# Parasitic Communication: Opportunistic Utilization of Interference Using Asymmetric Demodulation

Zhao Li, *Senior Member, IEEE*, Lijuan Zhang, Kang G. Shin, *Life Fellow, IEEE*, Jia Liu, *Senior Member, IEEE*, Yicheng Liu, *Graduate Student Member, IEEE*, Pintian Lyu, and Zheng Yan, *Fellow, IEEE*

***Abstract*—With the rapid advancement of wireless communication technologies, interference has become a key impediment to the improvement of wireless data transmission performance. Traditional interference management (IM) suppresses or adjusts interference at the cost of additional communication resources *without* exploiting interference effectively. Moreover, wirelessly transmitted data is susceptible to eavesdropping. To address these issues cooperatively, we propose *Opportunistic Parasitic Communication with Asymmetric Demodulation*(OPC-AD). In particular, we consider the interference experienced by the intended/target communication (i.e., parasitic) receiver (Rx) as the host signal. The target communication constructs a selection signal carrying parasitic indication information based on the data it intends to send and the data decoded by its Rx using asymmetric demodulation from the host signal, and then sends it to its Rx. This signal is used to instruct the parasitic Rx to extract the desired information from the host signal. OPC-AD allows for the exploitation of the interference (i.e., host signal) for data transmission to an interfered Rx. Using AD can also ensure the privacy of the host communication. Since the parasitic communication is concealed within the host signal, eavesdroppers cannot compromise the confidentiality of the parasitic transmission without precisely decoding the selection signal. Furthermore, considering more practical situations, we extend the OPC-AD design to cover a broader range of realistic scenarios. Our experimental results validate the applicability of OPC-AD, while our in-depth simulations demonstrate that parasitic communication can effectively thwart eavesdropping and achieve higher spectral efficiency (SE) than other existing IM methods, particularly in strong interference environments.**

Received 23 December 2024; revised 27 May 2025; accepted 16 June 2025. Date of publication 20 June 2025; date of current version 3 October 2025. This work was supported in part by the National Natural Science Foundation of China under Grant 62072351, Grant U23A20300, and Grant 62202359, in part by the 111 Center under Grant B16037, in part by JSPS KAKENHI under Grant JP25K15087, in part by the Science and Technology Research Project of Henan Province under Grant 252102211120, in part by the Project of Cyber Security Establishment with Inter-University Cooperation, in part by the Key Research Project of Shaanxi Natural Science Foundation under Grant 2023-JC-ZD-35, and in part by the U.S. National Science Foundation under Grant 2245223. Recommended for acceptance by F. Liu. *(Corresponding author: Jia Liu.)*

Zhao Li is with the School of Cyber Engineering, Xidian University, Xi'an 710126, China, and also with the School of Electronics and Information, Zhengzhou University of Light Industry, Zhengzhou 450001, China (e-mail: zli@xidian.edu.cn).

Lijuan Zhang, Yicheng Liu, Pintian Lyu, and Zheng Yan are with the School of Cyber Engineering, Xidian University, Xi'an 710126, China (e-mail: zyan@xidian.edu.cn).

Kang G. Shin is with the Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI 48109 USA (e-mail: kgshin@umich.edu).

Jia Liu is with the Center for Strategic Cyber Resilience Research and Development, National Institute of Informatics, Tokyo 101-8430, Japan (e-mail: jliu@nii.ac.jp).

Digital Object Identifier 10.1109/TMC.2025.3581798

***Index Terms*—Interference, parasitic communication, asymmetric demodulation, device-to-device, spectral efficiency.**

## I. Introduction

As mobile communication technology has entered the 5 G/6 G era, significant improvements in data transmission speed, latency, and connection density are anticipated [1]. However, to support large-scale data services and cater to the connectivity needs of intelligent devices, 5 G/6 G networks need denser deployment of base stations and wireless access points. This, in turn, creates more severe interferences than earlier-generation mobile communication technologies. Consequently, effective Interference Management (IM) becomes a crucial issue to be addressed. Furthermore, given the broadcast nature of wireless media, eavesdroppers within the coverage area of legitimate transmissions can intercept and decode the desired signals, thereby threatening communication security. Therefore, it is also crucial to enhance the security of wireless communications to effectively counteract eavesdropping activities.

To date, there have been numerous IM methods, including Successive Interference Cancellation (SIC) [2], Zero-Forcing (ZF) reception [3], Interference Neutralization (IN) [4], Interference Steering (IS) [5], etc. Of them, IN generates a neutralizing signal to counteract the disturbance, achieving interference-free reception of the desired signal. IS constructs a steering signal to adjust the interference into a subspace orthogonal to the desired signal at the interfered Rx, enabling interference-free recovery of the desired data. By focusing on the effective portion of the interference to the desired transmission, IS can consume less transmit power than IN.

Note that most conventional IM methods consider interference as harmful and thus focus on its elimination. However, with the advancement of research, researchers have recognized that in practice, interference often carries useful data from other users. This observation has triggered research on interference utilization. Among these designs, Energy Harvesting (EH) [6] converts ambient radio frequency (RF) interference to usable energy for communication devices. However, EH suffers from low efficiency of converting RF to electrical energy and does not leverage the data carried by the interference. The authors of [7] proposed Interference ReCycling (IRC), which leverages the interactions between interference and a generated recycling signal to transform the interference into a useful signal that carries the desired data. However, the effectiveness of IRC depends on the spatial characteristics of the interference and communication channels, and IRC may not be feasible when there is an insufficient power budget. Therefore, exploring novel ways of utilizing interference is of practical significance.

On the other hand, the open nature of the communication environment makes wireless transmissions more susceptible to malicious attacks compared to wired communications [8]. While encryption and decryption can enhance the security of data transmissions, they require computational resources [9] and introduce processing delays [10]. Additionally, key management, which involves both the generation and distribution of encryption keys, is a critical issue that must be addressed in implementing such methods [11]. It is important to note that security strategies based on cryptography achieve protection by increasing the computational cost for attackers attempting to decrypt data. However, traditional cryptographic strategies face significant challenges as attackers' computational power continues to increase.

In recent years, Physical-layer Security (PLS) has garnered widespread attention by securing communications through suppressing the received signal-to-noise ratio/signal-to-interference-plus-noise ratio (SNR/SINR) at the eavesdropper. The authors of [12] demonstrated that secure data transmission can be achieved when the channel capacity of the legitimate communication link exceeds the wiretap link's channel capacity between the legitimate Tx and the eavesdropper. The utilization of Artificial Noise (AN) for secure communication was first proposed in [13], where a portion of the transmit power is used to generate AN. This AN can disrupt eavesdroppers without affecting the desired communication. However, it consumes transmit power and may degrade the quality of other legitimate communications. Secure Beamforming (BF) technology confines legitimate communication within a specific beam range to reduce energy leakage of legitimate signals, enabling the legitimate Rx to obtain significantly higher received signal strength than the eavesdropper, thereby enhancing confidentiality [8]. However, the beamforming design problem is typically non-convex and non-concave, leading to high algorithm complexity. Additionally, implementing BF requires multiple antennas at the Tx, increasing hardware costs. Moreover, if eavesdroppers can determine the spatial location of the legitimate communication pair, they can eavesdrop on the legitimate communication link. PLS key techniques generate secure keys based on wireless channel characteristics [14], avoiding the key distribution challenges faced by traditional cryptographic methods. However, this method necessitates accurate channel estimation within coherent time. When channels change rapidly, it increases the complexity and cost of channel estimation. Attackers can disrupt the reciprocity of channel state estimation for the legitimate communication pair, rendering this method ineffective. To summarize, existing PLS methods still have their limitations. Developing a low-cost and robust PLS strategy is of significant research importance.

The aforementioned research only focuses on designing methods to address interference or eavesdropping threats individually. However, in practical communication scenarios, both of these threats may coexist. Therefore, developing a method that addresses both IM and eavesdropping defense simultaneously is of significant importance. The authors of [15] introduced an Immunizing Coding (iCoding) method that combines IM with Secure Communication (SC). With this approach, the desired Tx designs the transmitted data based on the desired data and interference characteristics so that the impact of interference at the intended Rx can be eliminated. The transmitted data, after undergoing immunizing coding, differs from the desired data, effectively preventing eavesdroppers from recovering the desired data. [16] presented a signal processing method that integrates SC and IM, where the desired Tx generates an IM signal to interact with interference at the desired Rx to achieve IM, while simultaneously disrupting eavesdropping to enable SC. Nevertheless, both of the above methods treat interference as a detrimental factor affecting communication, thus employing adversarial management strategies to eliminate it, without effectively utilizing interference.

Recognizing that interference usually carries undesired data from other communicating pairs, we propose an *Opportunistic Parasitic Communication with Asymmetric Demodulation* (OPC-AD) to facilitate the direct extraction of useful data from the interfering signal and achieve PLS simultaneously. OPC-AD treats the interference as the host signal. Consequently, the interfering Tx and Rx function as the host Tx and Rx, respectively. The target communication pair is disrupted by this interference. Unlike conventional transmission schemes where the target Tx directly transmits the desired signal, OPC-AD allows the target Tx to transmit a selection signal carrying "instructive" information to its intended Rx. Using such instructive/indication information, the target/interfered Rx can extract its desired data from the interference. Since the target communication is achieved by exploiting the interference (i.e., parasitizing on the host signal), we refer to it as *Parasitic Communication* (PC), involving the corresponding parasitic Tx and Rx. In addition, as the parasitic Rx directly detects the host signal, in order to prevent the unintended parasitic Rx from decoding the complete host information, we employ AD at the parasitic Rx. Specifically, we let the parasitic Rx detect the interference using a lower demodulation order than the modulation order used by the host communication pair, ensuring the privacy of the host communication. Furthermore, by having the parasitic Tx transmit a selection signal instead of its actual data, the proposed method can effectively enhance the PLS of the target communication.

The contributions of this paper are three-fold:

- Proposal of Parasitic Communication (PC). With PC, the parasitic Tx sends a selection signal carrying parasitic indication information. The parasitic Rx then extracts the desired data from the host signal (interference) based on this indication information. PC effectively utilizes the energy and data information carried by interference. Moreover, as the parasitic Tx transmits a selection signal rather than the desired signal, the security of the parasitic communication pair is ensured.
- Proposal of Asymmetric Demodulation (AD). In this method, the parasitic Rx employs a demodulation scheme with a lower modulation order compared to the host

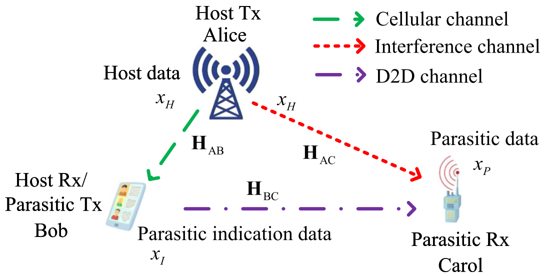


Fig. 1. System model.

communication pairs, allowing the parasitic Rx to detect the host signal but only recover partial host data, thereby ensuring the privacy of the host communication pair.

- Extended design of PC to more general scenarios. First, we present a method for implementing PC in the presence of time delay differences between the host and the parasitic communication pairs. Second, we extend the implementation of PC to more general modulation schemes. Finally, we propose Complete PC (CPC), which can achieve a 100% success probability for PC.

The rest of this paper is organized as follows. Section II describes the system model, while Section III presents the design of OPC-AD. Section IV explores the extended design of PC. Section V evaluates the performance of the proposed methods via USRP experiments and MATLAB simulations. Finally, we conclude this paper in Section VI.

Throughout this paper, we will use the following notations. Vectors and matrices are represented by lower- and upper-case bold letters. $(\cdot)^H$ denotes Hermitian; $\|\cdot\|$ and $|\cdot|$ denote the Frobenius norm and absolute value; and $\mathrm{E}(\cdot)$ represents the mathematical expectation.

## II. System Model

We consider the coexistence of device-to-device (D2D) communication with cellular downlink transmission.[1] As shown in Fig. 1, Alice is the base station (BS), Bob and Carol are mobile terminals. Alice and Bob form a downlink transmission pair, while Bob[2] simultaneously transmits data to Carol using D2D. Since Carol is within the coverage of Alice's signal, she experiences interference from Alice. To realize PC, we designate Alice as the host Tx. Bob functions as both host Rx and parasitic Tx simultaneously.[3] Meanwhile, Carol serves as the parasitic Rx.

Let $P_{t_1}$ and $P_{t_0}$ be the transmit power of Alice and Bob, respectively. Alice, Bob, and Carol are each equipped with $N_{\rm A}$, $N_{\rm B}$ and $N_{\rm C}$ antennas. We denote the data transmitted from Alice to Bob as $x_H$, satisfying $\mathrm{E}(|x_H|^2) = 1$. $x_H$ is generated using $M_{\rm H}$-order modulation. Accordingly, Bob decodes his desired data using $M_{\rm H}$-order demodulation. We assume that Bob intends to transmit data $x_P$ (satisfying $\mathrm{E}(|x_P|^2) = 1$) to Carol, where $x_P$ is a modulated symbol of order $M_{\rm P}$ ($M_{\rm P} \leq M_{\rm H}$). To avoid conflicts with, and achieve effective utilization of, the interference caused by Alice, we employ $M_{\rm P}$-order demodulation for Carol to detect the interference (i.e., host signal). Thus, Bob generates and transmits a selection signal carrying indication information $x_I$ (using $M_{\rm I}$-order modulation) in terms of the data Carol decodes from the host signal using $M_{\rm P}$-order demodulation (denoted as $\hat{x}_H$) and $x_P$, to Carol. This information can guide Carol in processing the decoded data from the interference. We assume that the processing delay for decoding $x_H$ and generating the selection signal at Bob is negligible [19].

We use $\mathbf{H}_{\rm AB}$ to denote the communication channel between Alice and Bob, while $\mathbf{H}_{\rm AC}$ represents the interference channel from Alice to Carol. The D2D link from Bob to Carol is denoted as $\mathbf{H}_{\rm BC}$. We use a spatially uncorrelated Rayleigh fading model to characterize the aforementioned channels, where the elements are independent and identically distributed complex Gaussian random variables with zero mean and unit variance. The channels are mutually independent and exhibit block fading characteristics [7]. We assume that Alice, Bob, and Carol can accurately acquire the channel state information (CSI) for implementing our methods.

## III. Design of OPC-AD

As mentioned earlier, under OPC-AD, the parasitic Tx (i.e., Bob) constructs and transmits a selection signal carrying indication information based on the desired data for the parasitic Rx (i.e., Carol) and the data it recovers from the host signal (i.e., interference), to the parasitic Rx. The parasitic Rx utilizes a demodulation method with a lower order than that of the modulation scheme employed by the host communication to detect the host signal. This allows the parasitic Rx to opportunistically extract the desired data from the host signal in terms of the indication information. Without loss of generality, we assume that both the host and parasitic communications employ multiple-input multiple-output (MIMO) transmission mechanism, i.e, $N_{\rm A} \geq 2$, $N_{\rm B} \geq 4$ (this enables Bob to receive with at least two antennas and transmit with the other multiple antennas simultaneously), and $N_{\rm C} \geq 2$ (this allows Carol to distinguish the selection signal and host signal in the spatial domain) should hold. Then, the received signal at Bob can be expressed as:

$$\mathbf{y}_{\rm B} = \sqrt{P_{t_1}}\mathbf{H}_{\rm AB}\mathbf{p}_{\rm A}x_H + \mathbf{n}_{\rm B}, \tag{1}$$

where the first term on the right-hand side (RHS) of Eq. (1) represents the desired signal of Bob originating from Alice. $\mathbf{p}_{\rm A}$ denotes the precoding vector at Alice. $\mathbf{n}_{\rm B}$ is the additive white Gaussian noise (AWGN) vector whose elements have zero mean and variance $\sigma_n^2$. Without loss of generality, we use Singular Value Decomposition (SVD) based precoding and filter design as an example, i.e., we apply SVD to $\mathbf{H}_{\rm AB}$ to obtain $\mathbf{H}_{\rm AB} =$

[1] This scenario is just one use case of our method. However, our method is not restricted to cellular systems and D2D communication.

[2] To enhance spectrum utilization efficiency, we let Bob employ in-band full-duplex (IBFD) to simultaneously receive signal from Alice and transmit signal to Carol through the same frequency channel [17]. Bob can mitigate the self-interference caused by his transmitter module to his receiver module by employing techniques such as passive suppression [18]. It is worth noting that existing full-duplex research often assumes the source and destination are identical. However, in practice, full-duplex transmission can be more flexible, as illustrated in our system model.

[3] This setup avoids interference data sharing between the host Rx and the parasitic Tx, thereby facilitating the application of the proposed method.

$\mathbf{U}_{\mathrm{AB}}\boldsymbol{\Sigma}_{\mathrm{AB}}\mathbf{V}_{\mathrm{AB}}^H$, and select the first column vector $\mathbf{v}_{\mathrm{AB}}^{(1)}$ from the right singular matrix $\mathbf{V}_{\mathrm{AB}}$ as the precoding vector, i.e., $\mathbf{p}_{\mathrm{A}} = \mathbf{v}_{\mathrm{AB}}^{(1)}$. Bob uses matched filtering to detect the signal from Alice. The first column vector $\mathbf{u}_{\mathrm{AB}}^{(1)}$ from the left singular matrix $\mathbf{U}_{\mathrm{AB}}$ is chosen as the filter vector $\mathbf{f}_{\mathrm{B}}$. Consequently, the estimated signal of Bob is:

$$\hat{y}_{\mathrm{B}} = \sqrt{P_{t_1}}\mathbf{f}_{\mathrm{B}}^H\mathbf{H}_{\mathrm{AB}}\mathbf{p}_{\mathrm{A}}x_H + \mathbf{f}_{\mathrm{B}}^H\mathbf{n}_{\mathrm{B}}. \tag{2}$$

While receiving the signal from Alice, the full-duplexed Bob also intends to transmit to Carol. However, Carol experiences interference from Alice. With OPC-AD, Bob no longer transmits the desired data $x_P$ to Carol; instead, he constructs a selection signal containing indication information $x_I$ and sends it to Carol. $x_I$ can be calculated according to Eq. (3) as:

$$x_I = (x_P^{(1)} \odot \hat{x}_{H_B}^{(1)}) \wedge (x_P^{(2)} \odot \hat{x}_{H_B}^{(2)}) \wedge \cdots \wedge (x_P^{(n)} \odot \hat{x}_{H_B}^{(n)}), \tag{3}$$

where $\hat{x}_{H_B}$ represents the data that Bob can recover[4] from the interference. $x_P^{(i)}$ and $\hat{x}_{H_B}^{(i)}$ ($i \in \{1, 2, \ldots, n\}$) denote the $i$th bit of $x_P$ and $\hat{x}_{H_B}$, respectively. $n = \log_2 M_{\mathrm{P}}$ where $M_{\mathrm{P}}$ is the demodulation order of Carol. The symbols $\odot$ and $\wedge$ represent the logical Exclusive NOR (XNOR) and logical AND operations.[5] It is important to note that under $M_{\mathrm{I}} = 2$, $x_I$ contains only 1 b indicating the status of PC. Specifically, $x_I \in \{0, 1\}$, where "0" and "1" indicate the failure and success of PC, respectively. When Carol decodes $\hat{x}_I = 0$, she should discard the recovered $\hat{x}_{H_C}$, where $\hat{x}_{H_C}$ represents the data that Carol recovers from the interference. Conversely, when $\hat{x}_I = 1$, Carol should keep the decoded $\hat{x}_{H_C}$. This way, Carol can extract the desired data from the interference (i.e., host signal).

The signal received by Carol can be expressed as:

$$\mathbf{y}_{\mathrm{C}} = \sqrt{P_{t_1}}\mathbf{H}_{\mathrm{AC}}\mathbf{p}_{\mathrm{A}}x_H + \sqrt{P_{t_0}}\mathbf{H}_{\mathrm{BC}}\mathbf{p}_{\mathrm{B}}x_I + \mathbf{n}_{\mathrm{C}}, \tag{4}$$

where the first term on the RHS of Eq. (4) represents the host signal (i.e., interference) from Alice. The second term denotes the selection signal from Bob, where $\mathbf{p}_{\mathrm{B}}$ is the precoding vector that Bob uses to process $x_I$. $\mathbf{n}_{\mathrm{C}}$ is the AWGN vector. We take SVD based signal processing as an example. Then, Bob applies SVD to $\mathbf{H}_{\mathrm{BC}}$ and selects the first column vector of its right singular matrix as $\mathbf{p}_{\mathrm{B}}$.

Carol needs to detect the selection signal and the host signal separately. To achieve this objective, Carol can employ ZF reception without loss of generality. Specifically, Carol designs two filter vectors $\overline{\mathbf{f}}_{\mathrm{C}}^{(1)}$ and $\overline{\mathbf{f}}_{\mathrm{C}}^{(2)}$ such that $\overline{\mathbf{f}}_{\mathrm{C}}^{(1)}$ is orthogonal to the spatial feature of the selection signal, denoted as $\mathbf{d}_{\mathrm{S}} = \frac{\mathbf{H}_{\mathrm{BC}}\mathbf{p}_{\mathrm{B}}}{||\mathbf{H}_{\mathrm{BC}}\mathbf{p}_{\mathrm{B}}||}$, and $\overline{\mathbf{f}}_{\mathrm{C}}^{(2)}$ is orthogonal to the spatial characteristic of the host signal, denoted as $\mathbf{d}_{\mathrm{H}} = \frac{\mathbf{H}_{\mathrm{AC}}\mathbf{p}_{\mathrm{A}}}{||\mathbf{H}_{\mathrm{AC}}\mathbf{p}_{\mathrm{A}}||}$. Then, $\overline{\mathbf{f}}_{\mathrm{C}}^{(1)}$ and $\overline{\mathbf{f}}_{\mathrm{C}}^{(2)}$ can be calculated by following $\overline{\mathbf{f}}_{\mathrm{C}}^{(1)} = \mathbf{d}_{\mathrm{H}} - \frac{\mathbf{d}_{\mathrm{S}}^H\mathbf{d}_{\mathrm{H}}}{\mathbf{d}_{\mathrm{S}}^H\mathbf{d}_{\mathrm{S}}}\mathbf{d}_{\mathrm{S}}$ and $\overline{\mathbf{f}}_{\mathrm{C}}^{(2)} = \mathbf{d}_{\mathrm{S}} - \frac{\mathbf{d}_{\mathrm{H}}^H\mathbf{d}_{\mathrm{S}}}{\mathbf{d}_{\mathrm{H}}^H\mathbf{d}_{\mathrm{H}}}\mathbf{d}_{\mathrm{H}}$, respectively. To avoid additional power amplification or attenuation at Carol, we need to normalize $\overline{\mathbf{f}}_{\mathrm{C}}^{(1)}$ and $\overline{\mathbf{f}}_{\mathrm{C}}^{(2)}$ to yield $\mathbf{f}_{\mathrm{C}}^{(1)}$ and $\mathbf{f}_{\mathrm{C}}^{(2)}$. We use $\mathbf{f}_{\mathrm{C}} = [\mathbf{f}_{\mathrm{C}}^{(1)}\mathbf{f}_{\mathrm{C}}^{(2)}]$ to denote Carol's filter matrix. Consequently, Carol's estimated signal after filtering can be expressed as:

$$\hat{\mathbf{y}}_{\mathrm{C}} = \sqrt{P_{t_1}}\mathbf{f}_{\mathrm{C}}^H\mathbf{H}_{\mathrm{AC}}\mathbf{p}_{\mathrm{A}}x_H + \sqrt{P_{t_0}}\mathbf{f}_{\mathrm{C}}^H\mathbf{H}_{\mathrm{BC}}\mathbf{p}_{\mathrm{B}}x_I + \mathbf{f}_{\mathrm{C}}^H\mathbf{n}_{\mathrm{C}}. \tag{5}$$

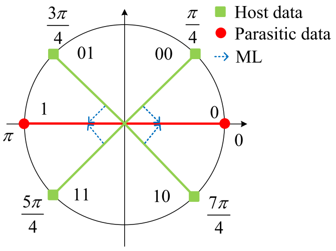


Fig. 2. Illustration of the principle of AD.

So far, we have discussed the design of PC under the assumption that the host signal is modulated with order $M_{\mathrm{H}}$ while the parasitic Rx demodulates the host signal with order $M_{\mathrm{P}}$. If $M_{\mathrm{P}} = M_{\mathrm{H}}$, Carol may access the complete host information, thus compromising the privacy of the host communication. To avoid this deficiency, we utilize AD to restrict $M_{\mathrm{P}}$ to be lower than $M_{\mathrm{H}}$. Consequently, even if Carol continuously demodulates the host signal, she remains unable to access the complete host information.

In what follows, we will first demonstrate the feasibility of AD and then analyze the performance of OPC-AD. As an example, we consider using Quadrature Phase Shift Keying (QPSK) for the host transmission and BPSK for parasitic transmission (where Carol detects the host signal using a demodulation scheme associated with BPSK). As plotted in Fig. 2, the desired constellation points for Carol correspond to phases 0 and $\pi$ (representing baseband information "0" and "1", respectively), both of which can be demodulated from the QPSK constellation points following the maximum likelihood (ML) criterion. For instance, to obtain the BPSK constellation point with phase 0, Carol can apply ML to the QPSK host constellation points with phases $\frac{\pi}{4}$ and $\frac{7\pi}{4}$. Therefore, AD can be used to decode partial information[6] from the host signal for parasitic communication purposes.

It should be noted that $M_{\mathrm{P}}$ cannot be greater than $M_{\mathrm{H}}$ when using OPC-AD. This is because when employing a high-order ($M_{\mathrm{P}}$) demodulation scheme to detect a low-order ($M_{\mathrm{H}}$) modulated signal, multiple high-order parasitic data symbols will correspond to one low-order host data symbol. This results in non-unique mapping, rendering OPC-AD inapplicable. Moreover, due to the stochastic nature of the source data, PC may

[4] The demodulation scheme that Bob utilizes to decode $\hat{x}_{H_B}$ should be identical to that Carol uses for detecting the host signal.

[5] Since the design of $x_I$ essentially involves a comparison between $x_P$ and $x_H$ for equality, the time complexity is $O(1)$, leading to minimal computational latency that can be considered negligible.

[6] This does not imply that Carol can compromise the secrecy of the host transmission. As illustrated in Fig. 2, when Carol demodulates the BPSK constellation points with phases of 0 or $\pi$, she can only correctly decode the second bit, i.e., "0" or "1", carried by the QPSK symbol, while the first bit of the host QPSK symbol remains inaccessible to her. Specifically, the decoding error for the first bit can be as high as 50% when Carol applies AD. The larger the difference between $M_{\mathrm{H}}$ and $M_{\mathrm{P}}$, the greater the privacy preserved for host communication. This is because the parasitic Rx can decode only $\log_2 M_{\mathrm{P}}$ bits per host symbol. Consequently, with a smaller $M_{\mathrm{P}}$, more host information remains confidential to the parasitic Rx. However, this reduction in $M_{\mathrm{P}}$ will decrease the efficiency of parasitic data transmission.

TABLE I
COMPARISON OF OPC-AD WITH OTHER IM METHODS

| Characteristic \ Method | IN | IS | ZF | SIC | EH | IRC | OPC-AD |
|---|---|---|---|---|---|---|---|
| Need for spatial DoF for interference transmission | ✗ | ✓ | ✓ | ✗ | ✗ | ✗ | ✓ |
| Power cost for IM | ✓ | ✓ | ✗ | ✗ | ✗ | ✓ | ✓ |
| Iteration processing and error propagation | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ |
| Exploitation of interference energy | ✗ | ✗ | ✗ | ✗ | ✓ | ✓ | ✓ |
| Exploitation of interference data | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ | ✓ |
| Secrecy of Communication | ✓ | ✗ | ✗ | ✗ | ✗ | ✓ | ✓ |
| Inapplicability due to strong interference | ✓ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ |

encounter failures. Continuing with the example depicted in Fig. 2, if the phase of the parasitic BPSK symbol that Bob intends to transmit to Carol is 0, while the phase of the host QPSK symbol is $\frac{3\pi}{4}$ or $\frac{5\pi}{4}$, the D2D communication will not be achieved using PC. In this example, it can be easily derived that the probability of successful parasitism is 50% . When we extend to more general PSK scenarios, where a $M_{\mathrm{P}}$PSK ($M_{\mathrm{P}}$-ary PSK) signal parasitizes on a $M_{\mathrm{H}}$PSK ($M_{\mathrm{H}}$-ary PSK) host signal, with the condition that $M_{\mathrm{P}} < M_{\mathrm{H}}$ is satisfied, we can derive that the probability of successful parasitism is $p = \frac{1}{M_{\mathrm{P}}}$. Additionally, we can also derive that the number of bits transmitted in a single parasitism is $\log_2 M_{\mathrm{P}}$.

Carol's SE, denoted as $r_C$ is constrained by both the capacity of the host signal transmission from Alice to Carol ($r_{AC}$) and the capacity of selection signal from Bob to Carol ($r_{BC}$). This is because in our design, we assume that Bob can accurately decode $x_H$ (i.e, $\hat{x}_{H_B} = x_H$ holds) from the signal sent by Alice and generate $x_I$ based on the desired data $x_P$ that he intends to transmit to Carol. If Bob cannot achieve this, he will be unable to produce the correct $x_I$, rendering PC infeasible. Moreover, since both Bob and Carol are mobile terminals in the system model, it is reasonable to assume that if Carol experiences strong interference from Alice, Bob, as Alice's intended recipient, can successfully decode $x_H$. Therefore, the transmission link from Alice to Bob is not a bottleneck for Carol's reception performance when applying PC. Consequently, when calculating Carol's data rate, we only consider $r_{AC}$ and $r_{BC}$ as given below:

$$\begin{cases} r_{AC} = \log_2(1 + P_{t_1} \|\mathbf{f}_{\mathrm{C}}^H \mathbf{H}_{\mathrm{AC}} \mathbf{p}_{\mathrm{A}}\|^2 / \sigma_n^2) \\ r_{BC} = \log_2(1 + P_{t_0} \|\mathbf{f}_{\mathrm{C}}^H \mathbf{H}_{\mathrm{BC}} \mathbf{p}_{\mathrm{B}}\|^2 / \sigma_n^2) \end{cases}. \tag{6}$$

Since each indication data corresponds to a host data, the achievable SE of Carol under OPC-AD weighted by $p$ is given below:

$$r_C = p \min\left\{ r_{AC}, \frac{\log_2 M_{\mathrm{P}}}{\log_2 M_{\mathrm{I}}} r_{BC} \right\}. \tag{7}$$

We can observe from Eq. (7) that $r_C$ primarily relies on $M_{\mathrm{P}}$, $r_{AC}$, and $r_{BC}$,[7] while being restricted by $p$. Additionally, when the interference (i.e., host signal) is strong, OPC-AD can achieve a high SE. In this scenario, leveraging interference is more advantageous than combating interference.

Table I compares OPC-AD with other typical IM methods, where symbols ✓and ✗ denote "having" and "not having" the corresponding characteristics, respectively. We can conclude from the table that OPC-AD can make full use of both interference data and energy. Moreover, strong interference can enhance the effectiveness of OPC-AD. Since both OPC-AD and IRC avoid directly transmitting the desired data, they can provide security against malicious users. The key distinction between these two methods lies in their design principles. In IRC, a recycling signal is generated and interacts with the interference at the interfered Rx, allowing the Rx to extract the desired data from the combined recycling signal and interference. In contrast, OPC-AD does not exploit the interaction between the host signal and the selection signal. Instead, the parasitic Rx must simultaneously detect both the host signal and the selection signal, demodulate them separately, and then use the parasitic indication information to select the desired data from the decoded interference data. Additionally, in the application of IRC, when the interference is too strong, there may be insufficient power to generate a strong enough recycling signal to convert the interference into a signal carrying the desired data, rendering the method ineffective. It is worth noting that our method can be effectively integrated with other IM methods. In scenarios with strong interference, where more interference can be leveraged, OPC-AD is more suitable for managing interference. Conversely, when the interference is weaker and less exploitable, it is more appropriate to employ classical IN or similar methods for IM.

## IV. GENERALIZATION OF PARASITIC COMMUNICATION

In this section, we first present an Offset PC (OFS-PC) with the consideration of the differences in both small-scale and large-scale fading between the selection signal and the host signal. Next, we will discuss the design of OPC-AD under more general modulation schemes. Then, to address the issue of the parasitic success probability being less than 1 for AD-OPC, we design Complete PC (CPC), which can elevate the parasitic success probability to 100% . In the end, we discuss the design of PC when multiple host transmissions can be exploited.

### A. Design of OFS-PC

The current design of parasitic communication has not accounted for the delay/phase difference between the host

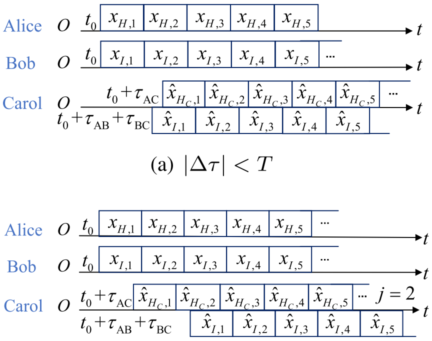
[7] It should be noted that $r_{AC}$ represents Carol's demodulation rate for $\hat{x}_{H_C}$. Although Bob intends to transmit $x_P$ to Carol, in the context of OPC-AD, Carol retrieves $x_P$ by demodulating $\hat{x}_{H_C}$ from Alice's interference and $\hat{x}_I$ from Bob's selection signal. She then extracts $x_P$ from $\hat{x}_{H_C}$ based on $\hat{x}_I$, as described below Eq. (3). Consequently, Carol's achievable rate $r_C$ is constrained by both $r_{AC}$ and $r_{BC}$.

signal and the selection signal reaching Carol. Consequently, the decoded $\hat{x}_I$ and $\hat{x}_{H_C}$ can ideally align, enabling the use of OPC-AD. However, in practice, due to the differences in channel conditions (i.e., small-scale fading denoted as $\tau_{\mathrm{S}}$) and various propagation path lengths (i.e., large-scale fading represented by $\tau_{\mathrm{L}}$), the aforementioned two signal components may arrive at Carol synchronously.[8] In such a case, the parasitic Tx needs to perform pre-alignment based on the estimation of $\tau_{\mathrm{S}}$ and $\tau_{\mathrm{L}}$, so that $x_I$ can be accurately associated with $\hat{x}_{H_C}$. Without loss of generality, we assume that the baseband symbol rates of the selection signal and the host signal are identical, denoted as $1/T$, where $T$ represents the symbol period of $x_I$ ($\hat{x}_I$) and $x_H$ ($\hat{x}_{H_C}$).

To conduct pre-alignment, Bob needs to know the locations of Alice and Carol, as well as $\mathbf{H}_{\mathrm{AC}}$, $\mathbf{H}_{\mathrm{AB}}$ and $\mathbf{H}_{\mathrm{BC}}$. We define the equivalent channel conditions between Alice and Bob, Alice, and Carol, and Bob and Carol as $\mathbf{f}_{\mathrm{B}}^H\mathbf{H}_{\mathrm{AB}}\mathbf{p}_{\mathrm{A}}$, $\mathbf{f}_{\mathrm{C}}^H\mathbf{H}_{\mathrm{AC}}\mathbf{p}_{\mathrm{A}}$, and $\mathbf{f}_{\mathrm{C}}^H\mathbf{H}_{\mathrm{BC}}\mathbf{p}_{\mathrm{B}}$, respectively. From these channel conditions, Bob can determine the phase offsets caused by small-scale fading as $\Delta\varphi_{\mathrm{AB}}$, $\Delta\varphi_{\mathrm{AC}}$ and $\Delta\varphi_{\mathrm{BC}}$. Then, the small-scale delays can be derived as $\tau_{\mathrm{S\_AB}} = \Delta\varphi_{\mathrm{AB}}T/2\pi$, $\tau_{\mathrm{S\_AC}} = \Delta\varphi_{\mathrm{AC}}T/2\pi$ and $\tau_{\mathrm{S\_BC}} = \Delta\varphi_{\mathrm{BC}}T/2\pi$. As a result, the small-scale delay difference between the selection signal and the host signal can be calculated as $\Delta\tau_{\mathrm{S}} = \tau_{\mathrm{S\_AB}} + \tau_{\mathrm{S\_BC}} - \tau_{\mathrm{S\_AC}}$. According to the assumptions on the channels in Section II, the value ranges of $\Delta\varphi_{\mathrm{AB}}$, $\Delta\varphi_{\mathrm{AC}}$ and $\Delta\varphi_{\mathrm{BC}}$ are $[0, 2\pi)$, indicating that $\tau_{\mathrm{S\_AB}}$, $\tau_{\mathrm{S\_AC}}$ and $\tau_{\mathrm{S\_BC}}$ are all less than $T$, leading to $-T < \Delta\tau_{\mathrm{S}} < 2T$. On the other hand, using the devices' location information, Bob can calculate the lengths of different links $d_{\mathrm{AB}}$, $d_{\mathrm{AC}}$ and $d_{\mathrm{BC}}$, and determine the large-scale delays $\tau_{\mathrm{L\_AB}}$, $\tau_{\mathrm{L\_AC}}$ and $\tau_{\mathrm{L\_BC}}$, as well as the large-scale delay difference $\Delta\tau_{\mathrm{L}} = \tau_{\mathrm{L\_AB}} + \tau_{\mathrm{L\_BC}} - \tau_{\mathrm{L\_AC}} > 0$.

Considering both $\Delta\tau_{\mathrm{S}}$ and $\Delta\tau_{\mathrm{L}}$, the overall delay difference between the host signal and the selection signal can be expressed as $\Delta\tau = \Delta\tau_{\mathrm{S}} + \Delta\tau_{\mathrm{L}}$. Since $-T < \Delta\tau_{\mathrm{S}} < 2T$ and $\Delta\tau_{\mathrm{L}} > 0$, we can have $\Delta\tau > -T$. Next, we will discuss the implementation of PC under $|\Delta\tau| < T$ and $|\Delta\tau| \geq T$, respectively, as illustrated in Fig. 3. In the figure, we use $t_0$ to denote the initial time instant, while $x_{H_C,i}$, $\hat{x}_{H_C,i}$, $x_{I,i}$ and $\hat{x}_{I,i}$ represent the $i$th $x_{H_C}$, $\hat{x}_{H_C}$, $x_I$ and $\hat{x}_I$ along the time axis. $\tau_{\mathrm{AB}}$, $\tau_{\mathrm{BC}}$, and $\tau_{\mathrm{AC}}$ are the delays (including both small-scale and large-scale delays) from Alice to Bob, Bob to Carol, and Alice to Carol, respectively.

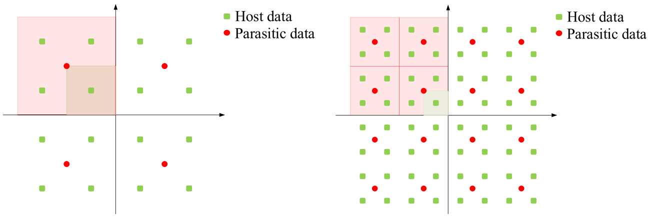
When $|\Delta\tau| < T$, even if the selection signal and the host signal are not perfectly aligned at Carol, $\hat{x}_{I,i}$ can still overlap with its corresponding $\hat{x}_{H_C,i}$ within the symbol period, thereby achieving parasitic indication. In this case, there is no need for pre-alignment. As illustrated in Fig. 3(a), although $\Delta\tau > 0$, Carol can detect correlated $\hat{x}_{H_C,i}$ and $\hat{x}_{I,i}$ in a symbol period. Therefore, by applying OPC-AD, the correct $x_{P,i}$ can be retrieved by Carol.



(a) $|\Delta\tau| < T$

(b) $|\Delta\tau| \geq T$

Fig. 3. Implementation of PC under non-zero $\Delta\tau$.



(a) $M_{\mathrm{H}} = 16$, $M_{\mathrm{P}} = 4$.

(b) $M_{\mathrm{H}} = 64$, $M_{\mathrm{P}} = 16$.

Fig. 4. $M_{\mathrm{P}}$QAM parastizing on $M_{\mathrm{H}}$QAM.

When $|\Delta\tau| \geq T$, the delay difference between the host signal and the selection signal at Carol is too large. In such a case, Bob needs to introduce latency to $x_{I,i}$ based on $\Delta\tau$ so as to align it with $\hat{x}_{H_C,i}$ at Carol. Recall that $\Delta\tau > -T$ holds, we can have $\Delta\tau \geq T$ under $|\Delta\tau| \geq T$. In other words, the host signal arrives at Carol before the selection signal by a time length greater than $T$, due to the significant large-scale delay difference. As Fig. 3(b) shows, $\hat{x}_{I,i}$ corresponds to $\hat{x}_{H_C,i+j-1}$ where $j = \lceil \Delta\tau/T \rceil$ ($\lceil\cdot\rceil$ represents the rounding up operation). Therefore, Bob needs to initialize the parasitic transmission to Carol from $\hat{x}_{H_C,j}$. We refer to this operation as *pre-alignment.*[9]

In summary, Bob needs to decide whether to perform pre-alignment based on $\Delta\tau$. In contrast, there is no additional processing burden placed on Carol. Moreover, since Bob sends a selection signal instead of the desired signal to Carol, and the selection signal needs to be pre-aligned with the interference based on the fading conditions, OPC-AD can ensure the secrecy of data transmission from Bob to Carol, even if there are potential eavesdroppers in the ambient environment.

### B. Extended Design of PC for General Modulation Schemes

In Section III, we have discussed the scenarios where host and parasitic communications employ different orders of PSK. In practice, PC can not only utilize $M$PSK signals as host signals but can also achieve parasitism using $M$-ary Quadrature Amplitude Modulation ($M$QAM) signals. This is further elaborated as follows.

Fig. 4 illustrates the extended implementation of PC where the host and parasitic communications employ $M_{\mathrm{H}}$QAM and

[8] Regarding the imperfect synchronization caused by clock bias among the communication entities, there are numerous techniques available, such as phase-locked loop (PLL)-based fine frequency compensation to achieve synchronization [20]. Given the availability of these well-established synchronization methods, we do not further elaborate on this issue.

[9] In practice, the symbol length typically ranges from a few to several tens of microseconds [21]. In contrast, large- and small-scale fading effects can result in a delay difference of only a few microseconds [22]. Consequently, the cost of counteracting signal misalignment is at most a few symbols.

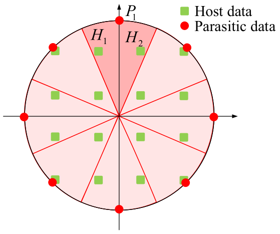


Fig. 5. Illustration of $M_{\mathrm{P}}$PSK parasitizing on $M_{\mathrm{H}}$QAM.

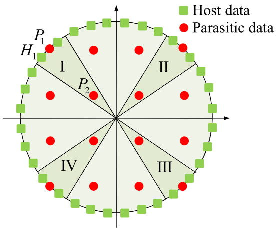


Fig. 6. Illustration of $M_{\mathrm{P}}$QAM parasitizing on $M_{\mathrm{H}}$PSK.

$M_{\mathrm{P}}$QAM, respectively. In Fig. 4(a), we set $M_{\mathrm{H}} = 16$ and $M_{\mathrm{P}} = 4$. As the figure shows, each quadrant contains four 16QAM constellation points and one 4QAM constellation point. Therefore, the data corresponding to the 4QAM constellation points can be transmitted by parasitizing on the 16QAM data symbols located in the same quadrant. Fig. 4(b) illustrates the implementation of PC under $M_{\mathrm{H}} = 64$ and $M_{\mathrm{P}} = 16$. As the figure plots, each quadrant contains four 16QAM constellation points and sixteen 64QAM constellation points. Each 16QAM point is evenly surrounded by four 64QAM points. Consequently, the data corresponding to a 16QAM constellation can be parasitic on the 64QAM data symbol nearest to it. Therefore, we can conclude that PC can be extended to the scenarios where the parasitic and host communications utilize different $M$QAM modulations.

Fig. 5 illustrates the extended implementation of PC where the host and parasitic communications employ 16QAM and 8PSK, respectively. As the figure plots, A circle is divided into 8 equal sectors. Within each sector, there are two host data constellation points and one parasitic data constellation. Therefore, we can transmit the parasitic data by leveraging the transmission of the host data in the same sector. To be specific, the parasitic Rx utilizes demodulation schemes corresponding to 8PSK modulation to decode the received 16QAM modulated signal. Then, according to the ML criterion, the perceived green dots (e.g., $H_1$ and $H_2$) can be approximated to their nearest red dot (e.g., $P_1$), thereby achieving PC.

Fig. 6 illustrates the extended implementation of PC where the host and parasitic communications employ 32PSK and 16QAM, respectively. As shown in the figure, the circle is equally divided into 12 sectors. However, we can see that in sectors indexed with I–IV, in Fig. 6, there are two parasitic data constellations in a single sector. This leads to non-unique parasitism, rendering PC partially infeasible. However, this does not imply that $M_{\mathrm{P}}$QAM cannot parasitize on $M_{\mathrm{H}}$PSK at all. By observing Fig. 6, we can find that the 12 outer 16QAM constellation points are distinguishable based on their phases. Therefore, we can associate these 12 constellation points with the 32PSK constellation points, enabling the extended implementation of PC. Nevertheless, such an extension discards the 4 inner points of 16QAM constellation. That is, in practice, we may need to trim the $M_{\mathrm{P}}$QAM constellation to ensure that each of the $M_{\mathrm{H}}$PSK points (i.e., host data) can be uniquely associated with a trimmed $M_{\mathrm{P}}$QAM point (i.e., parasitic data), so that PC can be still applicable.

When $M_{\mathrm{P}}$PSK parasitizes on $M_{\mathrm{H}}$PSK or $M_{\mathrm{H}}$QAM, and when $M_{\mathrm{P}}$QAM parasitizes $M_{\mathrm{H}}$QAM, the probability of successful parasitism for each parasitic data point is identical and can be calculated as $p = \frac{1}{M_{\mathrm{P}}}$. However, when $M_{\mathrm{P}}$QAM parasitizes $M_{\mathrm{H}}$PSK, the probabilities of successful parasitism for the parasitic constellation points differ. For instance, in Fig. 6, where 16QAM parasitizes 32PSK, the 4 inner points of the 16QAM constellation cannot parasitize on any of the 32PSK points, resulting in $p = 0$. The outermost 4 vertices of the 16QAM constellation can parasitize on the two nearest 32PSK points, with $p = \frac{1}{16}$. The remaining 8 points of the 16QAM constellation can parasitize on their three nearest 32PSK points, yielding $p = \frac{3}{32}$. Therefore, given the probabilities of parasitic data being the same, the average probability of successful parasitism can be calculated as $\frac{1}{16}(4 \times 0 + 4 \times \frac{1}{16} + 8 \times \frac{3}{32}) = \frac{1}{16} = \frac{1}{M_{\mathrm{P}}}$.

In summary, based on the discussions of Figs. 4–6, PC can be extended to scenarios involving more general modulation schemes.

### C. Design of CPC-AD

From the design of OPC-AD, we can see that the opportunity for PC cannot always be guaranteed, leading to the unstable quality of OPC-AD. To mitigate this deficiency, we can load more indication information bits onto a single $x_I$. Specifically, $x_I$ should consist of $\log_2 M_{\mathrm{P}}$ bits, i.e., $M_{\mathrm{I}} = M_{\mathrm{P}}$ holds. Each of these bits indicates to Carol whether she should retain the corresponding decoded bit in $\hat{x}_{H_C}$ unchanged or perform a bitwise NOT operation on the decoded bit before accepting it as the desired bit. This way, the probability of successful parasitism could increase to as high as 100%, indicating the full utilization of interference. Therefore, we call this method *Complete PC with AD* (CPC-AD).

In CPC-AD, $M_{\mathrm{I}}$ should match $M_{\mathrm{P}}$. This ensures that a bitwise correlation between the bits in $x_I$ and $\hat{x}_{H_C}$ ($\hat{x}_{H_B}$) can be established. Bob can design $x_I$ in terms of Eq. (8):

$$x_I = \hat{x}_{H_B} \oplus x_P, \tag{8}$$

where $\oplus$ represents the Exclusive OR (XOR) operation. Accordingly, after obtaining $\hat{x}_{H_C}$ and $\hat{x}_I$, Carol can recover the desired data $\hat{x}_P$ according to Eq. (9) below:

$$\hat{x}_P = \hat{x}_{H_C} \oplus \hat{x}_I, \tag{9}$$

where $\hat{x}_I$ is the parasitic indication information that Carol decodes from the selection signal.

From the above discussion, we can see that CPC-AD encodes more indication information bits into the selection signal, enabling continuous PC. Consequently, $p$ can increase to 100%, and interference can be fully utilized.

In practical applications of CPC-AD, we can determine the value of $M_\mathrm{I}$ based on the quality of the D2D link while ensuring that $M_\mathrm{I} = M_\mathrm{P} < M_\mathrm{H}$. Specifically, if Bob can transmit to Carol at a higher speed, he can modulate more indication information bits into the selection signal. Consequently, Carol can employ a higher $M_\mathrm{P}$ matching $M_\mathrm{I}$ to achieve CPC-AD. In contrast, when the quality of the D2D link is poor, we should decrease $M_\mathrm{I}$ to ensure its decoding correctness at Carol. In this case, Carol can either continue using CPC-AD by setting $M_\mathrm{P} = M_\mathrm{I}$ (where each indication data symbol contains $\log_2 M_\mathrm{P}$ bits of indication information), or switch to OPC-AD by employing BPSK modulation to generate $x_I$ (where each $x_I$ contains one bit of indication information).

### D. Design of PC Exploiting Multiple Host Transmissions

When multiple parallel host communications originate from Alice, our method can be extended by loading more bits of indication information onto the indication data $x_I$. Specifically, let the number of host transmissions be $K$. In this case, the parasitic Rx should be equipped with at least $K+1$ antennas to separate the $K$ host signals and one selection signal in the spatial domain. Then, in the case of OPC-AD, the parasitic Tx should load $K$ bits onto an indication data symbol $x_I$, where each bit indicates whether to keep or discard the data decoded from the corresponding host transmission. Similarly, in CPC-AD, we can load $K \log_2 M_\mathrm{P}$ indication bits onto $x_I$. Consequently, the parasitic Tx would need to employ a high-order modulation scheme to generate the selection signal. However, in practice, this may not always be feasible, as the selection and host signals could interfere with each other. The relatively stronger host signal may constrain the modulation order of the selection signal, as high-order modulation based communication in an interference environment can lead to a higher rate of bit errors. In this case, we can utilize the first $K'$ (where $K' < K$) strongest host signals and treat the remaining $K - K'$ interference components as a single effective interference [23]. This approach can circumvent the necessity of employing high-order modulation at the parasitic Tx and a larger number of antennas at the parasitic Rx.

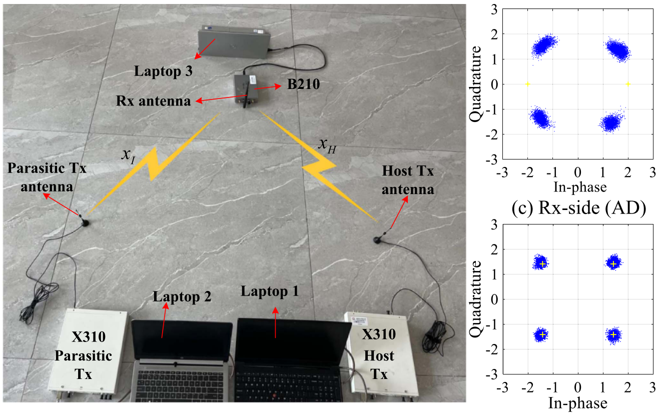
## V. Evaluation

We first use the USRP platform for experimental evaluation, demonstrating the validity of AD and assessing the bit-error rate (BER) of OPC-AD. Then, we use MATLAB simulations to evaluate the effectiveness and secrecy performance of both OPC-AD and CPC-AD.

### A. Hardware Experiment

Here, we focus on utilizing the USRP platform to demonstrate the validity of AD. Since the detection of the selection signal follows the same principles as conventional communication schemes — where the modulation order matches the demodulation order — the BER performance of OPC-AD and CPC-AD can be easily evaluated.

Fig. 7 shows our experimental setup and the observed constellations at Tx and Rx, respectively. As mentioned earlier, we primarily focus on validating the feasibility of parasitic communication. Therefore, we simplify the experiment by having the host Tx and parasitic Tx transmit the host signal and selection signal in two separate phases, eliminating any misalignment issues that could affect the use of parasitic communication.[10] As Figure 7(a) shows, we use one USRP X310 connected to Laptop 1 to serve as the single-antenna host Tx and another USRP X310 connected to Laptop 2 to serve as the parasitic Tx, respectively. Meanwhile, one USRP B210 connected to Laptop 3 acts as the single-antenna parasitic Rx. We first configure the host Tx to transmit using QPSK and the Rx to receive according to BPSK, to simulate the generation and detection of the host signal under OPC-AD. Then, we set the parasitic Tx to transmit using BPSK (or QPSK) and the Rx to receive using BPSK (or QPSK) to simulate the detection of the selection signal under OPC-AD (or CPC-AD). The total number of transmitted QPSK/BPSK symbols is $5 \times 10^5$. Based on the above experiment design, we can obtain the BER for the detection of the selection[11] and the host signals, denoted as $b_{S,\mathcal{M}}$ and $b_{H,\mathcal{M}}$, respectively, where the subscript $\mathcal{M}$ can be either $OPC-AD$ or $CPC-AD$. Therefore, the BER of method $\mathcal{M}$ can be evaluated as $b_\mathcal{M} = b_{S,\mathcal{M}} + b_{H,\mathcal{M}} - b_{S,\mathcal{M}} b_{H,\mathcal{M}}$. The main parameters used in the experiment are listed in Table II. Fig. 7(b) and (c) show the observed constellations at the Tx and the Rx, respectively, where the Tx employs QPSK and the Rx utilizes BPSK. The transmit gain is set to 8 dB. As subfigure (b) illustrates, the Tx can transmit a QPSK modulated signal, demonstrating a concentrated and clear QPSK constellation. With BPSK demodulation, the Rx observes an attenuated constellation, as illustrated in subfigure (c). Although it resembles a QPSK constellation, the Rx treats the constellation points as BPSK symbols for decoding.



(a) Experimental setup

(c) Rx-side (AD)

(b) Host Tx-side

Fig. 7. Experimental setup and observations.

Fig. 8 compares the BER performances of OPC-AD and CPC-AD, denoted as $b_{OPC-AD}$ and $b_{CPC-AD}$, respectively. We set

[10] In practice, the cost of counteracting signal misalignment is only a few symbols, while the transmission can contain hundreds of data symbols; thus, the waste introduced by propagation delay is negligible.

[11] Regarding the effect of $x_I = 0$ on the BER, since our experiment aims to validate the feasibility of parasitic communication, while the performance evaluation is left for the simulation section (see Figs. 9 and 10), the BER results illustrated in Fig. 8 assume that no parasitic failures occur.

TABLE II
PARAMETER SETTINGS OF THE EXPERIMENT

| Parameter | Carrier freq. | Symbol rate | Interpolation factor | Sampling rate (baseband) | Roll-off factor of raised cosine filter | Transmit gain |
|---|---|---|---|---|---|---|
| Value | 1GHz | 0.2MBaud | 2 | 0.4MHz | 0.5 | [2,10]dB |

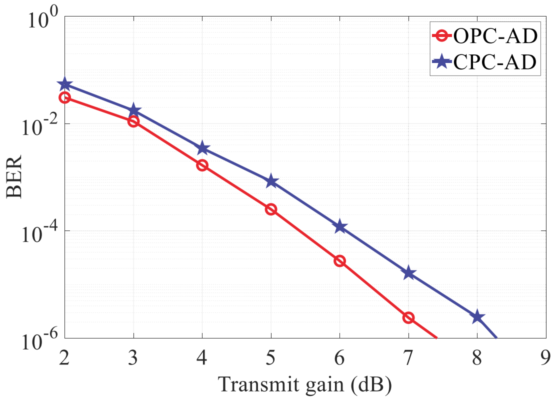


Fig. 8. BER performances of OPC-AD and CPC-AD.

the transmit gain to [2,10]dB. As the figure shows, all BER curves decrease as the transmit gain rises. Given a fixed transmit gain, $b_{OPC-AD}$ slightly outperforms $b_{CPC-AD}$. This is because CPC-AD uses QPSK demodulation, whereas OPC-AD employs BPSK demodulation. Since BPSK is more noise-tolerant than QPSK, OPC-AD can achieve better BER performance.

### B. Simulation of the Transmission Performance of PC

We use MATLAB simulation to evaluate the performance of OPC-AD and CPC-AD in comparison with other existing transmission schemes. Alice and Carol are each equipped with 2 antennas, while Bob, operating in full-duplex mode, has 4 antennas (2 for reception and 2 for transmission). The transmit powers of Alice and Bob are denoted by $P_{t_1}$ and $P_{t_0}$. We define $\varepsilon = 10\lg(P_{t_1}/\sigma_n^2)$dB, and set $\varepsilon \in [0, 30]$dB in the simulation. Without loss of generality, we let both the host and parasitic communications utilize MPSK[12] in the simulation. Each indication data corresponds to a host data symbol at Carol.

Fig. 9 illustrates the performance of OPC-AD where the host communication employs 32PSK and transmits 5000 host data symbols. Carol employs $M_{\text{P}}$PSK where $M_{\text{P}} \in \{2, 4, 8, 16\}$. Fig. 9(a) shows the parasitic states (i.e., success or failure) of OPC-AD on the 5000 host data symbols for various $M_{\text{P}}$s. There, we also show the amount of transmitted data in a single parasitism and calculate the probability of successful parasitism. As Fig. 9(a) shows, given 5000 host data symbols, the probability of successful parasitism, denoted as $p_{5000}$, is the highest when $M_{\text{P}} = 2$. As $M_{\text{P}}$ grows, $p_{5000}$ decreases. Here, the subscript 5000 represents that a total of 5000 host symbols are studied. As for the amount of information transmitted in a single parasitism, when $M_{\text{P}} = 2$, only one bit of parasitic information is allowed to parasitize on a host data symbol for transmission. As $M_{\text{P}}$ grows, more bits of information can parasitize on a host symbol.

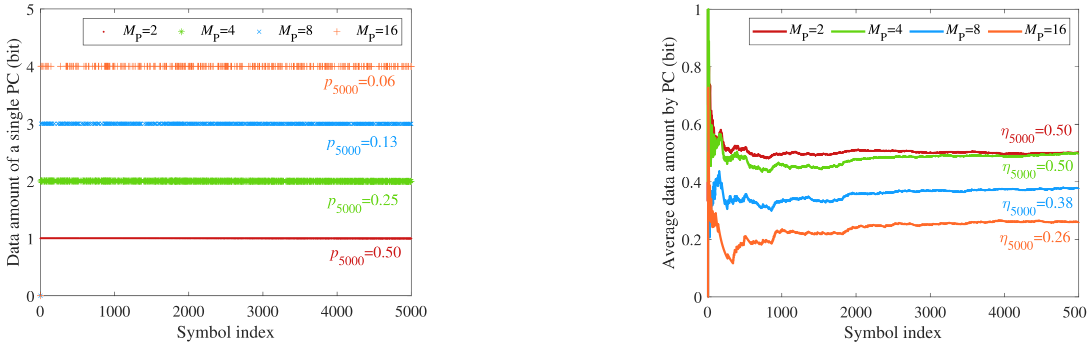
Fig. 9(b) plots the average amount of parasitic information transmitted in a single parasitism, denoted as $\eta$, under various $M_{\text{P}}$s. Due to the randomness of $x_H$ and $x_P$, $\eta$ is shown to exhibit significant random fluctuations when considering a smaller number of host symbols. However, as the number of host symbols grows, $\eta$ tends to stabilize. Moreover, $\eta_{5000}$ decreases with an increase in $M_{\text{P}}$, as analyzed below. As discussed in Section III, $p = \frac{1}{M_{\text{P}}}$, and the amount of information transmitted in a single parasitism is $\log_2 M_{\text{P}}$. Therefore, we can have $\eta = \frac{\log_2 M_{\text{P}}}{M_{\text{P}}}$. Then, by differentiating $\eta$ with respect to $M_{\text{P}}$, and setting the derivative to 0, we can get $\frac{1/\ln 2 - \log_2 M_{\text{P}}}{M_{\text{P}}^2} = 0$. We can then easily see that $\eta$ increases as $M_{\text{P}}$ grows within the interval $(0, e)$ and decreases as $M_{\text{P}}$ grows beyond $e$. Thus, $\eta$ reaches a maximum value when $M_{\text{P}} = 2^{(1/\ln 2)} = e$. Recall that $M_{\text{P}}$ should be a power of 2, we can achieve the maximum $\eta$ under $M_{\text{P}} = 2$. It is worth noting that when $M_{\text{P}} = 4$, $\eta$ can also be maximized. Therefore, in practice, we can either choose $M_{\text{P}} = 4$ for a larger amount of information transmission in a single parasitism at the expense of a lower $p$, or select $M_{\text{P}} = 2$ to achieve a higher $p$ but with only one bit of information parasitizing on a host symbol. Both can achieve the maximum $\eta$.

Next, we compare Carol's SE under different transmission schemes, including IN, IS, IRC, OPC-AD, CPC-AD, as well as non-IM (where Bob employs SVD-based precoding and Carol utilizes MF reception, i.e., no interference management). In the simulation of IN, IS, and IRC, Bob's transmission to Carol switches to non-IM if they encounter infeasibility. Moreover, as IN and IS may consume too much transmit power, leaving very little power for the transmission of the desired signal, to prevent excessive power consumption for IM, we restrict Bob's power cost for IN or IS to be no more than $0.7P_{t_0}$ in the simulation. To obtain Fig. 10, we define the transmit power ratio as $\gamma = P_{t_1}/P_{t_0}$, and adopt $\gamma \in \{4, 8\}$.[13]

Fig. 10 plots the variation of Carol's SE with $\varepsilon$ under different $\gamma$s. Fig. 10(a) sets $\gamma = 4$. As the figure shows, IRC achieves the highest SE, followed by CPC-AD, then comes OPC-AD, IS ranks the fourth, IN the fifth, and non-IM outputs the lowest SE. IRC achieves the best SE by utilizing both the power of interference and the power of the recycling signal. In contrast, CPC-AD only utilizes interference for transmission. When $\varepsilon$ is high, OPC-AD outperforms IN and IS in Carol's SE. This is because under strong interference, IN and IS need to consume more power for IM, making less power available for the desired signal transmission. Consequently, SE of IN and IS is inferior

[12] Under OPC-AD, the selection signal fixedly uses BPSK modulation.

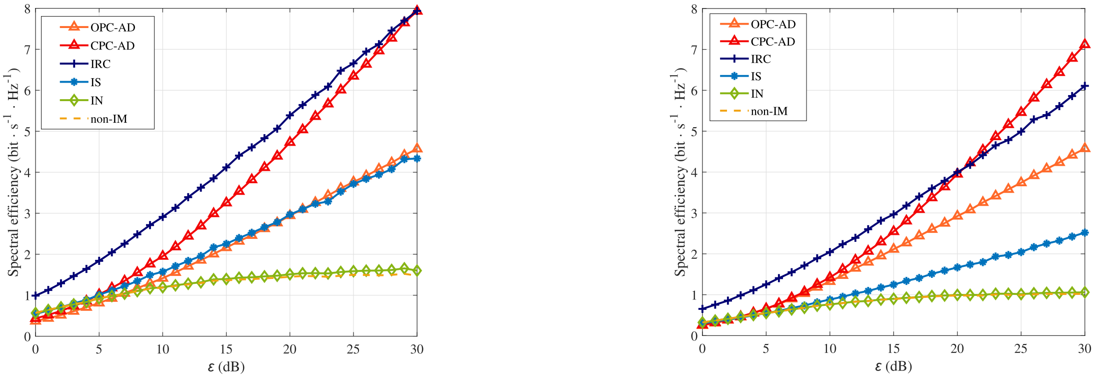
[13] The transmit power of a mobile device can be set to 23 dBm [24], while for the BS, its transmit power can range from 24dBm to 38 dBm [25]. This results in Alice's power being approximately the same as Bob's or up to 30x greater than Bob's power.



(a) Parasitic states and the amount of information transmitted in a single parasitism.

(b) The average amount of information transmitted in a single parasitism.

Fig. 9. The performance of OPC-AD under $M_{\mathrm{H}} = 32$ and various $M_{\mathrm{P}}$s.



(a) $\gamma = 4$

(b) $\gamma = 8$

Fig. 10. Comparison of Carol's SE with various transmission schemes under different $\varepsilon$s and $\gamma \in \{4, 8\}$.

to that of OPC-AD. Due to the influence of the probability of successful parasitism (i.e., $p$), SE of OPC-AD is lower than that of CPC-AD. Furthermore, as $\varepsilon$ becomes excessively large, SE of IN approaches that of non-IM. This is because when $\gamma = 4$ and $\varepsilon$ is very high, interference becomes too strong for IN. As a result, IN is switched off, and non-IM is adopted as a substitution. As for non-IM, although the interference at Carol strengthens as $\varepsilon$ increases, the constant $\gamma$ ensures that the strength of the desired signal transmitted from Bob also increases accordingly. This results in a stabilizing SINR and SE at Carol when $\varepsilon$ becomes higher. When $\varepsilon$ is small, Carol's SE with OPC-AD becomes inferior to that of non-IM. This is because in such a case, the noise is stronger than the interference, and OPC-AD's SE depends on the strength of the interference (i.e., host signal). However, as $\varepsilon$ grows larger than 8dB, the interference becomes strong enough, yielding OPC-AD's SE to be better than non-IM's.

Fig. 10(b) plots the variation of Carol's SE with different transmission schemes under $\gamma = 8$. As the figure shows, CPC-AD exhibits the highest SE, followed by IRC, then comes OPC-AD. OPC-AD's SE is comparable to that of IS, while IN demonstrates a similar SE to non-IM, which is the lowest among all the methods. We analyze this trend as follows. As the interference becomes stronger at $\gamma = 8$, IRC may become inapplicable, resulting in a decrease in Carol's SE compared to that shown in Fig. 10(a). In contrast, CPC-AD achieves data transmission by parasitizing on the interference, allowing it to perform better as the interference strength increases. Therefore, the SE of CPC-AD eventually surpasses that of IRC. Similarly, SE of OPC-AD also improves when $\gamma = 8$. However, this improvement is limited by $p$. Nevertheless, as $\varepsilon$ increases, SE of OPC-AD gradually exceeds that of IS. Moreover, the SE of IN overlaps with that of non-IM. This is because under strong interference, the probability of IN becoming inapplicable approaches 1. Consequently, it is more likely for Bob's transmission to Carol to switch to the non-IM scheme. On the other hand, since the power cost for IS is less than that of IN, the impact of strengthening interference on IS is smaller than on IN. As a result, IS exhibits a superior SE for Carol compared to IN.

Note that Carol's SE with OPC-AD and CPC-AD, as shown in Fig. 10, represents the upper bound performance obtained by Eq. (6) under $p = \frac{1}{M_{\mathrm{P}}}$ and $p = 1$, respectively. In practice, however, since Carol needs to employ a lower-order demodulation than

TABLE III
EVE'S EAVESDROPPING CAPABILITY UNDER VARIOUS ADVERSARY MODELS

| Index | Adversary model | |
|---|---|---|
| | Information available at the eavesdropper | Eavesdropper's signal processing |
| I | The CSI between Bob and Eve, i.e., $\mathbf{H}_{\mathrm{BE}}$ | Apply matched filter to the selection signal and interference as a whole |
| II | $\mathbf{H}_{\mathrm{BE}}$ and the CSI between Alice and Eve, i.e., $\mathbf{H}_{\mathrm{AE}}$ | Employ ZF reception to detect the selection signal |
| III | $\mathbf{H}_{\mathrm{BE}}$, $\mathbf{H}_{\mathrm{AE}}$, and the utilization of CPC-AD | Employ ZF reception to decode $\hat{x}_I$ and $\hat{x}_H$, and apply Eq. (9) to retrieve $\hat{x}_P$ |

the host signal, her SE will be degraded. Furthermore, the accuracy of the indication information is essential for implementing OPC-AD and CPC-AD. In other words, the quality of the D2D link could potentially act as a bottleneck for the SE performance of our methods. Note, however, that in cases where the host signal is strong, even with a low-order modulated selection signal, we can still achieve high-speed parasitic transmission instantaneously by leveraging a high-order modulated host signal.

### C. Simulation of the Secrecy Performance of PC

Next, we use secrecy capacity as the metric against eavesdropping attacks, and consider three typical adversary models as detailed in Table III. In Model I, the eavesdropper's (Eve's) capability is limited, as she is only aware of the CSI between Bob and herself, resulting in the mixed signal comprising the selection signal and host signal being processed as a whole, which leads to poor eavesdropping performance. In Model II, Eve's capability is enhanced. She is able to acquire the CSI between herself and both Bob and Alice. Consequently, Eve utilizes ZF reception to detect the selection signal transmitted from Bob to Carol. However, Eve mistakenly regards the decoded indication information as Carol's desired data since she is unaware of the use of CPC-AD in the transmission from Bob to Carol, leading to poor eavesdropping performance. Lastly, in adversary Model III, Eve possesses a strong eavesdropping capability. She can obtain the CSI between herself and both Bob and Alice, along with the knowledge of the utilization of CPC-AD. As a result, Eve can separately detect the selection signal and host signal, and utilize Eq. (9) to recover the information that Bob intends to transmit to Carol. In this scenario, despite Eve's awareness of the use of CPC-AD by Bob and Carol, her lack of knowledge of $\mathbf{H}_{\mathrm{BC}}$, which is used to design the transmission from Bob to Carol, deteriorates the decoding of $x_I$ due to the randomness of channel states. Therefore, even if Eve can utilize Eq. (9) to retrieve the data intended for Carol by Bob, her eavesdropping capacity still remains lower than the channel capacity between Bob and Carol. Regarding the adversary model III, we have not considered the scenario where Eve is aware of the use of OPC-AD by Bob and Carol. This is because, even if Eve has this knowledge, she is still unable to intercept the data information that Bob intends to send to Carol, as the demodulation scheme adopted by Carol is confidential to Eve.

Since parasitic communication differs from conventional transmission schemes, we employ the following method to evaluate the channel capacities of Carol and Eve's eavesdropping on Bob. According to information theory, channel capacity is characterized by the maximum average mutual information [20]. Then, Carol's capacity can be calculated as:

$$\begin{aligned} c_C &= \max\{I(X_P;\hat{X}_P)\} \\ &= \max\left\{\sum_{x_P\in X_P}\sum_{\hat{x}_P\in\hat{X}_P} P(x_P,\hat{x}_P)\log_2\frac{P(x_P,\hat{x}_P)}{P(x_P)P(\hat{x}_P)}\right\}, \end{aligned} \tag{10}$$

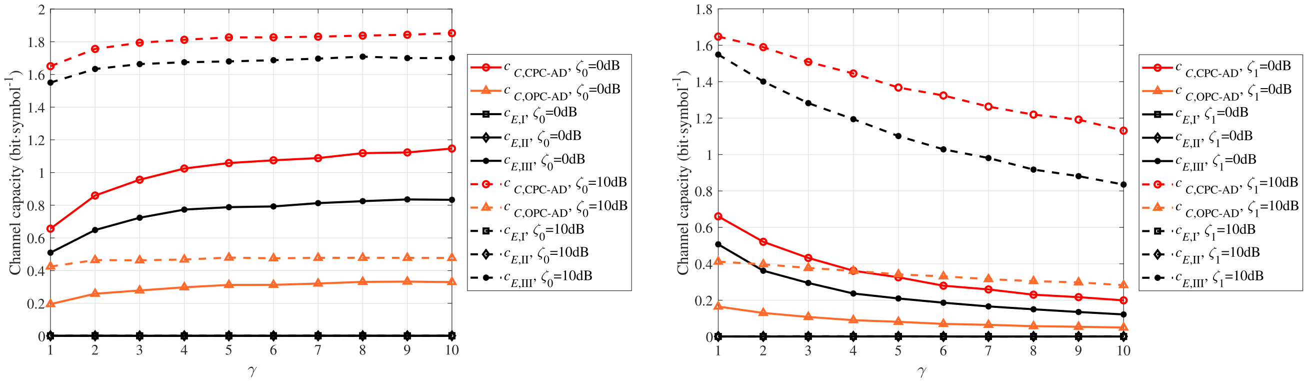
where $I(X_P;\hat{X}_P)$ represents the average mutual information. $x_P$ and $\hat{x}_P$ denote the parasitic data that Bob intends to deliver to Carol and the data that Carol actually estimates, respectively. Meanwhile, $X_P$ and $\hat{X}_P$ denote the parasitic data sets intended for Carol and estimated by Carol, respectively. It holds that $x_P \in X_P$ and $\hat{x}_P \in \hat{X}_P$. In either OPC-AD or CPC-AD, the parasitic data $\hat{x}_P$ obtained by Carol is derived from the detected host data $\hat{x}_H$ and the parasitic indication data $\hat{x}_I$. The probabilities of $x_P$ and $\hat{x}_P$ are represented by $P(x_P)$ and $P(\hat{x}_P)$, while their joint probability density is $P(x_P,\hat{x}_P)$. Similarly, the eavesdropping capacity of Eve, denoted as $c_E$, can be computed according to $c_E = \max\{I(X_P;\hat{X}_E)\}$, where $\hat{X}_E$ represents the estimated or eavesdropped data at Eve.

Consequently, the secrecy capacity $c_S$ can be obtained by subtracting the wiretap channel capacity $c_E$ from $c_C$, as:

$$c_S = \max\{c_C - c_E, 0\}. \tag{11}$$

In the evaluation, we assume that Bob can accurately decode $\hat{x}_{H_B}$, based on which $x_I$ is generated. Consequently, Carol's reception depends on her detection of the host signal and selection signal. Therefore, we compare the data recovered by Carol using the decoded $\hat{x}_I$ and $\hat{x}_{H_C}$ according to Eq. (9) with the desired data $x_P$. The number of symbols (i.e., $x_H$, $x_P$, and $x_I$) for the evaluation is set to be $10^4$. When Bob employs OPC-AD, we utilize the probability of successful parasitism under OPC-AD to weigh the average mutual information of Carol obtained under CPC-AD. We then treat this result as the capacity of Carol under OPC-AD, denoted as $c_{C,\mathrm{OPC-AD}}$. We define the noise-normalized transmit power of Alice and Bob as $\zeta_1 = 10\lg(P_{t_1}/\sigma_n^2)$ and $\zeta_0 = 10\lg(P_{t_0}/\sigma_n^2)$, and set $\gamma \in [1,10]$.

Fig. 11 illustrates the variation of $c_{\mathrm{C,CPC-AD}}$, $c_{\mathrm{C,OPC-AD}}$ and $c_E$ along with $\gamma$ under different $\zeta_0$s and $\zeta_1$s. Recall that $\gamma = P_{t1}/P_{t0}$, we can conclude that given fixed $\zeta_0$ (or the transmit power of Bob), $\zeta_1$ (or the transmit power of Alice) increases as $\gamma$ grows. As subfigure (a) shows, $c_{C,\mathrm{CPC-AD}}$, $c_{C,\mathrm{OPC-AD}}$ and $c_{E,\mathrm{III}}$ increase with $\gamma$ and gradually reach saturation, while $c_{E,\mathrm{I}}$ and $c_{E,\mathrm{II}}$ remain close to zero irrespective of the variation of $\gamma$ (the subscripts I–III indicate the indices of the adversary models). This is because Carol needs to detect both the selection signal and the host signal to recover her desired data. When $\zeta_0$ is fixed, $\zeta_1$ increases with $\gamma$, meaning the intensity of the



(a) $\zeta_0 \in \{0, 10\}$dB.

(b) $\zeta_1 \in \{0, 10\}$dB.

Fig. 11. Variation of capacity performance with $\gamma$ under various $\zeta_0$s and $\zeta_1$s.

interference strengthens, increasing both $c_{C,\mathrm{CPC-AD}}$ and $c_{C,\mathrm{OPC-AD}}$. In contrast, the strength of the selection signal does not increase when $\zeta_0$ remains constant. Therefore, as the host signal strengthens, $c_{C,\mathrm{CPC-AD}}$ and $c_{C,\mathrm{OPC-AD}}$ will be constrained by the quality of the selection signal. As a result, with the continued increase of $\gamma$, both $c_{C,\mathrm{CPC-AD}}$ and $c_{C,\mathrm{OPC-AD}}$ gradually saturate. Regarding $c_E$, in adversary Models I and II, Eve is unable to intercept the desired information, resulting in $c_{E,\mathrm{I}}$ and $c_{E,\mathrm{II}}$ being close to zero. In these cases, even if the interference is strengthened, $c_{E,\mathrm{I}}$ and $c_{E,\mathrm{II}}$ remain unaffected. In adversary Model III, since Eve employs CPC-AD for eavesdropping, the analysis for the variation of $c_{E,\mathrm{III}}$ along with $\gamma$ is the same as that for $c_{C,\mathrm{CPC-AD}}$. Additionally, we can observe from Fig. 11(a) that $c_{C,\mathrm{CPC-AD}}$, $c_{C,OPC-AD}$, and $c_{E,\mathrm{III}}$ improve as $\zeta_0$ increases. This is because Bob's transmit power grows with an increase of $\zeta_0$, thereby enhancing the strength of the selection signal at both Carol and Eve. This enables them to more accurately recover the desired information from the interference (host signal), leading to the improvement of $c_{C,\mathrm{CPC-AD}}$, $c_{C,OPC-AD}$ and $c_{E,\mathrm{III}}$. Moreover, due to the influence of the probability of successful parasitism on $c_{C,\mathrm{OPC-AD}}$, given the same $\zeta_0$, $c_{C,\mathrm{CPC-AD}}$ outperforms $c_{C,\mathrm{OPC-AD}}$. The analysis for $c_{C,\mathrm{CPC-AD}}$ being superior to $c_{E,\mathrm{III}}$ is that Bob's transmission to Carol matches $\mathbf{H}_{\mathrm{BC}}$. Due to the independence of $\mathbf{H}_{\mathrm{BE}}$ and $\mathbf{H}_{\mathrm{BC}}$, the eavesdropping of $x_I$ from the selection signal based on the knowledge of $\mathbf{H}_{\mathrm{BE}}$ does not perfectly align with $\mathbf{H}_{\mathrm{BC}}$, leading to a decrease in $c_{E,\mathrm{III}}$.

Fig. 11(b) sets $\zeta_1 \in \{0, 10\}$ dB for capacity analysis. As the figure shows, $c_{C,\mathrm{CPC-AD}}$, $c_{C,\mathrm{OPC-AD}}$, and $c_{E,\mathrm{III}}$ decrease with the increase of $\gamma$, while $c_{E,\mathrm{I}}$ and $c_{E,\mathrm{II}}$ remain constant and close to 0 regardless of the variation of $\gamma$. This is because, when $\zeta_1$ is fixed, $\zeta_0$ gradually decreases as $\gamma$ grows, resulting in a reduction in $P_{t_0}$. Consequently, the strength of the selection signal weakens. In this situation, the selection signal at Bob and Carol under adversary model III is not strong enough to guide them in recovering data from the interference. As a result, $c_{C,\mathrm{CPC-AD}}$, $c_{C,\mathrm{OPC-AD}}$, and $c_{E,\mathrm{III}}$ decrease with an increase of $\gamma$. Furthermore, since $P_{t_0} = \frac{P_{t_1}}{\gamma}$, a higher $P_{t_1}$ leads to a larger $P_{t_0}$ for the same $\gamma$. Hence, when $\zeta_1 = 0$ dB, the values of $c_{C,\mathrm{CPC-AD}}$, $c_{C,\mathrm{OPC-AD}}$, and $c_{E,\mathrm{III}}$ are lower than those under $\zeta_1 = 10$ dB. Moreover, when the selection signal is strong enough, it is apparent that the greater the value of $\zeta_1$, the stronger the interference (or host signal) perceived by Carol and Eve, resulting in higher $c_C$ and $c_{E,\mathrm{III}}$. The reasons for $c_{E,\mathrm{I}}$ and $c_{E,\mathrm{II}}$ not varying with $\gamma$ and $\zeta_1$ are consistent with the analysis provided in Fig. 11(a). To avoid redundancy, we will not repeat the explanation here.

In summary, without knowledge of the application of CPC-AD at Bob and Carol (i.e., adversary models I and II), Eve cannot successfully eavesdrop. However, if Eve is aware that Bob communicates with Carol using CPC-AD and processes the received interference and selection signal based on the principles of CPC-AD (i.e., adversary model III), the secrecy capacity will degrade. In this case, CPC-AD can still rely on the delay difference between the selection signal and the interference to ensure secure communication from Bob to Carol, as discussed in Section IV-A.

## VI. Conclusion

In this paper, we have proposed an *Opportunistic Parasitic Communication* method with *Asymmetric Demodulation* (OPC-AD). With this method, data transmission can be achieved by leveraging interference. Furthermore, we developed *Complete PC with AD* (CPC-AD) by modulating multiple indication information bits into the selection signal. This enhancement can enhance the probability of successful parasitism to as high as $100\%$ . Both OPC-AD and CPC-AD can effectively utilize the interference. Through AD, the entire host information is guaranteed to remain transparent to the parasitic Rx, thereby safeguarding the privacy of the host communication. Moreover, since the parasitic communication is concealed within the host signal, eavesdropping can be effectively thwarted. Our comprehensive analysis, experimental, and simulation results have demonstrated the validity and effectiveness of the proposed methods in exploiting interference to achieve a higher SE than existing transmission mechanisms that consider interference as hostile without effective utilization.

## REFERENCES

[1] IMT Vision–Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond, ITU-R, 2015. [Online]. Available: https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf

[2] L. Dai, B. Wang, Y. Yuan, S. Han, I. Chih-Lin, and Z. Wang, "Non-orthogonal multiple access for 5G: Solutions, challenges, opportunities, and future research trends," *IEEE Commun. Mag.*, vol. 53, no. 9, pp. 74–81, Sep. 2015.

[3] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[4] D. Wu, C. Yang, T. Liu, and Z. Xiong, "Feasibility conditions for interference neutralization in relay-aided interference channel," *IEEE Trans. Sig. Process.*, vol. 62, no. 6, pp. 1408–1423, Mar. 2014.

[5] Z. Li, Y. Liu, K. G. Shin, J. Liu, and Z. Yan, "Interference steering to manage interference in IoT," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10458–10471, Dec. 2019.

[6] X. Lu et al., "Wireless networks with RF energy harvesting: A contemporary survey," *IEEE Commun. Surv. Tut.*, vol. 17, no. 2, pp. 757–789, Second Quarter 2015.

[7] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Interference recycling: Exploiting interfering signals to enhance data transmission," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Paris, France, 2019, pp. 100–108.

[8] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[9] Y. Xiao et al., "MAC security and security overhead analysis in the IEEE 802.15.4Wireless Sensor Networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2006, no. 2, pp. 81–93, 2006.

[10] G. Apostolopoulos, V. Peris, P. Pradhan, and D. Saha, "Securing electronic commerce: Reducing the SSL overhead," *IEEE Netw.*, vol. 14, no. 4, pp. 8–16, Jul./Aug. 2000.

[11] P. E. Abi-Char and C. F. Riman, "A lightweight and secure key management scheme for wireless sensor networks," in *Proc. Int. Conf. Telecommun. Signal Process.*, Prague, Czech Republic, 2023, pp. 187–192.

[12] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[13] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE Veh. Technol. Conf.*, Dallas, TX, USA, 2005, pp. 1906–1910.

[14] Y. Li, L. J. Cimini, and N. R. Sollenberger, "Robust channel estimation for OFDM systems with rapid dispersive fading channels," *IEEE Trans. Commun.*, vol. 46, no. 7, pp. 902–915, Jul. 1998.

[15] Z. Li, Y. Zhu, and K. G. Shin, "iCoding: Countermeasure against interference and eavesdropping in wireless communications," in *Proc. IEEE Glob. Commun. Conf.*, Madrid, Spain, 2021, pp. 1–6.

[16] Z. Li et al., "SCIM: Incorporating secure communication and interference management in one operation," *Digit. Commun. Netw.*, vol. 9, no. 2, pp. 512–522, 2023.

[17] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan, and R. Wichman, "In-band full-duplex wireless: Challenges and opportunities," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 9, pp. 1637–1652, Sep. 2014.

[18] E. Everett, A. Sahai, and A. Sabharwal, "Passive self-interference suppression for Full-Duplex infrastructure nodes," *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 680–694, Feb. 2014.

[19] N. Lee and C. Wang, "Aligned interference neutralization and the degrees of freedom of the two-user wireless networks with an instantaneous relay," *IEEE Trans. Commun.*, vol. 61, no. 9, pp. 3611–3619, Sep. 2013.

[20] Z. Li et al., "Decomposed and distributed modulation to achieve secure transmission," *IEEE Trans. Mobile Comput.*, vol. 23, no. 12, pp. 1–18, Dec. 2024.

[21] IEEE Std 802.11-2020, IEEE Standard for Information Technology — Telecommunications and Information Exchange between Systems — Local and Metropolitan Area Networks—Specific Requirements — Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Computer Society, 2020.

[22] D. Feng, L. Lu, Y. Yuan-Wu, G. Y. Li, S. Li, and G. Feng, "Device-to-device communications in cellular networks," *IEEE Commun. Mag.*, vol. 52, no. 4, pp. 49–55, Apr. 2014.

[23] Z. Li, X. Dai, and G. K. Shin, "Decoding interfering signals with fewer receiving antennas," in *Proc. Annu. IEEE Intl. Conf. Comput. Commun.*, 2016, pp. 658–666.

[24] Evolved Universal Terrestrial Radio Access (E-UTRA); User equipment (UE) radio transmission and reception, 3rd General Partnership Project (3GPP), TS 36.101 V18.3.0, 2023.

[25] Evolved Universal Terrestrial Radio Access (E-UTRA); Base station (BS) radio transmission and reception, 3rd General Partnership Project (3GPP), TS 36.104 V18.4.0, 2024.

**Zhao Li** (Senior Member, IEEE) received the BS degree in telecommunications engineering, the MS and PhD degrees in communication and information systems from Xidian University, Xi'an, China, in 2003, 2006, and 2010, respectively. He is currently an associate professor in the School of Cyber Engineering, Xidian University. He has published more than 60 technical articles with premium international journals and conferences, such as *IEEE Transactions on Mobile Computing (TMC)*, *IEEE Transactions on Information Forensics and Security (TIFS)*, *IEEE Transactions on Wireless Communications (TWC)*, and *IEEE INFOCOM*. His research interests include wireless communication, 5G communication systems, interference management, IoT and physical layer security.

**Lijuan Zhang** is currently working toward the master's degree in the School of Cyber Engineering, Xidian University. Her research interests include physical layer security and reconfigurable intelligent surface.

**Kang G. Shin** (Life Fellow, IEEE) is the Kevin & Nancy O'Connor Professor of Computer Science in the Department of Electrical Engineering and Computer Science, The University of Michigan, Ann Arbor. His current research focuses on safe and secure embedded real-time and cyber-physical systems as well as QoS-sensitive computing and networking. He has supervised the completion of 93 PhDs, and authored/coauthored about 1,000 technical articles, a textbook and about 60 patents or invention disclosures, and received numerous awards, including 2023 IEEE TCCPS Technical Achievement Award, 2023 SIGMOBILE Test-of-Time Award, 2019 Caspar Bowden Award for Outstanding Research in Privacy Enhancing Technologies, and the Best Paper Awards from 2023 VehicleSec, 2011 ACM International Conference on Mobile Computing and Networking (MobiCom'11), the 2011 IEEE International Conference on Autonomic Computing, 2010 and 2000 USENIX Annual Technical Conferences, as well as the 2003 IEEE Communications Society William R. Bennett Prize Paper Award and the 1987 Outstanding IEEE Transactions of Automatic Control Paper Award. He has also received several institutional awards, including the Research Excellence Award, in 1989, Outstanding Achievement Award, in 1999, Distinguished Faculty Achievement Award in 2001, and Stephen Attwood Award in 2004 from The University of Michigan (the highest honor bestowed to Michigan Engineering faculty); a Distinguished Alumni Award of the College of Engineering, Seoul National University in 2002; 2003 IEEE RTC Technical Achievement Award; and 2006 Ho-Am Prize in Engineering (the highest honor bestowed to Korean-origin engineers). He has chaired Michigan Computer Science and Engineering Division for 4 years starting 1991, and also several major conferences, including 2009 ACM MobiCom, and 2005 ACM/USENIX MobiSys. He was a co-founder of a couple of startups, licensed some of his technologies to industry, and served as an Executive Advisor for Samsung Research.

**Jia Liu** (Senior Member, IEEE) received the BE degree from the School of Telecommunications Engineering, Xidian University, Xi'an, China, in 2010, and the PhD degree from the School of Systems Information Science, Future University Hakodate, Japan, in 2016. He has published more than 70 academic papers at premium international journals and conferences, such as *IEEE Transactions on Dependable and Secure Computing (TDSC)*, *IEEE Transactions on Mobile Computing (TMC)*, *IEEE Transactions on Information Forensics and Security (TIFS)*, and *IEEE INFOCOM*. His research interests include wireless systems security, space-air-ground integrated networks, Internet of Things, 6G, etc. He received the IEEE Sapporo Section Encouragement Award, in 2016 and 2020.

**Yicheng Liu** (Graduate Student Member, IEEE) is currently working toward the PhD degree with the School of Cyber Engineering, Xidian University. His research interests include wireless communication, physical layer security, and interference management.

**Pintian Lyu** is currently working toward the master's degree in the School of Cyber Engineering with Xidian University. His research interests include physical layer security and interference management.

**Zheng Yan** (Fellow, IEEE) received the BEng degree in electrical engineering, the MEng degree in computer science and engineering from Xi'an Jiaotong University, Xi'an, China, in 1994 and 1997, respectively, the MEng degree in information security from the National University of Singapore, Singapore, in 2000, and the LicSc degree and DSc (Tech.) degree in electrical engineering from the Helsinki University of Technology, Helsinki, Finland, in 2005 and 2007, respectively. She is currently a distinguished Professor with Xidian University. She has published more than 400 papers in prestigious journals and conferences worldwide, including *IEEE Security and Privacy*, *IEEE Transactions on Information Forensics and Security (TIFS)*, *IEEE Transactions on Dependable and Secure Computing (TDSC)*, *IEEE INFOCOM*, and *ACM/ICCC ICSE*. She is the inventor and the co-inventor of more than 110 patents and 50 PCT patent applications. Her research interests include trust, security and privacy, social networking, cloud computing, networking systems, and data mining. She also serves as an executive editor-in-chief of Information Sciences and Area Editor/Associate Editor/Editorial Board Member of more than 60 journals, including *ACM Computing Surveys, Information Fusion*, *IEEE Internet of Things Journal*, *IEEE Network Magazine*, etc. She has served as a general chair or program committee chair for more than 40 international conferences and has delivered more than 30 keynote and invited talks at international conferences and renowned enterprises.