This is an electronic reprint of the original article.
This reprint may differ from the original in pagination and typographic detail.

Wang, Pu; Jiao, Long; Zeng, Kai; Yan, Zheng

Physical Layer Key Generation between Backscatter Devices over Ambient RF Signals

Published in:
INFOCOM 2021 - IEEE Conference on Computer Communications

DOI:
[10.1109/INFOCOM42981.2021.9488885](https://doi.org/10.1109/INFOCOM42981.2021.9488885)

Published: 01/05/2021

Document Version
Peer reviewed version

Please cite the original version:
Wang, P., Jiao, L., Zeng, K., & Yan, Z. (2021). Physical Layer Key Generation between Backscatter Devices over Ambient RF Signals. In *INFOCOM 2021 - IEEE Conference on Computer Communications* [9488885] (Proceedings - IEEE INFOCOM). IEEE. <https://doi.org/10.1109/INFOCOM42981.2021.9488885>

© 2021 IEEE. This is the author's version of an article that has been published by IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

Physical Layer Key Generation between Backscatter Devices over Ambient RF Signals

Pu Wang*, Long Jiao[†], Kai Zeng[‡] and Zheng Yan*[‡](✉)

*School of Cyber Engineering, Xidian University, Xi'an, China 710071

[†]Department of Electrical and Computer Engineering, George Mason University, Fairfax, VA, US 22030

[‡]Department of Comnet, Aalto University, Espoo, Finland 02150

Email: wangpu@stu.xidian.edu.cn, {ljiao, kzeng2}@gmu.edu, zyan@xidian.edu.cn

Abstract—Ambient backscatter communication (AmBC), which enables energy harvesting and ultra-low-power communication by utilizing ambient radio frequency (RF) signals, has emerged as a cutting-edge technology to realize numerous Internet of Things (IoT) applications. However, the current literature lacks efficient secret key sharing solutions for resource-limited devices in AmBC systems to protect the backscatter communications, especially for private data transmission. Thus, we propose a novel physical layer key generation scheme between backscatter devices (BDs) by exploiting received superposed ambient signals. Based on the repeated patterns (i.e., cyclic prefix in OFDM symbols) in ambient RF signals, we present a joint transceiver design of BD backscatter waveform and BD receiver to extract the downlink signal and the backscatter signal from the superposed signals. By multiplying the downlink signal and the backscatter signal, we can actually obtain the triangle channel information as a shared random secret source for key generation. Besides, we study the trade-off between the rate of secret key generation and harvested energy by modeling it as a joint optimization problem. Finally, extensive numerical simulations are provided to evaluate the key generation performance, energy harvesting performance, and their trade-offs under various system settings.

I. INTRODUCTION

Ambient backscatter communication (AmBC) as an important communication technology for enabling Internet of Thing (IoT), has received increasing attention due to its ultra-low power consumption [1]. In AmBC systems, backscatter devices (BDs) can transmit data by reflecting radio frequency (RF) signals in the air, such as TV and Wi-Fi signals, instead of generating power-hungry RF signals [2], [3]. With the AmBC, it not only achieves uplink transmission to a dedicated reader, but also realizes device-to-device (D2D) communications [4]–[7]. One of the attractive applications of AmBC is implanted and wearable sensor systems for physiological and medical purposes. Such sensors are resource-limited, which makes AmBC a suitable technology for data transmission and battery replenishment. However, the broadcast nature of backscatter makes it easy for illegal users to obtain information contents, which could lead to data interception and privacy breach. And their limitations of energy and computation resources make it extremely difficult to implement complex security solutions. Thus, it is challenging to devise practical security mechanisms to protect the backscatter communications among BDs with limited resources.

The conventional mechanisms to secure the backscatter communications are mainly based on lightweight symmetric cryptography [8], [9], which uses a shared secret session key to encrypt/decrypt messages between BDs. The session key could be derived from a long-term master secret key or generated with the Diffie-Hellman(D-H) key exchange protocol. The

former is subject to complex key distribution and heavy management overhead, especially in ad hoc scenarios where two BDs without any pre-shared secrets need to establish a secure communication channel. Furthermore, once the long-term master secret key is comprised, all the communications in the past will be comprised. That is, the long-term master key based solutions do not provide forward secrecy. Although the D-H key exchange protocol can provide forward secrecy, it introduces significant computational overhead, making it problematic and undesirable for resource-constrained BDs.

Alternatively, physical layer (PHY) key generation has been considered as a promising technology to provide a lightweight and information-theoretically secure key sharing solution with forward secrecy for resource-constrained systems [10], [11]. It extracts reciprocal randomness in the wireless fading channel to generate shared secret keys between devices without incurring significant computation overhead. In theory, the secrecy of the shared key is ensured by the fact that an adversary who is kept at a distance (larger than coherence distance) away from key generating devices will observe highly uncorrelated channel characteristics, thus will not be able to derive the same key. PHY key generation supports full flexibility and scalability by realizing independent key establishment on demand, instead of relying on the secret key distribution using central infrastructures or servers.

However, existing PHY key generation schemes cannot be directly applied for BDs. In existing schemes, two devices usually have to send channel probing signals to each other in order to measure highly correlated channel characteristics, such as received signal strengths (RSS), at both sides for key generation [12]–[14]. However, BDs are not able to generate channel probing signals by themselves, making the channel probing between two BDs fundamentally different from conventional ones. In order to probe the channel from one BD to the other, it has to exploit the received ambient RF signal. But a receiver BD will receive a superposed signal consisting of the backscattered signal and an original ambient RF signal. Since the channel from the RF source to one BD is not identical with the one from the RF source to the other, the superposed signals cannot be directly used as a shared random source to generate a shared key between BDs. Therefore, how to obtain reciprocal channel characteristic measurements for shared key generation between BDs is a non-trivial problem.

In this paper, we propose a novel PHY key generation scheme for two paired BDs in an AmBC network. In such a network, there are an RF source, which continuously transmits RF signals, and two paired BDs communicating with each

other in a time-division manner. The basic idea is as follows. By utilizing the repeated patterns (i.e., cyclic prefix in OFDM symbols) in the ambient RF signals, we propose a joint transceiver design of the BD backscatter waveform and the BD receiver. This joint design enables one BD to separate its downlink channel information and its backscatter channel information, which is the concatenation (or multiplication) of the other downlink channel (RF source to the other BD) and the inward reflecting channel (the other BD to itself), from the superposed signal with low complexity. Then by further multiplying the downlink channel and the backscatter channel, we can actually obtain a triangle channel, a multiplication of the two downlink channels and the inward reflecting channel at each BD, like three sides of a triangle formed by the RF source and the two BDs. The multiplications at both sides will be highly correlated if the reciprocity of the BD-to-BD channel holds well. Therefore, a random secret source can be established for key generation between the two BDs over ambient RF signals.

The main contributions of this paper are summarized as follows:

- We propose a novel PHY key generation scheme for the BDs relying only on ambient RF signals. To the best of our knowledge, this is the first work tackling this problem. The proposed scheme constructs a multiplication of three channels (i.e., three sides of the triangle formed by the RF source and the two BDs) as shared randomness.
- A transceiver design of BD backscatter waveform and BD receiver is proposed to extract the downlink signal and backscatter signal from the superposed signal, so as to obtain the triangle channel information with low complexity.
- A general joint optimization problem is further formulated to study the trade-off between the rate of secret key generation and the harvested energy.
- Finally, extensive numerical simulations are conducted to evaluate key generation and energy harvesting performance, and discuss their trade-offs under different system parameters. Simulation results show the effectiveness of the proposed key generation scheme.

The rest of the paper is organized as follows. We present the related work in Section II, and introduce our system model and assumptions in Section III. In Section IV, we present our proposed secret PHY key generation scheme and the adversary model. Section V gives the details of the BD backscatter waveform and BD receiver over the ambient OFDM carrier. Section VI analyzes the trade-off between the rate of secret key generation and harvested energy through a general joint optimization. Section VII reports performance test results based on simulations. Finally, we conclude the paper in the last section.

Notations: The main notations in this paper are described as below. $|\cdot|$ means the operation of taking an absolute value. $\mathcal{CN}(\mu, \sigma^2)$ denotes the circularly symmetric complex Gaussian (CSCG) distribution with mean μ and variance σ^2 . $\Re\{\cdot\}$ denotes the operation to get the real part of a complex number. $\mathbb{E}[\cdot]$ denotes the statistical expectation.

II. RELATED WORKS

A. Lightweight Cryptography

In the existing literature, most security solutions tailored for backscatter communication are based on concepts of lightweight cryptography, such as DESL, Present, Salsa20, LEX and lightweight ECC [8], [9]. To further reduce computation cost, Chine [15] even presented an ultra-lightweight protocol that only requires simple bit-wise operations to provide authentication and integrity. While these algorithms provide good security against some attacks, they also exhibit unexpected limitations [16]–[18], such as the reliance on key generation, distribution and management. They require resources to support exchanges of cryptographic credentials over a backscatter channel, which can be intercepted by an eavesdropper, even if encrypted. Besides, the above solutions only support traditional backscatter systems with a dedicated RF reader, which could be unsuitable for AmBC systems.

B. Physical Layer Security Solution

Another way to provide security in backscatter systems while overcoming the limitations of cryptography is to apply PHY security mechanisms. Unlike the computational nature of cryptography, PHY security exploits the inherent randomness of the wireless channel to achieve communication confidentiality [19]. Except that a secure backscatter channel is established with the help of proper coding, signal design and power allocation [20]–[22], PHY key generation also has gained much attention in the literature [11], [23]. It exploits the randomness and reciprocity of a wireless channel as a shared source to generate secret keys. For example, the channel state information (CSI), such as amplitude and phase, can be estimated by sending probing signals for key generation between two users [13], [14]. In [24], the received signal strength (RSS) trajectories of two moving wearable devices are exploited to achieve secret key establishment. Besides, secret group key generation schemes were proposed by exploiting different channel information and considering various topologies in multi-device systems [25]–[27].

In current literature, all existing PHY key generation schemes require two communication parties to measure the channel properties by alternately transmitting probing signals. However, in AmBC systems, BDs depend on ambient RF signals in the air to transmit information. They cannot directly estimate the channel characteristics like conventional schemes by transmitting probing signals. Besides, BDs receive RF signals both from the RF source and other BDs that pass different wireless channels, making it impossible to apply the RSS of RF signals as a random source. Therefore, it is challenging to apply existing methods of physical key generation in AmBC systems, especially for backscatter-based D2D communications.

III. SYSTEM MODEL

As illustrated in Fig. 1, there are two co-existing communication systems. One is a legacy system that employs an RF source (e.g., TV tower, Wi-Fi AP) to transmit RF signals to its dedicated users. The other is an AmBC system that consists of multiple BDs, which can communicate with each other in a time-division manner by backscattering the ambient RF signals emitted by the RF source. We are interested in

Fig. 1. System model for ambient backscatter communications over ambient RF signals.

the physical layer key generation between two paired BDs in the AmBC system, which is trivial to extend to multiple BDs scenarios [27]. We assume that there are only one legacy RF source and two passive (or semi-passive) BDs with a single-antenna. The BDs contain a backscatter modulator (i.e., a switched load impedance), an information receiver, an RF-energy harvester and other modules (i.e., sensors). BDs can operate in a backscattering mode and a listening mode. To transmit information, BDs operate in the backscattering mode to reflect incident signals by intentionally altering their amplitude and/or phase. To receive information, the antenna of BDs is switched to the listening mode and BDs decode information from a part of received signals [6], while remaining signals are used to harvest energy.

In our adversary model, we assume a passive eavesdropper Eve, which only overhears all communications between BDs and tries to infer information about the generated key. This assumption implies that Eve is not interested in disrupting the key establishment, neither jamming the communication channel nor modifying any message exchanged between BDs. But Eve will measure the characteristics of the channels from all received signals while BDs are backscattering information to other BDs for key extraction. Thus, Eve can obtain the channel information from the ambient original signals of the RF source and the reflected signals of BDs. However, we assume that Eve cannot be very close (less than a few multiples of the wavelength) to any BDs while they are generating the shared key. This will ensure that Eve measures different and uncorrelated wireless channels [11].

Let $h_i(t)$ denote the multi-path Rayleigh fading channels between the RF source and BD A_i or Eve A_e , and $h_{i,j}(t)$ for the channel between A_i and A_j ($i, j \in \{1, 2, e\}, i \neq j$), respectively. A channel is given in the form of $h = \vartheta d^{-\frac{\alpha}{2}}$, where ϑ is a CSCG variable, d is the distance between the considered transmitter and receiver, and α is the path-loss exponent. For convenience subsequently, we define that the downlink channel of A_i is h_i and the inward channel of A_i and A_j is $h_{i,j}$, and the backscatter channel $h_{i,j}h_i$, which is a concatenation of $h_{i,j}$ and h_i , as shown in Fig. 1. All relevant channels are mutually independent, and assumed to remain unchanged during a period of time slots, i.e., coherence time T_{ch} [11], [28].

A. Signal Model in AmBC Systems

Denote a bandpass signal transmitted from the RF source during a symbol interval as

$$\tilde{s}(t) = \Re\{\sqrt{p}s(t)e^{j2\pi f_c t}\}, \quad (1)$$

where $s(t)$ is a unit baseband signal with transmission power p , and f_c represents carrier frequency. The ambient signal received at A_i can be represented as [29]

$$\tilde{c}_i(t) = \Re\{[\sqrt{p}h_i(t)s(t)]e^{j2\pi f_c t}\}, \quad (2)$$

where $c_i(t) = \sqrt{p}h_i(t)s(t)$ is the baseband representation of $\tilde{c}_i(t)$.

Let $b_i(t)$ be the signal of A_i to be transmitted. By denoting α as the reflection coefficient at BDs, the signal backscattered from A_i is $\alpha\tilde{c}_i(t)b_i(t)$. This modulation technique exempts BDs from generating RF signals locally and thus significantly reduces their power consumption [3].

The received superposed signal at A_j can be expressed as,

$$\tilde{y}_j(t) = \alpha h_{i,j}(t)\tilde{c}_i(t)b_i(t) + h_j(t)\tilde{s}(t) + \tilde{w}_j(t), \quad (3)$$

where $\tilde{w}_j(t)$ is the received passband additive white Gaussian noise (AWGN) at A_j . The baseband representation of (3) is

$$y_j(t) = y_j^b(t) + y_j^d(t) + w_j(t), \quad (4)$$

where $y_j^b(t) = \alpha h_{i,j}(t)c_i(t)b_i(t)$ is the backscatter signal reflected from A_i , $y_j^d(t) = \sqrt{p}h_j(t)s(t)$ is the original ambient signal directly from the RF source, and $w_j(t)$ is the baseband representation of $\tilde{w}_j(t)$ with power σ_j^2 , i.e., $w_j(t) \sim \mathcal{CN}(0, \sigma_j^2)$.

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. For convenience, we write the discrete-time representation of the received signal at A_j as

$$y_j[n] = y_j^b[n] + y_j^d[n] + w_j[n], \quad (5)$$

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

IV. THE PROPOSED KEY GENERATION SCHEME

In this section, we first provide an overview of the basic physical layer key generation scheme and the reason why it is not applicable in AmBC systems. Then, we describe our basic idea and show the challenge to extract a secret key from the received RF signals between two paired BDs, and define the achievable secret key rate (SKR) with our assumed eavesdropping model.

A. Conventional Secret Key Generation

In basic point-to-point key generation schemes, there are two devices, A_1 and A_2 , which wish to agree on a secret key through a wireless channel. Three main steps are needed to generate a shared key: (1) shared randomness extraction, (2) information reconciliation, (3) privacy amplification [11].

To extract the shared randomness, A_1 and A_2 successively transmit a unit probing signal x to the other. The received signal at A_2 at time t is

$$y_2(t) = h_{1,2}(t)x(t) + n_2(t). \quad (6)$$

Similarly, the received signal at A_1 at time t' is

$$y_1(t') = h_{2,1}(t')x(t') + n_1(t'), \quad (7)$$

where $h_{1,2}(t)$ and $h_{2,1}(t')$ are the channels between A_1 and A_2 , respectively, $n_1(t)$ and $n_2(t')$ are AWGN. If $(t' - t) < T_{ch}$, then due to channel reciprocity, $h_{1,2} \approx h_{2,1}$. Variables $Y_1 = \{y_1(1), y_1(2), \dots, y_1(m)\}$ and $Y_2 = \{y_2(1), y_2(2), \dots, y_2(m)\}$, measured by A_1 and A_2 for a period of time, are highly correlated in statistics, thus can be used as the shared randomness for key generation.

However, the traditional scheme cannot be applied to AmBC systems for BDs, since BDs cannot directly estimate the inward channel information between them. That is, they cannot generate determined RF signals as probing pilots, only relying on the ambient RF signals, which is uncontrollable, even unknown for BDs. In AmBC systems, BDs receive either the downlink signal from the RF source while no backscattering, or the superposed signals, which is the superposition of the downlink signal and the backscattered signal from the other BD. The downlink signals at two BDs are uncorrelated due to passing through different downlink channels. For superposed signals at BDs, they are even more uncorrelated because of the superposition of uncorrelated downlink signals and backscattered signals. Thus, the measurement of such received signals cannot be used as shared common randomness. But the superposed signal includes the information of three channels, including the downlink channels h_1 and h_2 , and the inward channel $h_{1,2}$ (or $h_{2,1}$), which are common and identical for two paired BDs. Therefore, we can exploit the superposed signal to construct shared randomness for key generation.

B. Basic Idea of the Proposed Scheme

In this subsection, we briefly introduce our physical layer key generation scheme based on the superposed signal. As shown in Fig. 1, the system consists of an RF source, two BDs A_1 and A_2 , which communicate in a time-division manner. Our proposed scheme proceeds as follows:

Step 1: In the time slot t , the RF source transmits the constant signal $s(t)$ and A_2 operates in the backscattering mode. A_1 operates in the listening mode and receives signals, including the signal backscattered from A_2 and the signal directly from the RF source, as

$$y_1(t) = \alpha h_{2,1}(t) h_2(t) s(t) + h_1(t) s(t) + w_1(t), \quad (8)$$

where $w_1(t)$ is the AWGN.

Step 2: Similarly, in the time slot t' , A_2 operates in the listening mode when A_1 is backscattering. The superposed signal at A_2 are

$$y_2(t') = \alpha h_{1,2}(t') h_1(t') s(t') + h_2(t') s(t') + w_2(t'), \quad (9)$$

where $w_2(t')$ is the AWGN.

After the above two steps, for easy understanding of our basic idea, let's assume there is no noise and BDs (A_1 and A_2) is able to estimate the corresponding channels with knowing the signal $s(t)$. Then the superposed channels at A_1 and A_2 are estimated respectively as

$$Y_1 = \alpha h_{2,1} h_2 + h_1, \quad (10)$$

$$Y_2 = \alpha h_{1,2} h_1 + h_2. \quad (11)$$

Step 3: Let's assume that A_1 is able to separate its downlink channel h_1 and the backscatter channel $h_{2,1} h_2$ from the superposed channel Y_1 , and A_2 can do the same to separate h_2 and $h_{1,2} h_1$ from Y_2 . Then A_1 and A_2 can construct a

triangle channel by multiplying the downlink channel and the backscatter channel as follows, respectively,

$$v_1 = h_1 h_{2,1} h_2, \quad (12)$$

$$v_2 = h_2 h_{1,2} h_1. \quad (13)$$

As illustrated in Fig. 1, A_1 , A_2 and the RF source form a triangle with three sides h_1 , h_2 and $h_{1,2}$ (or $h_{2,1}$). We define the product of three sides of the triangle as the *triangle channel*, which is theoretically identical if the channel reciprocity ($h_{2,1} = h_{1,2}$) holds. In this way, each of A_1 and A_2 can obtain a sequence of the triangle channel information ($V_1 = \{v_1(1), \dots, v_1(m)\}$ and $V_2 = \{v_2(1), \dots, v_2(m)\}$) as common randomness for shared secret key generation.

C. Secret Key Rate

In our eavesdropping model, Eve can intercept signals from A_1 , A_2 and the RF source and estimate the channels as

$$C_e = h_e, \quad (14a)$$

$$Y_{1,e} = \alpha h_{1,e} h_1 + h_e, \quad (14b)$$

$$Y_{2,e} = \alpha h_{2,e} h_2 + h_e. \quad (14c)$$

Then, Eve can follow two eavesdropping models to intercept the secret key information as follows by assuming Eve is close to A_1 (the same for closing to A_2),

$$v_e^1 = h_e h_{2,e} h_2, \quad (15a)$$

$$v_e^2 = h_{1,e} h_1 h_{2,e} h_2. \quad (15b)$$

Thus, with channel estimation sequences V_1 , V_2 at A_1 , A_2 and $V_e^1 = \{v_e^1(1), \dots, v_e^1(m)\}$, $V_e^2 = \{v_e^2(1), \dots, v_e^2(m)\}$ at Eve, the achievable secret key rate of the key generation source model is given by

$$C_{SK} = \min\{I(V_1; V_2 | V_e^1), I(V_1; V_2 | V_e^2)\} \quad (16)$$

If Eve is located at a sufficient distance d ($> \lambda/2$) from A_1 and A_2 , $h_{e,1}$ and $h_{e,2}$ are uncorrelated with $h_{1,2}$, and h_e is uncorrelated with h_1 and h_2 . In this case, both the sequences V_e^1 and V_e^2 at Eve are independent with V_2 or V_1 . Thus, Eve is unable to intercept any information of the shared secret information V_1 or V_2 . If Eve is much close to A_1 , Eve could intercept some information of the triangle channel, which can be modeled with a cross correlation coefficient between h_e and h_1 , as well between $h_{2,e}$ and $h_{2,1}$ [30]. The effect of two overhead methods will be analyzed with the correlation coefficient in the simulation section.

D. Challenges

In some cases, training symbols i.e., preamble or pilot, utilized in some wireless systems for synchronization and channel estimation, could be exploited by BDs to directly estimate the superposed channel. However, because of the single omni-directional antenna of BDs, it is extremely challenging for BDs to differentiate the downlink signal and the backscattered signal. This limitation renders BDs impossible to separate the downlink channel and the backscatter channel from the superposed channel without increasing immense hardware and software complexity, even if BDs are able to conduct channel estimation. Besides, channel estimation with complex computation is unsuitable for resource-constrained BDs, since it consumes much computational resources and

Fig. 2. OFDM signals at different stages ($K = 1$), one OFDM symbol for $B = 1$ and another for $B = 0$.

energy. Therefore, in order to apply the proposed scheme in practice, in the next section, we will present how to construct and obtain the triangle channel information directly from the received RF signals, instead of conducting channel estimation. It can realize low computational complexity for resource-limited BDs by jointly designing the backscatter waveform and the receiver of BDs.

V. TRANSCIVER DESIGN OVER OFDM CARRIER

The orthogonal frequency division multiplexing (OFDM) transmission scheme is widely used in current wireless systems, such as Digital Audio Broadcasting (DAB), LTE and Wireless Local Area Networks (LANs) [31]. In OFDM signals, a cyclic prefix (CP) is used to extend an OFDM symbol by copying last samples of the OFDM symbol into its beginning, so as to avoid interblock interference (ISI) caused by the multi-path delay spread of wireless channels [31]. By exploiting this repeated CP pattern, we propose a joint transceiver design, including the BD backscatter waveform and the receiver, which enable BDs to extract the downlink signal and backscatter signal from the superposed signal with low complexity. This design is similar to the direct-link interference cancellation mechanism [3], which mainly focuses on the backscatter transmission in AmBC systems. But we aim to extract the downlink signal and backscatter signal from the superposed signal and then construct the triangle channel information. Finally, we discuss the feasibility of the transceiver design with other repeated patterns in OFDM symbols, as well as the synchronization problem.

As presented in Section III.A, we assume an OFDM modulated signal is the baseband signal $s(t)$. We consider a multi-path delay spreads in the downlink channel $h_i(t)$ and the inward channel $h_{i,j}(t)$, denoted as τ_{h_i} and $\tau_{h_{i,j}}$, respectively. Let f_s be the sampling rate of the OFDM signal. The all discrete-time channel spreads are denoted as $L_{h_i} = \lfloor \tau_{h_i} f_s \rfloor$, $L_{h_j} = \lfloor \tau_{h_j} f_s \rfloor$ and $L_{h_{i,j}} = \lfloor \tau_{h_{i,j}} f_s \rfloor$, respectively. Denote the total discrete-time length of the backscatter channel spread as $L_{b_j} = L_{h_i} + L_{h_{i,j}}$ and the maximum channel spread at A_j as $L_j = \max\{L_{h_j}, L_{b_j}\}$. Let N be the number of subcarriers of the OFDM signal $s(t)$ and CP length N_{cp} be much longer than the maximum channel spread in the AmBC system.

A. BDs Backscatter Waveform Design

In the listening mode, BDs receive ambient OFDM signals and split them for information receiving and energy harvesting. In the backscattering mode, they backscatter the OFDM signal to transmit information. When BDs are backscattering, specifically, we can design the duration of each BD symbol to be 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. 2, the BD A_1 uses the waveform $b[n]$ in (17) to convey information bit $B = 1$ in a BD symbol, for $k = 0, \dots, K - 1$.

$$b[n] = \begin{cases} 1, & \text{for } n = kN_t, \dots, \frac{2k+1}{2}N_t - 1, \\ -1, & \text{for } n = \frac{2k+1}{2}N_t, \dots, (k+1)N_t - 1. \end{cases} \quad (17)$$

Similarly, the following $b[n]$ conveys information bit $B = 0$,

$$b[n] = -1, \text{ for } n = kN_t, \dots, (k+1)N_t - 1. \quad (18)$$

Thus, to transmit a '1' bit, the BDs will alternate its antenna impedance between two states, one state causes a phase shift of π and another with no phase shift, and the state transition is in the middle of each OFDM symbol period. While transmitting a '0' bit, the BD keeps its antenna impedance constant with no phase shift. The waveform design aims to enable the receiver BDs to separate the backscatter signal and downlink 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 FM0 waveform widely used in commercial radio frequency identification (RFID) tags [3].

B. Receiver Design

In this part, we further present the receiver design to obtain the triangle channel information. For convenience, we choose $K = 1$, without loss of generality. As characterized in Eq. (5), for example, at BD A_2 , the downlink signal $y_2^d[n]$ and the backscatter signal $y_2^b[n]$ pass different multi-path channels h_2 and $h_{1,2}h_1$, respectively. However, both $y_2^d[n]$ and $y_2^b[n]$ have repeated CP in an OFDM symbol as in Fig. (2). With the effect of multi-path channel, the superposed signal $y_2[n]$ consists of the signal component only from one OFDM symbol when $L - 1 \leq N \leq N + N_{cp} - 1$. Otherwise, it consists of signals from different OFDM symbols [32]. Our proposed scheme uses only the repeated CP part to construct the triangle channel information.

To be specific, due to the repeated CP and the multi-path effect, two CP parts of each OFDM symbol at A_2 in the downlink signal $y_2^d[n]$, are identical, i.e.,

$$y_2^d[n] = y_2^d[n + N], \quad n = L_{h_2} - 1, \dots, N_{cp} - 1. \quad (19)$$

Similarly, the feature of the repeated CP holds at A_1 , i.e.,

$$y_1^d[n] = y_1^d[n + N], \quad n = L_{h_1} - 1, \dots, N_{cp} - 1. \quad (20)$$

Based on (17) and (20), when A_1 transmits bit $B = 1$, it modulates $y_1^d[n]$ with $b[n]$. Thus, the received signal $y_2^b[n]$ at A_2 has the following repeated structure,

$$y_2^b[n] = -y_2^b[n + N], \quad n = L_b - 1, \dots, N_{cp} - 1. \quad (21)$$

By utilizing the repeated CP of $y_2^d[n]$ and $y_2^b[n]$, as well as the superposed signal $y_2 = y_2^b[n] + y_2^d[n]$, for $L - 1 \leq n \leq N_{cp} - 1$, we obtain the information in A_2 as follows,

$$\begin{aligned} z_2^b[n] &= y_2[n] - y_2[n + N] = 2y_2^b[n] \\ &= 2\alpha\sqrt{p}h_{1,2}[n]h_1[n]s[n]. \end{aligned} \quad (22)$$

$$\begin{aligned} z_2^d[n] &= y_2[n] + y_2[n+N] = 2y_2^d[n] \\ &= 2\sqrt{p}h_2[n]s[n]. \end{aligned} \quad (23)$$

Thus, $z_2^b[n]$ only contains the backscatter channel information $h_{1,2}[n]h_1[n]$, and $z_2^d[n]$ contains the downlink channel information $h_2[n]$.

After all processes, A_2 can construct the triangle channel information by multiplying $z_2^d[n]$ and $z_2^b[n]$ as

$$z_2[n] = z_2^b[n]z_2^d[n] = 4\alpha p h_2[n]h_{1,2}[n]h_1[n]s^2[n] + w_2[n], \quad (24)$$

where $w_2[n]$ denotes all noises for simplicity. Clearly, the downlink channel and the backscatter channel related to A_2 in the formula keep constant for $J = N_{cp} - L + 1$ (less than the coherence time), which stands for the repeated length in one OFDM symbol of the superposed signals $y_2[n]$. For large N_{cp} , A_2 averages the constructed information of J samples,

$$\begin{aligned} v_2 &= \frac{1}{J} \sum_{n=L-1}^{N_{cp}-1} |4\alpha p h_2[n]h_{1,2}[n]h_1[n]s^2[n] + w_2[n]| \\ &= 4p|\alpha h_2h_{1,2}h_1| + |w_2|, \end{aligned} \quad (25)$$

where $\frac{1}{J} \sum_{n=L-1}^{N_{cp}-1} |s^2[n]| = 1$ because of the unit power of the baseband OFDM signal $s[n]$. Thus, the BD A_2 is able to separate the downlink signal and the backscatter signal from the superposed signal with the single antenna only, while not incurring extra hardware complexity. Then, it can **obtain the triangle channel information with two extracted signals without conducting channel estimation**.

Similarly, if A_2 is backscattering, A_1 can also obtain the same triangle channel information as follows,

$$v_1 = 4p|\alpha h_1h_{2,1}h_2| + |w_1|. \quad (26)$$

Because of the channel reciprocity within T_{ch} , i.e., $h_{1,2} = h_{2,1}$, the identical triangle channel information ($v_1 = v_2$) can be used as a shared random source. Therefore, each of A_1 and A_2 can get a sequence of the triangle channel information by exchanging multiple rounds for shared secret key generation.

For the average power of the repeated CP samples, most existing works assume that the baseband OFDM signal $s[n]$ is transmitted with unit power [3], [4] and its power keeps constant even in different OFDM symbols. Nevertheless, because of the incomplete randomization of data bits for OFDM modulation, the total power is not uniformly distributed at all samples of an OFDM symbol. The imperfect condition will affect the average power of $s[n]$ in the repeated CP part, especially with few samples, thus degrading the correlation of sequences at A_1 and A_2 . But by increasing the length of the repeated CP part, including enlarging the length of the OFDM symbols and the BD symbol duration, we can improve the correlation of sequences at each BD.

C. Discussion

1) *Other Repeated Patterns in Ambient Signals*. For some OFDM modulations, zero-padding (ZP), one-padding (OP) or 1-0 bit sequence is selected as a guard interval in OFDM symbols to avoid ISI. Our proposed scheme still works by only setting the duration of one BD symbol to the length of two OFDM symbols. That is, the same guard interval in each OFDM symbol will repeat in two successive OFDM symbols. And the state transition of the BD symbol is set in the middle

of the duration of two OFDM symbols, instead of the middle of one OFDM symbol. Moreover, the stable and fixed average power of ZP, OP, preamble or pilot will alleviate the effect of the varied average power of CP symbols. Similarly, our design can achieve key generation between two BDs even without OFDM-based RF signals, because other available repeated patterns, such as PHY preamble in RFID systems, [33] can be exploited to construct the triangle channel information by setting the duration of a BD symbol to the length of two data frames.

2) *Synchronization*. Since BDs know the synchronization preamble in ambient OFDM signals, they can estimate the start of an OFDM symbol and then calculate the middle of an OFDM symbol, by using the cross-correlation based method or other algorithms in [34]. For the case in which the BD does not know the synchronization preamble, it can still estimate the start of an OFDM symbol with repeated CP structures [3]. Moreover, our design does not strictly require BDs to switch in the middle of each OFDM symbol, as long as BDs are able to construct a reversed and repeated structure as in (21). For example, BDs can alternate their state at any positions within the range of $[N_{cp} - 1, N + L_{h_1} - 1]$, while not affecting the repeated CP structure.

VI. OPTIMIZATION OF KEY GENERATION AND ENERGY HARVESTING

In the AmBC system, BDs are passive or semi-passive devices that need to continuously harvest enough energy from RF signals for circuit operations. With various RF signal strengths in different positions, the requirement and potential ability of key generation and energy harvest are quite different. For example, some BDs may require a strong secret key for high security, while others may be hungry for harvesting energy when almost running out of batteries. Thus, the ratio of power splitting should be adjusted to balance the energy harvest and information reception, which affects the key generation rate, according to system requirements.

At each BD, the received superposed signals are split into two signal streams. We assume a ratio ρ_i ($0 < \rho_i < 1$) of power for information reception to estimate the triangle channel information and the remaining $(1 - \rho_i)$ for energy harvesting. The BDs also harvest remaining signal power when they are backscattering [5], but we do not consider this harvested energy because it is constant.

For BDs, the part of signal $\sqrt{\rho_i}y_i[n]$ is used to obtain the triangle channel information and the other part $\sqrt{1 - \rho_i}y_i[n]$ for scavenging energy. Based on eqs. (26) and (25), the estimations of the triangle channel at A_1 and A_2 are respectively,

$$v_1 = 4p\rho_1|\alpha h_1h_{2,1}h_2| + |w_1|, \quad (27)$$

$$v_2 = 4p\rho_2|\alpha h_2h_{1,2}h_1| + |w_2|. \quad (28)$$

Even though $4p\rho_i|\alpha h_jh_{j,i}h_i|$ in two formulas with the variances, $\sigma_i^2 = \rho_i^2 P$ ($P = |4p\alpha h_ih_{j,i}h_j|^2$), are not Gaussian random variables, the upper bound of the mutual information of two sequences can be expressed as [12], [35],

$$I(V_1; V_2) = \frac{1}{2} \log \left(1 + \frac{\rho_1^2 \rho_2^2 P}{\rho_2^2 N_1 + \rho_1^2 N_2 + \frac{N_1 N_2}{P}} \right), \quad (29)$$

where N_1 and N_2 are the variances of the noise $|w_1|$ and $|w_2|$, respectively. According to (29), the mutual information is determined by the power of signals p and the ratio ρ_i .

In the AmBC system, the direct signal is typically much stronger than the backscattered signal and the noise, because of the two-round fading backscatter channel and the backscatter coefficient. Thus, the harvested energy at the BD A_i can be described as below

$$E_i = \zeta p(1 - \rho_i)(\alpha h_{j,i} h_j + h_i)^2 + N_i \approx \zeta p(1 - \rho_i) h_i^2, \quad (30)$$

where ζ is the conversion efficiency of the energy harvesting process at BDs and $i \neq j \in \{1, 2\}$.

With the formulas (29) and (30), the key generation rate and the harvested energy can be balanced by changing the ratio $\rho = [\rho_1, \rho_2]$. To analyze this problem and achieve optimum of power efficiency, we formulate a convex optimization problem as below,

$$\begin{aligned} \max_{\rho} \quad & I(V_1; V_2) \\ \text{s.t.} \quad & E_i \geq \bar{E}_i, \quad i = 1, 2 \\ & 0 \leq \rho_i \leq 1, \quad i = 1, 2 \end{aligned} \quad (31)$$

where $\bar{E}_i$ is the threshold of the harvested energy to satisfy the energy requirement of BDs. Thus, the BDs can jointly maximize the key generation rate while satisfying their energy requirements. For example, if a BD has a higher energy requirement, it needs to increase the energy harvest constraint which could degenerate the rate of key generation. On the contrary, with more energy in their capacitor, BDs can split more RF signals to improve the key agreement rate.

VII. PERFORMANCE EVALUATION

In this section, we carry out Monte Carlo simulations to analyze the effects of all parameters, including the performance of key generation with different settings, secret key rate with the eavesdropping model and the tradeoff between key generation and energy harvesting. The numerical results offer insights to design a secure key generation scheme in practical AmBC systems.

A. Parameter Setup and Metrics

Each channel tap is modeled by an independent complex Gaussian random variable (Rayleigh fading) with its average power that follows an exponentially decaying power delay profile and its path-loss exponent is set as $\lambda = 3$ [36]. We set distances $d_{s1} = 8, d_{s2} = 7$ between the RF source and BD A_1, A_2 , and $d_{1,2} = 3$ between two BDs, respectively. Correspondingly, we set $\alpha = 0.3 + 0.4i$ and $\tau_{h_{s1}} = 8, \tau_{h_{s2}} = 7$ and $\tau_{h_{12}} = 3$, which implies $L = 10$. As mentioned in Section IV, A_1 and A_2 obtain m rounds of the triangle channel information. Next, the estimated sequences are mapped to binary bits with a level crossing algorithm in [11]. Once we have the secret bits, we quantify them by using the following metrics:

1) Mutual Information (MI): measures the mutual dependence between two random variables to verify the feasibility of the constructed triangle channels as shared randomness. A larger MI value indicates a higher key generation rate..

2) Bit Disagreement Ratio (BDR): gives the ratio of the unmatching bit number to the bit sequence length at the two

parties. This BDR, characterizing the robustness of the key generation scheme, should be small.

3) Leaked Information: measures the mutual information among A_1 's estimated sequence, A_2 's estimated sequence and Eve's overheard sequence. It represents the information that could be eavesdropped by Eve.

B. Simulation Results

In the first case, we use all RF signals for key generation ($\rho = 1$) and keep all distances fixed. And we decrease the noise power to increase the signal-to-noise ratio (SNR) with a fixed transmission power of ambient signals ($p = 1$).

We first discuss the performance of key generation with a quasi-static indoor channel. Fig. 3(a) plots the MI of the bit sequences versus the SNR for different parameters, including the length of the OFDM frame and the CP part, and the BD symbol duration K . We observe that under all parameter settings, the MI increases with the growth of SNR by reducing the noise power. And by increasing the length of the OFDM symbol and CP part ($N_{cp} = \frac{1}{4}N$), the bit sequences become more statistically correlated as their MI rises. With another way to make the repeated CP part longer by increasing K , the MI of bit sequences also significantly grows. These indicate MI will improve as the length of the repeated CP part increases, i.e., extending OFDM symbol N or BD symbol duration K . Furthermore, while we decrease the maximum spread by reducing the multi-path channel spread of each channel (by setting $\tau_{h_{s1}} = 4, \tau_{h_{s2}} = 3, \tau_{h_{12}} = 2$ while implying $L = 5$), MI will be improved significantly in the cases with the short length of the CP part, i.e., $N = 64, N_{cp} = 16$. This is because more samples of the CP part can be exploited for obtaining the triangle channel information, which reduces the effect of noise and varied power of CP samples. For example, only 6 samples of the CP part ($N_{cp} = 16$) with $L = 10$ are available, but 11 samples with $L = 5$. But with the longer length of the CP part, the multi-path channel spread has a negligible impact on MI, even slightly weakening the MI performance with large noise (low SNR).

With the same various OFDM parameters above, BDR of bit sequences is illustrated in Fig. 4(a). Likely, BDR declines with the growth of the SNR or by increasing the length of the repeated CP part. And the bit sequences at BDs have a quite low disagreement for all parameters, especially with small noise. Therefore, based on the results of MI and BDR, the proposed scheme is entirely feasible with the BD waveform and the receiver design by using the repeated CP part of OFDM signals.

For other repeated patterns of OFDM signals, such as ZP, OP and 1-0 bit sequence, Fig. 3(b) and Fig. 4(b) show their performance of MI and BDR, respectively. The ZP, with the worst performance, could not be suitable for key generation, since the ZP part with zero power makes BD receive noise signal only in the CP part. But MI performance of OP and bit 1-0 sequence is superior to that of the repeated CP part. This is because the constant signal power of OP or bit 1-0 sequence reduces the disagreement of the sequence of triangle channel estimation at each BD, compared with the varied power of OFDM symbols in the CP part.

In this part, we analyze the performance of key generation with an outdoor channel modeled by a Jakes model [36]. The correlation of the downlink channel and the reciprocity of the

(a) OFDM frame setting (number of FFT and CP), BD symbol duration K and maximum multi-path spread L .

(b) Different repeated patterns of OFDM: Zero padding (ZP), One padding (OP) and 1-0 bit sequence.

(c) Slow fading channel with Doppler frequency $f_d = 10\text{Hz}$.

Fig. 3. (a)(b) MI versus SNR with a quasi-static indoor channel, (c) MI versus time delay with an outdoor channel ($N = 256, L = 1, L = 10$).

(a) OFDM frame setting (number of FFT and CP), BD symbol duration K and maximum multi-path spread L .

(b) Different repeated patterns of OFDM: Zero padding (ZP), One padding (OP) and 1-0 bit sequence.

(c) Fast fading channel with Doppler frequency $f_d = 100\text{Hz}$.

Fig. 4. (a)(b) BDR versus SNR with a quasi-static indoor channel, (c) MI versus time delay with an outdoor channel ($N = 256, L = 1, L = 10$).

inward channel will decay with increasing time delay of two measurements at BDs. As shown in Fig. 3(c) and Fig. 4(c), MI of bit sequences between BDs decreases with the growth of the measurement delay, which makes channels less correlated. Besides, MI will change versus Doppler spread f_d , which determines the time-domain correlation in the channel gain. For example, when the time delay is 0.01s, MI in slow fading channel ($f_d = 10\text{MHz}$) can still get a large positive value, but zero in fast fading channel ($f_d = 100\text{MHz}$) because of the coherence time limitation. Furthermore, MI in the triangle channel model is slightly worse than that in the conventional scheme by using the inward channel only, especially with large noise. That is, the triangle channel model ($h_i h_{j,i} h_{j,j}$), including two additional downlink channels, will introduce more noise than one inward channel model.

Then, we analyze the security of the key generation with the metric SKR under an eavesdropping attacker, which can select two eavesdropping models defined in Eq. (27). Similarly, we compare the SKR performance of the triangle channel with the conventional scheme by using the inward channel. We assume Eve is close to BD A1. If Eve locates more than half a wavelength distance from A1, the correlation between legitimate channels ($h_{1,1}, h_{2,1}$) and the eavesdropping channels ($h_{1,e}, h_{2,e}$) is set as $cor = 0$, which indicates the wireless channels uncorrelated. If Eve is much closer to A1, it will partly obtain a part of legitimate channel information by

assuming the correlation $cor = 0.6$.

Fig. 5 shows SKR increases with the growth of SNR. And the SKR of our scheme under both eavesdropping models ($V|ve^1$ and $V|ve^2$) outperforms the traditional scheme. This is because the triangle channel brings more randomness with more channels, which makes Eve eavesdropping more difficult. Fig. 6 illustrates the advantage from another perspective that the leaked information intercepted by Eve in the inward channel model exceeds that in the triangle channel model. Besides, with $cor = 0$, the eavesdropping capability of Eve with the second eavesdropping model is superior to that with the first model as shown in Fig. 6, making SKR under the second model less than the first model. This is because eavesdropping channels $h_{1,e}$ and $h_{2,e}$ with short distance bring less randomness compared with $h_{2,e}$ and $h_{e,e}$, which makes $h_{1,e} h_{1,1} h_{2,e} h_{2,1}$ selected by Eve, more correlated with the triangle channel $h_{1,1} h_{2,1} h_{2,1}$ than $h_{e,e} h_{2,e} h_{2,1}$. Since channels $h_{2,e}$ and $h_{e,e}$ become more correlated with $h_{2,1}$ and $h_{1,1}$ with the high correlation $cor = 0.6$, Eve with the first overheard model will have a better eavesdropping capability than the second model. This is because it still has an independent channel $h_{1,e}$ in $h_{1,e} h_{1,1} h_{2,e} h_{2,1}$ which introduce more randomness. But, when reducing the eavesdropping distance, the eavesdropper is more likely to be physically detected by A1.

As shown in Fig. 7, we analyze the effect of the distance among BDs and RF source on MI, SKR and leaked informa-

Fig. 5. Secret key rate versus SNR under different eavesdropping models ($N_{FFT} = 256, N_{CP} = 64, K = 1$).

Fig. 6. Leaked information versus SNR under different eavesdropping models ($N_{FFT} = 256, N_{CP} = 64, K = 1$).

Fig. 7. MI, SKR and Leaked information versus SNR with different distances ($\text{cor} = 0$).

Fig. 8. MI - energy harvesting constraint region.

tion. MI and SKR both reduce with the growth of distances, either between the RF source and BDs (d_1, d_2) or between two BDs (d_{12}). The leaked information keeps constant because it only relies on the channel correlation determined by the distance between Eve and BDs. For example, as the distance ($d_{1,2}$) between BDs increases, both MI and SKR decline, due to the reduction of the received signal power. But its effect will diminish with the growth of SNR by reducing the noise power.

Fig. 8 shows the achievable MI- E_{TH} region by solving Eq. (31), which is subject to a tradeoff between MI and energy harvest. Maximizing E_{TH} , which requires to split more signal power for energy harvest, would result in a decline of MI and SKR. Besides, the tradeoff region can be improved by allowing two paired BDs to adjust their own ratio, instead of keeping the same ratio for them. Another observation is that increasing the transmitted power will enlarge the tradeoff region while increasing noise power will lessen it by only decreasing the MI. With the same weight coefficient for key generation and energy harvest, the rectangle area ($K1, K2, K3$) represents the efficiency of received RF signals. As shown in Fig. 8, the area of $K2$ is evidently larger than $K1$ and $K3$. Thus, an optimal power splitting ratio can be obtained to achieve maximum efficiency of received RF signals.

VIII. CONCLUSION AND FUTURE WORK

In this paper, we proposed a novel scheme of physical secret key generation for legitimate BDs over ambient RF signals. By exploiting the repeated (e.g., cyclic prefix in OFDM signals) parts in the ambient signals, we presented a joint design of BD backscatter waveform and receiver to enable BDs to extract the downlink signal and the backscatter signal from the superposed

signal with low complexity. By multiplying the downlink signal and the backscatter signal, BDs can obtain the triangle channel information as shared secret randomness for secret key generation. The tradeoff between secret key generation and energy harvest was also discussed as a joint optimization problem. Finally, the performance of the proposed scheme was evaluated under various signal settings through numerical simulations. The results show that the proposed scheme has great potential to provide a lightweight key sharing solution for securing backscatter communication in low-power AmBC Networks. The proposed scheme can also be implemented by utilizing other repeated patterns embedded in RF signals, such as the time-domain (TD) pilot in OFDM and the PHY preamble in RF signals. In the future, as the dense deployment of BDs in AmBC, lightweight group key generation among multiple BDs deserve further investigation. Besides, physical layer security techniques, such as artificial noise injection and waveform design for securing backscatter communications and improving energy harvesting, and fingerprinting for identity authentication, are other research directions worth studying.

IX. ACKNOWLEDGEMENT

This work was supported in part by the National Natural Science Foundation of China under Grant 62072351; in part by the Academy of Finland under Grant 308087 and Grant 335262; in part by the Shaanxi Innovation Team Project under Grant 2018TD-007; in part by the 111 Project under Grant B16037; and in part by Huawei Technologies Group Co., Ltd; as well as in part by the Commonwealth Cyber Initiative, an investment in the advancement of cyber R&D, innovation and workforce development. For more information about CCI, visit cyberinitiative.org.

REFERENCES

- [1] W. Liu, K. Huang, X. Zhou, and S. Durrani, "Next generation backscatter communication: systems, techniques, and applications," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, pp. 1–11, 2019.
- [2] N. Van 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.
- [3] G. Yang, Y.-C. Liang, R. Zhang, and Y. Pei, "Modulation in the air: Backscatter communication over ambient OFDM carrier," *IEEE Transactions on Communications*, vol. 66, no. 3, pp. 1219–1233, 2018.
- [4] V. Liu, A. Parks, V. Talla, S. Gollakota, D. Wetherall, and J. R. Smith, "Ambient backscatter: Wireless communication out of thin air," *ACM SIGCOMM Computer Communication Review*, vol. 43, no. 4, pp. 39–50, 2013.
- [5] K. Han and K. Huang, "Wirelessly powered backscatter communication networks: Modeling, coverage, and capacity," *IEEE Transactions on Wireless Communications*, vol. 16, no. 4, pp. 2548–2561, 2017.
- [6] X. Lu, H. Jiang, D. Niyato, D. I. Kim, and Z. Han, "Wireless-powered device-to-device communications with ambient backscattering: Performance modeling and analysis," *IEEE Transactions on Wireless Communications*, vol. 17, no. 3, pp. 1528–1544, 2018.
- [7] S. Gong, L. Gao, J. Xu, Y. Guo, D. T. Hoang, and D. Niyato, "Exploiting backscatter-aided relay communications with hybrid access model in device-to-device networks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 4, pp. 835–848, 2019.
- [8] A. Juels, "RFID security and privacy: A research survey," *IEEE journal on selected areas in communications*, vol. 24, no. 2, pp. 381–394, 2006.
- [9] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel, "A survey of lightweight-cryptography implementations," *IEEE Design & Test of Computers*, vol. 24, no. 6, pp. 522–533, 2007.
- [10] T. Chou, S. C. Draper, and A. M. Sayeed, "Secret key generation from sparse wireless channels: Ergodic capacity and secrecy outage," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1751–1764, 2013.
- [11] K. Zeng, "Physical layer key generation in wireless networks: challenges and opportunities," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 33–39, 2015.
- [12] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 240–254, 2010.
- [13] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM journal on computing*, vol. 38, no. 1, pp. 97–139, 2008.
- [14] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," *IEEE Transactions on Mobile Computing*, vol. 12, no. 5, pp. 917–930, 2013.
- [15] M. Chen, S. Chen, and Y. Fang, "Lightweight anonymous authentication protocols for RFID systems," *IEEE/ACM Transactions on Networking*, vol. 25, no. 3, pp. 1475–1488, 2017.
- [16] X. Wang, Z. Su, and G. Wang, "Relay selection for secure backscatter wireless communications," *Electronics Letters*, vol. 51, no. 12, pp. 951–952, 2015.
- [17] B. Defend, K. Fu, and A. Juels, "Cryptanalysis of two lightweight RFID authentication schemes," in *Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PerComW'07)*. IEEE, 2007, pp. 211–216.
- [18] H.-J. Chae, M. Salajegheh, D. J. Yeager, J. R. Smith, and K. Fu, *Maximalist cryptography and computation on the WISP UHF RFID tag*. Springer, 2013, pp. 175–187.
- [19] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 347–376, 2016.
- [20] Q. Yang, H.-M. Wang, Y. Zhang, and Z. Han, "Physical layer security in MIMO backscatter wireless systems," *IEEE Transactions on Wireless Communications*, vol. 15, no. 11, pp. 7547–7560, 2016.
- [21] W. Saad, X. Zhou, Z. Han, and H. V. Poor, "On the physical layer security of backscatter wireless systems," *IEEE transactions on wireless communications*, vol. 13, no. 6, pp. 3442–3451, 2014.
- [22] B. Zhao, H. Wang, and P. Liu, "Safeguarding RFID wireless communication against proactive eavesdropping," *IEEE Internet of Things Journal*, vol. 7, no. 12, pp. 11 587–11 600, 2020.
- [23] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. Part I: Secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.
- [24] Z. Li, Q. Pei, I. Markwood, Y. Liu, and H. Zhu, "Secret key establishment via RSS trajectory matching between wearable devices," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 3, pp. 802–817, 2018.
- [25] H. Liu, J. Yang, Y. Wang, Y. Chen, and C. E. Koksai, "Group secret key generation via received signal strength: Protocols, achievable rates, and implementation," *IEEE Transactions on Mobile Computing*, vol. 13, no. 12, pp. 2820–2835, 2014.
- [26] P. Xu, K. Cumanan, Z. Ding, X. Dai, and K. K. Leung, "Group secret key generation in wireless networks: Algorithms and rate optimization," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 8, pp. 1831–1846, 2016.
- [27] C. D. T. Thai, J. Lee, J. Prakash, and T. Q. S. Quek, "Secret group-key generation at physical layer for multi-antenna mesh topology," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 1, pp. 18–33, 2019.
- [28] C. Boyer and S. Roy, "Space time coding for backscatter RFID," *IEEE Transactions on Wireless Communications*, vol. 12, no. 5, pp. 2272–2280, 2013.
- [29] S. S. Haykin, *Digital communications*. Wiley New York, 1988.
- [30] J. Zhang, B. He, T. Q. Duong, and R. Woods, "On the key generation from correlated wireless channels," *IEEE Communications Letters*, vol. 21, no. 4, pp. 961–964, 2017.
- [31] A. Goldsmith, *Wireless communications*. Cambridge university press, 2005.
- [32] T. Hwang, C. Yang, G. Wu, S. Li, and G. Y. Li, "OFDM and its wireless applications: A survey," *IEEE transactions on Vehicular Technology*, vol. 58, no. 4, pp. 1673–1694, 2008.
- [33] E. Global, "EPC radio-frequency identity protocols class-1 generation-2 UHF RFID protocol for communications at 860 MHz-960 MHz," *Version*, vol. 1, no. 0, p. 23, 2008.
- [34] M. Morelli, C. Kuo, and M. Pun, "Synchronization techniques for orthogonal frequency division multiple access (OFDMA): A tutorial review," *Proceedings of the IEEE*, vol. 95, no. 7, pp. 1394–1427, 2007.
- [35] L. Lai, Y. Liang, and H. V. Poor, "A unified framework for key agreement over wireless fading channels," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 480–490, 2012.
- [36] Y. S. Cho, J. Kim, W. Y. Yang, and C. G. Kang, *MIMO-OFDM wireless communications with MATLAB*. John Wiley & Sons, 2010.