Distributed Modulation Exploiting IRS for Secure Communications

Zhao Li, *Senior Member, IEEE*, Lijuan Zhang, Siwei Le, Kang G. Shin, *Life Fellow, IEEE*, Jia Liu, *Senior Member, IEEE*, and Zheng Yan, *Fellow, IEEE*

***Abstract*—Due to the broadcast nature of wireless communications, users' data transmitted wirelessly is susceptible to security/privacy threats. The conventional modulation scheme "loads" all of the user's transmitted information onto a physical signal. Then, as long as an adversary overhears and processes the signal, s/he may access the user's information, hence breaching communication privacy. To counter this threat, we propose IRS-DMSC, a *Distributed Modulation based Secure Communication* (DMSC) scheme by exploiting *Intelligent Reflecting Surface* (IRS). Under IRS-DMSC, two sub-signals are employed to realize legitimate data transmission. Of these two signals, one is directly generated by the legitimate transmitter (Tx), while the other is obtained by modulating the phase of the direct signal and then reflecting it at the IRS in an indirect way. Both the direct and indirect signal components superimpose on each other at the legitimate receiver (Rx) to produce a waveform identical to that obtained under traditional centralized modulation (CM), so that the legitimate Rx can employ the conventional demodulation method to recover the desired data from the received signal. IRS-DMSC incorporates the characteristics of wireless channels into the modulation process, and hence can fully exploit the randomness of wireless channels to enhance transmission secrecy. However, due to the distribution and randomization of legitimate transmission, it becomes difficult or even impossible for an eavesdropper to wiretap the legitimate user's information. Furthermore, in order to address the problem of decoding error incurred by the difference of two physical channels' fading, we develop *Relative Phase Calibration* (RPC) and *Constellation Point Calibration* (CPC), to improve decoding correctness at the legitimate Rx. Our method design, experiment, and simulation have shown the proposed IRS-DMSC to prevent eavesdroppers from intercepting legitimate information while maintaining good performance of the legitimate transmission.**

***Index Terms*—Physical-layer security, secure communication, anti-eavesdropping, intelligent reflecting surface (IRS), distributed modulation.**

I. Introduction

OVER the past several decades, wireless technologies have been developing rapidly to meet the continuous growth of the number of mobile subscribers and their data traffic demand. In 5G (Fifth Generation) wireless communication, mobile communication networks are predicted to connect more than 100 billion devices and provide services to more than 7 billion users all over the world, and moreover, the device connection density will reach 1 million per square kilometer [1]. Wireless communication utilizes open space as transmission medium; its broadcast nature incurs vulnerability of legitimate transmission as attackers in the coverage of user's signal may intercept his/her data without permission, hence threatening the secrecy of communication [2]. Moreover, with the increasing numbers of wireless access points and devices, the threats of malicious attack, eavesdropping, and abuse of wireless devices have been continuously growing [3]. Meanwhile, wireless network and mobile services are widely used in personal and commercial activities, yielding wireless transmission of a large amount of sensitive information involving personal privacy and business secrets. Once the signal carrying the above-mentioned private information is intercepted and accessed by adversaries, a great loss/harm may occur. Therefore, Secure Communication (SC) is key to wireless technologies, and crucial to the wider application of future wireless data services.

Existing wireless networks employ the Transmission Control Protocol/Internet Protocol (TCP/IP) based architecture, in which each layer independently provides protection and security measures for the entire protocol stack, so as to guarantee the secrecy and integrity of data transmission. For example, the application layer encrypts and decrypts data to prevent unauthorized access of a legitimate user's plain-text information; network and transportation layers employ authentication schemes to authenticate/validate the identity of data sender/receiver, e.g., Wi-Fi Protected Access (WPA) and WPA2 in network layer, and Secure Sockets Layer (SSL) and Transport Layer Security (TLS) in transportation layer. These security techniques are mainly based on cryptography in which conventional encryption and

Received 21 June 2024; revised 3 April 2025; accepted 10 June 2025. Date of publication 16 June 2025; date of current version 3 September 2025. This work was supported in part by the National Natural Science Foundation of China under Grant 62072351, Grant U23A20300, Grant 62202359, in part by the 111 Center under Grant B16037, in part by the Science and Technology Research Project of Henan Province under Grant 252102211120, in part by JSPS KAKENHI under Grant JP25K15087, 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 C. S. Xin. *(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, Siwei Le, and Zheng Yan are with the School of Cyber Engineering, Xidian University, Xi'an 710126, China (e-mail: happyacce@163.com; lesiwei6@gmail.com; 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.2025.3579960

decryption are realized based on key generation and complex computations therein, while authentication always adopts a digital signature technique derived from asymmetric encryption. Although cryptography-based encryption and authentication can effectively enhance communication privacy, complicated operations increase computational complexity. This not only demands higher computing power for devices, but also incurs extra processing delay, thereby impeding its broad application in wireless devices, such as Internet of Things (IoT) devices and Backscatter devices. Moreover, with the rapid development of computing science, the eavesdropper's computing power continuously grows. Therefore, traditional cryptography based security built with computational complexity is facing practical challenges.

To counter the above challenges and threats, Physical-Layer (PHY) wireless security technologies have been attracting extensive attention in recent years [4]. As the bottom layer of TCP/IP protocol stack, PHY provides fundamental basis for transmission secrecy. After years of research, there have been numerous PHY security technologies to improve wireless privacy [5], [6], [7], [8], [9], [10], which can be divided into two categories. The first one (denoted as type-I) is featured as data encoding or signal processing based on information theory, with which Signal-to-Interference-plus-Noise Ratio (SINR) of the legitimate Rx can be superior to that of the eavesdropper, hence enhancing secrecy capacity.[1] The other type (denoted as type-II) of PHY security technologies exploits the characteristics of wireless channels to encrypt legitimate transmission or authenticate the identity of legitimate user-pair, so that wiretapping and disguising from attackers can be prevented.

Besides the above-mentioned PHY security techniques, newly emerging communication equipments and devices, such as relay [13], Large Intelligent Surfaces (LIR) [14], as well as continuous evolvement of communication systems' architectures and data transmission mechanisms, also influence the design of PHY security strategies. With the emergence of Micro-Electro-Mechanical Systems (MEMS) and meta-material in recent years, using a programmable surface to control the reflecting signal's phase-shift in real time becomes available, prompting a new type of wireless device — Intelligent Reflecting Surface (IRS). IRS can be composed of a large number of low-cost passive reflection units, each of them introduces a phase-shift to and then reflects the incoming signal under the control of an IRS controller, so that the reflecting signal and the directly transmitted signal can either constructively or destructively combined at a Rx. IRS can be flexibly deployed in wireless networks to improve data transmission [15], realize PHY security [16], [17], [18], [19], and facilitate mobile edge computing [20], thus is regarded as a revolutionary technology in the field of wireless communications [21].

Although the above-mentioned PHY security methods can realize secure communication to a certain extent, they rely on conventional Centralized Modulation (CM), i.e., all of the user's information is loaded onto a single physical signal for transmission. In other words, signal from the legitimate Tx carries entire user data. Once an eavesdropper intercepts and processes such physical signal, the legitimate user's information may be accessed unauthorizedly, thus breaching communication privacy. Motivated by the availability of exploiting interactions among multiple wireless signals in transmission schemes design [22], we suggest that legitimate Tx can divide its transmitted data into two parts, and load each part onto an individual signal for transmission; these two signals propagate along uncorrelated/independent physical channels and superimpose on each other at the legitimate Rx to output a waveform identical to that obtained under conventional CM. We call such Tx-side processing *Distributed Modulation* (DM). The Rx can employ traditional demodulation method to decode the desired data from the received mixed signal. As for the eavesdropper, wiretapping one signal can only yield the legitimate user's partial information without complete meaning; however, intercepting both signal components simultaneously and precisely obtaining their combination need accurate propagation characteristics of the two physical channels. Since acquiring such information is expensive or even impossible in practice, eavesdropping can be prohibited.

Motivated by the above observation, we will employ IRS[2] to design a *Distributed Modulation Secure Communication* (DMSC) scheme — named as *IRS-DMSC*, in this paper. With IRS-DMSC, a desired signal waveform is at first equivalent to two sub-waveforms. Next, the legitimate Tx generates one sub-waveform and sends it to the legitimate Rx and IRS simultaneously. At the IRS, the incoming/incident direct signal is phase-shifted to yield an indirect signal and then reflected to the Rx. Both the direct and indirect/reflecting signals superimpose on each other at the legitimate Rx to produce the desired waveform the same as that obtained under traditional CM, so that the Rx can employ conventional demodulation method to recover the desired data from the received mixed signal. Under IRS-DMSC, the desired signal waveform only manifests at the intended Rx, hence the eavesdropper can't extract meaningful legitimate information by intercepting the signal components during their transmission. Moreover, since IRS-DMSC incorporates the characteristics of two independent/uncorrelated wireless channels into the modulation process, it can fully exploit the randomness of wireless channels to guarantee the transmission privacy. However, as the eavesdropper can't obtain all of the related channel information in practice, h/she is incapable of detecting legitimate user's data from the intercepted signal(s), hence eavesdropping is crippled.

The main contributions of this paper are three-fold:

- Proposal of IRS-DMSC under QPSK. With this method, the legitimate Tx only modulates user's partial data information onto a signal to generate a direct BPSK signal, such

[1] In [11], [12], Shannon and Wyner defined secrecy capacity as the difference of the channel capacity of legitimate Rx and that of the eavesdropper.

[2] Existing research categorizes the IRS into two types: passive IRS and active IRS. The former considers software and hardware costs, limiting the adaptability of the amplitude coefficient of IRS elements. In contrast, the active IRS integrates a power amplifier, enabling adjustment of the amplitude coefficient of the IRS elements beyond 1. To avoid introducing additional power consumption, we confine the amplitude coefficient of the IRS within the range of $[0, 1]$. Therefore, the IRS employed in our work falls under the passive category.

a signal is on one hand directly sent to the legitimate Rx, and on the other hand phase-modulated at IRS to yield an indirect BPSK component and then reflected to the Rx. The legitimate Rx can recover the desired data from the received mixed signal with conventional demodulation method. We also design a phase-calibration method to compensate for the difference of two physical channels' fading so that the correctness of reception under DM can be guaranteed.

- Extension of IRS-DMSC to more general high-order modulation schemes. First, we present the decomposition of a high-order modulated signal, including M-ary Quadrature Amplitude Modulation (MQAM) and M-ary Phase Shift Keying (MPSK), into two sub-waveforms. Based on such decomposition, IRS-DMSC can be directly applied. Consequently, we develop a constellation calibration method to adjust the received mixed signal's amplitude and phase, so that the legitimate Rx can accurately estimate a symbol that corresponds to the desired data from its received signal, enabling the correct recovery of the desired information.
- Experimental validation of the proposed method using the USRP platform. By utilizing a USRP device to emulate the generation of the indirect signal component and the reflection of such a signal to the target Rx, we have demonstrated that employing distributed modulation can produce the desired signal at the intended Rx and ensure the security of the legitimate communication.

The rest of the paper is organized as follows. Section II introduces state-of-the-art PHY security schemes. Section III describes the system model, while Section IV details the design of IRS-DMSC and phase calibration under QPSK. In Section V, we discuss the extension of IRS-DMSC to high-order modulation scenarios and constellation point calibration method to assure reception correctness. We evaluate the performance of the proposed IRS-DMSC in Section VI, and finally conclude the paper in Section VII.

II. Related Works

As aforementioned, existing PHY security methods can be divided into two categories. Typical type-I PHY security methods include artificial noise [5], [6], transmit beamforming [7], etc. In [5], [6], a portion of legitimate Tx's power is used for generating an interfering signal, named as Artificial Noise (AN), which degrades eavesdropper's reception quality while its influence at the legitimate Rx can be eliminated. Therefore, SINR of legitimate Rx is higher than that of eavesdropper. The authors of [7] designed secure transmit beamforming in multi-antenna communication system. By adjusting the spatial feature of the legitimate Tx's signal, desired signal components constructively and destructively combine with each other at their destination and the eavesdropper, respectively, hence maximizing legitimate Rx's SINR while reducing eavesdropper's. [8] proposed an Interference Alignment (IA) based anti-eavesdropping strategy, with which the legitimate Tx generates AN either individually or cooperatively with relay to interrupt the wiretap channel while avoiding impacts on the legitimate Rx. The principle of type-II PHY security measure is similar to that of cryptography based method, with which a legitimate communication-pair estimates the transmission channel and exploits the randomness and reciprocity of wireless channel to generate encryption/decryption key. This scheme doesn't need third-party to execute key distribution and management, hence is easy to implement [9]. The authors of [10] proposed a PHY security algorithm based on constellation phase rotation and amplitude randomization. The legitimate Rx can recover the original constellation via an inverse transformation after establishing synchronization with its Tx, while eavesdroppers can't realize such synchronization and thus is unable to obtain legitimate information. In this scheme, constellation phase rotation and amplitude randomization function as the secret key for PHY encryption.

In terms of IRS-aided PHY security methods, the authors of [16] considered an IRS assisted Gaussian Multiple-Input Multiple-Output (MIMO) wiretap channel; to maximize the secrecy rate of this channel, they proposed an alternating optimization algorithm to jointly optimize the transmit covariance at Tx and the phase-shift coefficient at IRS. [17] employed IRS to maximize the secrecy capacity of an AN-aided MIMO system. In this work, IRS is used to modify the phase of the signal from legitimate Tx, such a phase-shifted reflecting signal acts as AN to disturb the eavesdropper. Since the legitimate Tx doesn't need to generate AN, its transmit power is saved. In this scheme, Lagrange multiplier method was used in joint optimization of the transmit precoding matrix, covariance matrix of AN, and phase-shifts at the IRS. The authors of [18] virtually partitioned the IRS elements into two parts. By configuring the phase shifts of different partitions, they improved the desired signal at the intended Rx while enhancing the impact of AN on an unintended Rx. In [19], an IRS-aided secure communication scheme for Multiple-Input Single-Output (MISO) system was proposed. By optimally adjusting the phase-shifts of the IRS's reflection units, the reflecting signal from IRS and the non-reflecting signal constructively add to each other at the legitimate user, while destructively add at the eavesdropper to cancel his/her received signal, so that the secrecy rate of legitimate user can be maximized. However, this method needs the Channel State Information (CSI) [23] related to eavesdropper. Nevertheless, in practice, it is difficult to get such information due to the passive feature of eavesdropper.

Table I highlights the primary differences between IRS-DMSC and other typical security schemes, where symbols "○" and "×" indicate having and not having the corresponding feature, respectively. "–" indicates that some methods some methods have the feature, while the others do not. From the table, we can observe the advantages of IRS-DMSC compared to the other schemes.

III. System Model

We consider a wireless communication system consisting of a legitimate Tx (Alice), an IRS controlled by the legitimate Tx, a legitimate Rx (Bob), and an eavesdropper (Eve), as shown in Fig. 1. Alice has N_T transmit antennas, while Bob and Eve are equipped with N_R receiving antennas. The IRS is composed of M reflection units. Let $\mathbf{H}_{xy}$ denote the legitimate channel

TABLE I
COMPARISON OF IRS-DMSC AND OTHER EXISTING SECURITY MEASUREMENTS

Feature \ Method	Cryptography based method	Type-I PHY security method	Type-II PHY security method	IRS-aided security method	IRS-DMSC
Increase of computational complexity	○	×	○	×	×
Security key management	○	×	×	×	×
Transmit power consumption	×	○	×	×	×
Dependence on eavesdropper's CSI	×	–	×	–	×
Single signal carrying all user information	○	○	○	○	×

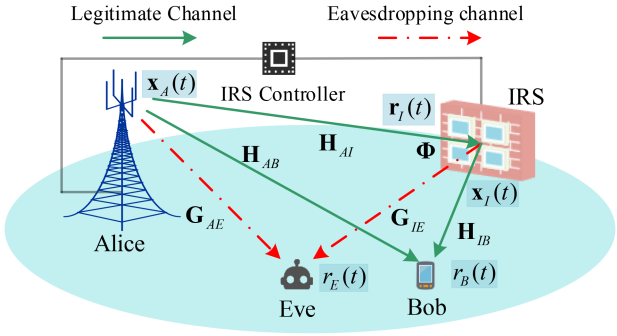


Fig. 1. System model.

matrix associated with Alice or/and Bob, while $\mathbf{G}_{xy}$ denotes the wiretap channel matrix associated with Eve. The subscript pair xy represents a transmission pair of devices x and y. Specifically, $\mathbf{H}_{AI} \in \mathbb{C}^{M\times N_T}$, $\mathbf{H}_{AB} \in \mathbb{C}^{N_R\times N_T}$, and $\mathbf{H}_{IB} \in \mathbb{C}^{N_R\times M}$ represent the channel fading (a.k.a. channel status information (CSI)) from Alice to IRS, Alice to Bob, and IRS to Bob, respectively. Additionally, $\mathbf{G}_{AE} \in \mathbb{C}^{N_R\times N_T}$ and $\mathbf{G}_{IE} \in \mathbb{C}^{N_R\times M}$ denote the channel fading from Alice to Eve and IRS to Eve, respectively. We employ a spatially uncorrelated Rayleigh flat fading [24] channel model, so that the elements in $\mathbf{H}_{xy}$ and $\mathbf{G}_{xy}$ can be modeled as independent and identically distributed (i.i.d.) zero-mean unit-variance complex Gaussian random variables. We assume that all channels exhibit block fading characteristics, i.e., channel parameters in a block consisting of several successive transmission cycles remain constant in the block and vary randomly across blocks. Since Alice controls the IRS, she can obtain $\mathbf{H}_{AI}$. Moreover, Bob can estimate $\mathbf{H}_{AB}$ and $\mathbf{H}_{IB}$ accurately, and feed this information back to Alice via a control link. We assume reliable links for the delivery of CSI and signaling. The delivery delay is negligible relative to the time scale at which the channel state varies [25]. We assume that the eavesdropper can estimate $\mathbf{G}_{AE}$ and $\mathbf{G}_{IE}$, but cannot obtain $\mathbf{H}_{AB}$, $\mathbf{H}_{AI}$, and $\mathbf{H}_{IB}$.

As Fig. 1 shows, IRS connects to Alice via an IRS controller. Alice coordinates CSI[3] collection and signaling between her and IRS via the controller. Each reflection unit of the IRS independently introduces an adjustable phase shift to the incoming signal from Alice, and then reflects the phase-modulated signal to Bob. The reflection coefficient matrix of the IRS, denoted as $\mathbf{\Phi} \in \mathbb{C}^{M\times M}$, is a diagonal matrix, that can also be expressed as $\mathbf{\Phi} = \text{diag}([\alpha_1\alpha_2\cdots\alpha_M])$, where $\text{diag}(\cdot)$ denotes the diagonalization of a vector. We use $\alpha_i = \beta_i e^{j\theta_i}$ to indicate the ith ($i \in \{1, 2, \ldots, M\}$) reflection coefficient of the IRS, where $\beta_i \in [0, 1]$ is the amplitude distortion and $\theta_i \in (-\pi, \pi]$ is the phase offset. For simplicity, we set $\beta_i = 1$ and neglect the signal components reflected more than once [15].

Before delving into details, we present the main symbols used in this paper in Table II.

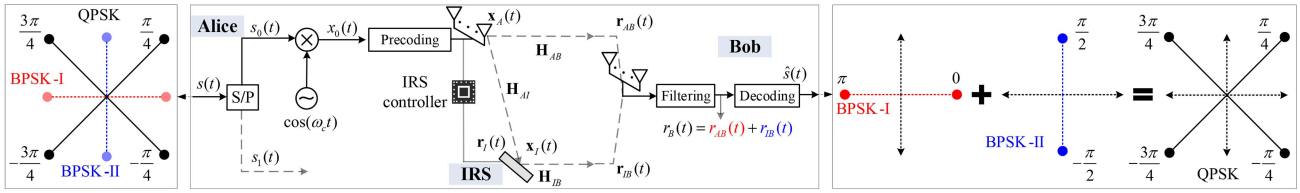
TABLE II
TABLE OF SYMBOLS

Symbols	Description
P_T	Transmit power of Alice
N_T	The number of Alice's antennas
N_R	The number of Bob and Eve's antennas
$\mathbf{H}_{AI}$, $\mathbf{H}_{AB}$	Channel matrices between Alice and IRS/Bob
$\mathbf{H}_{IB}$	Channel matrix between IRS and Bob
$\mathbf{G}_{AE}$, $\mathbf{G}_{IE}$	Channel matrices between Alice/IRS and Eve
$\mathbf{h}_{AI}^{(i)}$, $\mathbf{h}_{IB}^{(i)}$	The i^{th} element of $\mathbf{H}_{AI}$ and $\mathbf{H}_{IB}$
M	The number of IRS elements
Φ	Reflection coefficient matrix of IRS
α_i, β_i, θ_i	Reflection coefficient along with its amplitude and phase-shift coeffs. of the i^{th} IRS element
$s(t)$	Transmitted bipolar data sequence
$s_0(t)$, $s_1(t)$	The sub-data sequences of $s(t)$
$\mathbf{r}_{AB}$	The signal sent from Alice to Bob
$\mathbf{r}_{IB}$	The signal reflected by the IRS to Bob
r_B, r_E	The mixed signal received by Bob/Eve
$\hat{r}_B$	The estimated signal at Bob
$\mathbf{p}$	Precoding vector at Alice
$\mathbf{f}$	Filtering vector at Bob
T_s	Symbol period
x_0, x_1	BPSK-I and BPSK-II symbols
$\mathbf{z}$, σ_n^2	AWGN and its power
h	Fading characteristics
$\mathcal{J}(\cdot)$	The effective data symbol carried in a signal
$\mathcal{S}$, ζ, $\theta_{\mathcal{S}}$	The modulated symbol along with its amplitude and phase offset
$e^{j\phi}$	Pre-attenuation factor of r_{AB}
c_B, c_E, c_S	The legitimate/wiretap/secrecy channel capacity
$P(x)$, $P(\hat{x})$	The probabilities of x and $\hat{x}$
$P(x, \hat{x})$	The joint probability density of x and $\hat{x}$
η	The normalized ratio of Alice's transmit power to noise power
p_B, p_E	Bob and Eve's BER

IV. DESIGN OF IRS-DMSC UNDER QPSK

In this section, we take QPSK as an example to present the design of IRS-DMSC, and then propose the corresponding calibration method to combat the decoding error caused by the

[3]Although the CSI may be imperfect in practice, our method remains applicable, albeit with some performance degradation. Since our focus is on designing and validating the secure transmission scheme, we will not discuss the impact of imperfect CSI on the method's performance. However, this aspect can be addressed similarly to [26], [27].



(a) Decomposition of Tx-side QPSK constellation into two orthogonal BPSK constellations

(b) Workflow of IRS-DMSC

(c) Two BPSK constellations combine to be a QPSK constellation at the Rx-side (w/o channel fading)

Fig. 2. Illustration of IRS-DMSC's realization under QPSK modulation.

difference of fading in two independent/uncorrelated transmission channels.

A. Basic Design of IRS-DMSC

The main idea of IRS-DMSC is based on the fact that a QPSK modulation can be decomposed into two orthogonal BPSK components [28]. Under IRS-DMSC, user's data information is at first divided into two parts. Then, Alice directly generates a BPSK signal carrying one part of the divided user's information and sends it to Bob and IRS. Meanwhile, IRS modulates the incoming signal's phase under the control of Alice, so as to yield another BPSK signal which contains the other part of user's information and is orthogonal to the direct one. Both signals superimpose at Bob to produce a QPSK signal. In this way, distributed modulation and transmission of legitimate user's information is realized.

Fig. 2 plots the realization of IRS-DMSC under QPSK. Without of loss of generality, we denote the BPSK modulation whose symbol's phase is either 0 or π as BPSK-I. Similarly, the other BPSK signal whose symbol's phase is selected from set $\{-\frac{\pi}{2}, \frac{\pi}{2}\}$ is denoted as BPSK-II. As Fig. 2(a) shows, a QPSK constellation whose phase set is $\{-\frac{3\pi}{4}, -\frac{\pi}{4}, \frac{\pi}{4}, \frac{3\pi}{4}\}$ can be equivalent to the combination of BPSK-I and BPSK-II. Fig. 2(b) plots the workflow of IRS-DMSC, where we denote the transmitted bipolar data sequence as $s(t)$. By applying Serial-to-Parallel (S/P) conversion to $s(t)$, we can have two sub-data sequences, i.e., $s_0(t)$ and $s_1(t)$. Without loss of generality, we let Alice select $s_0(t)$ to multiply by a carrier signal $\cos(\omega_c t)$, so that a *direct* BPSK signal is obtained as:

$$x_0(t) = s_0(t)\cos(\omega_c t). \tag{1}$$

Then, Alice applies the precoding vector $\mathbf{p} \in \mathbb{C}^{N_T \times 1}$ to $x_0(t)$ (will be detailed in Section IV-B) to obtain $\mathbf{x}_A(t) = \mathbf{p}x_0(t)$ and simultaneously transmits it to Bob and the IRS with transmit power P_T. We use $\mathbf{r}_{AB}(t)$ to represent the signal sent from Alice and directly received by Bob. Similarly, the signal sent from Alice and perceived by IRS is denoted as $\mathbf{r}_I(t)$. IRS modulates the incoming signal's phase under the control of Alice via the IRS controller, so we can get an *indirect* signal reflected from IRS as $\mathbf{x}_I(t)$. We use $\mathbf{r}_{IB}(t)$ to represent the signal reflected by the IRS and received by Bob. Bob post-processes the superimposed signal $\mathbf{r}_{AB}(t) + \mathbf{r}_{IB}(t)$ with a receive filter $\mathbf{f} \in \mathbb{C}^{N_R \times 1}$ to obtain a filtered signal r_B, from which the desired data $\hat{s}(t)$ is decoded. In what follows, we will discuss the realization of IRS-DMSC within one symbol period T_s ($kT_s < t \leq (k+1)T_s$) where k is the index of the kth BPSK symbol and T_s is the symbol duration. For simplicity, we omit the time index t in the following discussion. Additionally, since x carries the same information as s, we can without ambiguity equate[4] them as synonyms. Correspondingly, x_0 and x_1 represent the BPSK-I and BPSK-II symbols, respectively. At the Rx-side, Bob processes the superimposed signal with $\mathbf{f}$ to obtain:

$$r_B = \sqrt{P_T}\mathbf{f}^H\mathbf{H}_{AB}\mathbf{p}x_0 + \sqrt{P_T}\mathbf{f}^H\mathbf{H}_{IB}\mathbf{\Phi}\mathbf{H}_{AI}\mathbf{p}x_0 + \mathbf{f}^H\mathbf{z} \tag{2}$$

where $\mathbf{z}$ represents an Additive White Gaussian Noise (AWGN) vector whose elements have zero mean and variance σ_n^2. Recall that we set $\beta_i = 1$, the key to IRS-DMSC's design is determining the phase-shift coefficient θ_i so as to output r_B which has the same waveform as that yielded by conventional centralized QPSK modulation.

Without causing ambiguity, we call the channel from Alice to Bob *Direct Transmission Channel (DTC)* whereas that from Alice to IRS and then to Bob *Indirect Reflection Channel* (IRC). Then, we can represent the filtered/post-processed DTC signal component and IRC signal component in (2) as:

$$r_{AB} = \sqrt{P_T}\mathbf{f}^H\mathbf{H}_{AB}\mathbf{p}x_0 \tag{3}$$

and

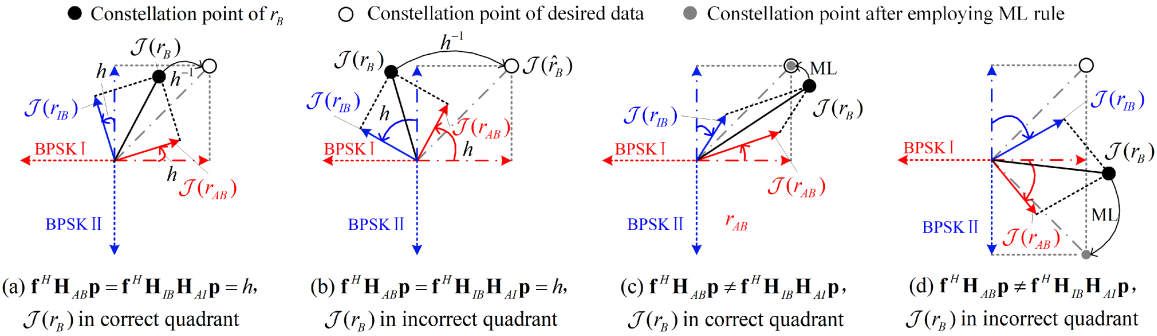
$$r_{IB} = \sqrt{P_T}\mathbf{f}^H\mathbf{H}_{IB}\mathbf{\Phi}\mathbf{H}_{AI}\mathbf{p}x_0. \tag{4}$$

Due to the independence of DTC and IRC, their distinct fading characteristics may lead to different reception and decision outcomes, as illustrated in Fig. 3. For ease of presentation, we first assume that all reflection coefficients of the IRS are identical, i.e., $\theta_i = \hat{\theta}$, and both the DTC and IRC demonstrate identical fading characteristics, i.e., $\mathbf{f}^H\mathbf{H}_{AB}\mathbf{p} = \mathbf{f}^H\mathbf{H}_{IB}\mathbf{H}_{AI}\mathbf{p} = h$ holds. The design of IRS-DMSC for more general scenarios will be discussed subsequently. Then, (2) can be simplified to:

$$r_B = \sqrt{P_T}h\left(x_0 + \sum_{i=1}^{M} e^{j\hat{\theta}}x_0\right). \tag{5}$$

We can see from (1) that x_0 is the BPSK-I signal which modulates data s_0 onto carrier $\cos(\omega_c t)$. Then, IRS should convert

[4]This equivalence involves the down-conversion of the frequency signal to obtain a baseband signal, similar to the operator $\mathcal{J}(\cdot)$ introduced in the discussion of Fig. 3.



(a) $\mathbf{f}^H\mathbf{H}_{AB}\mathbf{p} = \mathbf{f}^H\mathbf{H}_{IB}\mathbf{H}_{AI}\mathbf{p} = h$, $\mathcal{J}(r_B)$ in correct quadrant

(b) $\mathbf{f}^H\mathbf{H}_{AB}\mathbf{p} = \mathbf{f}^H\mathbf{H}_{IB}\mathbf{H}_{AI}\mathbf{p} = h$, $\mathcal{J}(r_B)$ in incorrect quadrant

(c) $\mathbf{f}^H\mathbf{H}_{AB}\mathbf{p} \neq \mathbf{f}^H\mathbf{H}_{IB}\mathbf{H}_{AI}\mathbf{p}$, $\mathcal{J}(r_B)$ in correct quadrant

(d) $\mathbf{f}^H\mathbf{H}_{AB}\mathbf{p} \neq \mathbf{f}^H\mathbf{H}_{IB}\mathbf{H}_{AI}\mathbf{p}$, $\mathcal{J}(r_B)$ in incorrect quadrant

Fig. 3. Various situations of the effective data carried in r_B.

TABLE III
PHASE-SHIFT VALUES OF IRS FOR VARIOUS QPSK DATA SYMBOLS

QPSK symbol	BPSK-I		BPSK-II		$\hat{\theta}$
	s_0	Phase	s_1	Phase	
$(-1,-1)$	-1	0	-1	$\frac{\pi}{2}$	$\frac{\pi}{2}$
$(-1,+1)$			$+1$	$-\frac{\pi}{2}$	$-\frac{\pi}{2}$
$(+1,-1)$	$+1$	π	-1	$\frac{\pi}{2}$	$-\frac{\pi}{2}$
$(+1,+1)$			$+1$	$-\frac{\pi}{2}$	$\frac{\pi}{2}$

its perceived version of x_0, i.e., hx_0, to BPSK-II signal which is equivalent to a modulated signal obtained by multiplying s_1 by $\sin(\omega_c t)$, and reflect such an indirect modulated signal to Bob. So, Bob can see a filtered superimposed signal r_B who has a QPSK signal's waveform attenuated by the fading coefficient h. Based on the above analysis, the term $\sum_{i=1}^{M} e^{j\hat{\theta}}x_0$ in (5) should be the BPSK-II signal in which s_1 is carried. According to Fig. 2(a) and (c), phase difference of BPSK-I and BPSK-II signals is either $-\frac{\pi}{2}$ or $\frac{\pi}{2}$ depending on the data carried in both signals. Therefore, in order to obtain a combined QPSK signal at Bob, we need to set $\hat{\theta} \in \{-\frac{\pi}{2}, \frac{\pi}{2}\}$. Table III shows the phase-shift values corresponding to various QPSK data symbols, using Gray code as an example.

In order to intuitively illustrate the relationships between various signal components, we define operator $\mathcal{J}(\cdot)$ to denote the effective data symbol carried in a signal. Note that for different signals, $\mathcal{J}(\cdot)$ may stand for various operations [29], e.g., $\mathcal{J}(s_0 \cos \omega t)$ represents applying coherent demodulation [28] to $s_0 \cos \omega t$ to obtain s_0. By employing $\mathcal{J}(\cdot)$, we can map signal to a constellation map where an effective data symbol carried in the signal can be represented by a two-dimensional vector starting from the origin and ending at the effective data point. In Fig. 3, we take the desired QPSK constellation point lying in the first quadrant as an example to show various situations of the effective data $\mathcal{J}(r_B)$ carried in the mixed signal r_B. Fig. 3(a) and (b) are plotted under the assumption of $\mathbf{f}^H\mathbf{H}_{AB}\mathbf{p} = \mathbf{f}^H\mathbf{H}_{IB}\mathbf{H}_{AI}\mathbf{p} = h$. As the figures show, since both DTC and IRC incur identical attenuation including amplitude distortion and phase deviation to a signal transmitted therein, $\mathcal{J}(r_B)$ is away from the standard constellation point associated with the desired data. Fortunately, we can see from (5) that r_B is actually a QPSK signal that has experienced fading h; therefore, Bob can employ h^{-1} as the post-processing coefficient to obtain an estimated signal as:

$$\hat{r}_B = h^{-1}r_B = \sqrt{P_T}x_0 + M\sqrt{P_T}e^{j\hat{\theta}}x_0 \tag{6}$$

where $\hat{\theta}$ can be determined according to Table III.

In this example, we can without loss of generality encode the QPSK symbol as "00" [28], which corresponds to the bipolar symbol $(-1,-1)$. Then, according to Table II, as long as we set $\hat{\theta} = \frac{\pi}{2}$ (ensuring all reflected signal components are coherently combined with each other to maximize the amplitude of r_{IB}), $\hat{r}_B$ will become the QPSK signal plotted in Fig. 2(c) which is the combination two orthogonal BPSK signals and carries data s. Bob can then adopt traditional demodulation method, such as coherent demodulation [28], to recover desired data from $\hat{r}_B$. It should be noted that either in the case plotted in Fig. 3(a) where the channel fading is moderate so that $\mathcal{J}(r_B)$ is close to the desired standard constellation point, or in the situation shown in Fig. 3(b) where channel fading is so severe that $\mathcal{J}(r_B)$ is steered into an incorrect quadrant, Bob can process r_B with h^{-1} according to (6) to obtain the estimated signal $\hat{r}_B$ correctly.

The above discussion assumed that both DTC and IRC have the same fading features. However, in practical use, fading coefficients of various channels are always different. Therefore, in Fig. 3(c) and (d), we plot the estimation of effective data $\mathcal{J}(r_B)$ under $\mathbf{f}^H\mathbf{H}_{AB}\mathbf{p} \neq \mathbf{f}^H\mathbf{H}_{IB}\mathbf{H}_{AI}\mathbf{p}$. In these two figures, BPSK-I and BPSK-II signals experience different fading. So, post-processing given in (6) becomes inapplicable. By noting that in Fig. 3(c), $\mathcal{J}(r_B)$ is close to the desired QPSK constellation point, Bob can employ Maximum Likelihood (ML) to compare r_B with four standard QPSK waveforms so that the correct QPSK point can be determined. That is, the ML-based estimated symbol (denoted by a grey dot) coincides with the correct standard QPSK point (represented by a circle). In Fig. 3(d), severe fading causes $\mathcal{J}(r_B)$ to be far away from the desired data point. In such a case, applying ML would yield an estimated symbol identical to the standard QPSK point in an incorrect quadrant, thus incurring decoding error. It should be noted that, in cases (c) and (d) of Fig. 3, due to the different fading of DTC and IRC, Bob can't accurately calculate the phase compensation coefficient, h^{-1}, in (6). As a result, $\mathcal{J}(\hat{r}_B)$ is not depicted in the figure, but instead, we employ ML directly on $\mathcal{J}(r_B)$.

Under $\mathbf{f}^H\mathbf{H}_{AB}\mathbf{p} = \mathbf{f}^H\mathbf{H}_{IB}\mathbf{H}_{AI}\mathbf{p}$, Bob can process r_B in terms of (6), so that the identical fading of two channels is compensated, yielding a correct decoding. However, in practice, $\mathbf{f}^H\mathbf{H}_{AB}\mathbf{p} = \mathbf{f}^H\mathbf{H}_{IB}\mathbf{H}_{AI}\mathbf{p}$ is usually not true, i.e., signal components transmitted over DTC and IRC experience various amplitude distortions and phase deviations (as Fig. 3(c) and (d) show). So, Bob can't use a single post-processing coefficient to compensate for different fading, or decoding error occurs. Moreover, it should be noted that since IRS is passive reflecting device, IRS-DMSC can only adjust r_{IB}'s phase via setting IRS's phase-shift coefficient θ, so as to yield a correct estimated constellation point at Bob. In the next subsection, we will propose *Relative Phase Calibration* (RPC) to combat the decoding error caused by the differences in two uncorrelated/independent transmission channels (as plotted in Fig. 3(d)).

From the above-mentioned discussion, we can see that the basic principle of DM is to involve the propagation environment, i.e., characteristics of wireless channels, into modulation process. The signal's waveform perceived at the desired Rx under DM is identical to that with conventional CM; however, during propagation, DM and CM yield different signal's waveforms. This is because DM is completed at the Rx, while CM is finished at the Tx. So, under CM, as long as the eavesdropper wiretaps the signal sent from the legitimate Tx, the secrecy of transmission is breached; whereas for DM, user's full data is distributedly modulated onto a superimposed signal just at the legitimate Rx, but the eavesdropper can only conduct wiretapping during signals' prorogation, thus eavesdropping becomes difficult.

B. Design of Relative Phase Calibration

As aforementioned, DTC and IRC are independent of each other, thus yielding various fading and incurring decoding error at Bob. The main idea of RPC is to let the two signal components, say r_{AB} and r_{IB}, have the correct phases, i.e., r_{AB}'s phase should be either 0 or π, while r_{IB}'s is either $\frac{\pi}{2}$ or $-\frac{\pi}{2}$. In this way, the effective data $\mathcal{J}(r_B)$ carried in the filtered superimposed signal r_B will certainly locate in the right quadrant with respect to (w.r.t.) the desired constellation point, and then Bob can adopt ML to correctly recover the desired data.

Since r_{IB} is reflected from IRS to Bob, its phase can be affected by θ_i introduced at the IRS. As for r_{AB}, it is directly transmitted from Alice to Bob, hence its phase can be controlled by $\mathbf{p}$. Without loss of generality, we use Singular Value Decomposition (SVD) based precoding and filtering as an example. Specially, we apply SVD to $\mathbf{H}_{AB}$ to obtain $\mathbf{H}_{AB} = \mathbf{U}_{AB}\mathbf{\Lambda}_{AB}\mathbf{V}_{AB}^H$. Then, Alice selects $\mathbf{p} = \mathbf{v}_{AB}^{(1)}$ as the precoding vector, while Bob employs filtering vector $\mathbf{f} = \mathbf{u}_{AB}^{(1)}$, where $\mathbf{u}_{AB}^{(1)}$ and $\mathbf{v}_{AB}^{(1)}$ represent the first columns of the left and right singular matrices $\mathbf{U}_{AB}$ and $\mathbf{V}_{AB}$, respectively. So, r_B can be rewritten as:

$$r_B = \sqrt{P_T}\lambda_{AB}^{(1)}x_0 + \sqrt{P_T}\sum_{i=1}^{M}[\mathbf{u}_{AB}^{(1)}]^H\mathbf{h}_{IB}^{(i)}e^{j\theta_i}\mathbf{h}_{AI}^{(i)}\mathbf{v}_{AB}^{(1)}x_0 + [\mathbf{u}_{AB}^{(1)}]^H\mathbf{z} \tag{7}$$

TABLE IV
PHASE-SHIFT VALUES OF IRS WITH RPC FOR VARIOUS QPSK DATA SYMBOLS

QPSK symbol	BPSK-I		BPSK-II		θ_i
	s_0	Phase	s_1	Phase	
$(-1,-1)$	-1	0	-1	$\frac{\pi}{2}$	$-\text{ang}\{[\mathbf{u}_{AB}^{(1)}]^H\mathbf{h}_{IB}^{(i)}\mathbf{h}_{AI}^{(i)}\mathbf{v}_{AB}^{(1)}\} + \frac{\pi}{2}$
$(-1,+1)$			$+1$	$-\frac{\pi}{2}$	$-\text{ang}\{[\mathbf{u}_{AB}^{(1)}]^H\mathbf{h}_{IB}^{(i)}\mathbf{h}_{AI}^{(i)}\mathbf{v}_{AB}^{(1)}\} - \frac{\pi}{2}$
$(+1,-1)$	1	π	-1	$\frac{\pi}{2}$	$-\text{ang}\{[\mathbf{u}_{AB}^{(1)}]^H\mathbf{h}_{IB}^{(i)}\mathbf{h}_{AI}^{(i)}\mathbf{v}_{AB}^{(1)}\} - \frac{\pi}{2}$
$(+1,+1)$			$+1$	$-\frac{\pi}{2}$	$-\text{ang}\{[\mathbf{u}_{AB}^{(1)}]^H\mathbf{h}_{IB}^{(i)}\mathbf{h}_{AI}^{(i)}\mathbf{v}_{AB}^{(1)}\} + \frac{\pi}{2}$

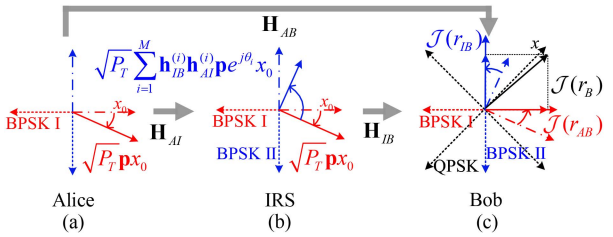


Fig. 4. Realization of IRS-DMSC employing RPC.

where $\lambda_{AB}^{(1)}$ denotes the largest singular value of the singular value matrix $\mathbf{\Lambda}_{AB}$. $\mathbf{h}_{AI}^{(i)}$ ($i \in \{1, 2, \ldots, M\}$) and $\mathbf{h}_{IB}^{(i)}$ represent the ith column vector of $\mathbf{H}_{AI}$ and the ith row vector of $\mathbf{H}_{IB}$, respectively.

Since $e^{j\theta_i}$ is a complex coefficient, we can have the filtered IRC signal component in (7) as:

$$r_{IB} = \sqrt{P_T}\sum_{i=1}^{M}[\mathbf{u}_{AB}^{(1)}]^H\mathbf{h}_{IB}^{(i)}\mathbf{h}_{AI}^{(i)}\mathbf{v}_{AB}^{(1)}e^{j\theta_i}x_0. \tag{8}$$

As each term in (8) is a complex number, and the phase of the filtered DTC component in (7) aligns with x_0, we need to ensure the phase of the post-processed IRC component align with x_1 so that a desired signal can be obtained at Bob. In what follows, we use $\|\cdot\|$ to denote the modulus of a complex number, while ang$(\cdot)$ represents calculating the phase angle of a complex number. We ensure that all the reflected signal components coherently superimpose with each other to maximize the amplitude of r_{IB}. Therefore, according to the principle of IRS-DMSC, (9) should satisfy.

$$\text{ang}\{[\mathbf{u}_{AB}^{(1)}]^H\mathbf{h}_{IB}^{(i)}\mathbf{h}_{AI}^{(i)}\mathbf{v}_{AB}^{(1)}\} + \theta_i = \pm\frac{\pi}{2}. \tag{9}$$

According to the above equation, θ_i can be calculated. Specifically, we show the values of θ_i under IRS-DMSC with RPC for various QPSK data symbols in Table IV.

To this end, utilizing the aforementioned precoding and filtering processing and setting θ_i according to Table IV, $\mathcal{J}(r_B)$ can be located in the same quadrant as the desired QPSK point. Fig. 4 takes the desired QPSK constellation point lying in the first quadrant as an example to illustrate the implementation of IRS-DMSC using RPC and transmitted/received signals at various communication entities. As Fig. 4(a) shows, Alice transmits a precoded signal $\sqrt{P_T}\mathbf{p}x_0$. As illustrated in Fig. 4(b), the IRS, upon receiving the signal from Alice, then constructs signal $\sqrt{P_T}\sum_{i=1}^{M}\mathbf{h}_{IB}^{(i)}\mathbf{h}_{AI}^{(i)}\mathbf{p}e^{j\theta_i}x_0$ for reflection. Finally, Bob

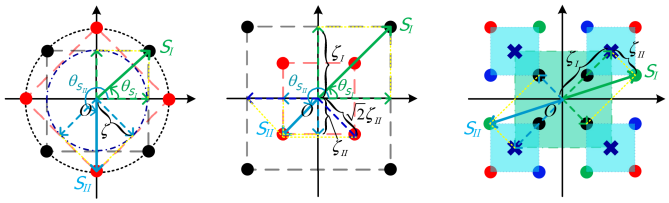


Fig. 5. Examples of decomposing high-order modulation constellation into multiple QPSK constellations.

post-processed the superimposed signal to obtain r_B. The filtered signal components r_{AB} and r_{IB}, as depicted in Fig. 4(c), carry their respective data symbols $\mathcal{J}(r_{AB})$ and $\mathcal{J}(r_{IB})$ which are located within the correct quadrants. As can be observed in Fig. 4(c), due to the lack of power control at the IRS, there may exist a distortion between $\mathcal{J}(r_B)$ and the desired QPSK symbol x, causing an offset between them. Nevertheless, since the phases of $\mathcal{J}(r_{AB})$ and $\mathcal{J}(r_{IB})$ are correct, $\mathcal{J}(r_B)$ is located within the correct quadrant. Therefore, methods such as ML can be employed to determine the correct desired data.

It should be noted that, since RPC focuses on compensating for the fading difference between DTC and IRC to obtain a desired data in the correct quadrant, it is only applicable to QPSK modulation. Furthermore, the distortion between $\mathcal{J}(r_B)$ and x as shown in Fig. 4(c) will lead to a reduction in noise resilience, thereby imposing limitations on its application. When a high-order MPSK ($M \geq 4$) is used or amplitude modulation is involved (e.g., MQAM modulation), RPC becomes inapplicable. In such cases, a more precise calibration method that incorporates both amplitude and phase compensation is required to accurately obtain the desired constellation point at Bob, which will be elaborated further in Section V-B.

V. Extended Design of IRS-DMSC to High-Order Modulation

In Section IV we took QPSK as an example to present the design of IRS-DMSC. Now we extend IRS-DMSC to more general high-order modulations including MQAM and MPSK where M denotes the modulation order and $M \geq 2^L$ ($L \in \{3, 4, \cdots\}$). In what follows, we will first illustrate the decomposition of a high-order modulated waveform into two sub-waveforms. Then, we will introduce a constellation calibration method to ensure the accurate generation of the desired waveform at the intended Rx.

A. Decomposition of High-Order Modulated Signal

The key of extending IRS-DMSC lies in the decomposition of a high-order modulated waveform into two distinct sub-waveforms. As Fig. 5(a) shows, an 8PSK waveform can be equivalent to two phase-shifted sub-waveforms with an identical amplitude ζ. For example, in order to acquire the 8PSK symbol $\mathcal{S}_I$ with a phase offset of $\theta_{\mathcal{S}_I}$, Alice can generate a direct signal with a phase offset of $\theta_{\mathcal{S}_I}$. Meanwhile, the IRS introduces a phase shift $\pi/2$ to this signal. This results in a reflected signal with a phase offset of $\theta_{\mathcal{S}_I} + \pi/4$. By superimposing the direct and reflected signal components, the waveform corresponding to the symbol $\mathcal{S}_I$ is produced at Bob. Similarly, the 8PSK symbol $\mathcal{S}_{II}$ with a phase offset of $\theta_{\mathcal{S}_{II}}$ can be achieved by combining a direct signal and a reflected signal with phase offsets $\theta_{\mathcal{S}_{II}} - \pi/4$ and $\theta_{\mathcal{S}_{II}} + \pi/4$, respectively. Note that $\mathcal{S}_I$ can be regarded as a symbol within a QPSK constellation formed by the four black points, while $\mathcal{S}_{II}$ can be considered as a QPSK symbol in the constellation defined by the four red points. These two symbols can be acquired by combining two orthogonal sub-waveforms. Since MPSK can be equivalent to $M/2$ QPSKs, the aforementioned extension of IRS-DMSC to 8PSK can be applied seamlessly.

Regarding MQAM, we will take 8QAM and 16QAM as examples to illustrate the extension of IRS-DMSC. As Fig. 5(b) shows, the 8QAM constellation can be equivalent to the combination of two QPSKs, labeled as QPSK-I and QPSK-II. These constellations are distinguished by different amplitudes, i.e., ζ_I and ζ_{II}, while sharing an identical phase set $\{-\frac{3\pi}{4}, -\frac{\pi}{4}, \frac{\pi}{4}, \frac{3\pi}{4}\}$. Consequently, an 8QAM symbol can be treated as either a QPSK-I symbol or a QPSK-II symbol, which can then be achieved by combining two sub-signal components. Specifically, for the data symbol $\mathcal{S}_I$, Alice transmits a signal offset by a phase of $\theta_{\mathcal{S}_I} - \pi/4$, while the IRS generates a reflecting signal with a phase offset of $\theta_{\mathcal{S}_I} + \pi/4$, both sharing the same amplitude ζ_I. Likewise, for symbol $\mathcal{S}_{II}$ in Fig. 5(b), Alice and the IRS generate signal components with an identical amplitude ζ_{II}, and various phase offsets of $\theta_{\mathcal{S}_{II}} - \pi/4$ and $\theta_{\mathcal{S}_{II}} + \pi/4$, respectively. Note, however, that the realization of IRS-DMSC in 8QAM is not unique. For example, to achieve $\mathcal{S}_{II}$, Alice could alternatively transmit a signal with a phase offset of $\theta_{\mathcal{S}_{II}} - \pi/4$ and an amplitude of ζ_I, while the IRS generates a reflected signal component with a phase offset of $\theta_{\mathcal{S}_{II}} + \pi/2$ and an amplitude of $\sqrt{2}\zeta_{II}$.

We now discuss the extension of IRS-DMSC in 16QAM. As depicted in Fig. 5(c), we can represent 16QAM as the combination of four QPSK constellations lying in the four quadrants of the coordinate system, respectively. To realize signal waveform decomposition, we plot an auxiliary QPSK centered at the origin and determined by the four "**x**" markers (referred to as QPSK-I). Correspondingly, the four QPSKs constituting 16QAM are labeled as QPSK-II. Then, one can easily see that the symbol $\mathcal{S}_I$ can be achieved by combining a QPSK-I signal with a phase offset of $\pi/4$ and a QPSK-II signal with a phase offset of $-\pi/4$. Similarly, the symbol $\mathcal{S}_{II}$ can be realized by combining a QPSK-I waveform with a phase offset of $-3\pi/4$ and a QPSK-II waveform with a phase offset of $3\pi/4$.

Based on the above discussion, other $M-$order modulations can be decomposed in a similar way.

B. Design of Constellation Point Calibration

It should be noticed that under MPSK ($M \geq 2^L$), more than one constellation point may exist in a quadrant (including on the axis of the quadrant). In such a case, RPC can not result the correct constellation point from multiple candidate points. This is because RPC aim at adjusting the effective data carried in r_B

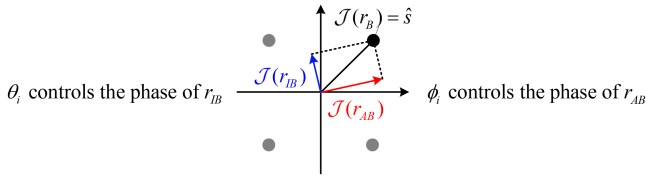


Fig. 6. Illustration of constellation point calibration.

to the same quadrant of the desired data, so that by employing ML the desired symbol can be determined. However, in the case of multiple constellation points (including the desired data point) existing in one quadrant, the use of ML may yield wrong decision and hence incurring decoding error. For example, under 8PSK, when IRS-DMSC with Relative Phase Calibration (w/ RPC) adopts ML to $\mathcal{J}(r_B)$, an incorrect 8PSK symbol may yield. Specifically, a black dot in Fig. 5(a) may be decided as its adjacent red dot, or vice versa. In such a case, erroneous decoding occurs. Moreover, although 8QAM constellation contains only four phases, amplitude information is required to differentiate multiple constellation points in a quadrant. Since RPC adjust signal's phase without amplitude modification, Bob can't distinguish the two constellation points with identical phase but different amplitudes. Therefore, decoding error can happen. As for 16QAM, IRS-DMSC w/ RPC can not be capable of distinguishing multiple points in one quadrant, which is similar to the cases of 8PSK and 8QAM. To summarize, IRS-DMSC w/ RPC are inapplicable for $M-$order modulation ($M \geq 2^L$, $L \in \{3, 4, \cdots\}$). So, in order to make IRS-DMSC usable, we need more accurate calibration method to yield an estimated symbol from the superimposed signal being close to the desired constellation point as much as possible.

According to the design principle of RPC, the IRS can manipulate the phase of r_{IB} by adjusting θ_i. Meanwhile, Alice can introduce a pre-attenuation factor $e^{j\phi}$ to modify the phase of r_{AB}. Then, as illustrated in Fig. 6, where we use two vectors to represent $\mathcal{J}(r_{AB})$ and $\mathcal{J}(r_{IB})$, by appropriately setting ϕ and θ_i to adjust the directions of these two vectors, their combined vector $\mathcal{J}(r_B)$ can reach the standard constellation point corresponding to the desired data $\hat{s}$. This process involves adjustment of both $\mathcal{J}(r_B)$'s phase and amplitude, thus we call it *Constellation Point Calibration* (CPC).

Now, we present the realization of CPC. Taking SVD-based precoding and filtering as an example, Alice selects $\mathbf{p} = e^{j\phi}\mathbf{v}_{AB}^{(1)}$ as the precoder, while Bob adopts $\mathbf{f} = \mathbf{u}_{AB}^{(1)}$ as the receive filter. So, the two superimposed filtered signal components at Bob can be rewritten as:

$$r_{AB} = \sqrt{P_T}\lambda_{AB}^{(1)} e^{j\phi} x_0 \tag{10}$$

and

$$r_{IB} = \sqrt{P_T}\sum_{i=1}^{M} [\mathbf{u}_{AB}^{(1)}]^H \mathbf{h}_{IB}^{(i)} \mathbf{h}_{AI}^{(i)} \mathbf{v}_{AB}^{(1)} e^{j(\theta_i+\phi)} x_0. \tag{11}$$

By denoting $\mathcal{J}(r_{AB})$ and $\mathcal{J}(r_{IB})$ as two vectors, we can express the projections of $\mathcal{J}(r_{AB})$ and $\mathcal{J}(r_{IB})$ on the horizontal (real) and vertical (image) axis as:

$$\begin{cases} \mathrm{Re}[\mathcal{J}(r_{AB})] = \sqrt{P_T}\lambda_{AB}^{(1)} s_0 \cos\phi \\ \mathrm{Im}[\mathcal{J}(r_{AB})] = \sqrt{P_T}\lambda_{AB}^{(1)} s_0 \sin\phi \end{cases} \tag{12}$$

and

$$\begin{cases} \mathrm{Re}[\mathcal{J}(r_{IB})] = \sqrt{P_T}\sum_{i=1}^{M} \Big\{ \|[\mathbf{u}_{AB}^{(1)}]^H \mathbf{h}_{IB}^{(i)} \mathbf{h}_{AI}^{(i)} \mathbf{v}_{AB}^{(1)}\| s_0 \cdot \\ \qquad \cos(\theta_i + \phi + \mathrm{ang}([\mathbf{u}_{AB}^{(1)}]^H \mathbf{h}_{IB}^{(i)} \mathbf{h}_{AI}^{(i)} \mathbf{v}_{AB}^{(1)})) \Big\} \\ \mathrm{Im}[\mathcal{J}(r_{IB})] = \sqrt{P_T}\sum_{i=1}^{M} \Big\{ \|[\mathbf{u}_{AB}^{(1)}]^H \mathbf{h}_{IB}^{(i)} \mathbf{h}_{AI}^{(i)} \mathbf{v}_{AB}^{(1)}\| s_0 \cdot \\ \qquad \sin(\theta_i + \phi + \mathrm{ang}([\mathbf{u}_{AB}^{(1)}]^H \mathbf{h}_{IB}^{(i)} \mathbf{h}_{AI}^{(i)} \mathbf{v}_{AB}^{(1)})) \Big\} \end{cases}. \tag{13}$$

Therefore, to realize CPC, we can jointly adjust ϕ and θ_i to obtain appropriate $\mathrm{Re}[\mathcal{J}(r_{AB})]$, $\mathrm{Im}[\mathcal{J}(r_{AB})]$, $\mathrm{Re}[\mathcal{J}(r_{IB})]$, and $\mathrm{Im}[\mathcal{J}(r_{IB})]$, such that (14) can be satisfied:

$$\begin{cases} \mathrm{Re}[\mathcal{J}(r_B)] = \mathrm{Re}[\mathcal{J}(r_{AB})] + \mathrm{Re}[\mathcal{J}(r_{IB})] = s_0 \\ \mathrm{Im}[\mathcal{J}(r_B)] = \mathrm{Im}[\mathcal{J}(r_{AB})] + \mathrm{Im}[\mathcal{J}(r_{IB})] = s_1 \end{cases}. \tag{14}$$

Recall that we need to configure θ_i to achieve a coherent combination of the M reflected signal components, thereby maximizing the amplitude of r_{IB}. Specifically, $\theta_i + \phi + \mathrm{ang}([\mathbf{u}_{AB}^{(1)}]^H \mathbf{h}_{IB}^{(i)} \mathbf{h}_{AI}^{(i)} \mathbf{v}_{AB}^{(1)}) = \Theta$ should hold where Θ represents the target phase of r_{IB}. Consequently, we can have:

$$\begin{cases} \sqrt{P_T}\lambda_{AB}^{(1)} s_0 \cos\phi \\ \quad + \sqrt{P_T}\sum_{i=1}^{M} \|[\mathbf{u}_{AB}^{(1)}]^H \mathbf{h}_{IB}^{(i)} \mathbf{h}_{AI}^{(i)} \mathbf{v}_{AB}^{(1)}\| s_0 \cos\Theta = s_0 \\ \sqrt{P_T}\lambda_{AB}^{(1)} s_0 \sin\phi \\ \quad + \sqrt{P_T}\sum_{i=1}^{M} \|[\mathbf{u}_{AB}^{(1)}]^H \mathbf{h}_{IB}^{(i)} \mathbf{h}_{AI}^{(i)} \mathbf{v}_{AB}^{(1)}\| s_0 \sin\Theta = s_1 \end{cases}. \tag{15}$$

From (15), both ϕ and Θ can be solved. Furthermore, according to $\theta_i + \phi + \mathrm{ang}([\mathbf{u}_{AB}^{(1)}]^H \mathbf{h}_{IB}^{(i)} \mathbf{h}_{AI}^{(i)} \mathbf{v}_{AB}^{(1)}) = \Theta$, the value of θ_i can be determined.

CPC exploits the principle of vector combination. By calibrating the phases of two signal components, $\mathcal{J}(r_B)$ can coincide with the desired standard constellation point, so that IRS-DMSC can be extended to more general high-order modulations. However, it should be noted that when signal's transmission experiences severe fading, the strength of r_{AB} and r_{IB} may be too small to yield a signal r_B whose effective data coincides with the desired data symbol. That is, $\|r_{AB}\|$, $\|r_{AI}\|$ and $\|r_{IB}\|$ are far less than $\|s\|$, yielding no solutions for ϕ and θ_i. In such a case, traditional CM becomes infeasible as well, i.e., an outage of data transmission occurs.

So far, we have discussed the design of IRS-DMSC for a single pair of legitimate Tx and Rx. When multiple legitimate Txs and/or Rxs are present, the Txs need to collaborate in designing their precoders and the reflection matrix of the IRS to enable each legitimate Rx to differentiate multiple current data transmissions. Specifically, when there are multiple Txs and one legitimate Rx, we can leverage the interactions among multiple wireless signal components to obtain an effective aggregated signal at the IRS and receiver, respectively, as demonstrated in [30]. Our method can then be applied directly. When there is one Tx and multiple legitimate Rxs, we can employ a multi-user

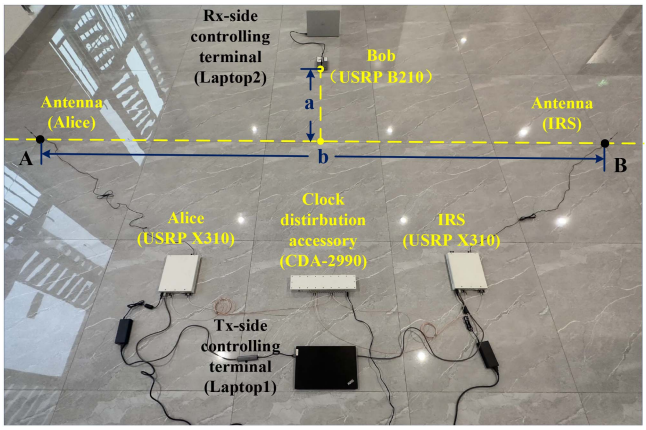


Fig. 7. Hardware implementation of IRS-DMSC.

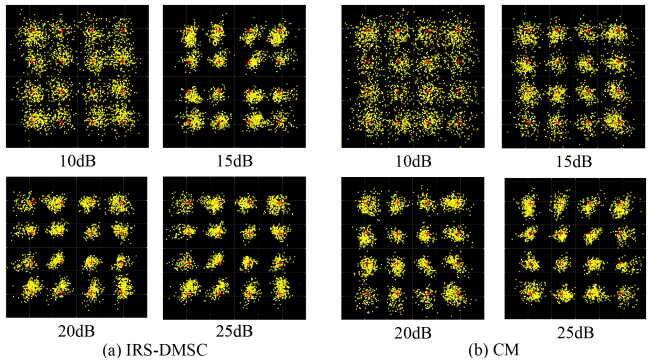


Fig. 8. Comparison of 16QAM constellations at Bob under IRS-DMSC and CM.

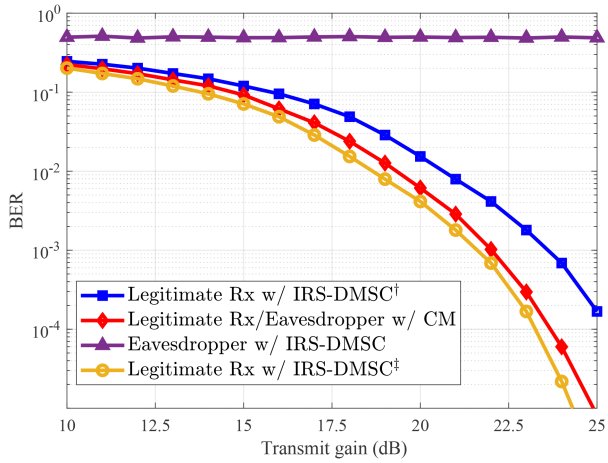


Fig. 9. BER performance of legitimate Rx and eavesdropper using IRS-DMSC and CM.

scheduling method to allow one Rx to receive its signal at a time, making our method applicable.

VI. Evaluation

In this section, we first utilize the universal software radio peripheral (USRP) platform to implement IRS-DMSC and demonstrate its validity. Specifically, we use constellation maps and Bit Error Rate (BER) to verify the feasibility of IRS-DMSC in legitimate transmission, and employ BER to exhibit the prevention of eavesdropping with IRS-DMSC. Then, we use MATLAB simulation to evaluate the BER and secrecy capacity of IRS-DMSC. We employ QPSK and 16QAM as an examples. Similar results can be obtained under other modulation schemes. We adopt CM as the baseline method.[5]

A. Hardware Implementation and Experiments

We employ two USRP X310 devices, each equipped with a UBX-160 daughter board, as Alice and IRS, respectively. Additionally, we utilize a USRP B210 device as the Rx. To simplify the experiment, all devices are equipped with a single antenna. Furthermore, we omit the implementation of the transmission from Alice to the IRS. Instead, we allow the X310 device serving as the IRS to directly transmit to the Rx. This way, signal reflection is emulated.

As Fig. 7 shows, the two X310 devices, controlled by the Tx-side terminal (denoted by Laptop1), realize the processing of Alice and IRS, respectively, and the positions of the antennas connected to the devices represent the spatial locations of Alice and IRS. The X310 devices are connected to a CDA-2990 which generates a high-accuracy 1 pulse per second (PPS) and 10 MHz reference signal for device synchronization via cables of equal length. The B210 device acts as the legitimate Rx (i.e., Bob) to detect the received mixed signal. The B210 device is connected to another terminal (Laptop 2), which controls the signal detection and data demodulation.

In the experiment, all the devices are deployed in a plane. For simplicity, the Rx is located on the mid-perpendicular of the line connecting Alice and IRS. This configuration ensures that the direct and reflected signal components experience similar attenuation and can reach the Rx synchronously. Consequently, there is no need for the estimation of the direct and reflecting links' CSI, or for phase or constellation point calibration. In the experiment, Bob estimates the equivalent CSI between him and Alice and the IRS based on the mixed pilot signals received from Alice and IRS (we use Barker code as the pilot sequence), and then compensates the equivalent channel accordingly. For clarity, we use the parameter-pair $[a, b]$ to represent the distance between Alice and IRS, and between Bob and the line connecting Alice and IRS. In the experiment, we set $[a, b]$ to $[1\text{ m}, 2\text{ m}]$, $[2\text{ m}, 5\text{ m}]$, and $[3\text{ m}, 8\text{ m}]$. The main parameters used in the experiment are shown in Table V.

In Figs. 8 and 9, we evaluate the variation of Rx-side constellation and BER performance along with the increase of transmit gains under $[a, b] = [1\text{ m}, 2\text{ m}]$ and 16QAM. In addition to the proposed IRS-DMSC, we also implement conventional CM for comparison. In this approach, Alice directly transmits a 16QAM

[5]To the best of our knowledge, all existing transmission schemes utilize CM, which loads all of user's information onto a single signal, thus lacking signal-level security. Furthermore, as we have discussed in the Section II, existing PHY security schemes either entail additional transmit power usage (e.g., AN), impose computational power consumption (e.g., PHY encryption and decryption), or require CSI estimation and signaling overheads (e.g., the PHY secret key based method). In contrast, our approach does not incur these costs/overheads. So, there is no common basis for comparing our method with existing secure schemes.

TABLE V
PARAMETER SETTINGS OF IRS-DMSC

Parameter	Carrier freq.	Symbol rate	Interpolation factor	Sampling rate (base-band)	Roll-off factor of raised cosine filter	Transmit gain
Value	915MHz	0.2MBaud	2	0.4MHz	0.5	[5dB,25dB]

signal to Bob without the assistance of the IRS. When realizing IRS-DMSC, we decompose 16QAM into two QPSK signal components with an identical phase set (i.e., $\{-\frac{3\pi}{4}, -\frac{\pi}{4}, \frac{\pi}{4}, \frac{3\pi}{4}\}$) and various amplitudes (where the larger amplitude is twice that of the smaller one), as depicted in Fig. 5(c). Specifically, we employ one Tx to generate the QPSK component with a larger amplitude to emulate Alice's direct transmission, while adopting the other Tx to transmit the QPSK component with a smaller amplitude to emulate the IRS's reflection to Bob. In practice, the reflecting link is composed of two sub-links, resulting in a more severe path loss than the direct link. Therefore, the transmit power configuration at the two Txs is aligns with the practical situation. The two QPSK components reach Bob and superimpose with each other to produce the desired 16QAM signal. Consequently, Bob performs QPSK demodulation. When implementing 16QAM using CM, we turn off one X310 and use the other X310 as a 16QAM signal source, while the processing at Bob is identical to that under IRS-DMSC.

For a fair comparison, we set the same transmit power for both IRS-DMSC and CM. It is worth noting that, in the IRS-DMSC, we employ one X310 to serve as the IRS, and its power should not be counted as the transmit power of the IRS-DMSC, since in practice the reflected signal originates from Alice while the IRS only forwards it to Bob. Specifically, the transmit gain in Table V is for controlling the signal strength of Alice. Moreover, as the transmitted signal strength is determined by the amplitude of the baseband symbol and the transmit gain cooperatively, in the experiment, we set the same transmit gain for Alice and the IRS under IRS-DMSC, and adjust the amplitude of their baseband symbols to ensure that Alice's symbol amplitude is twice that of the IRS's symbol, so that the combination of Alice and the IRS's signals can have the same average power as that obtained under CM.

As Fig. 8 shows, both IRS-DMSC and CM can yield 16QAM constellation at the Rx. The constellation points become more concentrated as the transmit gain increases. As a comparison, there is a minor distortion between the constellations of IRS-DMSC and CM under the same transmit gain. This is because the modulated signal in CM is generated by a single Tx, and the Rx can accurately estimate the channel fading and compensate for it, while the received 16QAM waveform under IRS-DMSC is obtained by superimposing two QPSK signals over the air interface at the Rx, and the experimental setup shown in Fig. 7 can't completely eliminate the fading difference between the two QPSK components. Thus, a slightly distorted constellation results. Nevertheless, it is evident from Fig. 8 that data transmission using IRS-DMSC can achieve comparable performance to that with CM.

According to Table IV, the wavelength of the 915 MHz carrier signal is approximately 32.79 cm, and the manual deployment of devices can ensure that the difference in signal propagation distance is less than 2 cm, so the delay difference of the two QPSK components at Bob can be ignored. However, the experimental setup cannot make the fading experienced by the two signal components strictly identical, so the channel fading of the direct and reflected signals can't be ideally compensated for, resulting in a slight distortion of the constellation compared to that obtained under CM. In order to quantitatively illustrate the impact of the constellation distortion in IRS-DMSC on Bob's reception, we compare the BER performance of Bob by using IRS-DMSC and CM, respectively, to transmit 5×10^7 bits data with 16QAM modulation, and set the transmit gain to [10 dB, 25 dB], as shown in Fig. 9.

As the figure shows, the BER of Bob under both transmission schemes decreases as the transmit gain grows. CM outputs a better BER than IRS-DMSC. This is because in IRS-DMSC, the desired 16QAM signal is obtained by superimposing two signals at the desired Rx, but the Rx can't completely compensate for the different fading of the two signal components, hence resulting in slight distortion of the observed 16QAM constellation compared to that under CM, as shown in Fig. 9. Therefore, under the same transmit gain (and the same environmental noise), IRS-DMSC yields a worse BER than CM. To address this issue, one can apply CPC as proposed in Section V. In this way, the constellation shape at the Rx can be improved, so that IRS-DMSC's BER will approach CM's. However, since 16QAM employs varying amplitudes to carry data information, RPC is not applicable. It is important to note that in the aforementioned setup, we have included the transmit power used for emulating the function of IRS as part of the total transmit power overhead, to obtain the BER of Bob under IRS-DMSC. However, as IRS can leverage interference power for desired data transmission, the power cost for emulating IRS's reflection should not be factored in. Therefore, to accurately evaluate IRS-DMSC's performance, we allow Alice to transmit with the same power as that under CM when implementing IRS-DMSC. For clarity, we use superscripts and ‡ to differentiate between the IRS-DMSC schemes with and without accounting for the IRS power, respectively. That is, with the same transmit gain, the average power of the QPSK symbols sent by Alice under IRS-DMSC‡ should be the same as that of the 16QAM symbols sent by Alice under CM. As the figure plots, IRS-DMSC‡ can outperform both CM and IRS-DMSC† in terms of BER performance, attributed to the effective collection and utilization of signal power emitted from Alice to the IRS.

To verify the secrecy performance of IRS-DMSC, we move the legitimate Rx in Fig. 7 from its position on the mid-perpendicular of line AB to other positions, then the legitimate Rx becomes an eavesdropper. Assuming that the eavesdropper can accurately estimate the CSI between itself and the Txs, and

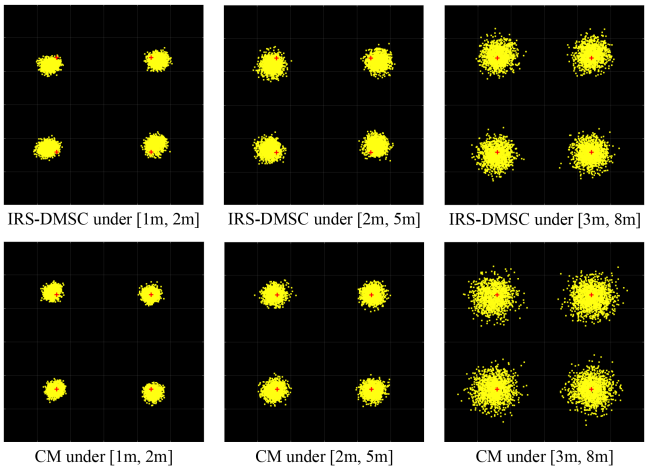


Fig. 10. Variation of QPSK constellation with propagation distances using IRS-DMSC and CM.

can perform channel compensation and signal detection based on the estimation, we can plot in Fig. 9 the BER of an eavesdropper employing 16QAM demodulation under two transmission methods. As the figure shows, the eavesdropper's BER remains around 50% and doesn't improve with the increase of transmit gain. This is because the two QPSK signals are asynchronously superimposed and interfere with each other at Eve. Additionally, due to the residual distinction between the direct and reflecting channels, Eve is unable to accurately compensate for the fading of the two sub-channels based on the estimation of the pilot from the received mixed signal. Therefore, the correct decoding of the desired 16QAM signal is thwarted. When the legitimate communication pair adopts CM for data transmission, Eve can achieve a comparable BER performance to Bob. This is because under CM, the desired signal is generated at the single Tx, and the eavesdropper can accurately estimate channel status based on the pilot carried in the received signal and realize fading compensation, resulting correct decoding. Based on the above analysis, it is evident that CM is not secure in physical-layer data transmission. In contrast, the proposed IRS-DMSC leverages the interactions of the direct and reflecting signal components to generate a secure physical waveform, thereby ensuring the secrecy of data transmission.

We also implement QPSK transmission using IRS-DMSC and CM, respectively, under various values of $[a, b]$. In realizing IRS-DMSC, we use two orthogonal BPSK signal components to produce the QPSK signal. Fig. 10 illustrates the QPSK constellations under $[1\text{ m}, 2\text{ m}]$, $[2\text{ m}, 5\text{ m}]$, $[3\text{ m}, 8\text{ m}]$, and a fixed transmit gain of 13 dB. As the figure shows, the constellation points become more scattered as the distances between the Txs and Rx increase. This observation is consistent with the case in Fig. 8, where the constellations vary with an increase in transmit gain, as the increase in signal propagation length can be equivalent to a decrease in transmit gain. Since the signal attenuation does not grow significantly as the distances between Alice, IRS, and Bob extend from a few meters to a dozen or so meters, the morphology of constellation points remains unchanged and their degree of dispersion experiences a slight increase, thereby not significantly impacting the BER performance. Fig. 10 verifies the applicability of IRS-DMSC under QPSK.

B. MATLAB Simulation and Analysis

We now use MATLAB simulation to evaluate the proposed scheme's performance. Channel capacity and BER are adopted to show the effectiveness and secrecy of IRS-DMSC. According to the information theory, the legitimate channel capacity c_B can be defined as the maximum average mutual information of the transmission from Alice to Bob. Similarly, the wiretap channel capacity c_E can be obtained by computing the maximum average mutual information of the transmission between Alice and Eve. Therefore, legitimate and wiretap channel capacity can be computed as:

$$\begin{aligned} c_{B/E} &= \max\{I(X;\hat{X})\} \\ &= \max\left\{\sum_{x\in X}\sum_{\hat{x}\in\hat{X}} P(x,\hat{x})\log_2\frac{P(x,\hat{x})}{P(x)P(\hat{x})}\right\} \end{aligned} \tag{16}$$

where the subscript B/E indicates that (16) can be used for calculating both c_B and c_E. $I(X;\hat{X})$ represents the average mutual information. x and $\hat{x}$ denote the transmitted and estimated symbol, and X and $\hat{X}$ are the symbol sets at Tx and Rx, respectively. $x \in X$ and $\hat{x} \in \hat{X}$ hold. The probabilities of x and $\hat{x}$ are represented by $P(x)$ and $P(\hat{x})$, and their joint probability density is $P(x,\hat{x})$.

Then, the secrecy capacity c_S, defined as the maximum transmission rate at which the eavesdropper is unable to acquire any legitimate user's information [12], can be obtained by subtracting the wiretap channel capacity, c_E, from c_B, as:

$$c_S = \max\{c_B - c_E, 0\}. \tag{17}$$

In the simulation, we let Alice select transmission symbols from the QPSK symbol set with the same probability, and then process and transmit the modulated signal in terms of IRS-DMSC. We adopt symbol rate $R_s = 4 \times 10^7$Baud, the carrier frequency f_c is set to be 2.4 GHz. Without loss of generality, we configure $N_T = 2$, $N_R = 2$, and $M = 4$, while, for simplicity, neglecting the large-scale path loss and the reflection loss of IRS. Since, in practical use, we deploy the IRS either close to Alice or Bob, the signal propagation lengths via DTC and IRC are similar, leading to a negligible delay difference between the signal propagation in DTC and IRC. In other words, the direct signal and the reflecting signal can arrive at the legitimate Rx synchronously. We define the transmit power of Alice normalized by noise power σ_n^2 as $\eta = 10\lg(P_T/\sigma_n^2)$ dB, and set. In the simulation, we randomly and independently generate 1000 legitimate and wiretap channel coefficients; under each channel coefficient set 2000 QPSK symbols are transmitted. By counting the numbers of x and $\hat{x}$, we can get $P(x)$, $P(\hat{x})$, and $P(x,\hat{x})$. Then, according to (16) and (17) the channel capacity can be calculated.

In what follows, we will simulate IRS-DMSC without calibration (IRS-DMSC w/o Cal.), IRS-DMSC with Relative Phase

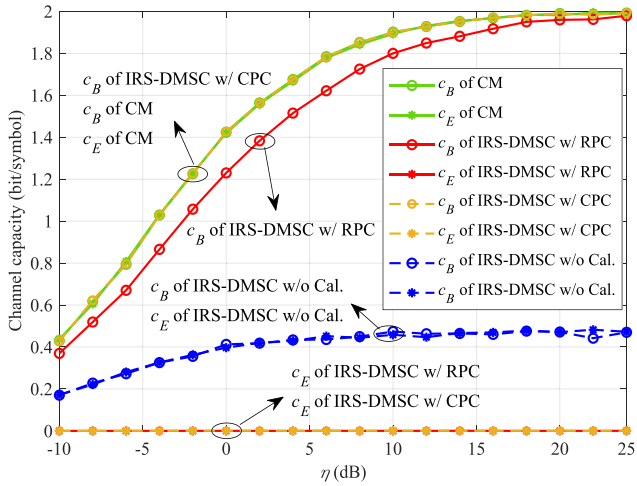


Fig. 11. Variation of c_B and c_E vs. η under different transmission schemes.

Calibration (IRS-DMSC w/ RPC), IRS-DMSC with Constellation Point Calibration (IRS-DMSC w/ CPC) and conventional Centralized Modulation (CM).[6] Note that IRS-DMSC w/ CPC only takes the samples where solutions for ϕ and θ_i exist into account, or neither CM nor IRS-DMSC w/ CPC is applicable. We assume that Eve can accurately estimate the wiretap channel $\mathbf{G}_{AE}$, but can't obtain the legitimate channel $\mathbf{H}_{AB}$, $\mathbf{H}_{AI}$, and $\mathbf{H}_{IB}$. Then, Eve can process the intercepted signal according to $\mathbf{G}_{AE}$. It should be noticed that, precise $\mathbf{G}_{AE}$ can facilitate Eve to achieving the maximum eavesdropping capacity, thus the following simulation results can be regarded as the upper bound of Eve's performance and the lower bound of the secrecy capacity.

Fig. 11 shows the variation of c_B and c_E along with η under various transmission schemes. As the figure shows, CM and IRS-DMSC w/ CPC yield the highest c_B, then followed by IRS-DMSC w/ RPC's c_B. This is because both CM and IRS-DMSC w/ CPC can obtain standard QPSK constellation point the same as the desired data point at Bob, whereas IRS-DMSC w/ RPC can only get data point (which is usually not standard constellation point) in the same quadrant as the desired data's constellation point. Therefore, the anti-noise capability of IRS-DMSC w/ RPC is weaker than that of CM and IRS-DMSC w/ CPC, thus yielding c_B of the former is lower than that of the latter. With the increase of η, c_B of CM and IRS-DMSC with calibration (i.e., RPC and CPC) gradually approaches to 2bits/symbol, the maximum channel capacity under QPSK modulation. The analysis is as follows. Given high η, the probability that Bob correctly estimates the data symbol from r_B is close to 1, hence $P(x,\hat{x})|_{\hat{x}=x}=1$ and $P(x,\hat{x})|_{\hat{x}\neq x}=0$ hold. Recall that for a QPSK symbol, we have $P(x)=P(\hat{x})=\frac{1}{4}$. Then, by substituting the above values into (16), we can calculate c_B of CM and IRS-DMSC with calibration as 2bits/symbol. As for IRS-DMSC w/o Cal., it outputs lower c_B than the other methods, and its c_B gradually increases to about 0.5 b/symbol as η grows high. This is because under IRS-DMSC w/o Cal., Alice directly sends the BPSK-I modulated signal carrying x_0 to Bob via $\mathbf{H}_{AB}$, while the IRS generates a reflected signal and directs it to Bob via cascaded channels $\mathbf{H}_{AI}$ and $\mathbf{H}_{IB}$. Since the fading in DTC and IRC are independent, Bob can only compensate for the fading in either the DTC or IRC. Note that the use of IRS-DMSC at the Tx-side can be transparent to the Rx, so Bob processes the superimposed signal as a whole rather than detecting them separately. Without loss of generality, we assume that Bob employs a receive filter matching $\mathbf{H}_{AB}$. Therefore, without considering noise and interference from the reflected signal, Bob may correctly obtain the estimated $\hat{x}_0$ such that $P(x_0,\hat{x}_0)|_{\hat{x}_0=x_0}=1$ and $P(x_0,\hat{x}_0)|_{\hat{x}_0\neq x_0}=0$. Moreover, recall that $P(x_0)=P(x_1)=\frac{1}{2}$ holds, we can compute the upper bound of the DTC's capacity using (16) as 1 b/symbol. Nevertheless, as Bob's filter is not adapted to the fading characteristics of IRC, he cannot guarantee that the decoded $\hat{x}_1$ will match the data carried in the reflected signal. In other words, an arbitrarily estimated $\hat{x}_1$ irrelevant to x_1 may be obtained. In such a case, $P(x_1,\hat{x}_1)=P(x_1)P(\hat{x}_1)$ holds. Therefore, the capacity of IRC is 0. Furthermore, in practice, mutual interference between the direct and reflected signal components is always inevitable, thus preventing the DTC capacity from achieving its upper bound of 1 b/symbol. As a result, c_B of IRS-DMSC w/o Cal. can only reach 0.5 b/symbol as η grows high, which is lower than that of IRS-DMSC with calibration and CM.

As for the eavesdropping capacity c_E, IRS-DMSC w/ RPC's and w/ CPC's are constant 0, not varying with η. This can be analyzed as follows. Similarly to (2), we can get the post-processed received signal of Eve as $r_E=\sqrt{P_T}\mathbf{f}^H\mathbf{G}_{AE}[e^{j\phi}\mathbf{v}_{AB}^{(1)}]x_0+\sqrt{P_T}\mathbf{f}^H\mathbf{G}_{IE}\mathbf{\Phi}\mathbf{H}_{AI}[e^{j\phi}\mathbf{v}_{AB}^{(1)}]x_0+\mathbf{f}^H\mathbf{z}$, where ϕ is set to be 1in the RPC method. Eve determines her receive filter according to $\mathbf{G}_{AE}$, while both the pre-attenuation coefficient ϕ (in CPC) and the phase-shift θ_i at the IRS are determined based on the legitimate channel matrices $\mathbf{H}_{AB}$, $\mathbf{H}_{AI}$, and $\mathbf{H}_{IB}$. Since these legitimate CSI are independent of $\mathbf{G}_{AE}$, Eve cannot accurately wiretap the desired data from r_E. In this case, the intercepted $\hat{x}$ is independent of the target desired data x, leading to $P(x,\hat{x})=P(x)P(\hat{x})$. Therefore, according to (16), we can have $c_E=0$. c_E of IRS-DMSC w/o Cal. overlaps with IRS-DMSC w/o Cal.'s c_B. This is similar to the case of Bob post-processing r_B without utilizing calibration. A detailed account of this can be found in the discussions of IRS-DMSC w/o Cal.'s c_B in the preceding paragraph. CM's c_E gradually increases to 2bits/symbol as η grows, because we assume that $\mathbf{G}_{AE}$ is precisely known to Eve. Therefore, Eve can employ a matched reception to achieve correct reception. This way, the channel fading can be accurately compensated for to yield the QPSK symbol only affected by noise.

[6]We can divide the transmission process into two phases. The first phase involves the generation of transmitted waveform, while the second phase pertains to signal propagation through the channel. Existing transmission schemes primarily focus on the design in the second phase. In contrast, IRS-DMSC puts emphasis on the first phase, which is more fundamental than the second-phase design, and constitutes our main contribution. This DM feature not only fundamentally prevents eavesdroppers from intercepting legitimate data transmission, but also sets our method apart from other PLS approaches that rely on conventional CM. Consequently, due to this fundamental difference, a simulation based comparison of IRS-DMSC with existing PLS methods is not feasible. Instead, we utilize Table I to perform a qualitative comparison between our method and other security approaches.

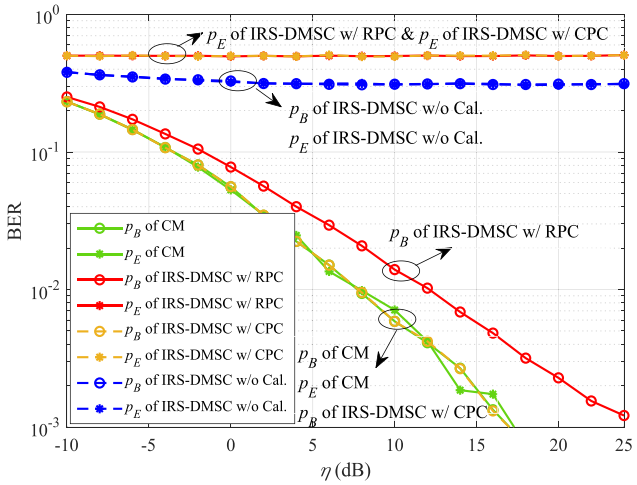


Fig. 12. Variation of Bob's and Eve's BER vs. η under different transmission schemes.

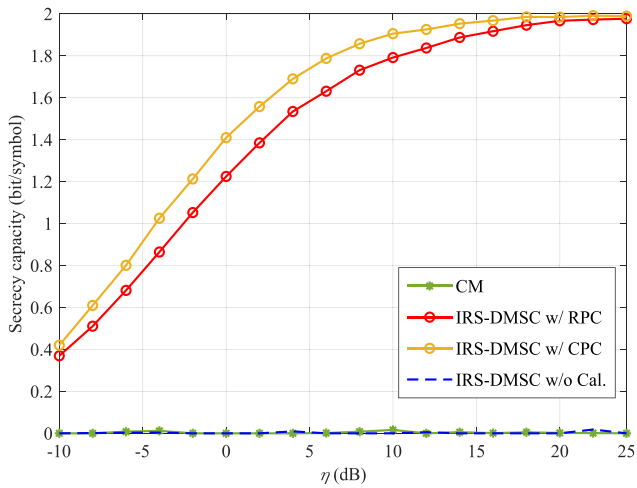


Fig. 13. Variation of c_S vs. η under different transmission schemes.

Fig. 12 shows the variation of Bob's and Eve's BER (denoted as p_B and p_E, respectively) along with η under different transmission schemes. As the figure shows, CM and IRS-DMSC w/ CPC output the lowest/best p_B, while under IRS-DMSC w/ RPC, p_B is slightly higher/worse. This is because CM and IRS-DMSC w/ CPC have identical anti-noise capability, being superior to that of IRS-DMSC w/ RPC. The detailed analysis can be found in the discussions about the anti-noise capability of the above-mentioned methods in Fig. 11. p_B under IRS-DMSC w/o Cal. decreases slowly as η grows and finally stabilizes at about 0.2. The reason is Bob can only recover partial desired data from the direct component of his received signal; nevertheless, decoding such partial data is also disturbed by the random reflecting component. The explanation is consistent with the analysis of c_B under IRS-DMSC w/o Cal. in Fig. 11. As for Eve, CM yields the lowest/best p_E, this is because Eve realizes matched reception in such a case. As for IRS-DMSC w/o Cal., it output p_E reducing to about 0.2 as η grows. This phenomenon and related analysis are the same as p_B under IRS-DMSC w/o Cal. IRS-DMSC w/ RPC and w/ CPC output the worst p_E, both are about 0.5in regardless of the variation of η. This is because under these two schemes, Eve's estimated symbol is completely random, i.e., the decoded symbol is independent of the desired data. The analysis can be found in the discussions about IRS-DMSC w/ RPC's and w/ CPC's c_E in Fig. 11 where c_E is constant 0.

In order to intuitively exhibit the secrecy performance of different methods, we plot in Fig. 13 the variation of secrecy capacity c_S with η under different schemes. As the figure shows, c_S of CM and IRS-DMSC w/o Cal. is 0. This is because under CM, Eve's reception can yield the same capacity as Bob's; whereas for IRS-DMSC w/o Cal., Bob and Eve can only achieve relative low and equal channel capacity as shown in Fig. 11. Therefore, c_S of CM and IRS-DMSC w/o Cal. is 0. IRS-DMSC with calibration has non-zero c_S which grows with an increase of η. To be specific, IRS-DMSC w/ CPC yields the highest c_S, then comes IRS-DMSC w/ RPC. This is because both IRS-DMSC w/ RPC's and w/ CPC's c_E are 0, while given the same η, IRS-DMSC w/ CPC excels IRS-DMSC w/ RPC in c_B. Then, according to (17) one can easily obtain that c_S of IRS-DMSC w/ CPC is higher than that of IRS-DMSC w/ RPC. Moreover, as η grows, c_S of IRS-DMSC w/ RPC and w/ CPC increases to 2bits/symbol (the maximum capacity under QPSK).

VII. Conclusion

We have proposed a *Distributed Modulation based Secure Communication* scheme by exploiting *Intelligent Reflecting Surface* — namely *IRS-DMSC*, in this paper. By incorporating the characteristic of wireless channel into modulation process, IRS-DMSC can fully exploit the randomness of wireless channel to secure user's transmission. Compared to conventional CM which modulates all of user's information onto a physical signal, IRS-DMSC employs two signals in realizing legitimate data transmission. Each of the signals only carries partial user's information, thus making it difficult for an eavesdropper to intercept the complete information. Under IRS-DMSC, the legitimate Tx generates one direct signal component; while the other signal is obtained by modulating the phase of such direct component and then reflecting at the IRS. With either phase calibration (i.e., RPC) or constellation point calibration (CPC), these two signal components can superimpose on each other at the legitimate Rx to produce a waveform identical to that obtained under CM. Then, the legitimate Rx can correctly recover the desired data from the received signal by using traditional demodulation method. As for the eavesdropper, due to the interference between the two signal components, s/he can't recover legitimate user's information from such disturbed signals, hence eavesdropping is effectively prevented. Our simulation results have shown the proposed IRS-DMSC to significantly improve the secrecy capacity while ensuring the transmission performance of the legitimate user.

REFERENCES

[1] Q. Wu, G. Y. Li, W. Chen, D. W. K. Ng, and R. Schober, "An overview of sustainable green 5G networks," *IEEE Wireless Commun.*, vol. 24, no. 4, pp. 72–80, Aug. 2017.

[2] 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.

[3] Y. Gao et al., "Physical layer security in 5G based large scale social networks: Opportunities and challenges," *IEEE Access*, vol. 6, pp. 26350–26357, 2018.

[4] P. Angueira et al., "A survey of physical layer techniques for secure wireless communications in industry," *IEEE Commun. Surv. Tut.*, vol. 24, no. 2, pp. 810–838, Second Quarter 2022.

[5] P. Yan, W. Duan, Q. Sun, G. Zhang, J. Zhang, and P. -H. Ho, "Improving physical-layer security for cognitive networks via artificial noise-aided rate splitting," *IEEE Internet Things J.*, vol. 11, no. 10, pp. 18932–18933, May 2024.

[6] T. V. Pham and A. T. Pham, "Energy efficient artificial noise-aided precoding designs for secured visible light communication systems," *IEEE Trans. Wireless Commun.*, vol. 20, no. 1, pp. 653–666, Jan. 2021.

[7] D. Luo, Z. Ye, B. Si, and J. Zhu, "Secure transmit beamforming for radar-communication system without eavesdropper CSI," *IEEE Trans. Veh. Technol.*, vol. 71, no. 9, pp. 9794–9804, Sep. 2022.

[8] N. Zhao, F. R. Yu, M. Li, and V. C. M. Leung, "Anti-eavesdropping schemes for interference alignment (IA)-Based wireless networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5719–5732, 2016.

[9] K. Zeng, "Physical layer key generation in wireless networks: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 33–39, Aug. 2016.

[10] X. Mao, K. Lin, and H. Liu, "A physical layer security algorithm based on constellation," in *Proc. IEEE Int. Conf. Commun. Technol.*, 2017, pp. 50–53.

[11] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.

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

[13] T. Cover and A. E. Gamal, "Capacity theorems for the relay channel," *IEEE Trans. Inf. Theory*, vol. IT-25, no. 5, pp. 572–584, Sep. 1979.

[14] S. Hu, F. Rusek, and O. Edfors, "Beyond massive MIMO: The potential of data transmission with large intelligent surfaces," *IEEE Trans. Signal Process.*, vol. 66, no. 10, pp. 2746–2758, May 2018.

[15] Q. Wu and R. Zhang, "Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming," *IEEE Tran. Wireless Commun.*, vol. 18, no. 11, pp. 5394–5409, Nov. 2019.

[16] L. Dong and H. Wang, "Secure MIMO transmission via intelligent reflecting surface," *IEEE Wireless Commun. Lett.*, vol. 9, no. 6, pp. 787–790, Jun. 2020.

[17] S. Hong, C. Pan, H. Ren, K. Wang, and A. Nallanathan, "Artificial-noise-Aided secure MIMO wireless communications via intelligent reflecting surface," *IEEE Trans. Commun.*, vol. 68, no. 12, pp. 7851–7866, Dec. 2020.

[18] S. Arzykulov, A. Celik, G. Nauryzbayev, and A. M. Eltawil, "Artificial noise and RIS-Aided physical layer security: Optimal RIS partitioning and power control," *IEEE Wireless Commun. Lett.*, vol. 12, no. 6, pp. 992–996, Jun. 2023.

[19] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Commun. Lett.*, vol. 8, no. 5, pp. 1410–1414, Oct. 2019.

[20] T. Bai, C. Pan, Y. Deng, M. Elkashlan, A. Nallanathan, and L. Hanzo, "Latency minimization for intelligent reflecting surface aided mobile edge computing," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 11, pp. 2666–2682, Nov. 2020.

[21] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network," *IEEE Commun. Mag.*, vol. 58, no. 1, pp. 106–112, Jan. 2020.

[22] Z. Li, J. Chen, K. G. Shin, and J. Liu, "Interference recycling: Exploiting interfering signals to enhance data transmission," in *Proc. IEEE Conf. Comput. Commun.*, 2019, pp. 100–108.

[23] J. Zhan and M. Gastpar, "Functional forwarding of channel state information," *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 1008–1018, Feb. 2014.

[24] M. Karlsson, E. Björnson, and E. G. Larsson, "Performance of in-band transmission of system information in massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 1700–1712, Mar. 2018.

[25] I. F. Akyildiz et al., "LTE-Advanced and the evolution to beyond 4G (B4G) systems," *Phys. Commun.*, vol. 10, pp. 31–60, 2014.

[26] S. Hong, C. Pan, H. Ren, K. Wang, A. Nallanathan, and H. Li, "Robust transmission design for intelligent reflecting surface-aided secure communication systems with imperfect cascaded CSI," *IEEE Trans. Wireless Commun.*, vol. 20, no. 4, pp. 2487–2501, Apr. 2021.

[27] P. Yang, L. Yang, and S. Wang, "Performance analysis for RIS-Aided wireless systems with imperfect CSI," *IEEE Wireless Commun. Lett.*, vol. 11, no. 3, pp. 588–592, Mar. 2022.

[28] C. Fan, *Principles of Communications*. 2nd ed. Beijing, China: Publishing House of Electronics Industry, 2015.

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

[30] Z. Li et al., "Exploiting interactions of multiple interferences for their cooperative interference alignment," *IEEE Trans. Wireless Commun.*, vol. 20, no. 11, pp. 7072–7085, Nov. 2021.

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 with Xidian University. Her research interests include wireless communication, physical layer security, and interference management.

Siwei Le 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 network simulation.

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.

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*, *IEEE Transactions on Dependable and Secure Computing*, 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.