Physical Layer Challenge-Response Authentication between Ambient Backscatter Devices

Yifan Zhang, *Graduate Student Member, IEEE,* Yongchao Dang, Masoud Kaveh, Zheng Yan, *Fellow, IEEE,* Riku Jäntti, *Senior Member, IEEE,* and Zhu Han, *Fellow, IEEE,*

***Abstract*—Ambient backscatter communication (AmBC) has become an integral part of ubiquitous Internet of Things (IoT) applications due to its energy-harvesting capabilities and ultra-low-power consumption. However, the open wireless environment exposes AmBC systems to various attacks, and existing authentication methods cannot be implemented between resource-constrained backscatter devices (BDs) due to their high computational demands. To this end, this paper proposes PLCRA-BD, a novel physical layer challenge-response authentication scheme between BDs in AmBC that overcomes BDs' limitations, supports high mobility, and performs robustly against impersonation and wireless attacks. It constructs embedded keys as physical layer fingerprints for lightweight identification and designs a joint transceiver that integrates BDs' backscatter waveform with receiver functionality to mitigate interference from ambient RF signals by exploiting repeated patterns in OFDM symbols. Based on this, a challenge-response authentication procedure is introduced to enable low-complexity fingerprint exchange between two paired BDs leveraging channel coherence, while securing the exchange process using a random number and unpredictable channel fading. Additionally, we optimize the authentication procedure for high-mobility scenarios, completing exchanges within the channel coherence time to minimize the impact of dynamic channel fluctuations. Security analysis confirms its resistance against impersonation, eavesdropping, replay, and counterfeiting attacks. Extensive simulations validate its effectiveness in resource-constrained BDs, demonstrating high authentication accuracy across diverse channel conditions, robustness against multiple wireless attacks, and superior efficiency compared to traditional authentication schemes.**

***Index Terms*—Ambient backscatter communication, physical layer security, challenge-response authentication, OFDM.**

I. Introduction

Ambient backscatter communication (AmBC) is a key enabler for the Internet of Things (IoT) and a promising technology for 6G massive communication, thanks to its energy-efficient and sustainable design [7], [30]. By harvesting energy from the environment and reflecting incident ambient RF signals (e.g., Wi-Fi, TV signals), backscatter devices (BDs) enable uplink communication to dedicated readers and device-to-device (D2D) interactions without additional energy consumption for radio frequency (RF) transmission [16], [19]. However, the broadcast nature of AmBC exposes the backscatter signals from BDs to be easily intercepted or manipulated, leaving systems vulnerable to impersonation [13] and wireless spoofing attacks [21]. In particular, this threat becomes even more pressing in distributed AmBC scenarios where resource-constrained BDs interact directly without a central reader's oversight. Therefore, implementing effective and robust BD-to-BD authentication is critical to safeguarding the integrity of AmBC and ensuring secure, reliable connectivity.

There are two potential approaches to enhancing authentication for AmBC systems: cryptography methods and physical layer authentication (PLA). Traditional cryptographic approaches, which rely on pre-shared identity keys and complex encryption algorithms [3], [5], [9], [25], demand significant computational resources, making them unsuitable for resource-limited BDs. In addition, while lightweight cryptographic protocols [4], [23], [24] reduce complexity through bitwise operations or cyclic shifts, they fail to provide robust security under various attacks. In contrast, PLA leverages unique device-specific or channel-specific RF characteristics as device fingerprints for lightweight authentication, eliminating the consumption of key management and data encryption. Device-based fingerprints [11], [15], [18], [26], [35] exploit intrinsic hardware features, while channel-based fingerprints [2], [27], [32]–[34] rely on uncorrelated spatial features to distinguish legitimate devices from attackers. These features position PLA as a feasible solution for lightweight and secure authentication in AmBC systems.

Despite their potential, existing PLA schemes still face significant challenges, particularly in adapting to BD-to-BD AmBC scenarios, accommodating device mobility, and defending against eavesdropping attacks. On the one hand, device-based fingerprints offer inherent uniqueness and high authentication accuracy [11], [15], [18], [26], [35], yet extracting them demands sophisticated signal-processing techniques, which is impractical for BDs. Although these fingerprints are stable against environmental changes, they struggle with fast channel fading and Doppler shifts in mobile scenarios, and their unencrypted nature makes them susceptible to eavesdropping. On the other hand, some schemes [11], [32] rely on stable channel characteristics, such as time of arrival and channel state information (CSI), to create unique fingerprints. However, these approaches depend on accurate channel estimation, which is an arduous task for BDs equipped with only simple demodulators [19]. Moreover, these schemes require minimal channel variation within the coherence time,

Y. Zhang, Y. Dang, M. Kaveh, and J. Riku are with the Department of Information and Communications Engineering, Aalto University, Espoo, 02150, Finland. (email: yifan.1.zhang@aalto.fi, masoud.kaveh@aalto.fi, yongchao.dang@aalto.fi, riku.jantti@aalto.fi)

Z. Yan (corresponding author) is with the State Key Lab of ISN, School of Cyber Engineering, Xidian University, Xi'an, Shaanxi, 710026 China. (email: zyan@xidian.edu.cn)

Z. Han is with the Department of Electrical and Computer Engineering, University of Houston, Houston, TX 77004 USA, and also with the Department of Computer Science and Engineering, Kyung Hee University, Seoul 446-701, South Korea (email: hanzhu22@gmail.com)

making them unsuitable for dynamic environments involving unmanned aerial vehicles (UAVs) or the Internet of vehicles (IoV). Although recent studies design protocols that explore spatial fingerprints [27] and joint CSI [33] to support mobile BDs, they still face challenges under high device mobility, remain vulnerable to eavesdropping, and depend on channel estimation. Thus, there is an urgent need for an authentication solution that can support BD-to-BD scenarios in AmBC systems, maintain effectiveness with device mobility, and ensure robust security against eavesdropping attacks.

In recent years, researchers have implemented the traditional challenge-response authentication framework [3], [5], [9], [25] at the physical layer, known as PL-CRA schemes [21], [22], [28]. These schemes leverage properties of the wireless medium (e.g., channel fading and noise) to secure key exchanges and utilize device-specific fingerprints embedded in response signals for authentication. In such schemes, a verifier first transmits a challenge signal to the target device, which may actively modulate its identity on the received challenge [21], [28] or passively reflect it [22] to respond to the verifier. The verifier then extracts identity features from the response using prior knowledge of the challenge and compares them with stored reference fingerprints for authentication. These methods have demonstrated effectiveness across diverse environments and offer resilience against eavesdropping [21]. However, they require the presence of powerful transceivers capable of active signal transmission and processing, rendering them unsuitable for authentication between two passive BDs. They also cannot be directly applied to ambient scenarios where an ambient RF source continuously transmits interference signals.

To address these challenges, we propose PLCRA-BD, a physical layer challenge-response authentication scheme designed explicitly between BDs in AmBC systems. PLCRA-BD uses embedded keys as unique fingerprints and designs a joint transceiver for mutual extraction while mitigating ambient interference. It also includes a challenge-response physical-layer authentication procedure that uses ambient RF signals for key exchange between passive BDs, eliminating active RF transmission and complex processing. Low-complexity operations and channel coherence ensure secure, mobility-resilient authentication, with security analysis confirming its robustness in dynamic AmBC environments. Specifically, the main contributions of this paper are summarized as follows:

- **Embedded Fingerprint Construction:** To facilitate low-complexity fingerprint transmission and verification, we design an embedded fingerprint construction method for BDs. This approach replaces traditional device features with low-density physical-layer identity (PID) keys stored in the memory unit of each BD as its unique fingerprint. These PID keys are transmitted using simple amplitude shift keying (ASK) modulation, allowing receiver BDs to easily extract the PID-bearing signals through harvested power detection. Additionally, the PID keys are shared among BDs to facilitate lightweight fingerprint verification.
- **Joint Transceiver Design:** To mitigate ambient interference in AmBC systems, a joint transceiver design integrates the backscatter waveform of BDs with their receiver functionality. By inserting an amplitude hop at the midpoint of the backscatter waveform and exploiting the repeated cyclic prefix structure of downlink orthogonal frequency division multiplexing (OFDM) signals, the receiving BD can isolate the backscatter signal from superposed components. This approach effectively avoids interference from the downlink signal and enables efficient message exchange between BDs.
- **One-way and Mutual Authentication:** Building on embedded fingerprint and integrated transceiver design, we propose a challenge-response authentication procedure to achieve one-way and mutual authentication between BDs in AmBC systems, ensuring high mobility and robust security. In one-way authentication, a verifier BD challenges a prover BD with a random number and its PID key within the channel coherence time. The prover mitigates channel effects by dividing the harvested power of the two received signals and uses the verifier's PID key to estimate the random number. The prover then responds with the estimated random number and its PID key. The verifier, in turn, estimates the prover's PID using a similar method and authenticates it accordingly. For mutual authentication, the process is repeated bidirectionally between the BDs. This method eliminates channel estimation and minimizes CSI fluctuations by exploiting channel coherence, as well as preserves shared PID key secrecy leveraging dynamically generated random numbers and unpredictable channel fading.
- **Security Analysis and Comprehensive Performance Evaluation:** We theoretically analyze the resistance of PLCRA-BD to impersonation, eavesdropping, replay, and counterfeiting attacks. Comprehensive simulation results further demonstrate the desirable performance of PLCRA-BD across key performance metrics, including effectiveness, authentication accuracy, robustness, and efficiency. The effectiveness of the scheme is validated through a proof-of-concept experiment and theoretical complexity analysis. High authentication accuracy is achieved under diverse channel conditions, such as varying speeds and distances between BDs. Robustness is evaluated under various wireless attacks. Furthermore, the scheme exhibits exceptional efficiency, characterized by low latency and minimal power consumption. Comparative evaluations with traditional schemes highlight the scheme's superior performance in most evaluated dimensions.

The remainder of this paper is organized as follows: Section II reviews related work. Section III describes the system model and outlines the problem. Section IV details the PLCRA-BD design, and Section V analyzes the security of PLCRA-BD. Section VI evaluates the performance of PLCRA-BD, and Section VII concludes the paper.

II. Related Works

This section reviews PLA schemes in BC systems and related PL-CRA schemes. Table I highlights that the existing

TABLE I: Comparison PLCRA-BD with existing PLA works in BC systems.
●: satisfy a criterion; ○: do not satisfy a criterion; ◐: partly satisfy a criterion.

Classification	Works	AmBC support	Authentication between BDs	Mobility		Attack Resistance			
				Device	Environment	IA	EA	RP	CA
Device Fingerprint	Harvestprint [18]	○	○	○	●	●	○	○	○
	Geneprint [11]	○	○	○	●	●	○	●	○
	RCID [15]	○	○	○	●	●	○	●	○
	RF-Mehndi [35]	○	○	○	●	●	○	●	○
	Hu-Fu [26]	○	○	○	●	●	○	●	○
Channel Fingerprint	Zanetti et al. [34]	○	○	○	○	●	○	○	○
	BatAu [32]	○	○	○	●	●	○	●	○
	APAuth [2]	○	○	○	●	●	○	●	●
	BCAuth [27]	○	○	◐	●	●	○	●	●
	BatchAuth [33]	○	○	◐	●	●	○	●	●
PLCRA-BD		●	●	●	●	●	●	●	●

1. IA: impersonation attacks; EA: eavesdropping attacks; RP: replay attacks; CA: counterfeiting attacks.
2. The results presented in the table are derived from the original results in the corresponding paper.

PLA schemes in BC systems lack BD-to-BD authentication in AmBC scenarios, full mobility support, and robust resistance to eavesdropping attacks, which our PLCRA-BD addresses.

A. Physical Layer Authentication in BC

Two types of RF fingerprints are mainly exploited by existing PLA schemes in BC systems: device fingerprints and channel fingerprints.

1) Device Fingerprints: Device fingerprints are derived from inherent hardware variations caused by random deviations during the manufacturing process. For example, Narayanan et al. [18] exploited unique energy discharge patterns in BD oscillators as fingerprints to prevent impersonation attacks. Han et al. [11] proposed Geneprint, leveraging covariance and power spectrum density similarities between successive backscattered signals as fingerprints, combined with supervised learning for BD identification. In a system called RCID [15], the reflection coefficient of a BD is captured as the fingerprint, which is then differentiated by training a multi-class neural network. RF-Mehnd [35] exploited the phase shift caused by the human touching of a BD array as an authentication fingerprint for both the BD and its holder. Then, a classifier is developed that uses a support vector machine to validate the fingerprint. Han et al. proposed Hu-Fu [26], which uses RF signal differences between BD pairs, leveraging power spectral density, energy spectrum, and a cross-correlation-based threshold for authentication.

The aforementioned schemes are capable of supporting environmental mobility, as hardware features are insensitive to changes in the surrounding environment. Most of these schemes [11], [15], [26], [35] demonstrate resilience against impersonation and replay attacks due to the uniqueness of device fingerprints. However, they generally overlook device mobility and are unable to prevent eavesdropping or counterfeiting attacks from learning the constant features of the backscatter signal [27]. Moreover, these schemes often require a complex analyzer on the verifier side for fingerprint extraction and analysis, making them unsuitable for resource-constrained BDs. Additionally, all these schemes operate in monostatic configurations and fail to address BD to BD authentication in AmBC scenarios.

2) Channel Fingerprints: Channel fingerprinting, using unique wireless signal characteristics like fading, reflection, and scattering, is widely studied in existing BC systems for authentication. Zanetti et al. [34] utilized average baseband power and time interval errors of backscatter signals to counter impersonation attacks, but their approach suffers from low accuracy of fingerprint extraction in dynamic environments. Yang et al. [32] proposed a batch authentication scheme using joint CSI with PD-NOMA techniques, effectively resisting impersonation and replay attacks while adapting to environmental mobility; however, its complex fingerprint extraction process limits its applicability for BDs. To simplify this, Chang et al. [2] introduced APAuth, enabling BDs to authenticate readers via harvested power volumes without complex operations. While lightweight, APAuth relies on pre-negotiated power levels, supports only reader-to-BD authentication, and does not address BD-to-BD scenarios. Additionally, the above schemes face challenges such as vulnerability to eavesdropping and counterfeiting attacks due to unencrypted signals and the open nature of wireless channels, their restriction to monostatic scenarios unsuitable for AmBC systems, and their limited consideration of device mobility, reducing their effectiveness in dynamic environments.

Recent works [27], [33] have designed robust authentication scheme for mobile BC scenarios and against wireless attacks on BDs. In BCAuth [27], the authors utilized the spatial information of a BD as its fingerprint and employed a tracing algorithm to update the fingerprint dynamically when the BD moves. BatchAuth [33] leveraged joint CSI to authenticate multiple BDs simultaneously, adapting to CSI variations of mobile BDs through channel correlation coefficients, which further improves the authentication efficiency for mobile BDs. Both BCAuth and BatchAuth support authentication for moving BDs but struggle in high-speed scenarios with rapid CSI changes. Moreover, fingerprints based on device location [27] and CSI [33] are still susceptible to eavesdropping and targeted counterfeiting based on the eavesdropping results in open wireless environments. Furthermore, these authentication protocols rely on channel estimation, which is incompatible with BDs due to their limited computational and communication

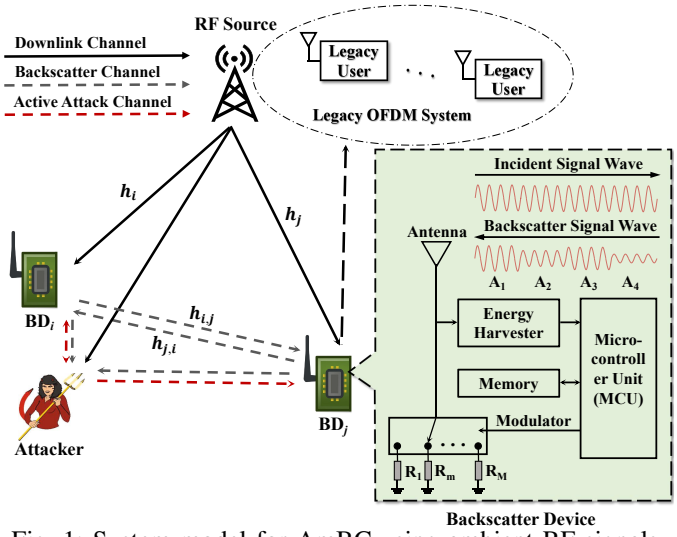


Fig. 1: System model for AmBC using ambient RF signals.

capabilities. More seriously, BDs in AmBC face challenges in isolating ambient signals for effective fingerprint extraction. Thus, an urgent need exists for a solution that enables authentication between BDs in AmBC systems, addresses mobility challenges, and ensures robust security.

B. PL-CRA

Several PL-CRA schemes have been proposed to achieve challenge-response authentication at the physical layer [6], [21], [22], [28]. For example, Shan et al. [21] first proposed PL-CRAM, a physical layer authentication mechanism, which eliminates pilot references to prevent attackers from estimating legitimate channels, while the verifier can decode the challenge-response messages without CSI by exploiting the former challenge signal to compensate for the channel fading in the latter response signal. Then, Wu et al. added artificial noise to protect the challenge-response process [28], and Shoukry et al. [22] deployed active actuators to continuously challenge the surrounding environment with random transmissions for attacker detection. The above-mentioned schemes can satisfy mobility and defend against various attacks. However, they require the verifier to emit challenge signals actively and perform signal processing to extract the challenge-response messages, which cannot apply to passive BDs due to their limited power and processing abilities. In addition, they neglect the ambient scenarios where an uncontrollable ambient RFS continuously broadcasts ransom signals, which could face difficulties when deploying in AmBC systems.

To this end, we introduce the PLCRA-BD. Unlike existing PL-CRA schemes, PLCRA-BD utilizes ambient OFDM signals to facilitate key exchange between passive BDs, eliminating the need for active RF transmission and complex signal processing. Additionally, it employs low-complexity operations and leverages channel coherence to ensure secure key exchange without relying on channel estimation or signal decoding, thereby minimizing the impact of mobility on authentication. In the next section, we describe the system model and state the problem that needs to be solved in this paper.

TABLE II: List of notations used in PLCRA-BD

Notation	Description
$\mathcal{CN}(\mu, \sigma^2)$	circularly symmetric complex Gaussian (CSCG) distribution.
$\|\cdot\|$	absolute value of a scalar or a complex number.
$\|\|\cdot\|\|_{l1}$	L_1-norm, sum of the absolute values of a vector.
$\min(\cdot)$, $\max(\cdot)$	minimum and maximum functions for a given set.
$O(L)$	asymptotic time complexity on the order of L.
$P(s(t))$	average power of the signal $s(t)$.
η_i	energy harvesting efficiency at the i-th device.

III. System Model and Problem Statement

A. System Model

As depicted in Fig. 1, the AmBC system consists of an ambient RF source (e.g., TV tower, cellular base station, or Wi-Fi transmitter) and two paired BDs, denoted as BD_i and BD_j. The RF source operates using a legacy OFDM system to transmit signals to its users, while the BDs communicate either with each other or with legacy users by reflecting the RF source's signals. Communication in the AmBC system follows a time-division structure, ensuring that each BD reflects the ambient RF signals exclusively within its assigned time slot, thereby avoiding inter-BD interference and maintaining efficient operation. In addition, the notations used in this paper are presented in Table II.

Each BD, equipped with a single antenna, consists of an energy harvester, a backscatter modulator, a memory module, and a microcontroller unit (MCU)—a standard configuration for passive backscatter devices [16], [19]. BDs operate in two primary modes: (i) backscattering, where the BD reflects incident signals and uses M adjustable impedances to implement M-ary amplitude shift keying (M-ASK) modulation [10], and (ii) listening, where the BD switches its antenna to harvest energy from incoming signals. The memory unit enables the storage of simple number sequences [8], such as the identity sequence of devices, while the MCU facilitates simple computations, such as multiplications, to enable authentication and streamline system operations.

B. Channel Model in AmBC Systems

The downlink channels from the RF source to BD_i, BD_j, and an attacker are represented as $h_i(t)$, $h_j(t)$, and $h_a(t)$, respectively. The inward channels between BD_i, BD_j, and the attacker are denoted as $h_{l,k}(t)$ with $l, k \in \{i, j, a\}$. A channel gain can be expressed as $h = \vartheta d^{\lambda/2}$, where ϑ is a CSCG variable, d is the transmitter-receiver distance, and λ is the path-loss exponent. Let $s(t)$ denote the signal transmitted from the RF source, which is usually OFDM-based for existing ambient RF sources, such as TV tower and Wi-Fi router. $b_i(t)$ denotes the backscatter signal of BD_i, which represents the reflection coefficient at BD_i in the M-ASK case. Thus, the received superposed signal at BD_j that contains the backscatter signals from BD_i and the downlink signals directly from the ambient source can be expressed as

$$\begin{aligned} y_j(t) &= h_{i,j}(t)h_i(t)b_i(t)s(t) + h_j(t)s(t) + w_j(t) \\ &= y_j^b(t) + y_j^d(t) + w_j(t), \end{aligned} \tag{1}$$

where $y_j^b(t) = h_{i,j}(t)h_i(t)b_i(t)s(t)$ is the backscatter signal reflected from BD_i, $y_j^d(t) = h_j(t)s(t)$ is the downlink

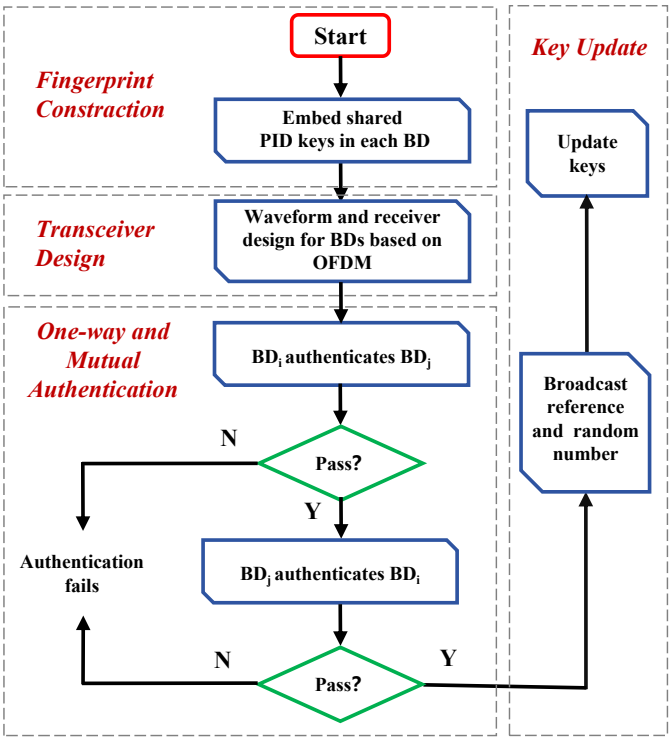


Fig. 2: PL-CRABD Overview

ambient signal directly from the RF source, and $w_j(t)$ is the received additive white Gaussian noise (AWGN) at BD_j, $w_j(t) \sim \mathcal{CN}(0, \sigma_j^2)$.

Let $h_i[n]$, $h_j[n]$ and $h_{i,j}[n]$ denote the discrete-time representation of $h_i(t)$, $h_j(t)$ and $h_{i,j}(t)$, respectively. The ambient signal is $s[n]$, and the backscatter signal at BD_i is $b_i[n]$. Thus, the representation in (1) of the received signal at BD_j can be rewritten to a discrete-time form as

$$y_j[n] = y_j^b[n] + y_j^d[n] + w_j[n], \tag{2}$$

where $y_j^b[n] = h_{i,j}[n]h_i[n]b_i[n]s[n]$, $y_j^d[n] = h_j[n]s[n]$ and $w_j[n] \sim \mathcal{CN}(0, \sigma_j^2)$.

C. Adversary Model

In this work, the attacker in Fig. 1 is assumed to employ four types of attacks: one impersonation attack and three wireless attacks. The impersonation attack, operating at the link or network layer, involves using known upper-layer identifiers to masquerade as a legitimate BD. In contrast, the wireless attacks are assumed to be aware of the PLA procedure and attempt to manipulate the signals in the physical layer. Specifically, they are defined as follows:

- *Impersonation Attacks:* The attacker leverages known upper-layer identifiers (e.g., reference numbers) of a genuine device to pose as a legitimate BD, thereby attempting to pass off its transmissions as originating from an authorized entity.
- *Eavesdropping Attacks:* Attackers intercept the signals exchanged between BDs to deduce their secret keys. We consider two types of eavesdroppers: a *native eavesdropper* positioned beyond the coherence distance with a legitimate BD, and a *smart eavesdropper* located within the coherence distance with a legitimate BD, thereby gaining more favorable conditions for signal interception.
- *Replay Attacks:* Attackers record a legitimate transmission and retransmit it at a later time, attempting to impersonate a legitimate BD.
- *Counterfeiting Attacks:* Attackers eavesdrop on and imitate the information exchanged between the two BDs during authentication, aiming to produce RF waveforms indistinguishable from those of legitimate devices and thereby deceive the verifier.

In this paper, we aim to propose a PL-CRABD scheme for authentication between BDs in the AmBC system, designed to support mobility and provide high robustness against impersonation and wireless attacks. To facilitate authentication, the scheme should address BDs' limitations in extracting fingerprints and mitigating interference from ambient downlink signals. For mobility support, the scheme should operate effectively with mobile BDs at various speeds and in diverse environments, including rural and urban scenarios. To ensure robustness, the scheme should perform robustly under various wireless attack scenarios. The next section presents the details of the proposed PL-CRABD design.

IV. PL-CRABD Design

In this section, we present the detailed design of the proposed PL-CRABD scheme. We first present a brief overview and then introduce the key components of the scheme.

A. Overview

As shown in Fig. 2, the proposed PL-CRABD scheme comprises five key components: fingerprint construction, transceiver design, one-way and mutual authentication, and key update. In the fingerprint construction, each BD is assigned a unique PID key that serves as its fingerprint. These keys are shared among BDs that can be transmitted vai simple ASK modulation. Next, a joint transceiver design enables BDs to extract the harvested power value of the backscattered signal while avoiding downlink interference. This is achieved by leveraging the CP repetition pattern in OFDM signals. Specifically, by introducing a controlled amplitude transition at the midpoint of the backscatter waveform, the receiver BD isolates the harvested backscattered signal power using the repeated CP pattern. Based on the fingerprint construction and the transceiver design, a one-way authentication procedure is further proposed that consists of a challenge and a response stage. In the challenge stage, the verifier BD transmits a random number and its PID key to the prover BD via backscattered ambient signals. Extracting the harvested power value of the two signals, the prover BD eliminates the channel fading effect using a simple division to derive a factor containing the random number and the verifier's PID. Using the stored PID key of the verifier, the prover calculates the random number value and backscatters the random number along with its own PID key to the verifier in the response stage. Using a similar computation, the verifier estimates the prover BD's PID key and compares it with the stored key to confirm authentication. After that, Mutual authentication is achieved by repeating

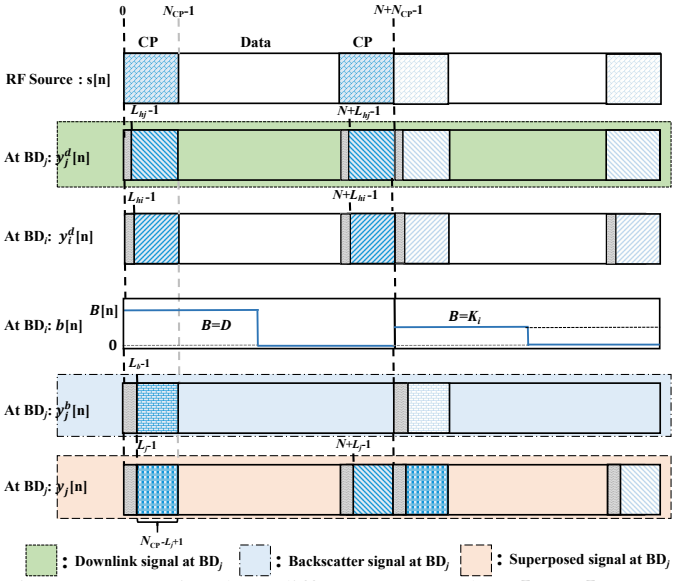


Fig. 3: OFDM signals at different stages when $L_j = L_{b_j}$, one OFDM symbol for $B = D$ and another for $B = K$. The superposed signals received at BD_j is $y_j[n] = y_j^b[n] + y_j^d[n]$

the one-way authentication procedure, allowing both BDs to authenticate each other in a secure and efficient manner. Finally, to enhance long-term security, both BDs broadcast their reference and newly generated random numbers. Thus, all BDs can find the target BD and update their shared PID keys dynamically using the random number, ensuring continued protection against potential security threats.

B. Fingerprint Construction

We embed PID keys in the memory of BDs as fingerprints to facilitate low-complexity fingerprint exchange and extraction. These keys are stored as fixed values and can be modulated by ASK, allowing the signals carrying the key information to be obtained by reading the harvested power of the received signals. In addition, they are shared between BDs for identity verification. For example, the key for BD_i is denoted as $|K_i|$. For an AmBC system with N BDs, total N keys $|K_1|, |K_2|, \ldots, |K_N|$ are stored in each BD for authentication. BD_i can display its key by backscattering a signal K_i with amplitude $|K_i|$. Then, the receiver BD (e.g., BD_j) can obtain a key-bearing signal that contains the key from its harvested power value for the signal K_i, denoted as $\eta P(s(K_i))$. By constructing the shard key as the fingerprint, BD_i and BD_j can perform authentication procedures to obtain each other's key-bearing signal without needing signal decoding.

C. Transceiver Design Over OFDM Carrier

For clarity, we present the design in a discrete-time AmBC system. The OFDM signal $s[n]$ includes CP that copies the tail of each OFDM sample to the start to mitigate inter-symbol interference (ISI) in multipath channels [20]. Let the downlink channel be $h_i[n]$ with delay spreads τ_{h_i} and the inward channel be $h_{i,j}[n]$ with delay spreads $\tau_{h_{i,j}}$, and let f_s be the OFDM sampling rate. Thus, $L_{h_i} = \lceil \tau_{h_i} f_s \rceil$ and $L_{h_{i,j}} = \lceil \tau_{h_{i,j}} f_s \rceil$. Define $L_{b_j} = L_{h_i} + L_{h_{i,j}}$ and $L_j = \max\{L_{h_j}, L_{b_j}\}$. Let N be the number of subcarriers, and let the CP length N_{cp} exceed the maximum channel spread, i.e., $\tau_j \leq T_{\text{CP}}$. Without loss of generality, consider BD_i sending a message to BD_j.

1) BD Backscatter Waveform Design: A backscatter waveform of BDs is designed in this subsection to make the backscatter signal arrive at a receiver that is distinguishable from the downlink signal. Specifically, in the backscattering mode, BD_i backscatters the OFDM signal to transmit information, where the duration of each BD symbol is equal to $K(K \geq 1)$ OFDM symbol periods, each of which consists of $N_t = N + N_{cp}$ total sampling periods. As shown in Fig. 3, BD_i uses the waveform $b[n]$ in (3) to convey message $B[n]$ in a BD symbol, for $k = 0, ..., K-1$.

$$b[n] = \begin{cases} B[n], & \text{for } n = kN_t, \ldots, \frac{2k+1}{2}N_t - 1, \\ 0, & \text{for } n = \frac{2k+1}{2}N_t \ldots, (k+1)N_t - 1. \end{cases} \tag{3}$$

Thus, to transmit a message '$B[n]$', the BD alternates its antenna impedance between two states; one state backscatters a signal with the backscatter coefficient '$B[n]$' and another with no backscatter. The state transition is in the middle of each OFDM symbol period. In the figure, $B[n] = D$ to convey the random number D and $B[n+1] = K_i$ to convey the identity key of BD_i. The waveform design aims to enable the other BD, to extract the harvested power value of the backscatter signal from the received superposed signals, as presented in the next subsection. Also, it can be easily implemented at BDs, since it is similar to the FMO waveform widely used in commercial BDs [31].

2) Receiver Design: After the backscatter of BD_i, the receiver BD_j aims to remove the downlink signal and obtain the harvested power from BD_i. Without loss of generality, let $K = 1$. As shown in (2), the downlink $y_j^d[n]$ and backscatter $y_j^b[n]$ signals pass through different multipath channels h_j and $h_{i,j}h_i$. Only the downlink signal $y_j^d[n]$ has a repeated CP in each OFDM symbol, while $y_j^b[n]$ does not due to the backscatter waveform design (see Fig. 3). Our approach uses this repeated CP to cancel $y_j^d[n]$ and isolate the backscatter message.

To be specific, two CP parts of each OFDM symbol in the downlink signal $y_j^d[n]$ at BD_j, are identical, i.e.,

$$y_j^d[n] = y_j^d[n+N], \quad n = L_{h_j} - 1, \ldots, N_{cp} - 1. \tag{4}$$

In contrast, $y_j^b[n]$ has only one CP. Thus, by subtracting:

$$z_j^b[n] = y_j[n] - y_j[n+N] = y_j^b[n] = h_{i,j}[n]h_i[n]B[n]\tilde{s}[n], \tag{5}$$

BD_j eliminates the downlink signal and obtain the backscatter component $h_{i,j}[n]h_i[n]B[n]\tilde{s}[n]$. Since BD_j can only measure power, it estimates the received message by evaluating the harvested power value as:

$$P(z_j^b[n]) = P(\eta_j h_{i,j}[n]h_i[n]B[n]\tilde{s}[n]). \tag{6}$$

3) Synchronization: Since the synchronization preamble in the RFS downlink signal is known to the BDs, they can use cross-correlation or methods from [17] to estimate the OFDM symbol start and identify its midpoint. Even without a synchronization preamble, BDs can rely on the repeated

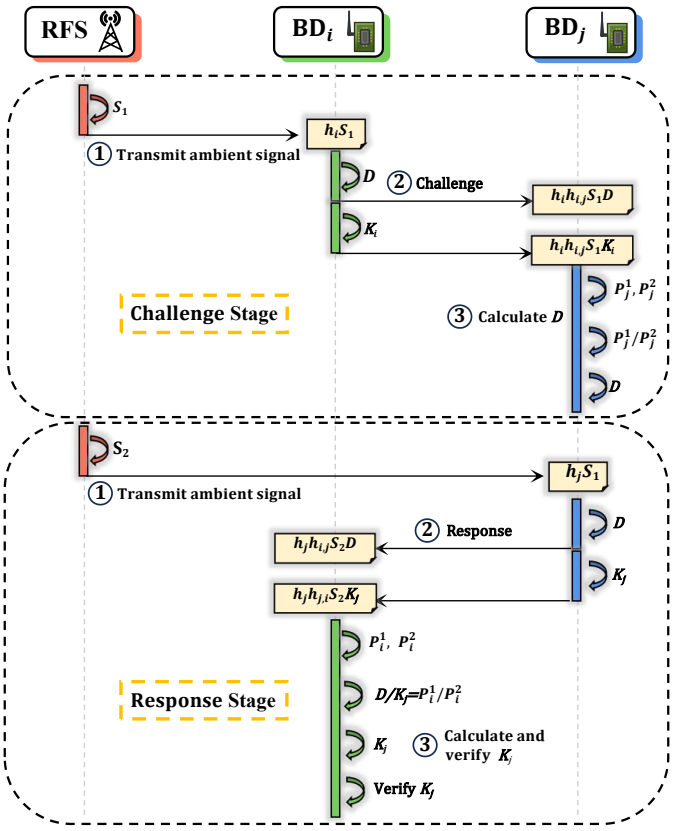


Fig. 4: The basic authentication procedure.

CP structure [31] or employ additional aids, such as light-based devices, for more accurate estimation [29]. Crucially, the backscatter waveform design does not require BDs to switch states precisely at the symbol midpoint. Instead, they can alternate states at any point within $[N_{cp}-1, N+L_i-1]$, as long as they maintain a reversed and repeated structure as in (3), thus preserving the repeated CP feature.

D. One-way and Mutual Authentication

Fig. 4 illustrates the basic one-way authentication procedure between BD_i and BD_j, which consists of two stages: a) *Challenge Stage* and b) *Response Stage*. Without loss of generality, we assume the BD_i authenticates BD_j first in the authentication procedure.

1) Challenge Stage: In the challenge stage, BD_i uses its own key K_i to challenge BD_j to request K_j for authentication, which contains the following three steps:

Step 1-1. RFS transmits ambient signals: The RF source broadcasts the ambient signal $s_1(t)$, after passing the channel, BD_i receives the signal as follow:

$$y_i(t) = h_i(t)s_1(t) + w_i(t), \tag{7}$$

where $w_i(t)$ is the AWGN at BD_i.

Step 1-2. BD_i challenges BD_j: Modulating on the incident signal from the RF source, BD_i backscatters two challenge signals in two successive time, denoted as t_1 and t_2, respectively, to BD_j. The time interval $[t_1,t_2]$ is limited within the channel coherence time by adjusting the length of the challenge signals in t_1 and t_2. The first signal contains a random number D to inform BD_j the authentication starts and secure the subsequent key exchange process. The random number can be generated using the environmental noise around the BD, which is common in existing BC systems [4]. The second signal contains the identity key of BD_i K_i. Note that the length of the D and K_i should be the same to let $t_1 = t_2$. Then, the signals arrive at BD_j in t_1 and t_2 are as follows:

$$y_j(t_1) = h_i(t_1)h_{i,j}(t_1)D(t_1)s_1(t_1) + h_j(t_1)s_1(t_1) + w_j(t_1), \tag{8a}$$

$$y_i(t_2) = h_i(t_2)h_{i,j}(t_2)K_i(t_2)s_1(t_2) + h_j(t_2)s_1(t_2) + w_i(t_2), \tag{8b}$$

where $w_j(t_1)$ and $w_j(t_2)$ is the AWGN.

Step 1-3. BD_j calculates D: After the above step, for easy understanding of our basic idea, let's assume there is no noise, while the effect of noise on authentication will be examined in Section VI. Then, BD_j can measure the harvest power value of the two challenge signals respectively as

$$P_j^1 = \eta_j P(h_i(t_1)h_{i,j}(t_1)D(t_1)s_1(t_1)), \tag{9a}$$

$$P_j^2 = \eta_j P(h_i(t_2)h_{i,j}(t_2)K_i(t_2)s_1(t_2)). \tag{9b}$$

When $t_1 + t_2 < T_c$, the channel fading in the harvested power of the backscatter link between two BDs is ideal [21], i.e., $h_i(t_1) \approx h_i(t_2)$, $h_{i,j}(t_1) \approx h_v(t_2)$, and the average power of ambient signal $s(t)$ rarely changes, i.e., $P(s_1(t_1)) \approx P(s_1(t_2))$. Therefore, BD_j can eliminate the effects of the channel and the signal $s(t)$ in (9a, 9b) by a division operation, as follows:

$$P_j^1/P_j^2 = D/K_i. \tag{10}$$

Then, BD_j can estimate the random number D by using its stored value of K_i to multiply $\frac{D}{K_i}$.

2) Response Stage: After the challenge, BD_j can respond to BD_i within a certain response time. Using the obtained random number D, BD_j replies with its key K_j in the response stage, which involves the following steps:

Step 2-1. RFS transmits ambient signals The RF source broadcasts the random signal s_2, after passing the channel, BD_j receives the signal as follow:

$$y_j(t) = h_j(t)s_2(t) + w_j(t), \tag{11}$$

where $w_j(t)$ is the AWGN at BD_j.

Step 2-2. BD_j responses BD_i : Similar to *Step 1-2*, BD_j backscatters the estimated random number and its own key K_j in two successive time slots t_3 and t_4. Refer to (8a-9b), BD_i can estimate the two harvest power values from the two received backscatter signals from BD_i as follows:

$$P_i^3 = \eta_i P(h_j(t_3)h_{j,i}(t_3)D(t_3)s_2(t_3)), \tag{12a}$$

$$P_i^4 = \eta_i P(h_j(t_4)h_{j,i}(t_4)K_j(t_4)s_2(t_4)). \tag{12b}$$

Step 2-3. BD_i calculates and verifies BD_j: Similarly, BD_i can obtain the value $\frac{D}{K_i}$ using a simple division operation. Then, BD_i can estimate K_j using its stored value of D to divide $\frac{D}{K_i}$. Due to the noise and slight differences between the channel fading in coherence time (i.e., the channel between the BDs from t_1 to t_2 and from t_3 to t_4, respectively), the calculated identity key of BD_j should

be similar to K_j but not ideal, due to the noise and slight changes of channel fading in the coherence time . We denote the calculated identity key at BD_i as K'_j. However, an attacker without knowledge of D and K_i cannot calculate K_j correctly, even if it knows the authentication procedure.

Then, BD_i can measure the similarity between K_j and K'_j to determine the incoming authentication request is from the genuine BD_j or an attacker. Given the limited computational ability of the BD, a simple and straightforward solution is to compare the Euclidean distance between K_j and K'_j with a predetermined threshold δ:

$$||K_j - K'_j||_{l1} \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\gtrless}} \delta, \tag{13}$$

where the value of δ represents the threshold for making the authentication decision. $\mathcal{H}_0$ and $\mathcal{H}_1$ represent binary hypothesis tests of the authentication failure and the authentication success, respectively. Specifically, they can be denoted as:

$$\begin{cases} \mathcal{H}_0 : K'_j = K_a + E_a \\ \mathcal{H}_1 : K'_j = K_j + E_j, \end{cases} \tag{14}$$

where E_a and E_j represent estimation error at the receiver for the attacker and BD_j, respectively. They are caused by AWGN and the slight difference between the channel fading in coherence time. K_a represents the attacker's fingerprint.

After BD_j passes the authentication in BD_i, BD_j can repeat the authentication procedure to verify the authenticity of BD_i for mutual authentication.

E. Key Update

In a D2D scenario, prolonged use of static device keys may lead to multiple physical-layer attacks, increasing the risk of key leakage [12]. Meanwhile, most existing challenge-response schemes rely on a centralized server for key updates [3], resulting in potential single-point failures and incompatibility with AmBC systems. To address this, BDs can update their identity keys using the random number generated during each authentication. Specifically, after each successful mutual authentication, BDs broadcast the random number and their upper-layer ID (i.e., reference number). Each BD then finds the identity of the updated key according to the received reference number and updates its stored PID keys using the random number. For instance, let D_i and D_j be the random numbers generated by B_i and B_j in the authentication, respectively. Each BD can update its key through a simple geometric mean operation as follows:

$$K_i^{new} = \sqrt{K_i \cdot D_i}, \tag{15a}$$
$$K_j^{new} = \sqrt{K_j \cdot D_j}, \tag{15b}$$

where we can find $\min(K_i, D_j) \leq K_i^{new} \leq \max(K_i, D_j)$ and $\min(K_j, D_j) \leq K_i^{new} \leq \max(K_j, D_j)$. The operation of geometric averaging smoothes the value of the key and reduces the effect of extreme values in the range of [0,1] for K_i and K_j. In addition, the key update process does not need a centralized service to allocate a new key, which enhances system scalability and reduces single points of failure.

V. Security Analysis

The proposed authentication's security relies on the attacker's uncertainties about the random number, shared secret keys, and unpredictable inward channels between BD_i and BD_j. These uncertainties prevent attackers from eavesdropping, replicating, or imitating the shared keys, ensuring resistance to impersonation, eavesdropping, replay, and counterfeiting attacks.

1) Impersonation Attack: The proposed authentication procedure can naturally resist impersonation attacks, as the PID keys (K_i, K_j) are unknown to them. Impersonation attackers aim to pass the identification mechanism of the system by imitating the upper-layer identity of a legitimate BD without the ability to manipulate or imitate wireless signals. Therefore, the identity keys are unknown to them and PLCRA-BD can easily identify impersonation attackers by comparing whether the upper-layer identity information of the attacker claim is consistent with the shared key computed at the physical layer.

2) Eavesdropping Attack: Eavesdropping attacks overhear communications between BD_i and BD_j during authentication and try to deduce $\{K_i, K_j\}$. Since the challenge stage and response stage are symmetrical, we only analyze the scenario where the attacker eavesdrops on the challenge stage and tries to deduce K_i. During the signal transmission period in the challenge stage, steps 1-1 does not need to be secured since it does not reveal the shared key or CSI. In steps 1-2, the attacker can obtain:

$$v_{i,a}^1 = \eta_e P(h_i(t_1)h_{i,e}(t_1)D(t_1)s_1(t_1)), \tag{16a}$$
$$v_{i,a}^2 = \eta_e P(h_i(t_2)h_{i,e}(t_2)K_i(t_2)s_2(t_1)), \tag{16b}$$

Subsequently, We analyze the two specific eavesdropping attackers as follows.

The naive eavesdropping attacker: Naive eavesdropping attackers have no way to guess the shared key K_i during the authentication producer because the keys exchanged between BD_i and BD_j are masked by the channel naturally and they do not have knowledge of K_i or D. If the attacker is located at a sufficient distance $d > \frac{\lambda}{2}$, the attacker cannot get any information about h_i since the channel between h_i and h_a is uncorrelated. The attacker also cannot estimate $h_{i,e}$ since the backscattered signal from the BD_i does not contain any pilot reference. Therefore, the attacker cannot directly obtain the transmitting message from BD_i by channel estimation. We further assume that the attacker knows the authentication procedure and tries to eliminate the channel fading by dividing the two factors. In this case, they can only obtain $\frac{v_{i,a}^1}{v_{i,a}^2} = \frac{D}{K_i}$. Since the attackers do not have the knowledge of D or K_i, they cannot solve any of them.

The smart eavesdropping attacker: A smart eavesdropping attacker, who is very close to BD_i, may get more information. If the attacker is very close to BD_i, we have $h_i \approx h_e$ and $h_{i,e} \approx 1$. Since the ambient signal from the source usually contains a pilot reference, the attacker can estimate h_e and derive the approximate value of D and K_i from (16a) and (16b) in the step 1-2, respectively. However, this kind of attack is hard to launch and easy to detect in practice. For example, if 900 MHz frequency is used, then

$\frac{\lambda}{2} \approx$16.65 cm, a very short distance within which an attacker can be easily identified by legitimate users [21].

3) Replay Attack: Replay attackers are hard to succeed because the random number and the shared keys change after each authentication round. We assume that the attacker knows the authentication procedure and replays both response signals to BD_i in the step 2-2, trying to pass the authentication at BD_i. In this case, the attacker cannot succeed since BD_i accepts the request from BD_j first, while the random number and the shared key change when the attacker's authentication request arrives at BD_i. Thus, the effectiveness of D has expired, and the shared keys have been updated. As a result, BD_i will calculate a wrong key using the outdated D or K_j received from the attacker.

4) Counterfeiting Attack: Counterfeiting attackers are hard to succeed since they cannot obtain the value of the shared key. A counterfeiting attacker mimics the authentication fingerprint of a legitimate BD, such as power and frequency, to make its RF signals indistinguishable from those of a genuine BD. However, in PLCRA-BD, the attacker cannot directly obtain the authentication fingerprint (i.e., shared keys) by eavesdropping, as analyzed before. Assuming that the attacker knows the authentication procedure in the physical layer, the attacker can only randomly guess the value of the shared keys K_i and K_j in steps 1-2 and 2-2, respectively. Denote attacker use the factor C_i to counterfeit K_i and the factor C_j to counterfeit K_j, the response signals sent by the attacker in the step 2-2 are $h_{j,e}h_{e,i}DC_i/K_i$ and $h_{j,e}h_{e,i}C_j$. As a result, BD_i will obtain K_i/C_iC_j. The attacker can succeed when $K_i/C_iC_j = K_j$, but it could need thousands of attempts, which consume significant resources.

VI. Performance Evaluation

This section presents the simulation setup and evaluates the proposed authentication scheme's performance in terms of effectiveness, accuracy, robustness, and efficiency.

A. Simulation Setup

1) Simulation Settings: Monte Carlo simulations are conducted in a Matlab platform to analyze the authentication performance under different system parameters, scenarios, and attacks. We consider an AmBC system composed of a fixed ambient RF source (RFS) and multiple BDs, where some BDs are stationary and others may be mobile. In the simulation, two paired BDs exploit the ambient signal from the RFS to perform authentication, including one-way authentication and mutual authentication. Additionally, we introduce an attacker positioned near a legitimate BD, aiming to eavesdrop on the communication link or circumvent the authentication process between the two BDs. Following the adversary model described in Subsection III-C, this attacker may engage in impersonation, eavesdropping, replay, or counterfeiting attacks. The default parameter settings used throughout the simulations, as presented in Table III, referred to those commonly adopted in authentication schemes and AmBC systems [14], [21], [27], [31].

TABLE III: Parameter Settings

Notation	Description	Setting
f_c	carrier signal frequency	900 Mhz
σ^2	received noise power	-30 dBm
P_T	maximum average power of the RFS	1 dBm
D_i,D_j	the distance between RFS and B_i,B_j	3 m
$D_{i,j}$	the distance between BDs	[1,10] m
D_a	the distance between a BD and a attacker	[0.1,2] m
$v_{i,j}$	the relative spend between BDs	[0,30] m/s
keylength	the length of the shared PID key in BDs	[5,30]
h	channel model	Rayleigh fading
$\|h\|$	channel gain	$10^{-2}d^{-2}$
N_{auth}	authentication number	1000

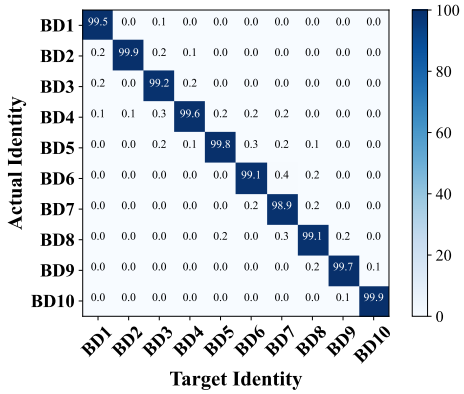


Fig. 5: Confusion matrix for BD authentication with each box showing the percentage of devices identifying as the corresponding identity.

2) Baselines: Two conventional authentication schemes, **Baseline1** [4] and **Baseline2** [25], are compared with PLCRA-BD. **Baseline1** uses a lightweight handshake protocol that shares a secret key between devices through a combination of random numbers and XOR operations. This scheme imposes minimal computational and hardware requirements, making it suitable for resource-constrained BDs, but it provides only limited security protection. In contrast, **Baseline2** utilizes hash functions to secure the key exchange process, delivering stronger security but increasing complexity. As a result, it is generally impractical for severely constrained devices. We do not compare with existing PLA schemes because they cannot be implemented between BDs in an AmBC system.

3) Evaluation Metrics: Following previous PLA works in [21], [27], [33], we evaluate authentication accuracy under spoofing attacks using: **1) True positive rate (TPR)**, defined as the rate that a genuine BD is truly accepted, and **2) False positive rate (FPR)**, defined as the rate at which attackers are incorrectly accepted. Then, the **receiver operating characteristic (ROC)** curve is used to illustrate the trade-off between TPR and FPR across different thresholds δ in (13), where its range is determined through empirical training. In addition, the mutual information between signals received from legitimate devices and attackers is measured to reflect the secrecy of authentication schemes, referred to as **leaked information (LI)** [14]. Regarding efficiency, the **authentication latency** and **power consumption** are considered.

TABLE IV: Complexity comparison of PLCRA-BD and baselines.

Scheme	Time Complexity	Decoding Avoidance	Physical Layer Implementation	AmBC Support
Baseline1	$O(N)$	○	●	●
Baseline2	$O(N)$	○	○	○
Ours	$O(1)$	●	●	●

B. Effectiveness and complexity analysis

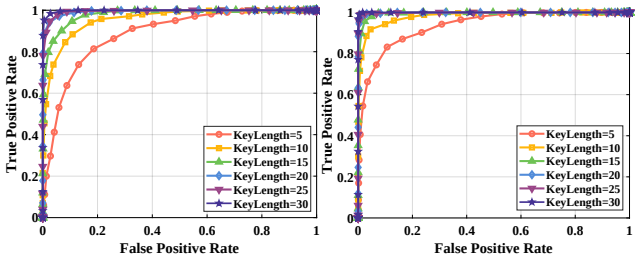
1) Effectiveness analysis: We conducted a basic authentication experiment to evaluate the effectiveness of PLCRA-BD in identifying legitimate BDs. The experiment follows a straightforward principle: a prover BD is identified as the identity (i.e., actual device) whose PID key most closely matches its own. As illustrated in Fig. 5, we tested 10 legitimate BDs, each assigned a PID key of length 10. The results show that the authentication accuracy for all legitimate BDs exceeds 99%, demonstrating the scheme's ability to accurately distinguish between devices. Although a small probability of false identification exists for devices with similar PID keys, this issue can be mitigated by increasing the key length, thereby enhancing key differentiation and improving device identification.

2) Complexity analysis: Table IV compares the computational complexity and device requirements of PLCRA-BD against two baseline schemes. Both baselines incur $O(n)$ complexity due to XOR and hash-based encryption operations. In contrast, our scheme requires transmitting only constant-length bits for the random number and the PID key, achieving $O(1)$ complexity. Additionally, Baseline1 and Baseline2 must decode the transmitted signal to extract the random number and key, thereby increasing power consumption. Our scheme avoids this step entirely by deriving fingerprints directly from the energy harvester's output, eliminating the need for decoding. Furthermore, the baseline2 relies on hash operations typically implemented at the upper software layer, such as for password verification or digital signatures, which is impractical in AmBC systems given the limited capabilities of BDs. In comparison, both the simple XOR operation in Baseline1 and the backscatter operations in our proposed scheme function at the physical layer, aligning with passive BDs.

C. Authenticaion Accuracy

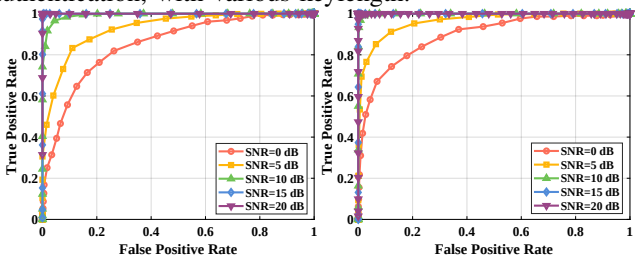
This subsection simulates an impersonation attack where an attacker uses intercepted upper-layer IDs to bypass authentication. We evaluate the accuracy of PLCRA-BD under varying conditions, including key length, SNR, BD distance, and velocity.

1) Impact of key length: Fig. 6 presents the ROC curves for one-way and mutual authentication under varying lengths of the shared keys K_i and K_j. A larger area under the ROC curve corresponds to higher authentication accuracy. As the key length increases, the ROC curves consistently shift upward, indicating improved performance. This enhancement arises because longer keys better differentiate legitimate BDs from attackers, making it increasingly difficult for adversaries to accurately guess the keys. Furthermore, comparing the ROC



(a) One way Authentication (b) Mutual Authentication

Fig. 6: ROC of (a) one-way authentication and (b) mutual authentication, with various keylength.



(a) One-way Authentication (b) Mutual Authentication

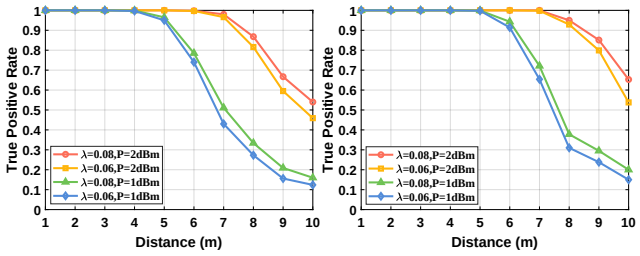
Fig. 7: ROC of (a) one-way authentication and (b) mutual authentication, under various SNR values.

curves in Fig. 6(a) and Fig. 6(b) shows that the accuracy of mutual authentication outperforms that of one-way authentication. This is due to the stricter requirement in mutual authentication, where attackers must correctly guess both K_i and K_j simultaneously, a significantly more challenging task than guessing a single key.

2) Impact of noise: Fig. 13 illustrates the ROC performance at a receiver BD for SNR values ranging from 0 to 20 dB, with the SNR adjusted by varying the transmitting power level. The results indicate that authentication accuracy improves as SNR increases, since higher SNR facilitates more accurate key extraction and identification. Notably, the TPR remains at 1 regardless of changes in the FPR when the SNR exceeds 15 dB for one-way authentication and 10 dB for mutual authentication. This result confirms that our scheme can achieve high authentication accuracy by increasing SNR, a goal attainable through practical measures such as reducing the distance between BDs or increasing the transmitting power of the RFS.

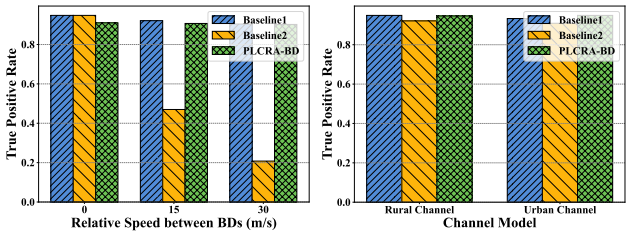
3) Impact of the distance between BDs: Fig. 8 illustrates the effect of the distance between BDs on authentication accuracy. The TPR decreases as the distance increases, primarily due to greater large-scale attenuation in the inward channel between the BDs, which lowers the SNR at the verifier BD. The results also indicate that TPR can be improved by increasing the RFS transmitting power or by lowering the FPR limit. Increasing the transmitting power is a standard approach in wireless systems, while lowering the FPR threshold involves a trade-off, as it reduces the scheme's ability to correctly identify attackers. For subsequent simulations, the distance between the two BDs is fixed at 3 m.

4) Impact of the BD and environment mobility: Fig. 9(a) presents the effect of BD speed on the TPR. It can be seen that PLCRA-BD maintains a nearly constant TPR even



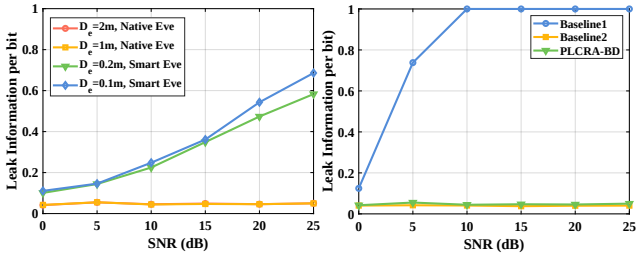
(a) One-way Authentication (b) Mutual Authentication

Fig. 8: TPR vs. the distance between BDs of (a) one-way authentication and (b) mutual authentication.



(a) BD mobility (b) Environment Mobility

Fig. 9: TPR comparison between PLCRA-BD and baselines with (a) BD mobility and (b) environment mobility. The TPR is tested at a FPR limit of 0.



(a) Different eavesdropping attacks (b) Different schemes

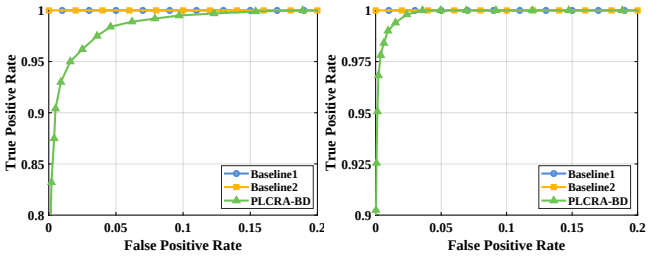
Fig. 10: Leaked information vs. SNR under eavesdropping attacks

at speeds up to 30 m/s, indicating robust support for BD mobility. Meanwhile, Fig. 9(b) shows the impact of different channel conditions, where we employ the rural/urban channel models defined in [1], characterized by 4/12 multipaths, fixed amplitudes, and random phase shifts. The TPR of PLCRA-BD remains stable under these diverse environmental conditions, demonstrating adaptability to environmental mobility. Furthermore, both subfigures reveal that the TPR values of Baseline1 and PLCRA-BD are closely aligned, while those of Baseline2 are lower. This confirms that PLCRA-BD achieves authentication accuracy on par with commonly employed traditional methods [3]–[5], [9], [23]–[25].

D. Attack Robustness

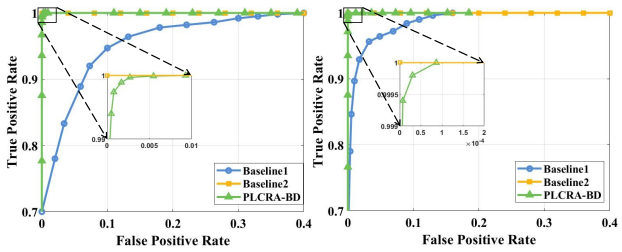
This subsection evaluates the robustness of the authentication procedure against wireless attacks, including eavesdropping, replay, and counterfeiting, and compares it with the baseline methods.

1) Robustness against eavesdropping attacks: Fig. 10(a) illustrates the variation of LI with SNR values for PLCRA-BD under different eavesdropping attacks. In naive eavesdropping



(a) One-way Authentication (b) Mutual Authentication

Fig. 11: ROC of (a) one-way authentication and (b) mutual authentication, under replay attacks.



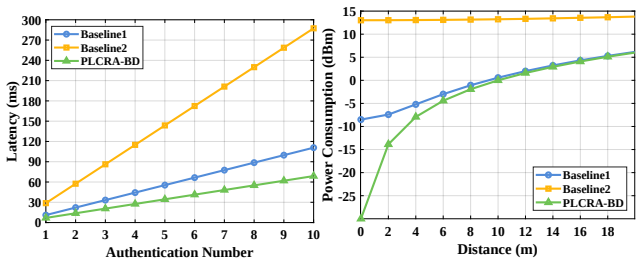
(a) One-way Authentication (b) Mutual Authentication

Fig. 12: ROC of (a) one-way authentication and (b) mutual authentication, under counterfeiting attacks.

scenarios, the LI is minimal at approximately 0.04 and remains nearly constant despite increasing SNR or decreasing distance D_a. This demonstrates the strong robustness of our scheme against naive eavesdropping attacks. Conversely, the figure shows a higher LI (above 0.6) in smart eavesdropping cases as the SNR increases or D_a decreases, indicating the potential vulnerability of the scheme to smart eavesdropping. However, smart eavesdroppers are uncommon in practice and are also challenging to address with existing PLA methods in BC systems.

Fig. 10(b) compares the LI of PLCRA-BD with the baselines under naive eavesdropping attacks. The results show that the LI values of Baseline2 are very low. This is because the high secrecy of hash encryption in Baseline2 prevents attackers from obtaining the genuine message during authentication, leaving them to rely solely on random guesses of the shared keys. Meanwhile, the close LI values of Baseline2 and PLCRA-BD highlight the strong secrecy of our scheme. In contrast, Baseline1 is unable to resist naive eavesdropping attacks, as an eavesdropper can easily break the XOR encryption by comparing the exchanged ciphertext with the transmitted plaintext, thereby recovering the secret key.

2) Robustness against replay attacks: Fig. 11 compares the ROC performance of PLCRA-BD with baseline schemes under replay attacks. The results show that PLCRA-BD achieves a TPR of approximately 0.95 for one-way authentication and 0.99 for mutual authentication at a 0.02 FPR, indicating that our scheme can effectively prevent most replay attackers. In contrast, the baselines exhibit even greater robustness against replay attacks. This is primarily because these schemes are less susceptible to environmental factors, whereas the exchanged keys in PLCRA-BD are more vulnerable to channel fading and noise.



(a) Authentication Latency (b) Power Consumption

Fig. 13: Efficiency comparison between PLCRA-BD and baselines.

3) Robustness against counterfeiting attacks: Fig. 12 compares the ROC performance of PLCRA-BD with baselines under counterfeiting attacks. Of the three schemes, Baseline1 is the least robust to counterfeiting attacks, due to the fact that the key of Baseline1 can be easily estimated by eavesdropping attacks. Using estimated keys, counterfeiting attackers can increase their FPR performance. In contrast, the counterfeiting attackers in PLCRA-BD have approximately 0.005 and 10^{-4} FPR with 1 TPR limit for one-way and mutual authentication, respectively. This extremely low FPR demonstrates the strong robustness of our scheme against counterfeiting attacks. Although Baseline2 achieves the best performance, it cannot be achieved in AmBC systems due to its high complexity requirements. As a result, our scheme has close performance with the Baseline2 and can be implemented in AmBC systems.

E. Efficiency

The efficiency is evaluated under a one-way authentication procedure since the efficiency of mutual authentication is a simple linear relationship with the one-way authentication.

1) Authentication latency: Fig. 13(a) compares the authentication latency of PLCRA-BD with the baselines for different authentication numbers. For PLCRA-BD, we consider signal transmission time T_{tx}, random number generation time T_{rand}, and the key verifying time T_{verify}. $T_{\text{Our}} = 4T_{\text{tx}} + T_{\text{rand}} + T_{\text{verify}}$. For baseline1, we consider the signal transmission time, the random number generation time, the verifying time, bit operation time T_{XOR}, and signal decoding time T_{decoding}. $T_{\text{baseline1}} = 4T_{\text{tx}} + T_{\text{rand}} + T_{\text{verify}} + 2T_{\text{XOR}} + 4T_{\text{decoding}}$. For baseline2, we consider the signal generation time T_{gen}, hash encryption time T_{hash}, the signal transmission time, the random number generation time, and signal decoding time $T_{\text{Baseline2}} = 2T_{\text{gen}} + 2T_{\text{tx}} + 2T_{\text{hash}} + T_{\text{rand}} + T_{\text{verify}} + 2T_{\text{decoding}}$. From Fig. 13(a), it can be found that PLCRA-BD achieves the lowest authentication latency.

2) Power consumption: Fig. 13(b) provides an estimation of power consumption for PLCRA-BD and the baselines relative to the distance between BDs. The analysis includes computation, baseband, and RF transmission power. For a low-power BD, a simple decoding operation consumes approximately 0.03 mW, and an XOR operation consumes 0.01 mW, whereas a regular device requires 5–10 mW for hash encryption. The RF power at the transmitter BD must meet the SNR requirement of 10 dB for all schemes. As shown in Fig. 13(b), PLCRA-BD consumes less power than baseline1 and baseline2, demonstrating its superiority for practical deployment.

VII. Conclusion

In this paper, we introduced PLCRA-BD, a novel physical layer authentication scheme between BDs in AmBC systems based on challenge and response, achieving high-mobility support and robust security. First, we design a fingerprint embedding method and an integrated transceiver mode in resource-constraint BDs, which enables BDs to transmit and extract shared PID-bearing signals in a low-complexity way without the interference of the ambient signals. Building on this, a challenge-response authentication procedure is proposed that enables BDs to exchange shared PID keys in a secure way by exploiting a random number and channel fading, achieving both one-way and mutual authentication. The key update design further mitigates the risk of key leakage. Then, we theoretically analyze the resistance of the authentication procedure against impersonation, eavesdropping, replay, and counterfeiting attacks. Finally, the performance of PLCRA-BD was comprehensively evaluated under various system settings using numerical simulations. It demonstrates that the scheme can be easily implemented in resource-constraint AmBC systems with desirable accuracy, advanced robustness, and superior efficiency compared with conventional authentication schemes.

References

[1] 3GPP. Ts 45.005: GSM/EDGE radio transmission and reception. Technical report, 3GPP, Mar. 2009.

[2] Jingdong Chang, Jiajun Li, Yishan Yang, Yifan Zhang, Masoud Kaveh, and Zheng Yan. APAuth: Authenticate an access point by backscatter devices. In *IEEE International Conference on Communications*, pages 3616–3621, Jun. 2024.

[3] H. Y. Chien and C. Chen. Mutual authentication protocol for RFID conforming to epc class 1 generation 2 standards. *Computer Standards & Interfaces*, 29(2):254–259, Apr. 2007.

[4] Hung Yu Chien. Sasi: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity. *IEEE Transactions on dependable and secure computing*, 4(4):337–340, Nov. 2007.

[5] Jung Sik Cho, Young Sik Jeong, and Sang Oh Park. Consideration on the brute-force attack cost and retrieval cost: A hash-based radio-frequency identification (RFID) tag mutual authentication protocol. *Computers & Mathematics with Applications*, 69(1):58–65, Feb., 2015.

[6] Xianru Du, Dan Shan, Kai Zeng, and Lauren Huie. Physical layer challenge-response authentication in wireless networks with relay. In *IEEE Conference on Computer Communications (INFOCOM), Toronto, ON, Canada*, pages 1276–1284, Jul. 2014.

[7] Ruifeng Duan, Xiyu Wang, Huseyin Yigitler, Muhammad Usman Sheikh, Riku Jantti, and Zhu Han. Ambient backscatter communications for future ultra-low-power machine type communications: Challenges, solutions, opportunities, and future research trends. *IEEE Communications Magazine*, 58(2):42–47, Feb. 2020.

[8] Ander Galisteo, Ambuj Varshney, and Domenico Giustiniano. Two to tango: Hybrid light and backscatter networks for next billion devices. In *Proceedings of the 18th International Conference on Mobile Systems, Applications, and Services*, pages 80–93, 2020.

[9] Lijun Gao, Lu Zhang, Feng Lin, and Maode Ma. Secure RFID authentication schemes based on security analysis and improvements of the usi protocol. *IEEE Access*, 7:8376–8384, Jan 2019.

[10] Amus Chee Yuen Goay, Deepak Mishra, and Aruna Seneviratne. Optimal reflection coefficients for ASK modulated backscattering from passive tags. *IEEE Transactions on Communications*, early access, Sep. 2024.

[11] Jinsong Han, Chen Qian, Panlong Yang, Dan Ma, Zhiping Jiang, Wei Xi, and Jizhong Zhao. GenePrint: Generic and accurate physical-layer identification for UHF RFID tags. *IEEE/ACM Transactions on Networking*, 24(2):846–858, Feb. 2016.

[12] Michael Haus, Muhammad Waqas, Aaron Yi Ding, Yong Li, Sasu Tarkoma, and Jörg Ott. Security and privacy in device-to-device (D2D) communication: A review. *IEEE Communications Surveys & Tutorials*, 19(2):1054–1079, Jan. 2017.

[13] Debiao He and Sherali Zeadally. An analysis of RFID authentication schemes for internet of things in healthcare environment using elliptic curve cryptography. *IEEE Internet of Things Journal*, 2(1):72–83, Feb. 2015.

[14] Jiajun Li, Pu Wang, Long Jiao, Zheng Yan, Kai Zeng, and Yishan Yang. Security analysis of triangle channel-based physical layer key generation in wireless backscatter communications. *IEEE Transactions on Information Forensics and Security*, 18(4):948–964, Nov. 2022.

[15] Jiawei Li, Ang Li, Dianqi Han, Yan Zhang, Tao Li, and Yanchao Zhang. RCID: Fingerprinting passive RFID tags via wideband backscatter. In *IEEE Conference on Computer Communications (INFOCOM), London, United Kingdom*, pages 700–709, May 2022.

[16] Vincent Liu, Aaron Parks, Vamsi Talla, Shyamnath Gollakota, David Wetherall, and Joshua R Smith. Ambient backscatter: Wireless communication out of thin air. *ACM SIGCOMM Computer Communication Review*, 43(4):39–50, Aug. 2013.

[17] Michele Morelli, C C Jay Kuo, and Man On Pun. Synchronization techniques for orthogonal frequency division multiple access (OFDMA): A tutorial review. *Proceedings of the IEEE*, 95(7):1394–1427, Jul., 2007.

[18] Revathy Narayanan, Ambuj Varshney, and Panos Papadimitratos. Harvestprint: Securing battery-free backscatter tags through fingerprinting. *ACM HotNets*, page 178–184, Nov. 2021.

[19] Aaron N Parks, Angli Liu, Shyamnath Gollakota, and Joshua R Smith. Turbocharging ambient backscatter communication. *ACM SIGCOMM Computer Communication Review*, 44(4):619–630, Aug. 2014.

[20] John G Proakis and Masoud Salehi. *Digital communications*. McGraw-hill, 2008.

[21] Dan Shan, Kai Zeng, Weidong Xiang, Paul Richardson, and Yan Dong. PHY-CRAM: Physical layer challenge-response authentication mechanism for wireless networks. *IEEE Journal on selected areas in communications*, 31(9):1817–1827, Aug. 2013.

[22] Yasser Shoukry, Paul Martin, Yair Yona, Suhas Diggavi, and Mani Srivastava. Pycra: Physical challenge-response authentication for active sensors under spoofing attacks. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 1004–1015, New York, Oct. 2015.

[23] Hung Min Sun, Wei Chih Ting, and King Hang Wang. On the security of chien's ultralightweight RFID authentication protocol. *IEEE Transactions on Dependable and Secure Computing*, 8(2):315–317, Jul, 2009.

[24] G. Tsudik. YA-TRAP: yet another trivial RFID authentication protocol. In *Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops*, pages 639–643, Italy, Mar. 2006.

[25] Bin Wang and Maode Ma. A server independent authentication scheme for RFID systems. *IEEE Transactions on Industrial Informatics*, 8(3):689–696, Jan. 2012.

[26] Ge Wang, Haofan Cai, Chen Qian, Jinsong Han, Shouqian Shi, Xin Li, Han Ding, Wei Xi, and Jizhong Zhao. Hu-Fu: Replay-resilient RFID authentication. *IEEE/ACM Transactions on Networking*, 28(2):547–560, Jan. 2020.

[27] Pu Wang, Zheng Yan, and Kai Zeng. BCAuth: Physical layer enhanced authentication and attack tracing for backscatter communications. *IEEE Transactions on Information Forensics and Security*, 17:no. 2818–2834, Aug. 2022.

[28] Xiaofu Wu, Zhen Yang, Cong Ling, and Xiang Gen Xia. Artificial-noise-aided physical layer phase challenge-response authentication for practical OFDM transmission. *IEEE Transactions on Wireless Communications*, 15(10):6611–6625, Jun. 2016.

[29] Boxuan Xie, Alexis Dowhuszko, Kalle Koskinen, Lauri Mela, Jari Lietzén, Kalle Ruttik, Riku Jäntti, and Jyri Hämäläinen. Integration of visible light and backscatter communications for ambient internet of things. In *IEEE 99th Vehicular Technology Conference (VTC2024-Spring)*, pages 1–6, Singapore, Jun. 2024.

[30] Fang Xu, Touseef Hussain, Manzoor Ahmed, Khurshed Ali, Muhammad Ayzed Mirza, Wali Ullah Khan, Asim Ihsan, and Zhu Han. The state of AI-empowered backscatter communications: A comprehensive survey. *IEEE Internet of Things Journal*, 10(24):21763–21786, Jul. 2023.

[31] Gang Yang, Ying Chang Liang, Rui Zhang, and Yiyang Pei. Modulation in the air: Backscatter communication over ambient OFDM carrier. *IEEE Transactions on Communications*, 66(3):1219–1233, Nov., 2017.

[32] Yishan Yang, Masoud Kaveh, Jiajun Li, Yifan Zhang, Zheng Yan, and Kai Zeng. BatAu: A batch authentication scheme for backscatter devices in a smart home network. In *IEEE International Conference on Communications (ICC), Rome, Italy*, pages 4528–4533, May 2023.

[33] Yishan Yang, Jiajun Li, Niya Luo, Zheng Yan, Yifan Zhang, and Kai Zeng. BatchAuth: A physical layer batch authentication scheme for multiple backscatter devices. *IEEE Transactions on Information Forensics and Security*, 19:9452–9466, Oct. 2024.

[34] Davide Zanetti, Boris Danev, and Srdjan Oapkun. Physical-layer identification of UHF RFID tags. In *Proceedings of the International Conference on Mobile Computing and Networking (MobiCom), Chicago, Illinois, USA*, pages 353–364, Sep. 2010.

[35] C. Zhao, Z. Li, T. Liu, H. Ding, J. Han, W. Xi, and R. Gui. RF-Mehndi: A Fingertip Profiled RF Identifier. In *IEEE Conference on Computer Communications (INFOCOM), Paris, France*, pages 1513–1521, May 2019.