Decomposed and Distributed Modulation to Achieve Secure Transmission

Zhao Li, *Member, IEEE*, Siwei Le, Jie Chen, Kang G. Shin, *Life Fellow, IEEE*, Jia Liu, *Senior Member, IEEE*, Zheng Yan, *Fellow, IEEE*, and Riku Jäntti, *Senior Member, IEEE*

***Abstract*—With the rapid deployment and wide use of mobile services and applications, more and more sensitive user information is being transmitted wirelessly. Due to the broadcast nature of wireless transmissions, they are exposed to all surrounding entities and thus vulnerable to eavesdropping. To counter this vulnerability, we propose a new physical-layer secure transmission scheme, called DDM-Sec, based on decomposed and distributed modulation (DDM). We show that a high-order modulation can be decomposed into multiple quadrature phase shift keying (QPSK) modulations, each of which can be further represented by two mutually orthogonal binary phase shift keying (BPSK) modulations. Therefore, traditional modulation can be realized by two cooperative transmitters (Txs), each generating a BPSK signal, in a distributed manner. The legitimate receiver (Rx) can decode the desired/intended information from the mixed two received BPSK signals while preventing the eavesdropper from accessing the legitimate user's information. DDM-Sec can effectively exploit the randomness of wireless channels to secure data transmission, enrich the spatial signatures of the legitimate user's transmission by employing two cooperative Txs, and then distribute the user's information to two transmissions so that none of the decomposed signals alone carry the legitimate user's full information. Moreover, due to random deployment of the two Txs and Rx, delay difference of the two transmissions is introduced. This can be further utilized to make eavesdropping difficult. Our theoretical analysis and simulation have shown that DDM-Sec can effectively prevent the eavesdropping, and hence guarantee the secrecy of the legitimate user's data transmission.**

***Index Terms*—Distributed transmission, modulation, physical-layer security, secure communication.**

I. Introduction

With the rapid deployment of wireless communication technologies, information security/privacy has become an important issue. Due to the broadcast nature of wireless transmissions, wireless systems are facing more security threats than the wired counterpart. Eavesdroppers may illegally overhear users' sensitive information through a wireless channel [1], [2]. There exist security vulnerabilities in all levels of transmission control protocol/internet protocol (TCP/IP) protocol stack, of which physical-layer security (PLS) plays a fundamental role in improving information secrecy. A variety of PLS techniques [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17] have been developed, which can effectively improve communication secrecy and protect the user's information from eavesdropping. The basic principles of realizing PLS can be classified into two types: 1) implementation of encryption based on the characteristics (also known as the *fingerprint*) of a wireless channel [3], [4], [5], [6], [7], [8], and 2) realization of reliable transmission based on a secrecy capacity analysis, with which a certain rate of secure transmission can be achieved as long as the channel to be protected from eavesdropping has a higher capacity than that of the wiretap channel [9], [10], [11], [12], [13], [14], [15], [16], [17].

Although the above-mentioned methods are claimed to achieve transmission secrecy, they rely on the traditional modulation with which data information is modulated onto a physical signal; in such a case, if someone captures this signal, the information carried on it may probably be recovered using a certain method. If we divide the information at the very beginning of a transmission process, then employ two physical signals to carry and transmit the divided information, and recover the desired information only upon arrival of the signals at their intended receiver (Rx), capturing two physical signals and combining them precisely so as to achieve eavesdropping will be much more difficult and challenging. Based on this observation, we propose a novel secure physical-layer transmission scheme based on *decomposed and distributed modulation (DDM)*. DDM exploits the randomness of wireless channels to secure data transmission, and enrich the spatial features by employing two transmitters (Txs). The physical foundation of DDM is the utilization of the interactions among multiple concurrent wireless signals [18]. In our scheme, we first decompose a high-order modulation (the

Manuscript received 19 September 2023; revised 12 April 2024; accepted 16 April 2024. Date of publication 19 April 2024; date of current version 5 November 2024. This work was supported in part by the National Natural Science Foundation of China under Grant U23A20300, Grant 62072351, Grant 62372361, and Grant 62202359, in part by the Key Research Project of Shaanxi Natural Science Foundation under Grant 2023-JC-ZD-35, in part by JSPS KAKENHI under Grant JP23K16877, in part by the Project of Cyber Security Establishment with Inter-University Cooperation, in part by the 111 Project under Grant B16037, in part by the Academy of Finland under Grant 308087, Grant 3335262, and Grant 345072, and in part by the U.S. National Science Foundation under Grant 1317411. Recommended for acceptance by C. Xin. *(Corresponding author: Zheng Yan.)*

Zhao Li, Siwei Le, and Jie Chen are with the School of Cyber Engineering, Xidian University, Xi'an, 710126, China (e-mail: zli@xidian.edu.cn; lesiwei6@gmail.com; jiechen2395@gmail.com).

Kang G. Shin is with the Department of Electrical Engineering and Computer Science, The 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).

Zheng Yan is with the School of Cyber Engineering, Xidian University, Xi'an 710126, China (e-mail: zyan@xidian.edu.cn).

Riku Jäntti is with the Department of Communications and Networking, Aalto University, 02150 Espoo, Finland (e-mail: riku.jantti@aalto.fi).

Digital Object Identifier 10.1109/TMC.2024.3391344

modulation order is at least 4) into the combination of multiple QPSK modulations which can be further decomposed into two mutually orthogonal BPSK modulations, and then employ two cooperative Txs to modulate the data information onto two physical signals separately, in the end, the above-mentioned two distributedly transmitted signals are mixed and post-processed at the intended Rx so that the desired information can be recovered. As for the eavesdropper, s/he needs to acquire all the information about the distributively transmitted user's signals for eavesdropping, and thus the secrecy of legitimate user's transmission is guaranteed.

In essence, DDM-Sec focuses on the design of secure physical-layer waveform by utilizing two sub-signals, rather than using encryption. That is, DDM-Sec does not require key generation and management, thus eliminating the overhead and limitations of the aforementioned physical-layer key-based security techniques. The interactions between these two sub-signals can construct the desired signal waveform at the legitimate Rx, while introducing interference at the eavesdropper. Unlike the conventional artificial noise (AN) and cooperative jamming (CJ) based PLS methods, DDM doesn't incur extra power consumption. From a modulation perspective, DDM incorporates wireless channel characteristics into the modulation process, which is different from the conventional transmission where channel status is not involved with the modulation. DDM can fully exploit the spatial signatures of signal transmission, including the randomness of wireless channels and the distributed locations of cooperating Txs. The rich and complex environment can improve the secrecy of legitimate communication. As a result, the eavesdropper can't recover the data information unless s/he captures all the signals and combine them correctly, which is very hard, if not impossible, in practice. Moreover, the signal from any Tx doesn't carry the desired information directly, and thus can effectively prevent the eavesdropper from overhearing the user's information.

The main contributions of this paper are three-fold:

- Proposal of *decomposed and distributed*[1] *modulation* (DDM). We show that a high-order modulation can be decomposed into multiple QPSK modulations which can be further decomposed into two mutually orthogonal BPSKs. Therefore, modulation can be carried out by two cooperative Txs distributedly. The intended Rx can recover the desired data by post-processing the overall effect of the signal components from the two Txs. We develop two DDM realizations, including *precoding without power control* (Pw/oPC) and *precoding with power control* (Pw/PC). The former can be used for QPSK, while the latter is applicable to both M-ary phase shift keying (MPSK) and M-ary quadrature amplitude modulation (MQAM) with modulation order $M = 2^n$ where $n \in \{2, 3, \cdots\}$.
- Analysis of secrecy performance of the proposed method. We show that by exploiting the interactions among two signal components, randomness of wireless channels, and delay difference of two distributed transmissions due to the random deployment of the two Txs and Rx, the eavesdroppers can hardly recover the user's private information, and hence the secrecy of legitimate transmission is achieved.
- Hardware implementation of DDM. We employ universal software radio peripheral (USRP) platform to implement DDM and demonstrate its effectiveness. Compared to conventional modulation, which is realized at a single Tx, DDM can provide comparative legitimate transmission performance and obviously enhanced secrecy.

The rest of this paper is organized as follows. Section II introduces the related works, while Section III describes the system model. Section IV details the DDM and its two implementations and Section V generalizes the proposed DDM. Section VI analyzes the secrecy performance. Section VII evaluates the effectiveness of DDM-Sec through both hardware experiments and simulations. Finally, Section VIII concludes the paper.

In the rest of this paper, we will use the following notations. $\mathbb{C}$ represents the set of complex numbers, while vectors and matrices are denoted by bold letters. Let $\mathbf{X}^H$ and $\mathbf{X}^\dagger$ denote the Hermitian and pseudo inverse of matrix $\mathbf{X}$, respectively. $\|\cdot\|$ and $|\cdot|$ indicate the Euclidean norm and the absolute value, respectively. $\mathbb{E}(\cdot)$ denotes statistical expectation.

II. Related Work

As mentioned earlier, existing PLS methods can be classified into two types. The first type [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18] generates and manages secret keys by exploiting the randomness and reciprocity of wireless channels [3]. This idea is in essence similar to the traditional encryption technique. Under such a scheme, a pair of legitimate Tx and Rx generate an encryption/decryption key in terms of the communication link without requiring a central node for performing key distribution, so that both end-points of the legitimate transmission can dynamically generate the key. The authors of [4] proposed a PLS algorithm based on constellation phase rotation and amplitude randomization. The legitimate Rx can recover the original constellation via an inverse transformation after establishing the synchronization with its Tx, while eavesdroppers can't realize such synchronization. In this scheme, constellation phase rotation and amplitude randomization function as the secret key for physical layer encryption. In [5], a secure far proximity identification approach that can determine whether a remote device is far away or not was developed. Its key idea is to estimate the proximity from the unforgeable fingerprint of the proximity. The authors of [5] developed a technique that can extract the fingerprint of a wireless device's proximity from the physical-layer features of signals sent by the device. [6] designed a channel state information (CSI) feedback mechanism to prevent CSI forging without requiring any modification at the client side. With this method, Txs send a falsified known sequence instead of the genuine known sequence to mislead the CSI estimation process at malicious clients before malicious clients forge CSI in the CSI feedback. The authors of [7] proposed an efficient dual-permutation secret key generation

[1] In this paper, we use the term 'distributed' to indicate that the desired signal waveform is decomposed into two sub-signals and transmitted via two Txs. However, it's crucial to emphasize that the two Txs need to collaborate with each other to realize DDM. That is, the system implementing DDM is not inherently distributed.

method. They formulate the secret key agreement as a bipartite graph matching problem and determine the secret key by minimizing the discrepancy between two permuted received signal strength sequences in a holistic way, thereby reducing the error probability of the physical-layer key between the Tx and the Rx. A PLS scheme, called PLSSCS, is proposed in [8] which combines orthogonal frequency division multiplexing (OFDM) and compressed sensing (CS) to address the deficiency in existing OFDM-based PLS schemes, namely, their limited dynamism in secret keys derived from pre-extracted information. PLSSCS extracts the key from channel measurements, simplifying key management. Moreover, since the generated key changes with the variation of the OFDM frame, the key's dynamism can be improved. However, the aforementioned approaches require consistent channel estimation outcomes at both ends of the link. The rate of channel variation affects both the cost of channel estimation and their effectiveness. Nevertheless, inspired by these methods, we can further exploit the randomness of wireless channels by incorporating them into the modulation process, allowing us to fully utilize the channels' randomness to ensure secure transmission.

The secrecy capacity analysis methods [9], [10], [11], [12], [13], [14], [15], [16], [17] incorporate various PLS techniques such as insertion of AN, beamforming design, and CJ to realize information safety. Of them, [9], [10], [11], [12], [13], [14] considered the use of AN for secure communications. In [10], the Tx ensured communication secrecy by utilizing some of its power to produce AN so as to deteriorate the eavesdropper's channel. It has been shown that a non-zero rate for secret communication can be obtained regardless of the eavesdropper's position. The authors of [11] presented an AN-based scheme to enhance the secrecy of interference alignment (IA) based wireless networks, with which a Tx can design and generate AN individually or cooperatively with relay such that only the eavesdropper's channel is disrupted. In [12], two primary attacks at the physical layer of IA-based networks were studied, including adversarial jamming and eavesdropping. IA is used to solve adversarial jamming attacks, while AN can prevent eavesdropping attacks. In [13], a power allocation approach is proposed for AN-aided beamforming to enhance the PLS of multiple input single output (MISO) wiretap channels by minimizing the secrecy outage probability. Through the use of bisection search, the optimal power allocation factor can be easily determined with reduced computational complexity. [14] combined AN with IA to design a secrecy beamforming scheme that incorporates AN for secure transmission. It also introduced a modified IA scheme to enhance secrecy, making it suitable and stable for PLS in multi-user interference networks. [15] studied the secure physical-layer transmission employing multi-antenna beamforming with imperfect CSI. The authors of [16] proposed a CJ strategy to prevent eavesdroppers from obtaining user's information in the wireless network. In [17], a divide-and-conquer based CJ strategy was developed. With this method, the source encodes the message into multiple coded blocks, and then transmits each block one by one. It has been proved that secure transmission can be realized by selecting one jammer for each transmission so that any eavesdropper misses at least one code block. Nevertheless, the aforementioned methods demand extra Tx (i.e., hardware cost) and/or increased transmit power consumption. Some approaches may even require the knowledge of CSI related to the attacker or eavesdropper, which can pose challenges in practical applications. Inspired by this type of approaches, we can create and exploit internal interference within the physical waveform to counteract eavesdropping without requiring additional Txs or increasing transmit power consumption.

Before delving into details, we briefly compare DDM with other typical transmission mechanisms, such as beamforming (BF), spatial multiplexing (SM), space-time coding (STC), and IA. Similar to DDM, these methods involve the use of multiple antennas for transmitting separate data streams. Their differences can be described as follows:

- With BF, a single data stream is pre-processed by multiple Tx antennas for transmission. In contrast, DDM divides the original desired data into two sub-data streams and transmits them using two Txs separately. This fundamental difference in the transmission approach distinguishes DDM from BF.
- In SM, the Rx requires multiple antennas to detect and decode multiple data streams. In contrast, DDM does not rely on multiple antennas at the Rx. Even if the Rx has more than one antenna, it perceives only one mixed physical signal and detects and decodes it as a whole. In other words, under DDM, the Rx need not distinguish the two components that constitute the mixed received signal. This distinction sets DDM apart from SM.
- As for STC, it encodes data information in the time domain. In contrast, DDM doesn't utilize time domain encoding. As a result, STC requires more time to transmit the desired data than DDM, making DDM more efficient in terms of transmission time. Additionally, STC requires the Rx to have multiple antennas, while DDM allows the use of a single antenna at the Rx. Moreover, under STC, each transmit antenna transmits the entire encoded data information, albeit in different encodings. In contrast, in DDM, each antenna only transmits a portion of the data. Therefore, DDM is different from STC.
- IA encodes data across multiple antennas within the spatial domain at the Tx-side. In contrast, DDM does not encode data across the Txs or their antennas. Moreover, to apply IA, the Rx needs multiple antennas to perform spatial domain signal processing, so that various signal/interference components can be distinguished. Conversely, DDM can be implemented using a single receiving antenna, as its primary focus is on the precise combination of the two signal components at the Rx, rather than treating them individually.

III. System Model

Fig. 1 shows a communication scenario consisting two cooperative[2] Txs, i.e., Alice 0 and Alice 1, one desired Rx, Bob,

[2]The cooperation can be achieved through a dedicated control link, either wired or wireless. In our system model, we do not specify the exact form of cooperation, as the legitimate communication pair has the flexibility to choose between wired or wireless collaboration based on their preferences.

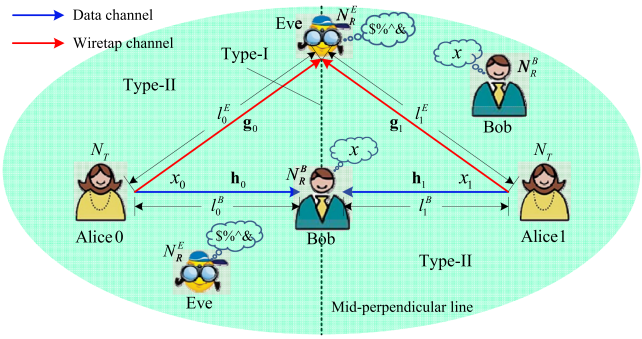


Fig. 1. System model.

and one eavesdropper, Eve. Both Alice 0 and 1 are equipped with $N_T \geq 2$ antennas. Bob and Eve are equipped with N_R^B and N_R^E antennas, respectively. We use P_T to denote the transmit power of Alice 0 and 1. As for the legitimate Rx (Bob) and eavesdropper (Eve), we divide their possible locations into two categories, i.e., Type-I and Type-II, without loss of generality. Type-I location is on the mid-perpendicular of the line of two Txs, and Type-II locations are those other than Type-I. That is, a Rx is either located at Type-I or Type-II location/position. For simplicity, we plot in Fig. 1 only one position of each type of Bob and Eve, respectively.

We use $\mathbf{h}_i \in \mathbb{C}^{N_R^B \times N_T}$ $(i \in \{0,1\})$ to denote the channel matrix from Alice i to Bob, while the channel matrix from Alice i to Eve is denoted by $\mathbf{g}_i \in \mathbb{C}^{N_R^E \times N_T}$. We adopt a spatially uncorrelated [6] Rayleigh flat fading channel to model the elements of the above matrices as independent and identically distributed zero-mean unit-variance complex Gaussian random variables. We assume that all Rxs experience block fading, i.e., channel parameters remain unchanged in a block consisting of several successive time slots and vary randomly between successive blocks. Bob can accurately estimate CSI with respect to Alice 0 and 1, i.e., $\mathbf{h}_0$ and $\mathbf{h}_1$, and feed it back to the two Alices via a error-free link. We assume reliable links for the delivery of CSI and signaling.

Let l_i^B and l_i^E be the distance from Alice i to Bob and Eve, respectively. We use c to represent the speed of light. When Alice 0 and 1 simultaneously send the signals, the differences of latency between the two received signals at Bob and Eve, representing the delay difference, are computed as $\delta_t^B = \frac{|l_1^B - l_0^B|}{c}$ and $\delta_t^E = \frac{|l_1^E - l_0^E|}{c}$, respectively. We use x to denote a high-order modulated data symbol that needs to be delivered to Bob. x_0 and x_1 are the outputs of two mutually orthogonal BPSK links (see in Fig. 2(a)). Both x_0 and x_1 are precoded and then sent by Alice 0 and 1, respectively.

IV. Design of Decomposed and Distributed Modulation

In this section, we will begin by presenting the basic signal processing of DDM. Then, we will propose two methods for compensating the different attenuation of two distributed transmission links. Finally, we will provide a brief qualitative comparison between DDM and other typical schemes.

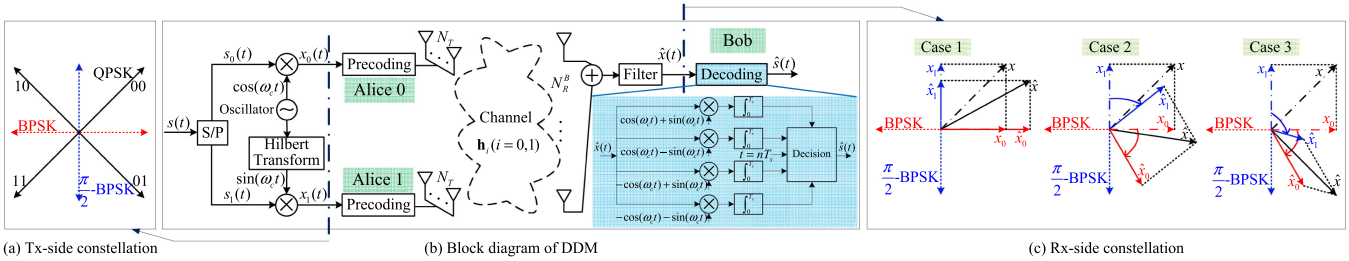
A. Basic Signal Processing of DDM

We first take QPSK modulation as an example to show the realization of DDM as plotted in Fig. 2. The input bipolar data sequence is denoted as $s(t)$. For simplicity, we assume the Rx is at Type-I location and two Alices transmit simultaneously so that the two signal components arrive at the Rx synchronously in the following discussion. The case of Type-II location of Rx and transmitting/receiving with delay difference will be studied in Section VI. After serial-to-parallel (S/P) conversion, $s(t)$ is divided into two subsequences, i.e., $s_0(t)$ and $s_1(t)$, which are then multiplied with $\cos(\omega_c t)$ and $\sin(\omega_c t)$ in the upper and lower BPSK links, respectively. ω_c represents for the carrier frequency. The outputs of two multipliers are $x_0(t) = s_0(t)\cos(\omega_c t)$ and $x_1(t) = s_1(t)\sin(\omega_c t)$. In conventional QPSK modulation, the output is $x(t) = x_0(t) + x_1(t)$ acting as one signal. The constellation map of the upper (BPSK) and lower ($\frac{\pi}{2}$-BPSK) links, as well as their combinational QPSK output are plotted in subfigure (a). As the figure shows, QPSK constellation can be realized by combining two mutually orthogonal BPSK modulations. To be specific, a QPSK symbol, corresponding to a constellation point in the constellation map (or the end-point of the vector in subfigure (a)), can be obtained by combining a BPSK and a $\frac{\pi}{2}$-BPSK symbol.

In the DDM scheme, $x_0(t)$ and $x_1(t)$ are precoded and transmitted by two collaborated Txs i.e., Alice 0 and 1. In practice, the two Alices can also serve as separate radio frequency (RF) endpoints of a single source. The source is responsible for the S/P conversion, while the two Alices handle modulation and transmission of subsequences. These two transmissions arrive at Bob through various wireless channels. Bob receives a mixed signal consisting of signals from Alice 0 and 1, and then post-processes it to obtain $\hat{x}(t)$. In the end, we employ the detection methods [19] such as maximum likelihood (ML), zero forcing (ZF), minimum mean squared error (MMSE), at the decoding stage so that the data information $\hat{s}(t)$ is recovered from $\hat{x}(t)$. It should be noted that the symbol rate for each subsequence remains unchanged, and they share the same spectrum, meaning no additional spectrum consumption.

In the above scheme, two collaborated Txs are employed to realize the modulation and transmission in a distributed manner. Although DDM is more complex than traditional centralized modulation (CM), with which the modulation is realized at a single Tx, from the security point of view, the randomness of a wireless channel can be fully exploited in DDM. To be specific, the inherent randomness of the two links causes interference among the sub-signals at the eavesdropper. Obtaining the status of the two links for precise sub-signal combination presents a significant challenge and is extremely costly for eavesdroppers to achieve. Furthermore, none of the transmission links carry the legitimate user's full information, hence significantly improving the secrecy of communication.

In what follows, we will detail the distributed implementation of QPSK using two collaborative Txs, and then extend it to more general modulation schemes in Section V. For clarity of exposition and without ambiguity, we omit the time index t in the following discussion. Without loss of generality, we assume



(a) Tx-side constellation (b) Block diagram of DDM (c) Rx-side constellation

Fig. 2. Realization and principle of DDM.

Alice 0 employs BPSK and Alice 1 adopts BPSK with $\frac{\pi}{2}$ phase shift. The BPSK-modulated data symbol, x_i ($i \in \{0, 1\}$), are then precoded by vector $\mathbf{p}_i$, before being sent from Alice i. Bob (located on the mid-perpendicular of the line of two Txs) post-processes the combination of the signals from Alice 0 and 1 with filter vector $\mathbf{f}$. We can then obtain the estimated signal as:

$$\hat{x} = \sqrt{P_T}\mathbf{f}^H\mathbf{h}_1\mathbf{p}_1x_1 + \sqrt{P_T}\mathbf{f}^H\mathbf{h}_0\mathbf{p}_0x_0 + \mathbf{f}^H\mathbf{z} \quad (1)$$

where $\mathbf{z}$ represents for the additive white Gaussian noise (AWGN) vector whose elements have zero-mean and variance σ_n^2. The first and second terms on the right-hand side (RHS) of (1) are $\hat{x}_1 = \sqrt{P_T}\mathbf{f}^H\mathbf{h}_1\mathbf{p}_1x_1, \hat{x}_0 = \sqrt{P_T}\mathbf{f}^H\mathbf{h}_0\mathbf{p}_0x_0$, respectively, representing the components of $\hat{x}$ after filtering. From the combination of the two terms on the RHS of (1), one can get the estimated desired information $\hat{s}$. Note that what we are interested is the overall effect of the two signal terms on the RHS of (1), not the individual components.

Since an arbitrary symbol can be represented by its magnitude and phase, x_i where $i \in \{0, 1\}$ can be expressed as $x_i = \rho_i e^{j\theta_i}$ where ρ_i and θ_i are the amplitude and phase of x_i, respectively. Since Alice 0 employs BPSK and Alice 1 adopts $\frac{\pi}{2}$-BPSK, we have $\theta_0 \in \{0, \pi\}$ and $\theta_1 \in \{\frac{\pi}{2}, \frac{3\pi}{2}\}$. For simplicity, we assume $\rho_i = 1$.

Since $\mathbf{h}_0$ and $\mathbf{h}_1$ are random and independent from each other, $\hat{x}$ will be an attenuated QPSK symbol. Fig. 2(c) shows three typical attenuations discussed as follows.

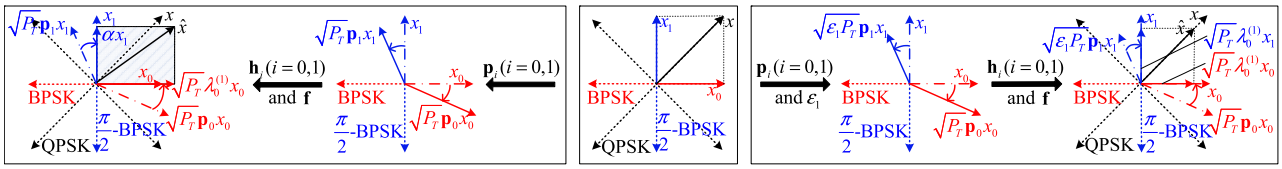
1) The magnitudes of $\hat{x}_0$ and $\hat{x}_1$, denoted by $\hat{\rho}_0$ and $\hat{\rho}_1$, respectively, have been attenuated during the propagation such that $\hat{\rho}_0 \neq \hat{\rho}_1$. Therefore, $\hat{x}$ is not a standard QPSK symbol (see Case 1 in Fig. 2(c)). In this situation, the desired information can still be correctly recovered based on the ML criterion. However, it should be noted that for other high-order modulation schemes, amplitude attenuation may probably incur incorrect decoding. That is, QPSK is less sensitive to amplitude attenuation than other M-order ($M > 4$) modulation schemes.
2) The phases of $\hat{x}_0$ and $\hat{x}_1$, denoted by $\hat{\theta}_0$ and $\hat{\theta}_1$, respectively, have been attenuated. As Case 2 of Fig. 2(c) shows, the vectors representing for $\hat{x}_0$ and $\hat{x}_1$ rotate certain angles compared to their original status at the Txs, indicated by the vectors of x_0 and x_1. In this example, the attenuated $\hat{x}$ lies in the bottom-right region which is different from its original status, i.e., the upper-right region. So, Bob will decode wrong data information.
3) In Case 3 of Fig. 2(c), both the amplitudes and phases of x_0 and x_1 have been attenuated, so that the filter outputs an incorrect QPSK symbol $\hat{x}$.

In summary, the filtered symbol $\hat{x}$ under attenuation may be steered away from its right position denoted by x (see Cases 2 and 3), thus incorrect decoding happens. However, we can appropriately design the precoding vectors and receive filter, at Txs and Rx, respectively, and employ power control (named as *precoding with power control (Pw/PC)*) or not (called *precoding without power control (Pw/oPC)*) at the Tx-side, to compensate for the attenuation, so that $\hat{x}_0$ and $\hat{x}_1$ can form a correct QPSK symbol from which Rx recovers its desired information.

The traditional CM generates a modulated signal using a single Tx. In contrast, DDM incorporates both wireless links associated with the two Txs into the modulation process. This approach leverages the randomness of wireless channels to achieve PLS. The implementation of DDM requires two collaborative Txs, each generating a sub-signal, to construct a desired signal waveform at the intended Rx. It is important to note that the DDM incurs hardware cost and processing overhead[3] primarily at the Tx-side. Moreover, accurate estimation of the fading between the two Txs and the intended Rx is essential for DDM. These estimation results serve as the foundation for determining the transmission parameters. We consider the fact that obtaining the CSI would be more challenging for the eavesdropper than for the legitimate Rx because the legitimate Rx collaborates with the Tx, whereas the eavesdropper does not. What's more, as for the data sharing and cooperation between the two Alices, they do introduce the signaling and control overheads. This requirement can be addressed by utilizing a dedicated high-speed backhaul link [21].

The Rx perceives an overlapping waveform and transparently treats it as a whole, regardless of its generation method, i.e., CM or DDM.

[3]Note that DDM performs singular value decomposition (SVD) on two $N_R^B \times N_T$ channel matrices separately instead of one $N_R^B \times 2N_T$ matrix. As discussed in [20], the computational complexity can be expressed with the number of real floating point operations (FLOPs). Then, the FLOPs required for applying SVD to two $N_R^B \times N_T$ channel matrices is $48(N_R^B)^2N_T + 96\,N_R^BN_T^2 + 108\,N_T^3$. In contrast, applying SVD to a $N_R^B \times 2N_T$ matrix costs $48(N_R^B)^2N_T + 192\,N_R^BN_T^2 + 432\,N_T^3$ FLOPs which is obviously higher. As a result, the spatial signal processing complexity and the signaling overhead of DDM is modest compared to processing multiple channel matrices as a whole.



(a) Pw/oPC based DDM (b) Tx-side constellation (c) Pw/PC based DDM

Fig. 3. Illustration of Pw/oPC and Pw/PC based DDM.

B. Compensation for Attenuation With Pw/oPC and Pw/PC

We first present the Pw/oPC based DDM under QPSK, and then detail the Pw/PC based DDM suitable for more general modulation schemes. We use $\mathbf{p}_i$ where $i \in \{0,1\}$ to denote the precoder used at Alice i. Bob employs $\mathbf{f}$ as the receive filter. We take SVD based pre- and post-processing as an example. Applying SVD to $\mathbf{h}_i$, we have $\mathbf{h}_i = \mathbf{U}_i\mathbf{\Lambda}_i\mathbf{V}_i^H$. Then, we adopt $\mathbf{p}_0 = \mathbf{v}_0^{(1)}$, $\mathbf{p}_1 = \{[\mathbf{u}_0^{(1)}]^H\mathbf{h}_1\}^\dagger / \|[\mathbf{u}_0^{(1)}]^H\mathbf{h}_1\}^\dagger\|$ (the derivation of $\mathbf{p}_1$ is elaborated as below), and $\mathbf{f} = \mathbf{u}_0^{(1)}$ where $\mathbf{v}_i^{(1)}$ and $\mathbf{u}_i^{(1)}$ denote the first column vectors of the right and left singular matrices, $\mathbf{V}_i$ and $\mathbf{U}_i$, respectively. Therefore, the estimated signal $\hat{x}$ is expressed as:

$$\hat{x} = \sqrt{P_T}[\mathbf{u}_0^{(1)}]^H\mathbf{h}_1\mathbf{p}_1 x_1 + \sqrt{P_T}\lambda_0^{(1)}x_0 + [\mathbf{u}_0^{(1)}]^H\mathbf{z}. \quad (2)$$

where $\lambda_0^{(1)}$ denotes the largest singular value of $\mathbf{h}_0$.

In order to obtain a correct QPSK symbol via the combination of the two signals from Alice 0 and 1, we can derive:

$$\sqrt{P_T}[\mathbf{u}_0^{(1)}]^H\mathbf{h}_1\mathbf{p}_1 = \alpha. \quad (3)$$

where α is a positive real number, representing for the amplitude gain of x_1 (see in Fig. 3(a)). That is, after receive filtering, the phases of both BPSK signals become identical to their original status at the Tx-side (see x_0 and x_1 in Fig. 3(b)). Then, according to (3), $\mathbf{p}_1$ can be obtained as:

$$\mathbf{p}_1 = \frac{\frac{\alpha}{\sqrt{P_T}}\{[\mathbf{u}_0^{(1)}]^H\mathbf{h}_1\}^\dagger}{\left\|\frac{\alpha}{\sqrt{P_T}}\{[\mathbf{u}_0^{(1)}]^H\mathbf{h}_1\}^\dagger\right\|} = \frac{\{[\mathbf{u}_0^{(1)}]^H\mathbf{h}_1\}^\dagger}{\left\|\{[\mathbf{u}_0^{(1)}]^H\mathbf{h}_1\}^\dagger\right\|}. \quad (4)$$

So, the received signal at Bob becomes:

$$\hat{x} = \alpha x_1 + \sqrt{P_T}\lambda_0^{(1)}x_0 + [\mathbf{u}_0^{(1)}]^H\mathbf{z}. \quad (5)$$

Fig. 3 illustrates the basic principle of Pw/oPC and Pw/PC based DDM. In subfigure (b), a QPSK symbol x is decomposed into two BPSK symbols, i.e., x_0 and x_1. Subfigure (a) shows the principle of Pw/oPC based DDM, and verifies its validity. Since no power control is employed at Alice 1, the amplitude of $\hat{x}_1$ is probably different from that of $\hat{x}_0$. As shown in the leftmost subplot of Fig. 3(a), $\|\alpha x_1\| = \alpha$ is smaller than $\|\sqrt{P_T}\lambda_0^{(1)}x_0\| = \sqrt{P_T}\lambda_0^{(1)}$. In practice, α can also be larger than $\sqrt{P_T}\lambda_0^{(1)}$. Therefore, the combined $\hat{x}$ is away from the desired QPSK symbol x. It can be easily seen that according to the ML criterion, since the Euclidean distance between $\hat{x}$ and x is smaller than that between $\hat{x}$ and other three standard QPSK constellation points, Bob can correctly recover $\hat{s}$ from $\hat{x}$. In addition, the value of α doesn't affect the correctness of decoding. Therefore, DDM based QPSK can be realized without Tx-side power control.

QPSK involves only phase modulation, but in practice, both amplitude and phase can be exploited in modulation. Moreover, the order of modulation can be much higher than 4, thus requiring power control at the Tx-side. Below we will present DDM based on Pw/PC.

Without loss of generality, we employ a power control factor, ε_1, at Alice 1. ε_1 is a positive real number. Then, Bob's filtered signal is expressed as:

$$\hat{x} = \sqrt{\varepsilon_1 P_T}[\mathbf{u}_0^{(1)}]^H\mathbf{h}_1\mathbf{p}_1 x_1 + \sqrt{P_T}\lambda_0^{(1)}x_0 + [\mathbf{u}_0^{(1)}]^H\mathbf{z}. \quad (6)$$

Similarly to the derivation of (4) from (3), we let:

$$\sqrt{\varepsilon_1 P_T}[\mathbf{u}_0^{(1)}]^H\mathbf{h}_1\mathbf{p}_1 = \sqrt{P_T}\lambda_0^{(1)}. \quad (7)$$

According to (7), transmission from Alice 1 to Bob (we call it *link 1* in the following discussion for ease of presentation, and as its counterpart, transmission from Alice 0 to Bob is called *link 0*) should not introduce any phase shift, as link 0 does (this requirement is the same as that in (3)); and moreover, both links should incur the same strength attenuation to x_0 and x_1 (this is stricter than (3)). Based on the above analysis, Alice 1 designs precoding vector $\mathbf{p}_1$ according to $\mathbf{h}_0$ shared by Alice 0 and its own $\mathbf{h}_1$ as follows:

$$\mathbf{p}_1 = \frac{\frac{\lambda_0^{(1)}}{\sqrt{\varepsilon_1}}\{[\mathbf{u}_0^{(1)}]^H\mathbf{h}_1\}^\dagger}{\left\|\frac{\lambda_0^{(1)}}{\sqrt{\varepsilon_1}}\{[\mathbf{u}_0^{(1)}]^H\mathbf{h}_1\}^\dagger\right\|} = \frac{\{[\mathbf{u}_0^{(1)}]^H\mathbf{h}_1\}^\dagger}{\left\|\{[\mathbf{u}_0^{(1)}]^H\mathbf{h}_1\}^\dagger\right\|} \quad (8)$$

which is the same as the result given in (4). That is, Pw/PC employs the same precoder as Pw/oPC does, but Pw/oPC only requires $\sqrt{P_T}[\mathbf{u}_0^{(1)}]^H\mathbf{h}_1\mathbf{p}_1$ to be a positive real number α rather than being equal to $\sqrt{P_T}\lambda_0^{(1)}$ as with Pw/PC.

Then, we have:

$$\varepsilon_1 = [\lambda_0^{(1)}]^2\left\|\{[\mathbf{u}_0^{(1)}]^H\mathbf{h}_1\mathbf{p}_1\}^\dagger\right\|^2. \quad (9)$$

From the above expression, it is worth noting that ε_1 can exceed 1, implying that Alice 1 might consume more power than P_T during the application of Pw/PC. In practice, to avoid such additional power consumption, we can leverage the collaboration between Alice 0 and 1 to proportionally adjust the transmit power of the two Txs so as to meet both (7) and the constant total transmit power constraint of $2P_T$. Consequently, Alice 0 and 1 should transmit with power of $\frac{2}{1+\varepsilon_1}P_T$ and $\frac{2\varepsilon_1}{1+\varepsilon_1}P_T$, respectively.

Based on the above discussion, we employ $\mathbf{p}_1$ and ε_1 in the precoding and transmit power control at Alice 1, with consideration of $\mathbf{f}$ employed by Bob, called Pw/PC, so that the amplitude and phase distortion of channel propagation can be compensated.

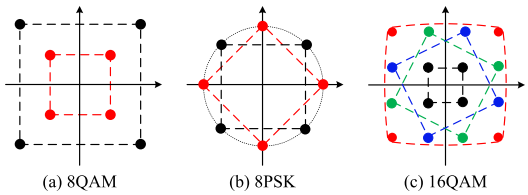


Fig. 4. Decomposition of various modulation schemes.

Then, Bob can see a correct QPSK symbol. DDM based QPSK can, therefore, be realized.

Bob's filtered signal can be expressed as:

$$\hat{x} = \sqrt{P_T}\lambda_0^{(1)}(x_1 + x_0) + [\mathbf{u}_0^{(1)}]^H \mathbf{z} = \sqrt{P_T}\lambda_0^{(1)} x + [\mathbf{u}_0^{(1)}]^H \mathbf{z}. \tag{10}$$

Finally, the desired data information can be decoded from $\hat{x}$ using ML detection.

Fig. 3(c) illustrates the principle of Pw/PC-based DDM. As the figure shows, we employ $\mathbf{p}_i$ ($i \in \{0, 1\}$) to pre-process x_i and then send it from Alice i. As for Alice 1, its power coefficient is ε_1. $\mathbf{p}_0$ is obtained via the SVD of $\mathbf{h}_0$ as mentioned above, whereas $\mathbf{p}_1$ is determined in terms of (8). The rightmost subplot of Fig. 3(c) plots the post-processed signals at Bob. For comparison, we also show the signals $\sqrt{P_T}\mathbf{p}_0 x_0$ and $\sqrt{\varepsilon_1 P_T}\mathbf{p}_1 x_1$ in this plot. Since we have properly designed $\mathbf{p}_1$ and ε_1, under the influence of $\mathbf{h}_i$ and $\mathbf{f}$, the inter-relationship of filtered $\hat{x}_0$ and $\hat{x}_1$ are the same as their original signals' at Alice 0 and 1, except for the introduction of an identical scaling factor $\sqrt{P_T}\lambda_0^{(1)}$. Therefore, a QPSK symbol, $\hat{x}$, is obtained at Bob, from which the desired information can be decoded.

In practice, Pw/oPC does not require control of the transmit power, making it easy to implement. On the other hand, Pw/PC introduces a power control factor ε_1 to adjust the power of one of the two signal components, thereby increasing complexity. Pw/PC at Bob can produce a standard QPSK modulated waveform, but, under Pw/oPC, due to the noticeable difference in fading through the two transmission links, the constellation point recovered from the received waveform may deviate from its standard position. In summary, when the attenuations from the two Alices to Bob are similar, Pw/oPC is the preferred choice. Conversely, when there is a significant difference in attenuation, we recommend adopting Pw/PC to ensure satisfactory reception performance at Bob.

The design of DDM does not impose any extra processing on Bob. That is, DDM is transparent to the Rx, and hence can effectively facilitate its application.

V. Extension of DDM to More General Modulation Schemes

So far, we have shown that QPSK can be realized by two mutually orthogonal BPSK modulations at two cooperative Txs distributedly. We now discuss the decomposition of more general high-order modulation schemes, such as MQAM and MPSK.

Fig. 4(a) plots the constellation of square 8QAM, showing that 8QAM can be decomposed into two QPSK modulations, representing by the inner and outer squares, respectively, with various amplitudes. When an 8QAM symbol is sent to Bob, Alice 0 and 1 first select a proper QPSK constellation (inner or outer square) from Fig. 4(a), and then send two BPSK signals that can constitute the symbol in the selected QPSK constellation, according to the realization of Pw/PC based DDM discussed in Section IV. Since two QPSKs with different magnitudes are involved, each Alice should generate BPSK signals with proper transmit power levels, $\varepsilon_i P_T |x_i|^2$ where $i \in \{0, 1\}$ indicates the upper and lower BPSK links as shown in Fig. 2(b). ε_i is the power allocation factor employed by Alice i. $|x_i| = \rho_i$ can be taken two different values related to the inner and outer QPSKs, respectively. In this example, the realization of DDM is sensitive to amplitude distortion in that the two constellation points in the same region/quadrant are of the same phase, so that they can be distinguished only by their amplitude information. Therefore, Alice 1 selects an appropriate power coefficient ε_1 in terms of (9), so as to compensate for the channel fading to Bob. Then, according to (10), Bob can see a QPSK symbol with correct amplitude based on the information of P_T and $\lambda_0^{(1)}$, from which the desired information is decoded. In practice, we can also let Alice 0 employ ε_0 to realize correct decoding.

Fig. 4(b) shows the decomposition of 8PSK, where 8PSK can be divided into two QPSK constellations with the same amplitude and different phase shifts. In this example, the black QPSK can be realized based on Pw/PC based DDM. As for the red one, it has $\frac{\pi}{4}$ phase shift compared to the black QPSK. So, the decomposed two BPSK constellations will thus have the same $\frac{\pi}{4}$ phase shift, yielding the phase sets of two BPSKs to be $\theta_0 \in \{\frac{\pi}{4}, \frac{5\pi}{4}\}$ and $\theta_1 \in \{\frac{3\pi}{4}, \frac{7\pi}{4}\}$, respectively. The values of each set indicate the initial phases of carriers used in the upper and lower modulation links in Fig. 2(b). Under 8PSK, DDM becomes sensitive to phase error, i.e., a constellation point of one decomposed QPSK can be attenuated such that it is incorrectly decided as a point of the other QPSK constellations. Therefore, Pw/PC based DDM should be employed. The case of MPSK ($M > 8$) is similar to 8PSK, thus needing Pw/PC. However, since QPSK doesn't have such a problem, both Pw/oPC and Pw/PC are applicable.

Based on the decomposed implementation of 8QAM and 8PSK, we can infer that most practical high-order modulation schemes can be similarly decomposed and realized in a distributed way. For clarity of exposition, we illustrate in Fig. 4(c) the decomposition of square 16QAM, showing that 16QAM can be decomposed into 4 QPSK constellations with various amplitudes and phase shifts. We use 4 different colors to denote the 4 QPSKs. Fig. 4(c) can be regarded as the combination of Fig. 4(a) and (b). Similarly to the discussion of Fig. 4(a), we first select a transmit symbol from one of the QPSK constellations decomposed from the 16QAM constellation, and then decompose the selected QPSK symbol into two mutual-orthogonal BPSKs and send them distributedly. Note that we should adopt power control at the Tx-side for channel compensation, so that Bob can decode desired information correctly from the right QPSK symbol.

In summary, most widely used high-order modulation schemes, such as MPSK and MQAM, can be realized by the proposed DDM.

VI. Analysis of Secrecy Performance

In this section, we will first present the calculation of secrecy capacity, and then discuss the influence of large-scale and small-scale fading on DDM's performance.

A. Calculation of Secrecy Capacity

Bob's capacity, $\mathcal{C}_B$, can be obtained by calculating the maximum average mutual information. Given the probability of transmitted symbol $P(x)$, the probability of a received symbol $P(\hat{x})$, and joint probability density $P(x,\hat{x})$,[4] the maximum average mutual information can be computed as:

$$\begin{aligned}\mathcal{C}_B &= \max_{P(x)}\{I(X;\hat{X})\} \\ &= \max_{P(x)}\left\{\sum_{x\in X}\sum_{\hat{x}\in\hat{X}} P(x,\hat{x})\log_2\frac{P(x,\hat{x})}{P(x)P(\hat{x})}\right\} \end{aligned} \tag{11}$$

where X and $\hat{X}$ denote the transmit and receive symbol sets $x\in X$ and $\hat{x}\in\hat{X}$, respectively. Note that (11) can also be used for calculating $\mathcal{C}_E$.

Consequently, the secrecy capacity $\mathcal{C}_S$, defined as the maximum transmission rate at which the eavesdropper is unable to acquire any legitimate user's information, can be obtained by subtracting $\mathcal{C}_E$ from $\mathcal{C}_B$ [22], as:

$$\mathcal{C}_S = \max_{P(x)}\{\mathcal{C}_B - \mathcal{C}_E, 0\}. \tag{12}$$

B. Analysis of the Influence of Large-Scale and Small-Scale Fading on DDM

In DDM, the reception performance of both legitimate Rx and eavesdropper is sensitive to the delay/phase difference of two signal components. Such delay/phase difference also affects the PLS of DDM. In this subsection, we will discuss the influence of large-scale fading (LSF) and small-scale fading (SSF) on the delay/phase difference. As for the delay/phase difference incurred by LSF, it depends on the propagation paths' length difference of two signals, while the delay/phase difference yielded by SSF results from the difference of two paths' CSI. We take the Rx employing coherent detection as an example, and for simplicity omit the noise term in the following derivation. Recall that the modulated symbols x_0 and x_1 can be represented as radio frequency (RF) signals $x_0 = s_0\cos(\omega_c t)$ and $x_1 = s_1\sin(\omega_c t)$, we can rewrite (1) as:

$$\hat{x} = \sqrt{P_T}\mathbf{f}^H\mathbf{h}_1\mathbf{p}_1 s_1\sin(\omega_c t) + \sqrt{P_T}\mathbf{f}^H\mathbf{h}_0\mathbf{p}_0 s_0\cos[\omega_c(t+t_\Delta)] \tag{13}$$

where t_Δ denotes the delay difference incurred by LSF, while the influence of SSF is reflected by the difference between $\mathbf{h}_0$ and $\mathbf{h}_1$. The Rx employs coherent detection to process $\hat{x}$. This involves multiplying $\hat{x}$ with carriers $\cos(\omega_c t)$ and $\sin(\omega_c t)$, and letting the outputted signals go through a low-pass filter (LPF) to remove the high-frequency components. Then, we can obtain the base-band estimated signals $\hat{x}_0$ and $\hat{x}_1$ as:

$$\hat{x}_0 = \frac{\sqrt{P_T}\mathbf{f}^H\mathbf{h}_0\mathbf{p}_0}{2}s_0\cos(\omega_c t_\Delta), \tag{14}$$

$$\hat{x}_1 = \frac{\sqrt{P_T}\mathbf{f}^H\mathbf{h}_1\mathbf{p}_1}{2}s_1 - \frac{\sqrt{P_T}\mathbf{f}^H\mathbf{h}_0\mathbf{p}_0}{2}\sin(\omega_c t_\Delta). \tag{15}$$

The coordinates of the base-band symbol obtained by the Rx can be expressed by $(\hat{x}_0,\hat{x}_1)$ in a constellation map. So, we can then apply ML to approximate $(\hat{x}_0,\hat{x}_1)$ to its closest standard constellation point, from the latter the Rx can recover its desired information $\hat{s}$. Note that due to LSF and SSF, $(\hat{x}_0,\hat{x}_1)$ is deviated from the original desired data point x (see in Fig. 3(b)) whose coordinates are (s_0,s_1). Such deviation will affect the reception accuracy. In (14) and (15), the SSF is indicated by the complex terms $\frac{\sqrt{P_T}\mathbf{f}^H\mathbf{h}_0\mathbf{p}_0}{2}$ and $\frac{\sqrt{P_T}\mathbf{f}^H\mathbf{h}_1\mathbf{p}_1}{2}$, whose argument and module values will influence the distance between $(\hat{x}_0,\hat{x}_1)$ and (s_0,s_1). As for the LSF, it is represented by the terms $\cos(\omega_c t_\Delta)$ and $-\frac{\sqrt{P_T}\mathbf{f}^H\mathbf{h}_0\mathbf{p}_0}{2}\sin(\omega_c t_\Delta)$. When $\omega_c t_\Delta \neq 2k\pi$ where $k\in\mathbb{Z}$ and $\mathbb{Z}$ denotes integer set, $(\hat{x}_0,\hat{x}_1)$ is different from (s_0,s_1).

For the phase difference incurred by SSF, we can use the methods proposed in Section IV to estimate CSI and design precoders $\mathbf{p}_0$ and $\mathbf{p}_1$ to let $\sqrt{P_T}\mathbf{f}^H\mathbf{h}_0\mathbf{p}_0 = \sqrt{P_T}\mathbf{f}^H\mathbf{h}_1\mathbf{p}_1$ hold. That is, by simultaneously scaling the amplitudes of two signal components, they can be orthogonal to each other at the intended Rx. As for the delay difference t_Δ incurred by LSF, we can properly deploy the Txs and Rx or adjust the two Txs' initial transmit time, so that two signal components can arrive at the legitimate Rx with $t_\Delta = 0$, then we can have $\cos(\omega_c t_\Delta) = 1$ and $-\sin(\omega_c t_\Delta) = 0$.

It should be noticed that when $\omega_c t_\Delta = 2k\pi$ where k is non-zero integer, although $\cos(\omega_c t_\Delta) = 1$ and $-\sin(\omega_c t_\Delta) = 0$ can hold, there is still a delay difference t_Δ in integer multiples of carrier periods between the two signal components. When $t_\Delta < T_s$ where T_s denotes the time-length of a base-band symbol, the two signal components can output partially correct QPSK modulated signal; however, the delayed BPSK component will overlap with the other signal component in the next symbol period, resulting partial errors in the superimposed QPSK waveform for that symbol period and affecting the correctness of demodulation. When $t_\Delta > T_s$, the superimposed QPSK signal is entirely incorrect, thus the Rx can't retrieve the desired data correctly. In summary, to eliminate delay difference incurred by LSF, one should let t_Δ be close to 0 as much as possible.

As discussed above, both the LSF and SSF can contribute to PLS. The former provides randomness to the outcome of the combined waveform, while the latter introduces a fixed delay difference between the two signal components associated with the locations of the Txs and Rx. If Eve (the eavesdropper) can estimate the LSF but not the SSF, she could potentially attain a satisfactory capacity by compensating for the LSF or adjusting her wiretapping position (see Fig. 16 in section VII). Nevertheless, due to the influence of SSF which degrades Eve's reception performance, given the same location, Eve's capacity will be lower than that of Bob (compare Figs. 16 and 15). On the other hand, if Eve can estimate SSF but not the LSF,

[4] In the simulation, both the numbers of transmitted symbols x and the estimated symbols $\hat{x}$ can be counted. As a result, their probabilities $P(x)$ and $P(\hat{x})$, as well as the joint probability density $P(x,\hat{x})$, can be calculated by dividing the corresponding number of symbols by the total number of symbols.

she could carry out signal processing to counter the random attenuation caused by the wireless channels. However, without the knowledge of LSF, even if Eve employs multiple antennas and can distinguish the two signal components, she still can't rectify the delay difference of two transmission links, hence yielding poor decoding performance. Nevertheless, Eve may still attempt to explore various wiretapping positions to potentially enhance her capacity. However, as Eve changes her position, she may need to re-estimate the SSF, which in turn introduces additional overhead. Based on the above discussion, we can conclude that SSF plays a more prominent role in enhancing PLS than LSF.

C. Discussion of Secrecy Performance Under Various Adversary Models

In practice, Bob can be randomly located in the communication area as shown in Fig. 1. Given Alice 0 and 1 transmit simultaneously, when Bob is on the mid-perpendicular of the line of two Txs (Type-I location), the transmission delays of the two paths are identical. When Bob is located at Type-II positions, the two decomposed BPSK signals will arrive at Bob with different delays — we define this delay difference or relative delay as δ_t^B to indicate the degree of delay difference of the two transmissions to Bob — and hence interfere with each other and decrease Bob's performance. In this case, we can employ *delay calibration* at the Tx-side so that two BPSK signals arrive at Bob at the same time, i.e., making $\delta_t^B = 0$. This way, Bob can obtain the desired signal as if he were on the mid-perpendicular of the line of two Txs.

As for the eavesdropper, it becomes more difficult to acquire the legitimate user's information with DDM than that employs the conventional modulation schemes realized at a single Tx. In what follows, we will analyze the effects of DDM-based transmission on the reception of eavesdropper.

The influence of distributed modulation: Since each transmitted signal doesn't carry the full legitimate user's information, the eavesdropper can't recover the legitimate user's data unless s/he can overhear both signals from the Txs. As for the legitimate Rx, it can receive the desired signal as if the signal were modulated in a conventional way.

The influence of delay difference (i.e., LSF): Since the transmissions from Alice 0 and 1 to Eve may have different delays, the two BPSK components probably interfere with each other, incurring random received signals at Eve. In practice, Alice may calibrate delay, i.e., make $\delta_t^B = 0$, to ensure Bob's reception, which can further randomize the combined waveform perceived by Eve. Since it is difficult and challenging for Eve to accurately acquire the arriving time of two BPSK signal components, she can't realize time alignment of the two components, making eavesdropping performance poor.

The influence of channel randomness (i.e., SSF): Since Bob and Eve undergo independent channel fadings, i.e., $\mathbf{h}_i$ and $\mathbf{g}_i$ where $i \in \{0, 1\}$ are random and independent of each other. Eve needs to know both $\mathbf{h}_i$ and $\mathbf{g}_i$ so as to achieve good post-processing output. However, since acquiring $\mathbf{h}_i$ is always challenging for Eve, the secrecy of legitimate transmission can be guaranteed.

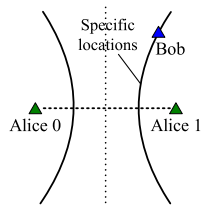


Fig. 5. Illustration of specific eavesdropping locations.

Based on the above discussion, we use Table I to show Eve's eavesdropping capability and performance under various adversary models. The table is obtained under the assumption that locations of Alice 0 and 1 are fixed while Bob's location is random as shown in Fig. 1. To guarantee the simultaneous arrival of the two distributedly transmitted signals at Bob, the two Alices perform delay calibration. We use "$\surd$" and "$\times$", respectively, to denote the *availability* and *unavailability* of certain information which can be used by Eve for eavesdropping.

As Table I shows, under adversary models 1–10 and 12–13, eavesdropping can only be realized at specific locations, whereas for the rest of the models Eve can eavesdrop without any location constraint. Fig. 5 illustrates the *specific locations* mentioned in Table I. In the figure, Alice 0 and 1 are at the two focuses of a hyperbolic curve, while Bob is on the hyperbolic curve. When Eve is on the same side of the hyperbolic curve of Bob which is referred to as the specific locations, the difference of the distances from Alice 0 and 1 to Eve is the same as that from Alices to Bob, hence yielding the same delay difference. Since the two Alices perform delay calibration for Bob, Eve can realize eavesdropping without delay difference. The last column of Table I qualitatively shows Eve's eavesdropping performance. Such performance is meaningful only when eavesdropping is available, i.e., under models 1–10 and 12–13 the performance is evaluated at the above-mentioned specific locations.

If Eve can access the distances from Alice i ($i \in \{0, 1\}$) to Bob and herself, i.e., l_i^B and l_i^E, she can then mitigate the delay difference of the two signals from Alice 0 and 1 at her receiver. However, in such a case, Eve should be equipped with two receiving antennas so as to distinguish the two signal components before combining them to extract the original high-order modulated desired signal. In general, the availability of $\mathbf{h}_i$ and $\mathbf{g}_i$ can help Eve design receive-filter matching channel conditions so as to eliminate the effect of the randomness of wireless channels; the knowledge of l_i^B and l_i^E contributes to the mitigation of delay difference so that synchronized combination of two distributedly transmitted signal components at the eavesdropper can be realized. As for adversary model 16, Eve's knowledge of $\mathbf{h}_i$, $\mathbf{g}_i$, l_i^B, and l_i^E could enable her to realize eavesdropping and render the `DDM-Sec` ineffective. However, in practice, obtaining the above information would be very difficult and costly. Specifically, to obtain $\mathbf{h}_i$, the eavesdropper must intercept the feedback/control link between the legitimate Rx and Txs; to estimate $\mathbf{g}_i$, the eavesdropper must be aware of the pilot signal sent by the legitimate Txs. Moreover, to get

TABLE I
EVE'S EAVESDROPPING CAPABILITY AND PERFORMANCE UNDER VARIOUS ADVERSARY MODELS

Index of adversary model	Information's availability for eavesdropping				Ability of eavesdropping	Performance of eavesdropping
	$\mathbf{h}_i$	$\mathbf{g}_i$	l_i^B	l_i^E		
1	×	×	×	×	Yes @ specific locations	Poor
2	√	×	×	×		
3	×	√	×	×		
4	×	×	√	×		
5	×	×	×	√		
6	√	√	×	×		Good
7	√	×	√	×		Poor
8	√	×	×	√		
9	×	√	√	×		
10	×	√	×	√		
11	×	×	√	√	Yes	
12	√	√	√	×	Yes @ specific locations	Good
13	√	√	×	√		
14	√	×	√	√	Yes	Poor
15	×	√	√	√		
16	√	√	√	√		Good

l_i^B and l_i^E, the eavesdropper needs to enlist collaborators to estimate the locations of legitimate Txs and Rx. Since involving multiple collaborative eavesdroppers can be both costly and complex, and our focus is on the scenario with non-cooperative eavesdroppers, we choose adversary models 3 and 6 as typical case studies to evaluate the secrecy performance of the proposed method in Section VII. The performance under the other models of Table I can be roughly estimated according to the results provided in those evaluations. For instance, by noting that the delay difference of the two transmissions can be calibrated only when both l_i^B and l_i^E are available at the Rx, Eve's performance under models with either l_i^B or l_i^E being available is equivalent to that with neither l_i^B nor l_i^E. Based on this fact, we compare model 5 with 6 and can find the main difference of these two models: Eve knows both $\mathbf{h}_i$ and $\mathbf{g}_i$ under model 6, yielding better eavesdropping performance than that of model 5. That is, we can infer Eve's capacity under model 5 from that of model 6.

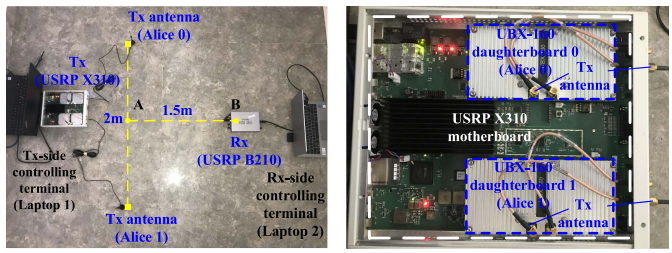
In summary, DDM-Sec exploits the distributed modulation, transmission delay difference, and channel randomness to realize secure transmission. Although the legitimate transmission becomes more sophisticated than the traditional centralized modulation, benefiting from the Tx-side cooperation/calibration, Bob's reception remains unchanged, i.e., no extra modification/processing is required at the legitimate Rx. As for Eve, her eavesdropping performance will be seriously degraded due to the above-mentioned three factors.

VII. EVALUATION

In this section, we first use the universal software radio peripheral (USRP) platform to implement DDM-Sec under the adversary model 3 of Table I and demonstrate its validity, and then use MATLAB simulation to evaluate DDM-Sec's performance under the adversary models 3 and 6. We employ QPSK as an example. Similar results can be obtained under other high-order modulation schemes.

A. Hardware Implementation of DDM

We employ a USRP X310 device equipped with two UBX-160 daughterboards as the Txs, and a USRP B210 device as the Rx, to implement DDM. For simplicity, we let the two UBX-160 daughterboards and B210 be equipped with a single antenna. As Fig. 6(a) shows, the two UBX-160 daughterboards realize the processing of Alice 0 and 1, respectively, and the positions of the antennas connected to the daughterboards represent the spatial locations of Alice 0 and 1. The B210 device acts as the legitimate Rx (i.e., Bob) to detect the received mixed signal. The X310 device connects to a terminal (laptop 1), which controls the two RF daughterboards to realize the BPSK modulations of Alice 0 and 1, and further transmit the modulated signal through the antennas. The B210 device is connected to another terminal (laptop 2), which controls the signal detection and data demodulation.



(a) Experimental setup (b) Internal structure of USRP X310

Fig. 6. Hardware implementation of DDM.

In the experiment, all devices are deployed in a 3 m×3 m plane. The two transmit antennas are approximately 2 m apart, and the Rx (point B) is located on the perpendicular bisector (i.e., AB) of the line connecting the transmit antennas, approximately 1.5 m away from point A. This experimental setup is limited by the length of the cable connecting the USRP X310 and transmit antennas, the relatively low power-efficiency of the antenna with respect to the signal frequency, and the transmit power constraint of the USRP X310. Since the inter-device distance primarily affects the received signal's strength rather than the precise combination of the distributed signal components, our method remains feasible even when the devices are far apart. The main parameters used in the experiment are shown in Table II.

According to the experimental setup shown in Fig. 6(a), signals x_0 and x_1 will experience approximately the same small-scale and large-scale fading before reaching Bob. Bob estimates the equivalent CSI between him and the Txs based on the mixed

TABLE II
PARAMETER SETTINGS OF DDM

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	0.4MBaud	0.5	[4dB,15dB]

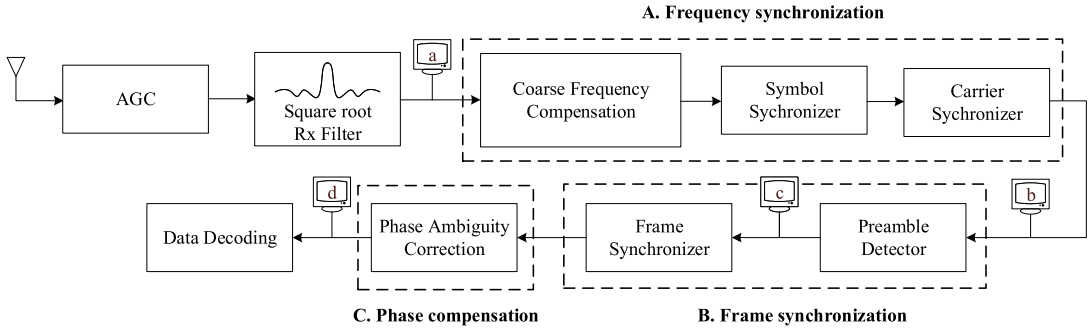


Fig. 7. Flowchart of Rx-side processing.

pilot signals received from Alice 0 and 1 (we use Barker code as the pilot sequence), and then compensates the equivalent channel accordingly and adopts the QPSK demodulation module to recover the desired data from the mixed signal. The DDM implementation at the Tx-side is transparent to Bob.

Fig. 6(b) shows the two UBX-160 daughterboards installed on an X310 motherboard, which provides a unified clock reference to the daughterboards for generating carrier signals of the same frequency. This configuration allows the two Txs to operate synchronously. In practice, GPS Disciplined Oscillator (GPSDO) can also be adopted for realizing long-distance synchronization with high precision. When dealing with multiple devices operating with non-synchronized clock sources, we can use techniques such as phase-locked loop (PLL)-based fine frequency compensation, timing recovery with fixed-rate re-sampling, bit stuffing/skipping, and frame synchronization, to achieve synchronization. In the existing communication systems, Tx-side synchronization can be implemented [23]. For simplicity, we equip both Alice 0 and 1 with a single antenna, while the B210 operates as a single-antenna Rx. In this configuration, there is no need to pre-code the data before transmission.

In the experiment, the Txs (Alice 0 and 1) follow the procedure shown in Fig. 2(b) to convert the data s into s_1 and s_2 through S/P conversion. Laptop 1 controls the UBX-160 daughterboard representing Alice 0 to modulate s_0 with BPSK using initial phase values of $\{0, \pi\}$ to obtain x_0, and controls the UBX-160 representing Alice 1 to modulate s_1 with BPSK using initial phase values of $\{-\frac{\pi}{2}, \frac{\pi}{2}\}$ to obtain x_1. Alice 0 and 1 simultaneously transmit their BPSK modulated signals to Bob (B210).

The signal processing of Bob is illustrated in Fig. 7, where automatic gain control (AGC) performs amplitude compensation to counteract path loss and channel attenuation, while the square root Rx filter ensures matching reception in accordance with the square root filter used for transmission. Subsequently, coarse frequency compensation, symbol synchronizer, and carrier synchronizer serve for frequency synchronization, while the preamble detector and frame synchronizer are employed for frame synchronization. Phase ambiguity correction realizes phase-offset compensation incurred by SSF, utilizing estimation results derived from the preamble sequence. Further details are available in [24]. It is worth noting that regardless of CM or DDM, the reception processing at the Rx is identical. The main differences between DDM and CM are described as follows.

First, as DDM utilizes two Txs, precise synchronization is essential for these two Txs. In our experiment, we use a unified clock source to mitigate frequency offset and achieve Tx-side frequency synchronization. Note, however, that without establishing Tx-side synchronization, the legitimate transmission cannot be achieved. In such a case, eavesdropping becomes meaningless. In other words, the utilization of DDM is contingent upon Tx-side synchronization.

Second, prior to data transmission, the legitimate Rx may need to assist the Txs in estimating both LSF and SSF for mitigating the differences between the two distributed transmissions.[5] As discussed in Section VI-C, the Txs can perform delay calibration based on the estimation of LSF. In our experiment setup, we deploy the legitimate Rx on the mid-perpendicular of the line of two Txs to minimize the delay difference of the two links. Regarding the impact of SSF, we can design the precoding vectors and receive filter based on sub-channel estimation, as discussed in Section IV-B. In the hardware implementation, on one hand, we carefully configure the experimental environment to ensure the similarity of SSF in both links; on the other hand, we let the Rx estimate SSL based on the received mixed signal,

[5]In practice, the attacker may attempt to intercept the feedback signal to obtain the controlling information and facilitate eavesdropping. However, such feedback information is intended to guide the Alices' transmission so that the two signal components can be combined to produce the desired signal at Bob. Therefore, in order to realize eavesdropping, Eve needs to use multiple receive antennas to distinguish the two signal components and obtain the large- and small-scale fading conditions between her and the two Alices, in addition to intercepting the controlling information. Nevertheless, acquiring such a large amount of information would significantly increase the cost of eavesdropping, thus rendering eavesdropping practically infeasible. Moreover, in order to prevent interception at the feedback stage, we can utilize data encryption to ensure the confidentiality of the feedback information.

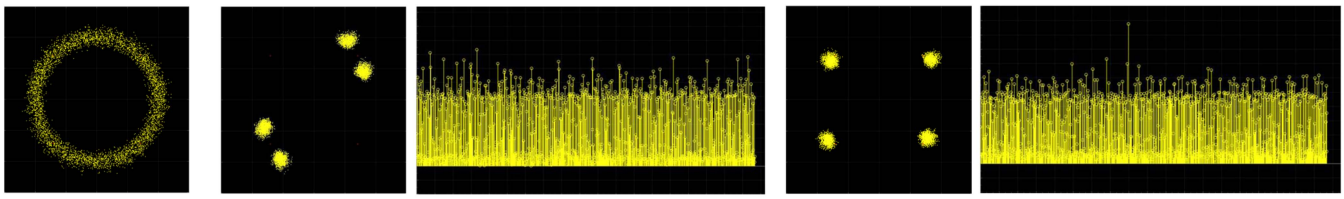


Fig. 8. Rx-side observations under DDM.

since we do not employ precoding to eliminate SSF difference. It is worth noting that in this implementation, since the Rx does not need to estimate the status of the two sub-channels, the transparency of the desired signal generation, whether in a centralized manner or following DDM, is guaranteed.

Fig. 8 shows the experimental observations at various points in the reception flowchart. In this figure, we illustrate QPSK transmission results under DDM. At point 'a', we can see that constellation points are arranged in ring(s) in Fig. 8(1), with the radius indicating the amplitude values of QPSK symbols. This phenomenon is a result of the AGC module compensating for amplitude attenuation caused by LSF. However, the frequency offset between the Txs and Rx introduces phase errors, preventing the appearance of QPSK constellation at this point. Moving to observation point 'b', after achieving frequency synchronization, a constellation map becomes visible. In subfigures (2) and (3), when the delay difference between two links is not calibrated, the outputted constellation distorts compared to standard one. Moreover, as the two signal components cannot be combined synchronously, we cannot recover the preamble sequence from the combined signal. Consequently, conducting frame synchronization does not yield a correlation peak of the preamble sequence. To address this problem, we must compensate for the delay difference of the two links. In our experiment, we accomplish this goal by adjusting the position of the Rx. Then, after frame synchronization, we can obtain an approximate standard constellation and correlation peak as subfigures (4) and (5) show. It is important to note that although the synchronized combination of two signal components can produce an effective signal equivalent to that generated with the conventional CM method, retrieving correct information from the constellation at point 'c' is hindered by the phase-offset incurred by channel fading. Therefore, we need to estimate the phase-offset from the detected preamble sequence and compensate for it before data decoding. This way, we can achieve a correct constellation at observation point 'd'. Since the constellation shapes at points 'd' and 'c' are similar, we omit showing the constellation at point 'd' for conciseness. In summary, the Rx flowchart in Fig. 7 is suitable for decoding signals generated by both CM and DDM. To implement DDM, the Txs should perform delay calibration and account for channel randomness. This ensures that the legitimate Rx can perceive an accurately combined signal identical to the desired signal generated by CM.

Fig. 9 compares the QPSK constellations of the de-modulated data at the legitimate Rx with DDM and CM under various transmit gains. With CM, a single Tx (implemented by a UBX-160 daughterboard connected to the X310 motherboard) employs QPSK modulation to transmit, while Bob (implemented by a B210 device) adopts QPSK demodulation to decode the data. Note that in the implementation of DDM, the baseband amplitude of the two BPSK signals is 1, while in the implementation of CM, the baseband amplitude of the QPSK modulated signal is $\sqrt{2}$. Therefore, although the CM method only employs one USRP device as the Tx, it has the same transmit power as DDM using two USRP devices at the same transmit gain. We can see from Fig. 9 that with the increase of the transmit gain, both DDM and CM can output more concentrated and clearer QPSK constellation points at Bob. The QPSK constellation points yielded by CM are precisely located at the four corners of a square. As a comparison, there is a minor distortion between the constellations of DDM and CM under the same transmit gain. This is because the modulated signal in CM is generated by a single Tx, while the received QPSK waveform under DDM is obtained by superimposing two BPSK signals over the air interface at the Rx, and the experimental setup shown in Fig. 6(a) can't completely eliminate the phase/delay difference between the two BPSK components. Thus, a slightly distorted constellation results. Nevertheless, it is evident from Fig. 9 that legitimate transmission using DDM can achieve comparable performance to that with CM.

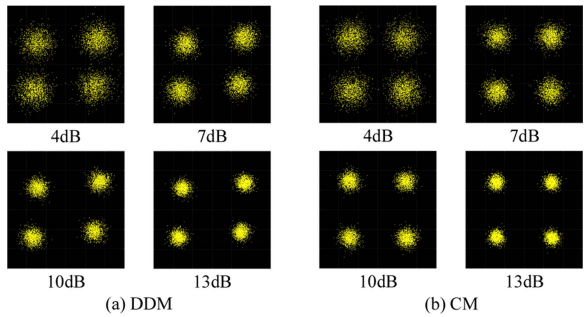


Fig. 9. Comparison of QPSK constellations at Bob under DDM and CM.

Then, we extend the experimental implementation from QPSK to 16QAM. As discussed in Section V, 16QAM can be equivalent to four QPSK constellations with various amplitudes and phase rotations. Then, each QPSK signal can be decomposed into two orthogonal BPSK components. However, it is important to note that DDM-Sec focuses on the design of secure physical-layer waveform, and the decomposition of a target desired signal is not unique. In this experiment, we

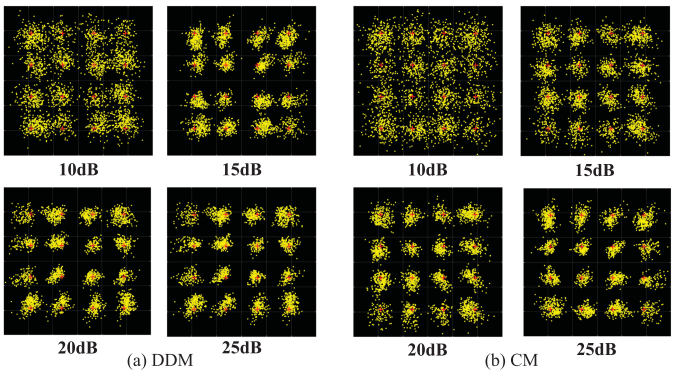


Fig. 10. Comparison of 16QAM constellations at Bob under DDM and CM.

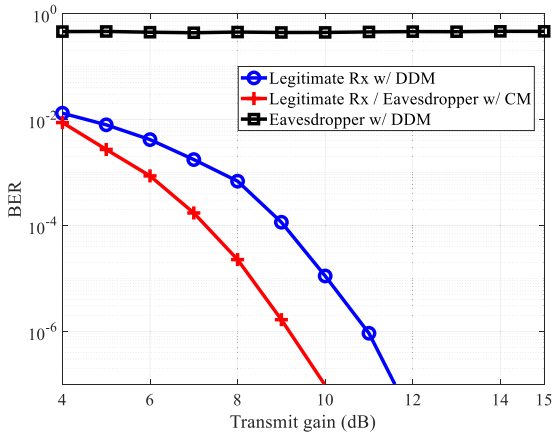


Fig. 11. BER performance legitimate Rx and eavesdropper with DDM and CM.

decompose 16QAM into two QPSK signal components with an identical phase set (i.e., $\{\frac{\pi}{4}, \frac{3\pi}{4}, \frac{5\pi}{4}, \frac{7\pi}{4}\}$) and various amplitudes [19] (specifically, where the larger amplitude is twice that of the smaller one). This way, we realize QPSK modulations with two required amplitudes at the two Txs. At the Rx, 16QAM demodulation is employed. Since the constellation points of 16QAM are denser than those of QPSK, we set the transmit gain to [10 dB, 25dB] to display the variation of constellation map with different transmit gains, and the rest experimental configurations remain unchanged in comparison to the QPSK case. Similar to Fig. 9, we illustrate the 16QAM constellations of the de-modulated data at the legitimate Rx with DDM and CM under various transmit gains in Fig. 10. As the figure shows, the constellation points become more concentrated as the transmit gain increases, which is consistent with the pattern observed in QPSK. Since the variation of 16QAM constellations with transmit gains is similar to that of QPSK constellations shown in Fig. 10, we omit a detailed discussion for conciseness. According to the above results of hardware experiment, the DDM method can be extended from QPSK to other high-order modulations, as discussed in Section V.

When extending to high-order modulation, DDM does not incur extra decoding complexity to the Rx. However, by comparing Figs. 8 and 9, we can see that under fixed channel conditions, both DDM and conventional CM may output a higher bit-error rate (BER) as the modulation order grows. Increasing transmit power may help counteract the effects of channel fading and enhance BER performance. Nevertheless, this approach inevitably makes it easier for eavesdroppers to intercept legitimate information under CM, while at the eavesdropper, the sub-signals will interfere with each other under DDM scheme, making DDM continues to effectively thwart eavesdropping. In essence, the secrecy of our scheme originates from the interactions of distributed sub-signal components, irrespective of the modulation order. The above experimental results under both QPSK and 16QAM indicate that, when the effects of SSF and LSF are minimized through precoding and delay calibration, DDM can achieve a transmission performance approximately as good as CM.

According to the discussion about phase/delay difference in Section VI-B, the wavelength of the 915 MHz carrier signal is approximately 32.79 cm, and the manual deployment of device can ensure that the difference in signal propagation distance is less than 2 cm, so the delay difference t_Δ caused by LSF can be ignored. However, the experimental setup cannot make the SSF experienced by the two signal components strictly identical, so the phase difference caused by SSF can't be completely eliminated, 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 DDM on the Rx's reception, we compare the BER performance of legitimate Rx and eavesdropper by using DDM and CM, respectively, to transmit 5×10^7 bits data with QPSK modulation, and set the transmit gain to [4 dB,15dB], as shown in Fig. 11.

As the figure shows, the BER of legitimate Rx under both transmission schemes decreases as the transmit gain grows. CM outputs better legitimate BER than DDM. This is because in DDM, the QPSK signal is obtained by superimposing two signals at the desired Rx, but the phase/delay difference between the two signal components is not completely eliminated, hence resulting in slight distortion of the observed QPSK constellation compared to that under CM, as shown in Fig. 9(a). Therefore, under the same transmit gain (and the same environmental noise), DDM yields a worse BER than CM. To address this issue, one can compensate for the phase/delay difference based on channel estimation and coordinate the two Txs' initial transmit time. In this way, the constellation shape at the Rx can be improved, so that DDM's BER will approach CM's.

To verify the secrecy performance of DDM, we move the legitimate Rx in Fig. 6(a) from its position on the AB line (Type-I position in Fig. 1) to other positions (Type-II positions in Fig. 1), then the legitimate Rx becomes an eavesdropper. Assuming that the eavesdropper can accurately estimate the CSI between itself and the Txs, and can perform channel compensation and signal detection based on the estimation, this corresponds to the adversary model 6 in Table I. We can plot in Fig. 11 the BER of an eavesdropper employing QPSK demodulation [24]. As the figure shows, the eavesdropper's BER remains around 50% and doesn't improve with the increase of transmit gain. This is because when the eavesdropper is at the type-II position, the two BPSK signals experience phase/delay difference caused by both

SSF and LSF. However, the eavesdropper can't obtain sufficient information to eliminate such phase/delay difference. So, the eavesdropper can't observe a well-shaped QPSK waveform, incurring incorrect QPSK symbol detection and data recovery. When legitimate communication adopts CM, the eavesdropper's BER curve completely overlaps with that of the legitimate Rx (for simplicity, we don't separately show them in the figure). This is because we assume that the eavesdropper can accurately estimate the CSI between itself and the Txs, and can perform channel compensation and matched reception based on the estimation. Consequently, the eavesdropper can successfully decode the legitimate information just like the intended Rx, resulting in the same BER performance. Therefore, CM lacks PLS, while DDM can fully exploit the phase/delay difference of the two signal components to impair the wiretapping, thus achieving fundamental secure data transmission.

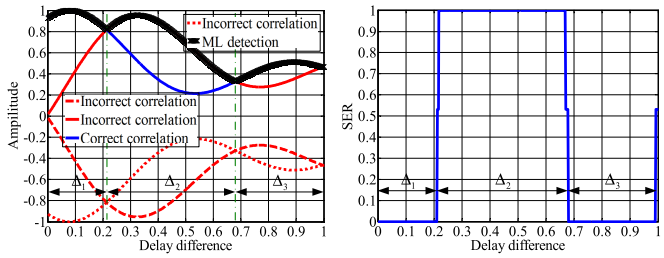
B. MATLAB Simulation of DDM

We now use MATLAB simulations to evaluate the proposed scheme's performance. We will first study the impact of delay difference of two distributed transmissions on the reception of desired symbol, and then investigate the influence of both phase and delay difference on the capacity of legitimate Rx and eavesdropper. Then, we will show Bob's capacity and Eve's eavesdropping performance under Pw/PC based DDM and conventional CM.

1) Influence of Delay Difference on Reception: We now study the impact of delay difference incurred by LSF, i.e., δ_t^B, on the decoding of the combined QPSK symbol at the intended Rx. For simplicity, we omit noise in the simulation, and assume there is guard interval being equal to or greater than δ_t^B between symbols, so that adjacent symbols don't overlap with each other. However, as $\delta_t^B \in [0, T_s]$, two signal components are not align in time, so they interfere with each other. We call this *partial* inter-symbol interference (ISI). Since we set $T_s = 5 \times 10^{-3}$s and $\omega_c = 2\pi \times 200$rad/s, there is $\xi = \frac{\omega_c T_s}{2\pi} = 1$ carrier cycle in a time interval of T_s. Symbol error rate (SER) is averaged over the reception of 10^3 randomly generated QPSK symbols.

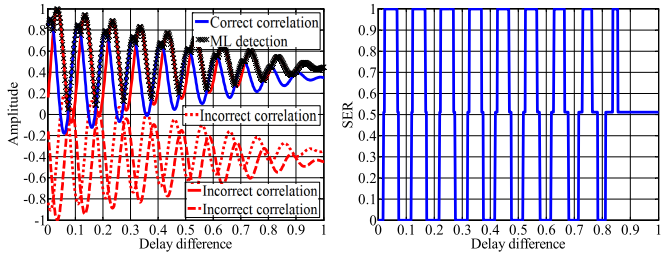
Under QPSK, there are 4 possible waveforms of the QPSK signal, thus 4 branches each containing one possible QPSK waveform and employing correlation operation [19], are involved in the ML detection structure. The detection structure is shown the blue part of Fig. 2(b). The delay difference is normalized by T_s, and only δ_t^B no greater than T_s is studied. Without loss of generality, we can let one of the BPSK signals be delayed while the latency of the other BPSK signal is 0. Then, an attenuated QPSK symbol will appear at the Rx. Given different QPSK symbols, various response waveforms will be yielded by a correlation branch. We use $y_j(t) = \int_{T_s} \hat{x}(t) h_j(t) dt$ where $j \in \{1, 2, 3, 4\}$ denotes the index of a branch, to represent the output of one correlation branch. $y_j(t)$ is fed to the decision module which produces at time nT_s (n denotes the index of symbol) the estimated $\hat{s}(nT_s)$ based on the comparison of $y_j(nT_s)$s.

Fig. 12(a) shows the output waveforms of the 4 correlation branches and the ML detection module with various delay differences given the input QPSK signal is $\hat{x}(t) = s_0(t)\cos(\omega_c t) + s_1(t)\sin(\omega_c t)$. The output of each branch/module is normalized by its maximum value under $\delta_t^B = 0$. In this case, the waveforms of four correlation detection branches are $h_1(t) = \cos(\omega_c t) + \sin(\omega_c t)$, $h_2(t) = \cos(\omega_c t) - \sin(\omega_c t)$, $h_3(t) = -\cos(\omega_c t) + \sin(\omega_c t)$ and $h_4(t) = -\cos(\omega_c t) - \sin(\omega_c t)$, respectively. One can see that when δ_t^B lies in the regions of Δ_1 and Δ_3, correct decoding is yielded, whereas for region Δ_2, the detection is 100% wrong. When $\delta_t^B \geq T_s$, the late-arrived BPSK component is delayed δ_t^B relative to the early arrived one, and hence only the first arrived BPSK component correlates with the QPSK waveforms in the reception structure. Then, according to Fig. 2(a) we can see that a correct BPSK symbol can determine which half-plane (i.e., left or right, upper or lower) the desired QPSK constellation point is located. For example, when $\hat{x}_0(t) = \cos(\omega_c t)$, i.e., $s_0(t) = 1$, enters the correlation branches, a QPSK constellation point on the right half-plane will be decided. Therefore, we can get approximately 50% SER. That is, in the above situation, the single BPSK component can still contribute to Bob's decoding.



(a) Correlation outputs. (b) SER.

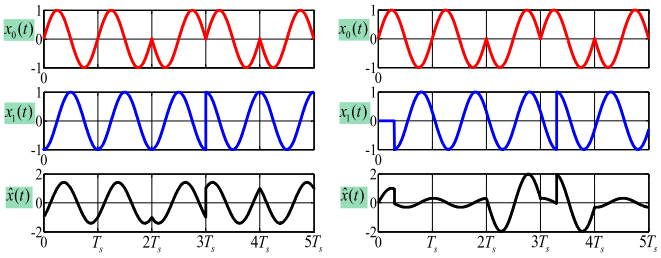
Fig. 12. Correlation outputs and SER of the decoding module under $\xi = 1$, two BPSK inputs (i.e., DDM based QPSK) and various δ_t^B (w/ partial ISI).



(a) Correlation outputs. (b) SER.

Fig. 13. Correlation outputs and SER of the decoding module under $\xi = 10$, two BPSK inputs (i.e., DDM based QPSK) and various δ_t^B (w/ partial ISI).

Then, we set $T_s = 5 \times 10^{-3}$s and $\omega_c = 2\pi \times 2 \times 10^3$rad/s while other conditions are identical to those in Fig. 12, to simulate Fig. 13. In Fig. 13(a), the outputs of the 4 correlation branches and the decision module decrease with an increase of δ_t^B. Similarly to Figs. 12(a), 13(a) only plots the outputs under the input signal $\hat{x}(t) = \cos(\omega_c t) + \sin(\omega_c t)$. As for Fig. 13(b), SER is averaged over all possible QPSK symbols like Fig. 12(b). One can see from the figure that SER alternates between 1 and 0 periodically with the delay difference. When $\delta_t^B > 0.85$, SER is dominated by the early arrived BPSK component, yielding approximate 50% SER.



(a) $\delta_t^B = 0$. (b) $\delta_t^B > 0$.

Fig. 14. DDM based QPSK w/o and w/ delay difference (w/ full ISI).

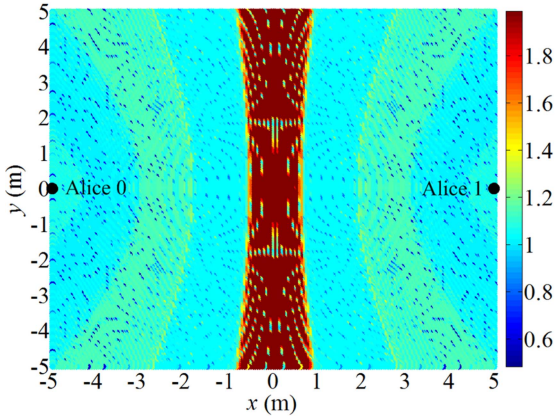


Fig. 15. Distribution of Bob's capacity w/ full ISI and w/o delay calibration.

When there is no guard interval between adjacent symbols, with non-zero delay difference, a symbol of one signal component will interfere with both its prior and subsequent symbols of the other component. We call this *full* ISI as compared to partial ISI. In such full ISI situation, Rx's reception performance will be further deteriorated. Fig. 14 shows the waveforms related to QPSK modulation, within a time-length of $5T_s$. No guard interval is considered. In T_s, we plot only one carrier cycle for clarity. The subplots in the first and second rows of Fig. 14 indicate the BPSK components sent from Alice 0 and 1, i.e., $x_0(t)$ and $x_1(t)$, respectively. The subfigure in the third row is the QPSK signal, i.e., $\hat{x}(t)$ produced by the filter in Fig. 2(b), perceived by the Rx. In Fig. 14(a), both BPSK signals arrive at the Rx at the same time, making an estimated QPSK signal identical to the desired one. As for Fig. 14(b), $x_1(t)$ is delayed $0.3T_s$ relative to $x_0(t)$, i.e., $\delta_t^B = 0.3T_s$. due to the influence of ISI, the output QPSK signal given by the third row of Fig. 14(b), is distorted compared to the one under $\delta_t^B = 0$. To illustrate ISI, let us take the second symbol of $x_0(t)$, denoted by $x_0(t)|_{t\in(T_s,2T_s)}$, as an example. The tail of the first symbol of $x_1(t)$, i.e., $x_1(t)|_{t\in(0.3T_s,1.3T_s)}$, interferes with the head of $x_0(t)|_{t\in(T_s,2T_s)}$. Moreover, the head of the second symbol of $x_1(t)$, i.e., $x_1(t)|_{t\in(1.3T_s,2.3T_s)}$ interferes with the tail of $x_0(t)|_{t\in(T_s,2T_s)}$.

Based on the above results and the discussions in Section VI, Alice 0 and 1 can generate two BPSK components arriving at the legitimate Rx at the same time, thus forming the desired high-order modulated symbol. That is, Bob can be free of the influence of delay difference and ISI by exploiting cooperative capability at Alice 0 and 1. However, for a randomly-located eavesdropper, it becomes too expensive and challenging for him/her to estimate and then mitigate the delay difference. So, the eavesdropper will suffer from ISI, hence making eavesdropping performance poor.

2) Capacity of Legitimate User and Eavesdropper: We simulate the capacity of the legitimate user and the eavesdropper so as to demonstrate the secrecy of the proposed DDM-based transmission. We set symbol rate $R_s = 1.2 \times 10^8$Baud, i.e., $T_s \approx 8.33 \times 10^{-9}$s. Carrier frequency is 2.4 GHz [25], and hence the wavelength is 0.125 m. Both delay difference and channel randomness are taken into account. For simplicity, we omit the amplitude attenuation of path loss. We assume the distance between Alice 0 and 1 is at least a half wavelength (so is the distance between the eavesdropper and the legitimate user) which is usually the case, so that the legitimate channel $\mathbf{h}_i$ and wiretap channel $\mathbf{g}_i$ where $i \in \{0, 1\}$ are independently and randomly generated in the simulation. QPSK symbol is selected with an identical probability from 4 possible waveforms and sent from two collaborating Txs according to DDM.

In the simulation, Txs and Rx are assumed located in a $10\,\text{m} \times 10\,\text{m}$ area. The coordinates of Alice 0 and 1 are set to be $(-5\,\text{m}, 0\,\text{m})$ and $(5\,\text{m}, 0\,\text{m})$, respectively. Given a delay difference $\delta_t^{\mathcal{X}} = T_s$ where the superscript $\mathcal{X}$ can be either B or E representing for Bob and Eve, respectively, the difference of distances from two Txs to Rx can be calculated as $\delta_l^{\mathcal{X}} = |l_1^{\mathcal{X}} - l_0^{\mathcal{X}}| = c\delta_t^{\mathcal{X}} = cT_s \approx 2.5$m. Therefore, under DDM based QPSK, when a large enough guard interval is employed between adjacent symbols, only partial ISI exists when $\delta_l^{\mathcal{X}} \in (0, 2.5]$m; while without guard interval, full ISI is yielded as long as $\delta_l^{\mathcal{X}} > 0$. Based on the above discussion, we study the distribution of capacity in a limited $10\,\text{m} \times 10\,\text{m}$ area. Capacity in extended regions can be inferred from the provided results. Transmit power of each Tx, P_T, normalized by the noise power σ_n^2, is 10 dB. Both Alice 0 and 1 are equipped with $N_T = 2$ antennas, while Bob and Eve have a single antenna and hence can't mitigate the delay difference of the two signals from Alice 0 and 1. Alice 0 and 1 send decomposed BPSK signals simultaneously, i.e., Alice 0 and 1 don't calibrate the delay difference for Bob. In the simulation, we divide the $10\,\text{m} \times 10\,\text{m}$ area into 200×200 cells. Next, for each cell we randomly generate 500 sets of channel status from Txs to Rx, which we call CSI snap shots. Under each snap shot, 500 QPSK symbols are simulated. Then, we can obtain the probabilities of the transmitted signal $P(x)$ and the received signal $P(\hat{x})$, as well as their joint probability density $P(x, \hat{x})$, so that the capacity of the Rx in a cell can be calculated in terms of (11).

Fig. 15 shows the distribution of Bob's capacity, averaged over 500 sets of channel status from Txs to Rx, with full ISI considered in the $10\,\text{m} \times 10\,\text{m}$ area. ISI is incurred because Alice 0 and 1 don't calibrate the delay difference for Bob. Due to full ISI, when $\delta_t^B > 0$, two BPSK components interferes with each other, as shown in Fig. 15, thus affecting Bob's decoding. Bob is shown to have high capacity when he is located on the mid-perpendicular of the line of two Txs; while as he moves away from this line, its capacity decreases. When $\delta_t^B \geq T_s$, two

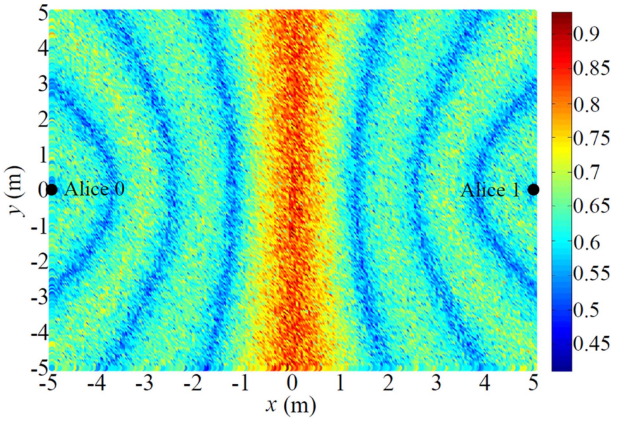


Fig. 16. Distribution of Eve's capacity.

BPSK signal components are completely randomly combined and then fed to the detection structure as plotted in Fig. 2(b), hence yielding low capacity with randomness.

In the above simulation, we assume Alice 0 and 1 transmit simultaneously without delay calibration. When Bob is located on the mid-perpendicular of the line of two Txs, neither delay difference nor ISI affects its reception, thus outputting high capacity. When Bob is at Type-II positions, as shown in Fig. 1, low capacity is yielded. However, in practice, Alices can cooperate with each other, so that the Tx with a shorter propagation distance can delay its transmission so as to achieve time alignment of both BPSK components at Bob (i.e., resulting $\delta_t^B = 0$). This way, Bob can obtain the desired QPSK symbol at the cost of some latency,[6] as if no delay difference existed. In summary, by exploiting the cooperative capability of Txs, Bob can achieve as good a capacity as that when he is located on the mid-perpendicular of the line of two Txs.

Fig. 16 simulates the distribution of Eve's capacity with consideration of full ISI. For simplicity, we assume Alice 0 and 1 don't employ delay calibration, i.e., Bob is located on the mid- perpendicular line between the two Txs and both Alices transmit to Bob simultaneously. In this simulation, we first divide the simulation area into 200×200 cells. Next, for each cell we randomly generate 500 sets (or snap shots) of $\mathbf{h}_i$ and $\mathbf{g}_i$ where $i \in \{0, 1\}$. Then, under each snap shot, 500 QPSK symbols are simulated, so that Eve's capacity in a cell can be calculated using (11) and then averaged over 500 snapshots. We assume Eve can only estimate the wiretap channel $\mathbf{g}_i$, but other information such as data channel $\mathbf{h}_i$, precoders employed by Alice i, i.e., $\mathbf{p}_i$, etc., is not available for Eve. That is, Eve can only determine her receive filter based on $\mathbf{g}_i$. As Fig. 16 shows, Eve's capacity is high on the mid-perpendicular of the line of two Txs which corresponds to the performance at *specific locations* mentioned in Table I except for the cases Eve knows $\mathbf{h}_i$ (specifically, Eve's capacity at such specific locations under adversary models 3, 9, 10 and 15 can be referred to the performance on the mid-perpendicular of the line of two Txs in Fig. 16), and decreases as she moves away from this line which shows the variation of Eve's capacity under models 3, 9 and 10 of Table I at these non-specific locations. Moreover, Eve's capacity shows some periodical feature in the simulated area which is similar to the output QPSK signal waveform with the delay difference given in Fig. 14(b). Due to the random variation of ISI and the interrelationship of $\mathbf{g}_i$ and $\mathbf{h}_i$, Eve's capacity, being inferior to Bob's, also exhibits randomness. Based on the results in Fig. 16, we can deploy a jammer [16], [17] in some insecure areas so that the secrecy of legitimate transmission can be achieved.

Fig. 1 plots Alice 0 and 1, Bob and Eve in the same plane, but such a deployment may not hold in practice. That is, these four entities can be located in a three-dimensional (3-D) space rather than a 2-D plane. In such a case, we only need to study the effective plane involving the two Txs and the Rx (i.e., either Bob or Eve) to be investigated. Then, the Rx's location in the effective plane belongs to either Type-I or Type-II location similar to that plotted in Fig. 1. So, the capacity performance of the Rx at various locations within the effective plane can be obtained using the same method with which Figs. 12–13 are obtained. For space limit, we omit the details in this paper.

In what follows, we will simulate Bob and Eve's capacity as well as secrecy capacity under the proposed DDM and CM, respectively. Under DDM, we assume Alices implement delay calibration so that the delay difference incurred by LSF is eliminated. As for Eve, a delay difference of $0.3T_s$ exists and full ISI between the two signal components is considered. With traditional CM, we let Alice 0 transmit to Bob whereas Alice 1 is shut off. Under DDM, the ratio of transmit power at each Alice to noise power, i.e., $\gamma_{DDM} = 10 \lg \frac{P_T}{\sigma_n^2}$, is set to be from 0 dB to 20 dB. For fairness, the ratio of transmit power at Alice 0 to noise power under CM, i.e., $\gamma_{CM} = 10 \lg \frac{2P_T}{\sigma_n^2}$, varies from 3 dB to 23 dB. We will study adversary models 3 and 6 in evaluating Eve's capacity and the secrecy capacity. Note, however, that Bob's capacity is independent of the adversary model which indicates Eve's capability.

Before delving into details, we first present the main features of adversary models 3 and 6. Under adversary model 3, Eve is aware of $\mathbf{g}_i$ ($i \in \{0, 1\}$) whereas $\mathbf{h}_i$ is unavailable. Then, Eve can design a receive filter according to $\mathbf{g}_i$ to decode the mixed received two signal components. Under adversary model 6, Eve can acquire $\mathbf{g}_i$ accurately, and estimate $\mathbf{h}_i$. Then, she designs a filter vector based on this information to realize eavesdropping. We regard the capability of eavesdropper under adversary model 3 as *medium* while under model 6 as *strong*. As for model 6, we also investigate the influence of the accuracy of estimation of $\mathbf{h}_i$ on eavesdropping. The non-ideal estimated channel information can be modeled as [26]:

$$\hat{\mathbf{h}}_i = \eta \mathbf{h}_i + \sqrt{1 - \eta^2} \boldsymbol{\Xi} \tag{16}$$

where $\mathbf{h}_i$ and $\hat{\mathbf{h}}_i$ denote the accurate and inaccurate channel matrices, respectively. The coefficient η indicates the degree of estimation imperfection. $\eta = 1$ means perfect estimation. Matrix $\boldsymbol{\Xi}$ is an $N_R^B \times N_T$ diagonal complex Gaussian matrix

[6]This latency is upper-bounded by the distance between the two Alices, denoted as l_{01}^A. For example, under $l_{01}^A = 10$m, the maximum delay can be calculated as $l_{01}^A/c \approx 3.33 \times 10^{-8}$s. Then, given $T_s \approx 8.33 \times 10^{-9}$s, we can see that the maximum delay is approximately equivalent to 4 symbol lengths. This latency is considered negligible in practice.

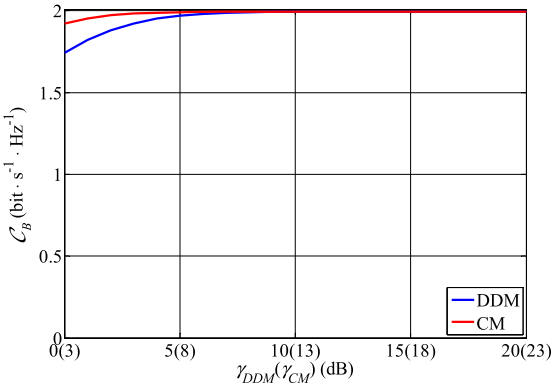


Fig. 17. Bob's capacity under DDM and CM.

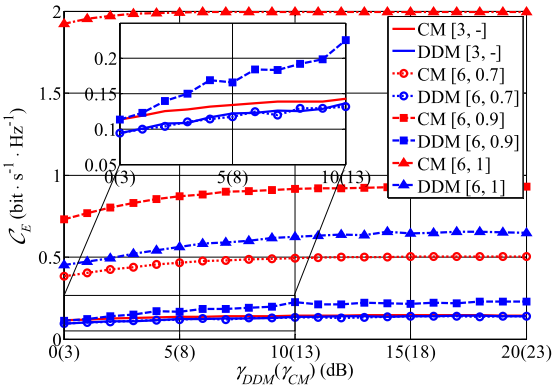


Fig. 18. Eve's capacity under DDM and CM.

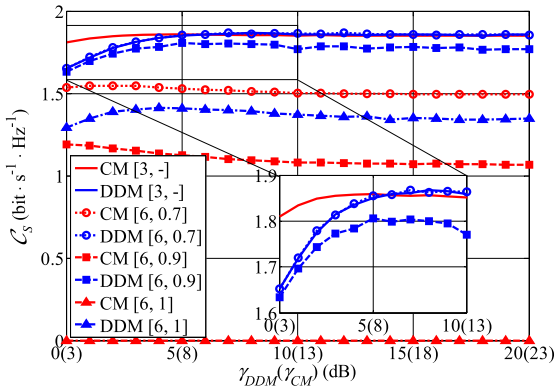


Fig. 19. Secrecy capacity under DDM and CM.

with zero mean and unit variance. In the following evaluation, we will adopt $\eta \in \{0.7, 0.9, 1\}$.

Fig. 17 shows Bob's capacity with DDM and CM, respectively, where a dual x-axis is used. Specifically, under the total transmit power constraint, $\gamma_{CM} = \gamma_{DDM} + 3$dB holds. Since Eve's capability doesn't affect Bob's capacity, $\mathcal{C}_B$ of a certain modulation scheme (i.e., CM or DDM) under various adversary models is identical. As the figure shows, given low $\gamma_{DDM}(\gamma_{CM})$, DDM yields smaller $\mathcal{C}_B$ than CM. This is because under DDM, two distributed transmissions are employed, and both are affected by the noise, whereas for traditional CM, only one link is used and influenced by the noise. Under low $\gamma_{DDM}(\gamma_{CM})$, noise dominates Bob's capacity, yielding $\mathcal{C}_B$ of DDM inferior to that of CM. As $\gamma_{DDM}(\gamma_{CM})$ increases, the influence of noise decreases, incurring $\mathcal{C}_B$ of both schemes increases and approaches 2 bps/Hz.[7]

Fig. 18 shows Eve's capacity of DDM and CM under various adversary models and ηs. For simplicity, we employ the vector $[\mathcal{M}, \eta]$ where $\mathcal{M} \in \{3, 6\}$ denotes the index of adversary model and $\eta \in \{0.7, 0.9, 1, -\}$, to indicate parameter settings. Note that the symbol "$-$" represents the in-applicability of η under $\mathcal{M} = 3$. Under adversary model 3, Eve only knows $\mathbf{g}_i$, due to the exploitation of channel randomness (CM and DDM) and delay difference (DDM), both DDM and CM yield very low $\mathcal{C}_E$. In the case of adversary model 6, Eve acquires $\mathbf{g}_i$ and estimates $\mathbf{h}_i$ with accuracy coefficient η. As one can see from the figure, due to the enhanced capability of eavesdropper, $\mathcal{C}_E$ of CM under adversary model 6 is clearly improved over that under model 3. This is because with CM, only the channel randomness is exploited in preventing the eavesdropping of desired transmission. Moreover, since such channel randomness is reduced as η grows, $\mathcal{C}_E$ increases with an increase of η under model 6. Furthermore, $\mathcal{C}_E$ of CM under $\eta = 1$ equals $\mathcal{C}_B$ of CM in Fig. 17, i.e., with sufficient channel information, Eve can decode the legitimate information as Bob does. In such a case, the secrecy capacity becomes 0. As for DDM, both channel randomness (under $\eta < 1$) and delay difference are exploited for secure transmission, so $\mathcal{C}_E$ of DDM under model 6 is slightly improved over that under model 3. Moreover, given the same η, DDM's $\mathcal{C}_E$ is much lower than CM's under model 6. Although $\mathcal{C}_E$ increases as η grows under model 6, $\mathcal{C}_E$ of DDM with $\eta = 1$ is still inferior to that of CM under $\eta = 0.9$. That is, DDM exhibits good secrecy performance when the eavesdropper's capability is strong.

Fig. 19 shows the secrecy capacity of DDM and CM under various adversary models and ηs. Recall that $\mathcal{C}_E$ of DDM is close to that of CM (see in Fig. 18) under adversary model 3, whereas $\mathcal{C}_B$ of DDM is lower than that of CM under small $\gamma_{DDM}(\gamma_{CM})$ (see in Fig. 17), the secrecy capacity, $\mathcal{C}_S$, of CM is higher than that of DDM with small $\gamma_{DDM}(\gamma_{CM})$ under adversary model 3 as shown in Fig. 19. As $\gamma_{DDM}(\gamma_{CM})$ grows, the influence of noise decreases, incurring $\mathcal{C}_S$ of DDM approaches that of CM in a high $\gamma_{DDM}(\gamma_{CM})$ region under adversary model 3. In the case of model 6, $\mathcal{C}_E$ of CM improves significantly as η increases (see in Fig. 18) whereas $\mathcal{C}_B$ of CM is independent of the adversary model and coefficient η. Thus in Fig. 19, $\mathcal{C}_S$ of CM decreases with an increase of η. Since DDM exploits both channel randomness and delay difference in assuring secrecy, even Eve can estimate $\mathbf{h}_i$ accurately, the improvement of $\mathcal{C}_E$ with DDM is still limited. Therefore, $\mathcal{C}_S$ of DDM under adversary model 6 decreases slightly compared to that under model 3.

[7]Since a high-order modulated signal is decomposed into two BPSK signal components, each of them carries 1-bit information per symbol. Moreover, according to the Nyquist Criterion [19], 2Baud/Hz is the highest possible unit bandwidth symbol rate, which is also called the *Nyquist rate*. In our simulation, we set unit bandwidth symbol rate to 1Baud/Hz; consequently, the simulated capacity is upper bounded by 2 bps/Hz.

Moreover, provided with the same η, $\mathcal{C}_S$ of DDM dominates that of CM. Given $\eta = 1$, $\mathcal{C}_S$ of CM becomes 0, whereas DDM's $\mathcal{C}_S$ is still around 1.4 bps/Hz.

From the simulation results in Figs. 14–16 and the discussions therein, we can conclude that the proposed DDM-Sec can guarantee secrecy transmission from Alices to Bob by exploiting both channel randomness and delay difference. As for CM, since its secrecy depends only on channel randomness, when the eavesdropper can get access to the channel information, s/he can even process the received mixed signal just like the legitimate receiver, hence resulting in almost zero secrecy capacity.

VIII. Conclusion

In this paper, we have proposed a novel physical-layer secure transmission scheme, called DDM-Sec, based on decomposed and distributed modulation (DDM). We have shown that a high-order modulation can be decomposed into multiple QPSK modulations, each of which can be further represented by two mutually orthogonal BPSK modulations. Our theoretical analysis and numerical evaluation show that the proposed DDM-Sec can effectively exploit the randomness of wireless channels and enrich the spatial signatures of the legitimate transmission, and can thus effectively cripple the eavesdropper, and guarantee the secrecy of the legitimate user's data transmission. In the design of DDM-Sec, we assume single Bob and Eve for clarity. However, this method can be readily applied to scenarios where multiple legitimate Rxs and eavesdroppers exist. First, when multiple Bobs need to be served, the transmissions can be realized by following the principle of multi-user multiple-input multiple-output (MU-MIMO). Specifically, Alice 0 and 1 generate multiple spatially distinguishable beams and send them to multiple Bobs, respectively. At each Bob, each two beams (signal components) originating from the two Alices can be combined to produce the desired signal. This way, the proposed method can be applied to the scenarios involving multiple Bobs. As for the scenarios involving multiple eavesdroppers, our principle of utilizing two signal components for distributed transmission allows for the precise construction of the desired signal at the intended receiver while introducing mutual interference at the eavesdropper, making it readily applicable in such scenarios.

Although we applied DDM to prevent eavesdropping, it can also be extended to other application scenarios. For example, by substituting one Tx in DDM with a cooperative interference source, we can encode the desired information in terms of the interference at the other Tx, achieving both interference and eavesdropping immunization [27] or enhancing the desired transmission through interference utilization [18], as in our previous studies. Therefore, the proposed DDM has the potential for extension and can effectively improve wireless communications. In future, we plan to explore these further.

References

[1] 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.

[2] Z. Zhang, D. Guo, B. Zhang, and J. Yuan, "Research on physical layer security technology of multi-antenna system," in *Proc. IEEE Int. Conf. Electron. Instrum. Inf. Syst.*, 2017, pp. 1–4.

[3] K. Zeng, "Physical layer key generation in wireless networks: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 33–39, Jun. 2015.

[4] 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.

[5] T. Wang, Y. Liu, and J. Ligatti, "Fingerprinting far proximity from radio emissions," in *Proc. Eur. Symp. Res. Comput. Secur.*, 2014, pp. 508–525.

[6] Y. Tung, S. Han, D. Chen, and K. Shin, "Vulnerability and protection of channel state information in multiuser MIMO networks," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2014, pp. 775–786.

[7] H. Liu, Y. Wang, Y. Ren, and Y. Chen, "Bipartite graph matching based secret key generation," in *Proc. IEEE Conf. Comput. Commun.*, 2021, pp. 1–10.

[8] J. Liu, Q. Hu, R. Suny, X. Du, and M. Guizani, "A physical layer security scheme with compressed sensing in OFDM-based IoT systems," in *Proc. IEEE Int. Conf. Commun.*, 2020, pp. 1–6.

[9] S. Liu, Y. Hong, and E. Viterbo, "Practical secrecy using artificial noise," *IEEE Commun. Lett.*, vol. 17, no. 7, pp. 1483–1486, Jul. 2013.

[10] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[11] 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, Aug. 2016.

[12] N. Zhao, Y. Cao, F. R. Yu, Y. Chen, M. Jin, and V. C. M. Leung, "Artificial noise assisted secure interference networks with wireless power transfer," *IEEE Trans. Veh. Technol.*, vol. 67, no. 2, pp. 1087–1098, Feb. 2018.

[13] D. Hu, P. Mu, W. Zhang, and W. Wang, "Minimization of secrecy outage probability with artificial-noise-aided beamforming for MISO wiretap channels," *IEEE Commun. Lett.*, vol. 24, no. 2, pp. 401–404, Feb. 2020.

[14] L. Hu, J. Peng, Y. Zhang, H. Wen, S. Tan, and J. Fan, "Artificial noise assisted interference alignment for physical layer security enhancement," in *Proc. IEEE Glob. Commun. Conf.*, 2022, pp. 4148–4153.

[15] L. Zhang et al., "The performance of the MIMO physical layer security system with imperfect CSI," in *Proc. IEEE Conf. Commun. Netw. Secur.*, 2016, pp. 346–347.

[16] J. Liu, Z. Liu, Y. Zeng, and J. Ma, "Cooperative jammer placement for physical layer security enhancement," *IEEE Netw.*, vol. 30, no. 6, pp. 56–61, Nov./Dec. 2016.

[17] Z. Liu, J. Liu, N. Kato, J. Ma, and Q. Huang, "Divide-and-conquer based cooperative jamming: Addressing multiple eavesdroppers in close proximity," in *Proc. IEEE Int. Conf. Comput. Commun.*, 2016, pp. 1–9.

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

[19] C. Fan, *Principles of Communications*, 2nd ed. Beijing, China: Electron. Ind. Press, 2015.

[20] Z. Li, J. Chen, L. Zhen, S. Cui, K. G. Shin, and J. Liu, "Coordinated multipoint transmissions based on interference alignment and neutralization," *IEEE Trans. Wireless Commun.*, vol. 18, no. 7, pp. 3347–3365, Jul. 2019.

[21] D. C. Chen, T. Q. S. Quek, and M. Kountouris, "Backhauling in heterogeneous cellular networks: Modeling and tradeoffs," *IEEE Trans. Wireless Commun.*, vol. 14, no. 6, pp. 3194–3206, Jun. 2015.

[22] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 2, pp. 256–266, Jun. 2011.

[23] S. Ruffini, M. Johansson, B. Pohlman, and M. Sandgren, "5G synchronization requirements and solutions," *Ericsson Technol. Rev.*, vol. 2021, no. 1, pp. 2–13, Jan. 2021.

[24] "MathWorks: QPSK Receiver with USRP hardware in simulink - MATLAB & simulink example," 2022. [Online]. Available: https://ww2.mathworks.cn/help/supportpkg/usrpradio/ug/qpsk-receiver-with-usrp-hardware-in-simulink.html?s_tid=srchtitle_USRP%20QPSK_3

[25] *Enhancements for Higher Throughput*, IEEE Standard 802.11n-2009, Institute of Electrical and Electronics Engineers, Piscataway, NJ, USA, 2009. [Online]. Available: http://www.ieee802.org

[26] Z. Li, Y. Liu, , K. G. Shin, J. Li, F. Guo, and J. Liu, "Design and adaptation of multi-interference steering," *IEEE Trans. Wireless Commun.*, vol. 18, no. 7, pp. 3329–3346, Jul. 2019.

[27] 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.

Zhao Li (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 with the School of Cyber Engineering, Xidian University. He was a visiting scholar and then research scientist with the Real-Time Computing Laboratory, Department of Electrical Engineering and Computer Science, The University of Michigan, during 2013–2015. He also visited the Department of Information and Communications Engineering, Aalto University, during 2022–2023. He has authored or coauthored more than 50 technical papers at premium international journals and conferences, such as *IEEE Transactions on Mobile Computing*, *IEEE Transactions on Wireless Communications*, IEEE INFOCOM, *IEEE Internet of Things Journal*, *IEEE Transactions on Vehicular Technology*, and *Computer Communications*. His research interests include wireless communication, 5G communication systems, resource allocation, interference management, IoT, and physical layer security.

Siwei Le is currently working toward the master's degree with the School of Cyber Engineering, Xidian University. His research interests include physical layer security and network simulation.

Jie Chen is currently working toward the master's degree with the School of Telecommunications Engineering, Xidian University. Her research interests include wireless communication, physical layer security, and interference management.

Kang G. Shin (Life Fellow, IEEE) received the BS degree in electronics engineering from Seoul National University, Seoul, South Korea, in 1970, and the MS and the PhD degrees in electrical engineering from Cornell University, Ithaca, New York, in 1976 and 1978, respectively. He is currently the kevin and nancy o'connor professor of computer science and the founding director of the Real-Time Computing Laboratory, Department of Electrical Engineering and Computer Science, The University of Michigan, Ann Arbor, MI, USA. At The University of Michigan, he has supervised the completion of 92 PhDs and also chaired the Computer Science and Engineering Division for four years starting in 1991. From 1978 to 1982, he was on the faculty of the Rensselaer Polytechnic Institute, Troy, NY, USA. He has authored or coauthored more than 1,000 technical articles (more than 360 of which are published in archival journals) and more than 60 patents or invention disclosures. His research interests include QoS-sensitive computing and networks and embedded real-time and cyber-physical systems. He was the recipient of numerous institutional awards and best paper awards. He is a Fellow of ACM.

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 authored or coauthored more than 70 academic papers at premium international journals and conferences, such as *IEEE Transactions on Dependable and Secure Computing*, *IEEE Transactions on Mobile Computing*, *IEEE Transactions on Information Forensics and Security*, and IEEE INFOCOM. His research interests include wireless systems security, space-air-ground integrated networks, Internet of Things, and 6G. He was the recipient of the IEEE Sapporo Section Encouragement Award in 2016 and 2020.

Zheng Yan (Fellow, IEEE) received the BEng degree in electrical engineering and the MEng degree in computer science and engineering from the Xi'an Jiaotong University, Xi'an, China, in 1994 and 1997, respectively, the second MEng degree in information security from the National University of Singapore, Singapore, in 2000, and the Licentiate of Science degree and the Doctor of Science degree in technology and electrical engineering from the Helsinki University of Technology, Helsinki, Finland, in 2005 and 2007, respectively. She is currently a professor with Xidian University, Xi'an, China, and a visiting professor with Aalto University, Espoo, Finland. She has authored more than 150 peer reviewed publications and solely authored two books. She is the inventor and co-inventor of more than 50 patents and PCT patent applications. Her research interests include trust, security and privacy, social networking, cloud computing, networking systems, and data mining. Prof. Yan is an associate editor for *Information Sciences*, *Information Fusion*, *IEEE Internet of Things Journal*, *IEEE Access Journal*, *Journal of Network and Computer Applications*, and *Security and Communication Networks*. She is a leading guest editor of many reputable journals, including ACM TOMM, FGCS, *IEEE Systems Journal*, and MONET. She was a steering, organization and program committee member of more than 70 international conferences.

Riku Jäntti (Senior Member, IEEE) received the MSc degree (Hons.) in electrical engineering and the DSc degree (Hons.) in automation and systems technology from the Helsinki University of Technology (TKK) in 1997 and 2001, respectively. He is currently a full professor of communications engineering and the head of the Department of Communications and Networking, School of Electrical Engineering, Aalto University, Finland. Prior to joining Aalto (formerly known as TKK) in 2006, he was a professor pro tem with the Department of Computer Science, University of Vaasa. His research interests include machine type communications, disaggregated radio access networks, backscatter communications, quantum communications, and radio frequency inference. He is a member of the Editorial Board of the *IEEE Transactions on Cognitive Communications and Networking*. He is a IEEE VTS Distinguished Lecturer (Class 2016).