The Trip to ZigBee Backscatter across a Decade—a Systematic Review

Yang Liu
School of Computer Science
University of Science and Technology of China
Hefei, China
current@mail.ustc.edu.cn

***Abstract*—The field of backscatter communication has undergone a profound transformation, evolving from a niche technology for radio-frequency identification (RFID) into a sophisticated paradigm poised to enable a truly battery-free Internet of Things (IoT). This evolution is built upon a deepening understanding of the fundamental principles governing these ultra-low-power links. Modern backscatter systems are no longer simple reflectors of continuous waves but are increasingly designed to interact with complex, data-carrying ambient signals from ubiquitous sources like WiFi, ZigBee, and cellular networks. This review systematically charts the journey of ambient backscatter, particularly focusing on its interaction with ZigBee and other commodity wireless protocols over the last decade. We analyze the progression from foundational proof-of-concept systems that established productive backscatter to modern high-throughput, concurrent, and cross-technology communication architectures. Key advancements in fine-grained modulation, robust synchronization, cross-technology physical layer emulation, and multi-tag coordination are detailed. A comparative analysis of state-of-the-art systems highlights the core trade-offs between performance metrics like data rate and range, power consumption, and compatibility with commodity hardware. Finally, we synthesize the primary challenges—including networking scalability, security vulnerabilities, the near-far problem, and practical deployment hurdles—and outline future research directions, such as integration with Reconfigurable Intelligent Surfaces (RIS) and 6G networks, that promise to further expand the capabilities of this transformative technology.**

***Index Terms*—Ambient Backscatter, ZigBee, Internet of Things (IoT), Low-Power Communication, Cross-Technology Communication, Systematic Review, Battery-Free.**

I. Introduction

A. Background

The proliferation of the Internet of Things (IoT) has created an unprecedented demand for low-power, low-cost, and ubiquitous wireless communication. At the heart of this demand lies the challenge of powering billions, and potentially trillions, of connected devices. Traditional battery-powered solutions are often impractical due to the immense cost and logistical burden of battery replacement and disposal, not to mention the environmental impact [1]. This has fueled intensive research into alternative communication paradigms that can operate with minimal or zero battery power, a concept often termed the Battery-Free Internet of Things (BF-IoT).

Two key technologies have emerged as central to this pursuit: the ZigBee protocol and backscatter communication. ZigBee, based on the IEEE 802.15.4 standard, is a widely adopted protocol for low-power, low-data-rate wireless personal area networks (WPANs). Its characteristics—including mesh networking, simple protocol stack, and notably low active and sleep power consumption—make it ideal for applications like smart homes, industrial control, and environmental monitoring [2]. However, even with its optimizations, active ZigBee radios still consume milliwatts of power during transmission, which can be a significant drain for devices intended to last for years without intervention.

Backscatter communication offers a more radical approach to power reduction. Instead of actively generating their own radio waves, backscatter devices (or "tags") communicate by reflecting and modulating existing radio frequency (RF) signals present in the environment [3]. This passive approach, where the power-hungry components of a traditional radio (like power amplifiers and oscillators) are eliminated, allows for devices that consume orders of magnitude less power—microwatts instead of milliwatts. This fundamental efficiency enables the vision of truly battery-free IoT devices that can be powered solely by harvesting energy from the very RF signals they use for communication [4].

B. Motivation and Significance

The motivation for combining ZigBee and backscatter communication is compelling and synergistic. By enabling passive tags to communicate using ambient ZigBee signals (or, more powerfully, to generate ZigBee-compatible signals by backscattering other ambient sources like WiFi), we can massively expand the IoT ecosystem. This fusion allows for the deployment of vast networks of simple, disposable, and battery-free sensors that can seamlessly integrate with existing ZigBee infrastructure. The application potential is immense, spanning from smart packaging that reports its status, infrastructure health monitoring sensors embedded in concrete, and dense sensor deployments in smart agriculture, to implantable medical devices that can communicate directly with commodity gateways like smartphones and smartwatches [1], [5]. This approach promises to unlock the full potential of a pervasive and sustainable IoT, breaking the energy barrier that has long constrained its growth.

C. Review Objectives and Scope

This paper aims to provide a systematic review of the evolution of ZigBee and related ambient backscatter communication technologies over the past decade (approximately 2015-2025). Our objective is to chart the journey from early foundational concepts that proved the feasibility of "productive" backscatter to the latest high-performance systems capable of multi-megabit throughput and cross-protocol translation. We identify the key technological advancements, synthesize and compare the performance metrics reported across the literature, and discuss the persistent challenges and promising future research directions. The scope is primarily focused on systems that leverage or create commodity-compatible signals—particularly ZigBee, WiFi, and Bluetooth—as these represent the most practical path toward widespread adoption and a truly interoperable IoT.

D. Paper Structure

This review is organized as follows. Section II details the foundational principles of modern backscatter systems, including channel characteristics and the key innovation of codeword translation. Section III charts the quest for higher throughput, analyzing the move to finer-grained modulation schemes. Section IV explores developments enabling communication in the heterogeneous IoT, focusing on cross-technology communication and concurrency. Section V delves into the key techniques and implementations covering system architectures, tag design, and receiver signal processing. Section VI provides a comprehensive synthesis, including a comparative performance evaluation, a discussion of core challenges and limitations. Finally, Section VII concludes the paper with a summary of the field's progress and an outlook on future directions.

II. Foundational Principles of Modern Backscatter

The evolution of backscatter communication from a simple RFID-like technology to a sophisticated paradigm capable of interacting with complex ambient signals is built upon a deeper understanding of its underlying principles. This section establishes the theoretical and practical bedrock of this new era of ambient backscatter, analyzing the physical channel, the critical interplay between performance and power, and the pivotal innovation that enabled backscatter to leverage productive, data-carrying wireless traffic.

A. The Backscatter Channel: Theory and Practical Limits

An ambient backscatter system involves three entities: a legacy transmitter (LT) providing the ambient RF signal (e.g., a WiFi AP), a backscatter device (BD) or tag, and a backscatter receiver (BR) [6]. The communication is governed by three distinct wireless links: the forward link (LT-to-BD), the backscatter link (BD-to-BR), and a direct interference link (LT-to-BR) [7]. Performance is often analyzed assuming a frequency-flat, block-fading channel model [6].

A critical metric is the outage probability. An outage occurs if the energy harvested by the tag is insufficient ($E_k < P_{c,k}T$) or the Signal-to-Interference-plus-Noise Ratio (SINR) at the receiver is too low ($\gamma_k^b < \gamma_{th}^b$) [6]. A key finding is that the co-channel interference from the direct LT-to-BR link is a dominant limiting factor, leading to "outage saturation." Beyond a certain point, increasing the LT's power provides diminishing returns, as the interference floor rises with the signal strength [6]. This reveals a fundamental performance ceiling.

Furthermore, obtaining complete Channel State Information (CSI) is often infeasible, necessitating noncoherent detection schemes. Seminal work derived the performance of both an optimal Maximum Likelihood (ML) detector and a lower-complexity joint-energy detector [7]. These noncoherent detectors often exhibit an "error floor" at high SNR, where the Bit Error Rate (BER) flattens out, not due to thermal noise, but due to channel characteristics [7]. This again highlights that performance gains must come from more sophisticated system design. The non-linearity of real-world energy harvesters (EH) further complicates this; assuming a simple linear EH model leads to an overly optimistic assessment of system performance [6].

B. Codeword Translation: The Gateway to Productive Backscatter

A pivotal innovation that unlocked the potential of ambient backscatter is "codeword translation" [8]. This technique allows a tag to operate using a *productive* ambient signal—a standard, data-carrying transmission from a commodity device like a WiFi router—rather than a simple, non-productive continuous wave.

The core concept is to transform a valid codeword from the ambient signal's codebook into another valid codeword from the *same* codebook during reflection. A "codeword" here is a physical layer signal symbol (e.g., a phase-modulated state). A "codebook" is the complete set of valid symbols defined by a protocol. The tag accomplishes this by manipulating the signal's amplitude, phase, or frequency. In a simple binary scheme, to send a '1', a tag might introduce a 180° phase shift to the incoming codeword; for a '0', it would apply no shift [8].

This technique necessitates a bistatic, dual-receiver setup. One receiver decodes the original, unmodified signal. A second receiver, often on an adjacent channel, decodes the backscattered signal. The tag's data is recovered by comparing the two decoded bit streams, typically via a bitwise XOR operation [8], [9]. This architecture, foundational to pioneering systems like FreeRider [8], proved that backscatter could coexist with and leverage active wireless traffic, paving the way for the integrated single-receiver systems that followed.

C. The Symbiotic Challenge of Synchronization and Power

High-performance backscatter demands precise synchronization with the incoming carrier, which requires power-intensive, high-bandwidth processing that runs counter to the

ultra-low-power ethos of the technology [10]. Early systems used simple energy detection, achieving only coarse synchronization and thus limiting data rates [3].

The SyncScatter system provided a canonical solution through a two-stage hierarchical wake-up and synchronization protocol, reframing synchronization as a power-managed, event-driven process [10].

- **Stage 1: Low-Power Wake-up.** A passive, low-bandwidth energy detector, consuming single-digit microwatts, monitors for a pre-specified wake-up signature (e.g., a sequence of WiFi packets with specific lengths).
- **Stage 2: High-Precision Synchronization.** Once awakened, the tag briefly activates a higher-power, higher-bandwidth active RF amplifier for a few microseconds—just long enough to achieve precise symbol-level synchronization (e.g., within 150 ns for WiFi).

This aggressive duty-cycling of power-intensive components is the key to minimizing average power consumption while achieving high performance when needed. This design was born from a holistic link budget analysis that considered FCC power limits, receiver sensitivity, path loss, and BER degradation from synchronization errors, establishing a target sensitivity and demonstrating that improving it further yields diminishing returns [10]. This cross-layer optimization approach is a crucial principle for nearly all high-performance, low-power wireless systems.

III. The Quest for Higher Throughput

The primary driver of innovation in backscatter has been the quest for higher data rates. Early systems, with throughputs in the kilobits-per-second range, were insufficient for a data-rich IoT. The journey to megabit-per-second backscatter is marked by a clear trend: moving from coarse-grained modulation of entire symbols towards fine-grained manipulation of the signal's fundamental components.

A. From Symbols to Samples: A Leap in Granularity for OFDM

Early attempts to backscatter Orthogonal Frequency Division Multiplexing (OFDM) signals, the foundation of WiFi, faced a formidable obstacle. When a tag introduced a phase shift at the symbol level to encode data, the WiFi receiver's phase error correction algorithm—which uses pilot subcarriers to cancel channel-induced phase errors—would interpret the tag's modulation as just another error and "correct" it, erasing the data [11].

The breakthrough came with TScatter, which introduced *sample-level* modulation [11]. Instead of one phase shift per $4\ \mu s$ symbol, the TScatter tag toggles its RF switch at the 20 MHz WiFi sample rate (every 50 ns), introducing a unique phase shift on *each individual sample*. The key insight was that this would cause the phase offsets on data-carrying subcarriers to differ from those on pilot subcarriers. This breaks the receiver's assumption of a common phase error. As a result, the receiver corrects the actual channel error using the pilots but leaves the tag's data-bearing phase information on the data subcarriers intact.

This innovation, combined with a demodulation model that estimates tag data by minimizing the Euclidean distance between received subcarrier values and their expected QAM constellation points, enabled a massive leap in performance. TScatter demonstrated throughputs up to 13.63 Mbps, three orders of magnitude higher than previous systems, while remaining compatible with unmodified commodity WiFi receivers [11].

B. Chip-Level Modulation: Unleashing ZigBee's Potential

A parallel evolution occurred in ZigBee backscatter. ZigBee uses Direct-Sequence Spread Spectrum (DSSS), where every 4 data bits are mapped to a 32-chip pseudo-random sequence [12]. Early systems like FreeRider used coarse-grained, symbol-level modulation for robustness, applying the same phase shift across eight consecutive symbols to encode a single tag bit. This came at the cost of a throughput reduction of over 32 times compared to active ZigBee [8].

The breakthrough, pioneered by systems like ChipScatter and EchScatter, was to modulate at the level of individual chips within a single symbol [13], [14]. The tag applies a carefully designed 32-chip phase modulation sequence to the 32 chips of the incoming symbol. This "enriches" codeword translation: the goal is to transform any of the 16 possible incoming ZigBee symbols into any of the other 15.

To achieve this, EchScatter designed 16 unique 32-chip phase modulation sequences, each corresponding to a 4-bit tag data value ($2^4 = 16$). When a tag sends a 4-bit value, it applies the corresponding phase sequence to the incoming ZigBee symbol. The resulting backscattered chip sequence, when processed by the commodity ZigBee receiver's minimum Hamming distance decoder, is uniquely decoded as one of the 16 possible output symbols. By comparing the original and backscattered symbols, a look-up table recovers the 4-bit tag data [14].

This fine-grained control allows a single ZigBee symbol to carry 4 bits of tag data, a dramatic improvement over FreeRider's 1 bit per 8 symbols. This catapulted ZigBee backscatter throughput to rates comparable to active ZigBee (e.g., 247 kbps), a 32-fold increase over symbol-level methods [14].

C. Intelligent Rate Adaptation for Mobile Backscatter Networks

Achieving high throughput also requires intelligently adapting the transmission rate to the dynamic wireless channel, especially in mobile scenarios. Early rate adaptation schemes for backscatter (e.g., Blink, CARA) relied on a static, pre-trained 2D map, selecting the optimal rate based on Received Signal Strength Indicator (RSSI) and packet loss rate [15], [16]. This approach is brittle, as the maps are highly hardware-dependent; a map trained for one tag model performs poorly on another [15].

MobiRate overcomes this by replacing the static map with a dynamic framework that leverages PHY-layer mobility information [15]. It introduces three key components:

1) **Velocity-Based Loss Rate Estimation:** Packet loss is not static. MobiRate provides a more accurate estimate of channel quality by re-weighing loss statistics based on the tag's velocity, derived from the Doppler shift in the signal's phase.
2) **Mobility-Assisted Probing Trigger:** Channel probing (testing different rates) is a source of overhead. MobiRate reduces this by using the tag's location and direction of movement to eliminate unnecessary probes.
3) **Selective, Collision-Free Probing:** To address probe collisions in multi-tag environments, MobiRate repurposes the 'SELECT' command of the ISO 18000-6C standard. This command, normally used for inventorying a subset of tags, is used to enable collision-free, point-to-point probing of individual tags.

By combining these techniques, MobiRate achieves throughput gains of up to 3.8x over previous systems, demonstrating the superiority of adaptive, PHY-aware systems in real-world mobile environments [15].

IV. The Heterogeneous IoT: Cross-Technology and Coexistence

The modern IoT is a dense, heterogeneous ecosystem where devices using different wireless standards like WiFi, ZigBee, and Bluetooth must coexist and, ideally, cooperate. Backscatter communication has emerged as a powerful technology to bridge these disparate worlds.

A. Cross-Technology PHY Emulation

The ultimate goal of Cross-Technology Communication (CTC) is to enable a device using one protocol to generate a signal that can be directly decoded by an unmodified commodity receiver of a different protocol. This requires physical-layer (PHY) emulation, where the tag acts as an on-the-fly protocol translator.

Early work like Interscatter demonstrated transforming BLE transmissions into standards-compliant WiFi and ZigBee signals [5]. This involved forcing the BLE transmitter to emit a simple, non-productive single-tone carrier, then using a sophisticated backscatter modulator to perform single-sideband modulation, impressing the target protocol's waveform onto the carrier.

Subsequent systems refined this. BumbleBee showed it was possible to use a *productive* BLE carrier, arguing that the tag's modulation could be made dominant enough to overwrite the BLE signal's information from the perspective of a less sensitive, narrowband ZigBee receiver [17].

Perhaps the most elegant solution was BlueBee, which achieved PHY emulation purely through payload manipulation [18]. Its key insight was that by carefully crafting the bit patterns in a standard BLE packet's payload, the resulting GFSK-modulated RF waveform could be made to physically resemble the waveform of a legitimate OQPSK-modulated ZigBee packet. The inherent error tolerance of the ZigBee receiver's DSSS design was sufficient to correctly decode this imperfect but recognizable emulated packet. This was achieved without modifying the BLE transmitter's firmware, demonstrating true transparency [18].

B. Concurrent Transmissions: Resolving Collisions in Dense Networks

As IoT deployments become denser, packet collisions become a primary bottleneck [19], [20]. A significant body of research has focused on physical-layer techniques for multi-packet reception (MPR), allowing a receiver to decode multiple, overlapping packets. Several approaches for ZigBee have emerged:

Interference Cancellation via Time Offsets (mZig/CmZig): These systems exploit the fact that collided packets almost always arrive with a slight time offset. By oversampling the signal, the receiver can identify a few collision-free samples at the start of the first packet's first chip. Leveraging the known half-sine pulse shape of a ZigBee chip, the receiver reconstructs the entire chip's waveform, subtracts it from the composite signal, and repeats the process for the next packet [12], [19]. CmZig refines this by incorporating channel estimation to more accurately model each transmitter's signal [12].

Reference-Based Decoding (PPM): The Preamble and Postamble-based MPR (PPM) system requires the transmitter to attach a short, known postamble to each packet. The receiver then has known, collision-free reference chips at both the beginning (preamble) and end (postamble) of the collided segment. These are used to construct a library of ideal waveforms for all possible overlap combinations, against which the collided signal is compared [20].

Orthogonal Waveforms (OrthZig): To avoid complex cancellation or waveform construction, OrthZig assigns mutually orthogonal spreading codes (Walsh codes) to different transmitters. The receiver can separate the linearly combined signals by correlating the composite signal with each transmitter's known orthogonal waveform. This offers high-precision resolution with low computational complexity [21].

C. Extending the Network Fabric: Multi-Hop Backscatter

Single-hop backscatter range is limited by the "doubly near-far" problem, where the signal suffers path loss on both the forward (LT-to-BD) and backscatter (BD-to-BR) links [1], [4]. Multi-hop communication, where tags relay signals, is a classic solution to extend network coverage.

X-Tandem was the first to demonstrate a practical multi-hop backscatter architecture compatible with commodity WiFi [9]. It is built on two key innovations:

1) **Analog Forwarding:** Instead of decode-and-forward, tags in X-Tandem perform analog forwarding. A relay tag receives the analog waveform from a previous-hop tag and, without decoding, simultaneously re-modulates it with its *own* data before reflecting it onward.

2) **Multiple Frequency Shifts (MFS):** To prevent interference between hops, X-Tandem uses MFS. The first tag receives the original signal at f_c and backscatters it at $f_c + f_1$. The second tag receives this and re-transmits at $f_c + f_1 + f_2$. The final receiver listens only at the final frequency, isolating the complete multi-hop packet.

This allows a single WiFi packet to travel through a chain of tags, accumulating data from each before being decoded by a single commodity WiFi receiver [9].

V. Key Techniques and Implementations

A. System Architectures

1) Monostatic vs. Bistatic: Backscatter systems are broadly categorized into two architectures. In a **monostatic** system, a single device acts as both the RF source (or "exciter") and the receiver. This is the classic architecture used in commercial RFID readers. It is simpler to deploy but suffers from strong self-interference, as the reader's own powerful transmission can easily overwhelm the tag's faint reflection.

In a **bistatic** architecture, the RF source and the receiver are separate entities. This is the dominant architecture in ambient backscatter research. For example, in FreeRider [8], the exciter is a commodity WiFi AP, and the receiver is a second commodity WiFi device. This separation provides spatial diversity and helps mitigate the direct-path interference, but it introduces the complexity of coordinating three separate devices.

2) Ambient Backscatter: This is a specific form of bistatic backscatter where the RF source is an "ambient" transmitter that is not part of the backscatter system itself, such as a public TV tower [3], a cellular base station [22], or a nearby WiFi access point [8]. The key advantage is that it eliminates the need to deploy a dedicated power-hungry exciter, allowing tags to communicate opportunistically using signals that are already pervasive in the environment. This is the most promising approach for enabling a truly ubiquitous and battery-free IoT.

B. Tag Design

1) Antenna and RF Front-end: The tag's front-end is remarkably simple. It consists of an antenna connected to an RF switch (typically a single transistor). The core principle of backscatter is impedance mismatch. When the switch is in one state (e.g., "off"), the antenna's impedance is matched to the load, and it absorbs maximum power from the incident RF wave. When the switch is in the other state ("on"), the impedance is mismatched, causing the antenna to reflect the incident wave. By toggling this switch, the tag modulates the reflected signal [4]. The evolution of tag design has focused on optimizing antenna efficiency and minimizing the power required to operate this switch.

2) Modulation Schemes: The data from the tag is encoded by the pattern of toggling the RF switch.

On-Off Keying (OOK): This is the simplest scheme, where the tag reflects to send a '1' and absorbs (does not reflect) to send a '0'. This is used in many early and simple backscatter systems.

Phase-Shift Keying (PSK): By using a more complex switching network, the tag can introduce a phase shift onto the reflected signal. Binary PSK (BPSK), where a 180° phase shift is used to encode data, is common. This is the basis for codeword translation in systems like FreeRider [8].

Frequency-Shift Keying (FSK): By toggling the switch at a specific frequency f_m, the tag can shift the frequency of the carrier signal, creating sidebands at $f_c \pm f_m$. This is used in systems like X-Tandem to separate signals from different hops [9]. More recent work has proposed frequency-phase shift (FPS) modulation, a fine-grained technique that creates a continuous phase shift to suppress spectrum sidelobes, improving spectral efficiency [23].

More advanced systems like EchScatter [14] use complex, pre-designed sequences of phase shifts applied at the chip level to achieve higher-order modulation.

3) Energy Harvesting: A key capability of passive tags is harvesting energy from the incident RF signal to power their own circuitry. The same antenna used for communication receives RF energy, which is fed to a rectifier circuit (typically using Schottky diodes) to convert it into a usable DC voltage. The efficiency of this process is a critical bottleneck, as typical RF energy densities are very low. As noted earlier, real-world energy harvesters exhibit significant non-linearity, a factor that must be considered for accurate performance analysis [6].

C. Receiver Design and Signal Processing

1) Interference Cancellation: The single greatest challenge at the receiver is canceling the overwhelmingly strong direct-path interference from the RF source. The receiver sees a composite signal containing the powerful signal directly from the source and the extremely weak, data-carrying reflection from the tag. Early systems like FreeRider [8] used a second receiver to obtain a clean copy of the source signal, which could then be subtracted from the composite signal. More advanced systems aim for single-receiver designs, employing sophisticated analog or digital cancellation techniques to isolate the backscattered signal.

2) Decoding Algorithms: Once the interference is canceled, the backscattered signal must be decoded. For simple OOK, this can be done with a simple energy detector. For PSK-based systems using codeword translation, the process is more complex. The receiver decodes the full packet and then compares the resulting bitstream to the original bitstream (obtained via a second receiver or known a priori) to extract the tag's data, often via a simple XOR operation [8]. In chip-level modulation systems like EchScatter, the receiver uses the known properties of the ZigBee DSSS decoder to determine which 4-bit data value the tag sent based on which symbol transformation occurred [14].

VI. Synthesis, Challenges, and Future Outlook

A. Performance Metrics Comparison

To distill the dense technical information from the surveyed literature, Table I presents a comparative analysis of key backscatter systems. This table highlights architectural

TABLE I: Performance and Architectural Comparison of Modern Backscatter Systems (Reformatted for Readability)

System	Excitation Signal / Data Rate	Target Protocol / Range	Key Innovation / Tag Power (μW) and Limitations
FreeRider [8]	**Excitation:** WiFi, ZigBee, BLE *Rate:* ∼60 Kbps (WiFi)	**Target:** Same as Excitation *Range:* up to 42m (WiFi)	**Innovation:** Symbol-level codeword translation *Power:* ∼30 μW. *Limits:* Requires dual-receiver setup
Interscatter [5]	**Excitation:** BLE (single-tone) *Rate:* 2–11 Mbps (WiFi)	**Target:** WiFi, ZigBee *Range:* N/S	**Innovation:** Single-sideband backscatter *Power:* 28 μW. *Limits:* Needs non-productive carrier
BlueBee [18]	**Excitation:** BLE (productive) *Rate:* 225 Kbps	**Target:** ZigBee *Range:* ∼10m	**Innovation:** Cross-tech PHY emulation *Power:* N/S. *Limits:* Bandwidth mismatch limits performance
X-Tandem [9]	**Excitation:** WiFi (productive) *Rate:* up to 200 bps	**Target:** WiFi *Range:* up to 8m (2-hop)	**Innovation:** Multi-hop analog forwarding, MFS *Power:* 14,200 μW (FPGA). *Limits:* Very low throughput, FPGA power
SyncScatter [10]	**Excitation:** WiFi (productive) *Rate:* 500 Kbps	**Target:** WiFi *Range:* 30+ m	**Innovation:** Hierarchical wake-up & sync *Power:* 30 μW. *Limits:* Custom ASIC needed for low power
TScatter [11]	**Excitation:** WiFi (OFDM) *Rate:* **13.63 Mbps**	**Target:** WiFi *Range:* up to 160 ft	**Innovation:** Sample-level modulation *Power:* 30.2 μW. *Limits:* Implemented on SDR, not commodity
EchScatter [14]	**Excitation:** ZigBee (productive) *Rate:* **247 Kbps**	**Target:** ZigBee *Range:* up to 20m	**Innovation:** Chip-level modulation *Power:* 280,000 μW (FPGA). *Limits:* High power on prototype (FPGA)
BumbleBee [17]	**Excitation:** BLE (productive) *Rate:* 218 Kbps	**Target:** ZigBee *Range:* up to 20m	**Innovation:** Dominant tag data overwrite *Power:* N/S. *Limits:* Relies on receiver error tolerance
Multiscatter [24]	**Excitation:** WiFi, BLE, ZigBee *Rate:* 278 Kbps (agg.)	**Target:** Same as Excitation *Range:* 20–28m	**Innovation:** Multiprotocol ID, Overlay Mod. *Power:* 2,000 μW (opt.). *Limits:* Requires custom carrier

choices, key innovations, and reported performance metrics, allowing for a direct comparison of their capabilities and limitations. It visualizes the design space, illustrating the trade-offs between throughput, range, power consumption, and compatibility.

B. Core Challenges

Synthesizing the literature reveals a set of common, fundamental challenges that researchers in this field continue to grapple with.

The Near-Far Problem: In any multi-tag system, the strong signal from a tag located near the receiver can easily drown out the much weaker signal from a tag that is farther away [1], [4]. This is a classic problem in wireless communication that is exacerbated in backscatter due to the passive nature of the tags. Mitigating this is essential for enabling reliable concurrent transmissions in dense networks. Potential solutions include power control where tags adjust their reflection coefficients or advanced receivers using Successive Interference Cancellation (SIC).

The Data Rate vs. Range Trade-off: There is an inherent trade-off between how fast a tag can transmit and how far away it can be. High data rates require more complex modulation and more precise synchronization, which in turn require more power and a stronger incident signal, limiting range [25]. Low-rate systems like those based on LoRa backscatter can operate at longer distances but are unsuitable for many emerging applications [25].

Multi-tag Collision: When multiple tags attempt to backscatter a signal simultaneously, their reflections interfere with each other at the receiver, causing a "collision" where no data can be decoded. While MAC protocols in active networks (like CSMA/CA) address this, designing efficient, ultra-low-power MAC protocols for passive tags is a significant challenge [19].

C. Research Limitations

Despite impressive results, much of the existing research has common limitations. A primary one is the reliance on controlled laboratory environments. Performance metrics reported in papers are often achieved under ideal line-of-sight conditions with minimal external interference. The robustness and reliability of these systems in complex, real-world deployments (e.g., a crowded public space or a dynamic industrial setting) remain largely unvalidated. Furthermore, many of the most advanced systems are prototyped on power-hungry FPGAs or SDRs [9], [14]. The transition to low-cost, ultra-low-power ASICs is a critical but difficult step that is necessary for practical deployment.

VII. Conclusion and Future Directions

A. Concluding Summary

The past decade has witnessed a remarkable evolution in ZigBee and ambient backscatter technology. The field has progressed from initial feasibility studies demonstrating basic codeword translation to sophisticated systems capable of high-throughput, cross-technology, and concurrent communication. The core progress has been driven by a move towards finer-grained modulation at the chip and sample level, a deeper, protocol-specific understanding of commodity receiver logic, and the development of novel techniques for synchronization and multi-tag coordination. These advancements have transformed backscatter from a simple RFID-like technology into a versatile communication primitive that is poised to become

a cornerstone of the battery-free Internet of Things. The shift from dual-receiver proof-of-concepts to more practical single-receiver designs marks a critical maturation point, signaling a move towards real-world deployability.

B. Future Research Directions

Based on the challenges and limitations identified, several promising research directions emerge for the future.

Security and Privacy: The passive and open nature of backscatter makes it vulnerable to eavesdropping, jamming, and spoofing attacks. Given the severe power and computational constraints of tags, traditional cryptography is often infeasible. Future work must focus on developing lightweight security mechanisms, potentially leveraging physical-layer properties like channel randomness to create secure, low-power communication links [26].

Networking and Standardization: While the physical layer has seen immense innovation, the MAC and networking layers for large-scale backscatter networks are still in their infancy. Designing scalable MAC protocols to manage channel access for thousands of tags is a critical open problem [21]. Standardization efforts are vital for creating an interoperable ecosystem.

Intelligent Surfaces and Beamforming: New technologies like Reconfigurable Intelligent Surfaces (RIS) offer exciting possibilities. An RIS is a planar surface with many passive elements that can be electronically controlled to reflect RF signals in a specific direction. Integrating RIS with backscatter could allow for intelligent focusing of ambient energy onto tags and steering of backscattered signals towards a receiver, dramatically overcoming path loss and extending range and reliability.

Cross-Technology Integration and Coexistence: Future research will likely deepen the integration with other wireless technologies. This includes not only cross-technology communication but also graceful coexistence with WiFi, 5G, and future 6G networks. This involves designing backscatter systems that can operate robustly in an increasingly crowded spectrum and potentially even leverage the complex signal structures of next-generation cellular networks as a source for high-quality ambient power and carriers.

REFERENCES

[1] T. Jiang, Y. Zhang, W. Ma, M. Peng, Y. Peng, M. Feng, and G. Liu, "Backscatter communication meets practical battery-free internet of things: A survey and outlook," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 3, pp. 2021–2073, 2023.

[2] A. Dementyev, S. Hodges, S. Taylor, and J. Smith, "Power consumption analysis of bluetooth low energy, zigbee and ant sensor nodes in a cyclic sleep scenario," in *2013 IEEE SENSORS*. IEEE, 2013, pp. 1–4.

[3] 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 the ACM SIGCOMM 2013 conference on Applications, technologies, architectures, and protocols for computer communication*, 2013, pp. 39–50.

[4] N. V. Huynh, D. T. Hoang, X. Lu, D. Niyato, P. Wang, and D. I. Kim, "Ambient backscatter communications: A contemporary survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 2889–2922, 2018.

[5] V. Iyer, V. Talla, B. Kellogg, S. Gollakota, and J. R. Smith, "Inter-technology backscatter: Towards internet connectivity for implanted devices," in *Proceedings of the 2016 conference on aCM SIGCOMM*, 2016, pp. 356–369.

[6] Y. Ye, L. Shi, X. Chu, and G. Lu, "On the outage performance of ambient backscatter communications," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7265–7278, 2020.

[7] J. Qian, F. Gao, G. Wang, S. Jin, and H. Zhu, "Noncoherent detections for ambient backscatter system," *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 1412–1422, 2017.

[8] P. Zhang, C. Josephson, D. Bharadia, and S. Katti, "Freerider: Backscatter communication using commodity radios," in *Proceedings of the 13th International Conference on emerging Networking EXperiments and Technologies*, 2017, pp. 389–401.

[9] J. Zhao, W. Gong, and J. Liu, "X-tandem: Towards multi-hop backscatter communication with commodity wifi," in *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*, 2018, pp. 155–167.

[10] 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 *18th USENIX Symposium on Networked Systems Design and Implementation (NSDI 21)*, 2021, pp. 923–937.

[11] X. Liu, Z. Chi, W. Wang, Y. Yao, P. Hao, and T. Zhu, "Verification and redesign of ofdm backscatter," in *18th USENIX Symposium on Networked Systems Design and Implementation (NSDI 21)*, 2021, pp. 953–967.

[12] Z. Wang, L. Kong, X. Liu, and G. Chen, "Embracing channel estimation in multi-packet reception of zigbee," *IEEE Transactions on Mobile Computing*, vol. 22, no. 5, pp. 2977–2990, 2023.

[13] S. Wang, Z. Xu, and W. Gong, "Poster: Enhanced zigbee backscatter communication using fine-grained chip-level modulation," in *The 21st Annual International Conference on Mobile Systems, Applications and Services*, 2023, pp. 616–616.

[14] J. Li, S. Wang, Z. Xu, W. Xi, S. Wang, and W. Gong, "Echscatter: Enriching codeword translation for high-throughput ambient zigbee backscatter," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 7, no. 1, pp. 1–26, 2023.

[15] W. Gong, S. Chen, J. Liu, and Z. Wang, "Mobirate: Mobility-aware rate adaptation using phy information for backscatter networks," in *IEEE INFOCOM 2018-IEEE Conference on Computer Communications*. IEEE, 2018, pp. 2492–2500.

[16] W. Gong, S. Chen, and J. Liu, "Towards higher throughput rate adaptation for backscatter networks," in *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems*, 2016, pp. 310–311.

[17] Z. Xu and W. Gong, "Bumblebee: Enabling the vision of pervasive zigbee backscatter communication," in *2023 IEEE International Conference on Pervasive Computing and Communications (PerCom)*. IEEE, 2023, pp. 109–119.

[18] W. Jiang, Z. Li, Z. Yin, S. M. Kim, and T. He, "Bluebee: a 10,000 x faster cross-technology communication via phy emulation," in *Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services*, 2017, pp. 127–139.

[19] L. Kong, D. Wu, A. V. Vasilakos, and X. Liu, "mzig: Enabling multi-packet reception in zigbee," in *IEEE INFOCOM 2015-IEEE conference on computer communications*. IEEE, 2015, pp. 558–566.

[20] Z. Wang, L. Kong, K. Xu, G. Chen, and L. He, "Ppm: Preamble and postamble-based multi-packet reception for green zigbee communication," *IEEE Transactions on Green Communications and Networking*, vol. 3, no. 3, pp. 817–827, 2019.

[21] Q. Wang, Z. Wang, L. Kong, Y. Liu, Y. Shao, and S. Mumtaz, "Orthzig: Concurrent transmissions based on waveform orthogonality in zigbee," in *2023 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2023, pp. 4480–4485.

[22] Z. Chi, Y. Yao, and X. Liu, "Leveraging ambient lte traffic for ubiquitous passive communication," in *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*, 2020, pp. 1–14.

[23] Z. Xu and W. Gong, "Enabling zigbee backscatter communication in a crowded spectrum," in *2022 IEEE 30th International Conference on Network Protocols (ICNP)*. IEEE, 2022, pp. 1–11.

[24] W. Gong and Q. Wang, "Multiprotocol backscatter for personal iot sensors," in *Proceedings of the 18th conference on embedded networked sensor systems*, 2020, pp. 15–28.

[25] 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 *19th USENIX Symposium on Networked Systems Design and Implementation (NSDI 22)*, 2022, pp. 1017–1032.

[26] 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," *ACM Computing Surveys (CSUR)*, vol. 54, no. 7, pp. 1–36, 2021.