] 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 ACM SenSys, Coimbra, Portugal, November 15-17, 2021*.
- [14] "WiFi frequency band." https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.a_glossary:w:wifi_frequencies.
- [15] "Wi-Fi Channels, Frequencies, Bands & Bandwidths." <https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/channels-frequencies-bands-bandwidth.php>.
- [16] A. N. Parks, A. Liu, S. Gollakota, and J. R. Smith, "Turbocharging ambient backscatter communication," in *Proceedings of ACM SIGCOMM*, 2014.
- [17] M. H. Mazaheri, A. Chen, and O. Abari, "mmTag: A millimeter wave backscatter network," in *Proceedings of ACM SIGCOMM*, pp. 463–474, 2021.
- [18] B. Kellogg, V. Talla, J. R. Smith, and S. Gollakota, "Passive WiFi: Bringing low power to WiFi transmissions," in *Proceedings of USENIX NSDI*, 2018.
- [19] V. Iyer, V. Talla, B. Kellogg, S. Gollakota, and J. Smith, "Inter-technology backscatter: Towards internet connectivity for implanted devices," in *Proceedings of ACM SIGCOMM*, 2016.
- [20] P. Zhang, D. Bharadia, K. Joshi, and S. Katti, "HitchHike: Practical backscatter using commodity WiFi," in *Proceedings of ACM SenSys*, 2016.
- [21] D. Bharadia, K. R. Joshi, M. Kotaru, and S. Katti, "BackFi: High throughput WiFi backscatter," in *Proceedings of ACM SIGCOMM*, 2018.
- [22] P. Zhang, C. Josephson, D. Bharadia, and S. Katti, "FreeRider: Backscatter communication using commodity radios," in *Proceedings of ACM CONEXT, Online, December 12-15, 2017*.
- [23] A. Abedi, F. Dehbashi, M. H. Mazaheri, O. Abari, and T. Brecht, "WiTAG: Seamless WiFi backscatter communication," in *Proceedings of ACM SIGCOMM*, 2020.
- [24] A. Wang, V. Iyer, V. Talla, J. R. Smith, and S. Gollakota, "FM backscatter: Enabling connected cities and smart fabrics," in *Proceedings of USENIX NSDI*, 2017.
- [25] J. F. Ensworth and M. S. Reynolds, "Every smart phone is a backscatter reader: Modulated backscatter compatibility with Bluetooth 4.0 Low Energy (BLE) devices," in *Proceedings of IEEE RFID*, 2015.
- [26] X. Guo, Y. He, N. Jing, J. Zhang, Y. Liu, and L. Shanguan, "A low-power demodulator for LoRa backscatter systems with frequency-amplitude transformation," *IEEE/ACM Transactions on Networking*, vol. 32, no. 4, pp. 3515–3527, 2024.
- [27] X. Guo, L. Shanguan, Y. He, J. Zhang, H. Jiang, A. A. Siddiqi, and Y. Liu, "Efficient ambient LoRa backscatter with ON-OFF keying modulation," *IEEE/ACM Transactions on Networking*, vol. 30, no. 2, pp. 641–654, 2022.
- [28] Y. Zou, X. Na, X. Guo, Y. Sun, and Y. He, "Trident: Interference avoidance in multi-reader backscatter network via frequency-space division," in *Proceedings of IEEE INFOCOM, Vancouver, BC, Canada, May 20-23, 2024*.
- [29] X. Guo, X. Zheng, and Y. He, "WiZig: Cross-technology energy communication over a noisy channel," in *Proceedings of IEEE INFOCOM*, 2017.
- [30] X. Guo, Y. He, J. Zhang, and H. Jiang, "WIDE: Physical-level CTC via digital emulation," in *Proceedings of IEEE/ACM IPSN*, 2019.
- [31] Z. Li and T. He, "WEBee: Physical-layer cross-technology communication via emulation," in *Proceedings of ACM MobiCom*, 2017.
- [32] D. Xia, X. Zheng, F. Yu, L. Liu, and H. Ma, "WiRa: Enabling Cross-Technology Communication from WiFi to LoRa with IEEE 802.11ax," in *Proceedings of IEEE INFOCOM*, 2021.
- [33] Y. He, X. Guo, X. Zheng, Z. Yu, J. Zhang, H. Jiang, X. Na and J. Zhang, "Cross-technology communication for the Internet of Things: A survey." <https://arxiv.org/abs/2203.14813v2>. Accessed 28-March-2022.
- [34] H.-W. Cho and K. G. Shin, "BlueFi: bluetooth over WiFi," in *Proceedings of ACM SIGCOMM*, 2021.
- [35] P. Gawlowicz, A. Zubow, and F. Dressler, "Wi-Lo: Emulation of LoRa using commodity 802.11b WiFi devices," in *Proceedings of IEEE ICC*, 2022.
- [36] J. Jung, J. Ryoo, Y. Yi, and S. M. Kim, "Gateway over the air: Towards pervasive Internet connectivity for commodity IoT," in *Proceedings of ACM MobiSys*, 2020.
- [37] A. Sirojuddin, D. D. Putra, and W. J. Huang, "Low-complexity sum-capacity maximization for intelligent reflecting surface-aided mimo systems," *IEEE Wireless Communications Letters*, vol. 11, no. 7, pp. 1354–1358, 2022.
- [38] M. Rossanese, P. Mursia, A. Garcia-Saavedra, V. Sciancalepore, A. Asadi, and X. Costa-Perez, "Designing, building, and characterizing rf switch-based reconfigurable intelligent surfaces," in *Proceedings of ACM MobiCom*, 2022.
- [39] K. Qian, L. Yao, X. Zhang, and T. N. Ng, "Millimirror: 3d printed reflecting surface for millimeter-wave coverage expansion," in *Proceedings of ACM MobiCom*, 2022.
- [40] Z. Li, C. Wu, S. Wagner, J. C. Sturm, N. Verma, and K. Jamieson, "Reits: Reflective surface for intelligent transportation systems," in *Proceedings of ACM HotMobile*, 2021.
- [41] P. K. Sharma and P. Garg, "Intelligent reflecting surfaces to achieve the full-duplex wireless communication," *IEEE Communications Letters*, vol. 25, no. 2, pp. 622–626, 2021.
- [42] A. Varshney, A. Soleiman, and T. Voigt, "Tunnelscatter: Low power communication for sensor tags using tunnel diodes," in *MobiCom*, ACM, 2019.
- [43] A. Varshney and L. Corneo, "Tunnel emitter: Tunnel diode based low-power carrier emitters for backscatter tags," in *Proceedings of ACM MobiCom*, 2020.
- [44] A. Varshney, W. Yan, and P. Dutta, "Judo: Addressing the energy asymmetry of wireless embedded systems through tunnel diode based wireless transmitters," in *Proceedings of ACM MobiSys*, 2022.
- [45] D. Dobkin, *The RF in RFID: UHF RFID in practice*. Newnes, 2012.
- [46] "Transmission-line theory." <https://s2629002012.files.wordpress.com/2012/11/huitransmissionlines.pdf>.
- [47] "Input impedance and reflection coefficient of transmission line." <https://www.sciencedirect.com/topics/computer-science/reflection-coefficient>.
- [48] "MOSFET ATF54143." <https://pdf1.alldatasheetcn.com/datasheet-pdf/view/102973/HP/ATF54143.html>.
- [49] "Smith chart." <https://www.maximintegrated.com/en/design/technical-documents/tutorials/7/742.html>.
- [50] A. Tang, Y. Kim, Y. Xu, and M.-C. F. Chang, "A 5.8 GHz 54 Mb/s backscatter modulator for WLAN with symbol pre-distortion and transmit pulse shaping," *IEEE Microwave and Wireless Components Letters*, vol. 26, no. 9, pp. 729–731, 2016.
- [51] "Wilkinson power splitter." <https://www.microwaves101.com/encyclopedias/wilkinson-power-splitters>.
- [52] "Quadrature Amplitude Modulation." https://eprints.soton.ac.uk/260296/1/QAM3-chaps_1-22-24.pdf.
- [53] C. Li, X. Guo, L. Shanguan, Z. Cao, and kyle Jamieson, "CurvingLoRa to boost LoRa network throughput via concurrent transmission," in *Proceedings of USENIX NSDI*, 2022.
- [54] D. Guo, C. Gu, L. Jiang, W. Luo, and R. Tan, "ILLOC: In-hall localization with standard LoRaWAN uplink frames," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 6, no. 1, pp. 1–26, 2022.
- [55] B. Liu, C. Gu, S. He, and J. Chen, "LoPhy: A resilient and fast covert channel over LoRa PHY," *IEEE/ACM Transactions on Networking*, pp. 1–16, 2024.
- [56] F. Farzami, S. Khaledian, B. Smida, and D. Erricolo, "Ultra-low power reflection amplifier using tunnel diode for RFID applications," in *Proceedings of IEEE International Symposium on Antennas and Propagation*, 2017.
- [57] S. Khaledian, F. Farzami, D. Erricolo, and B. Smida, "A full-duplex bidirectional amplifier with low DC power consumption using tunnel diodes," *IEEE Microwave and Wireless Components Letters*, vol. 27, no. 12, pp. 1125–1127, 2017.

[58] F. Amato, C. W. Peterson, B. P. Degnan, and G. D. Durgin, "A 45 uw bias power, 34 dB gain reflection amplifier exploiting the tunneling effect for RFID applications," in *Proceedings of IEEE RFID*, 2015.

[59] J. Lee and K. Yang, "RF power analysis on 5.8 GHz low-power amplifier using resonant tunneling diodes," *IEEE Microwave and Wireless Components Letters*, vol. 27, no. 1, pp. 61–63, 2017.

[60] J. Lee, J. Lee, and K. Yang, "Reflection-type RTD low-power amplifier with deep sub-mW DC power consumption," *IEEE Microwave and Wireless Components Letters*, vol. 24, no. 8, pp. 551–553, 2014.

[61] "Tunnel diode of AI301A." <https://www.amazon.com/Switching-Tunnel-AI301A-3I301A-military/dp/B00KRWS4LS>.

[62] Z. An, Q. Lin, and L. Yang, "Cross-frequency communication: Near-field identification of UHF RFIDs with WiFi!," in *Proceedings of ACM MobiCom*, 2018.

[63] G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang, and W. Xu, "DolphinAttack: Inaudible voice commands," in *Proceedings of ACM CCS*, 2017.

[64] D. Dai, Z. An, and L. Yang, "Inducing wireless chargers to voice out for inaudible command attacks," in *Proceedings of IEEE S&P*, 2023.

[65] "3 dBi omni-directional antenna in 2.45 GHz." <https://www.ebay.com/itm/2450Mhz>.

[66] "Xilinx Artix-7 FPGA." <https://www.xilinx.com/products/silicon-devices/fpga/artix-7.html>.

[67] "14-bit DAC AD9767." <https://www.analog.com/cn/products/ad9767.html#product-overview>.

[68] "Vector Network Analyser (VNA), CEYEAR 3672A." <https://mcs-testequipment.com/products/rf-mw-network-analysers/network-analysers/3672a-s>.

[69] "ZFL-1000VH+ 10-1000 MHz high dynamic range RF amplifier." <https://www.minicircuits.com/WebStore/dashboard.html?model=ZFL-1000VH%2B>.

[70] "FCC Rules for Unlicensed Wireless Equipment operating in the ISM bands." <http://afar.net/tutorials/fcc-rules/>.

[71] D. tutorials, "Fundamentals of direct digital synthesis (DDS)." <https://www.analog.com/media/en/training-seminars/tutorials/MT-085.pdf>. Accessed 30-May-2021.

[72] "2.4GHz LoRa chip SX1280." <https://www.semtech.com/products/wireless-rf/lora-24ghz/sx1280>.

[73] "Bluetooth transceiver CC2650." https://www.ti.com/lit/ds/symlink/cc2650.pdf?ts=1645762817519&ref_url=https%253A%252F%252Fwww.ti.com%252Fproduct%252FCC2650.

[74] "ZigBee transceiver CC2480." https://www.ti.com/lit/ds/swrs074a/swrs074a.pdf?ts=1645762704834&ref_url=https%253A%252F%252Fwww.google.com.hk%252F.

[75] M. E. Yuksel, "Power consumption analysis of a WiFi-based IoT device," *Electrica*, vol. 20, no. 1, pp. 72–70, 2020.

[76] "7 Series FPGAs Data Sheet: Overview." https://www.mouser.com/datasheet/2/903/ds180_7Series_Overview-1591537.pdf.

[77] "Artix-7 FPGAs Data Sheet: DC and AC Switching Characteristics." https://docs.xilinx.com/v/u/en-US/ds181_Artix_7_Data_Sheet.



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.



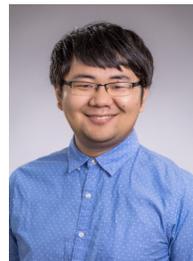
Yuan He is an associate professor in the School of Software and BNRist of Tsinghua University. He received his B.E. degree in the University of Science and Technology of China, his M.E. degree in the Institute of Software, Chinese Academy of Sciences, and his PhD degree in Hong Kong University of Science 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.



Jiacheng Zhang is currently a graduate student in Tsinghua University. He received his B.E. degree in Tsinghua University. His research interests include backscatter communication and wireless sensing.



Yunhao Liu received his BS degree in Automation Department from Tsinghua University. He received an MS and a Ph.D. degree in Computer Science and Engineering at Michigan State University, USA. Yunhao is now MSU Foundation Professor and Chairperson of Department of Computer Science and Engineering, Michigan State University, and holds Chang Jiang Chair Professorship at Tsinghua University. He is an ACM Distinguished Speaker and now serves as the Editor-in-Chief of ACM Transactions on Sensor Networks. 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.



Longfei Shangguan is a senior researcher at Microsoft Cloud & AI, Redmond. He received his B.E. degree in Xidian University, and his PhD degree in Hong Kong University of Science and Technology. His research interests include networking, IoT, and wireless systems.