Decomposed and Distributed Modulation to Achieve Secure Transmission

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

***Abstract*—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). `DDM-Sec` realizes traditional QPSK modulation by using 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 received signal while preventing the eavesdropper from accessing the legitimate user's information. `DDM-Sec` can effectively exploit the randomness of wireless channels to encrypt data transmission, enrich the spatial signatures of the legitimate transmission by employing two cooperative Txs. Moreover, `DDM-Sec` distributes user's information to two transmissions so that none of the decomposed signals alone carry the legitimate user's full information. Our theoretical analysis, hardware experiment, 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*—Physical-layer security, modulation, distributed transmission, secrecy capacity**

I. Introduction

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]. There exist security vulnerabilities in all levels of TCP/IP protocol stack, of which physical-layer security plays a fundamental role in improving information secrecy. Recently, a variety of physical-layer security techniques [2–8] have been developed, which can effectively improve communication secrecy and protect the user's information from eavesdropping. The basic principles of realizing physical-layer security can be grouped into two types: 1) implementation of encryption based on the characteristics (also known as the *fingerprint*) of a wireless channel 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.

The first type generates and manages secret keys by exploiting the randomness and reciprocity of wireless channels [2]. Under such a scheme, a pair of legitimate Tx and Rx generates 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. In [3], a secure far proximity identification approach that can determine whether a remote device is far away or not was developed. The authors of [3] proposed a method that can extract the fingerprint of a wireless device's proximity from the physical-layer features of signals sent by the device. [4] 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 they forge CSI in the CSI feedback.

The secrecy capacity analysis methods incorporate various physical-layer security techniques such as insertion of artificial noise (AN), beamforming design, and cooperative jamming to realize information safety. In [5], the Tx ensured communication secrecy by utilizing some of its power to produce AN so as to deteriorate the eavesdropper's channel. The authors of [6] 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. The authors of [7] proposed cooperative jamming strategies to prevent eavesdroppers from obtaining user's information in the wireless network.

The above-mentioned methods rely on 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 by using a certain method. Based on this observation, we propose a novel secure physical-layer transmission scheme based on *decomposed and distributed modulation (DDM)*, namely `DDM-Sec`. `DDM-Sec` exploits the randomness of wireless channels to encrypt data transmission, and enrich the spatial features by employing distributed Txs. The physical foundation of `DDM-Sec` is the utilization of the interactions among multiple

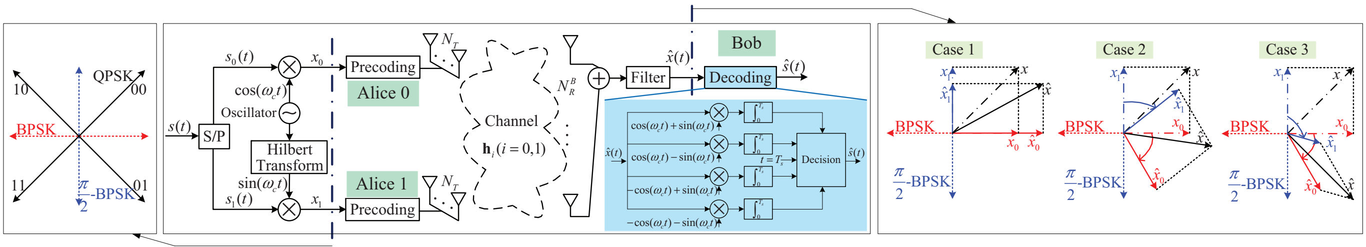
This work is supported in part by the National Natural Science Foundation of China (62072351), the Key Research Project of Shaanxi Natural Science Foundation (2023-JC-ZD-35), JSPS KAKENHI Grant Number JP23K16877, the Project of Cyber Security Establishment with Inter-University Cooperation, the Academy of Finland (345072, 350464), the 111 Project (B16037), and the Shaanxi Key Research & Development project (2023-YBGY-210), the open research project of ZheJiang Lab (2021PD0AB01).

Z. Li, S. Le, J. Chen, and Z. Yan are with the School of Cyber Engineering, Xidian University, Xi'an, China.

K. G. Shin is with the Department of Electrical Engineering and Computer Science, the University of Michigan, Ann Arbor, USA.

R. Jäntti is with the Department of Communications and Networking, Aalto University, Espoo, Finland.

J. Liu is with the Center for Strategic Cyber Resilience Research and Development, National Institute of Informatics, Tokyo, Japan.



(a) Tx-side constellation

(b) Block diagram of DDM-Sec

(c) Rx-side constellation

Fig. 2. Realization and principle of DDM-Sec.

concurrent wireless signals [8]. In our scheme, we first decompose a QPSK modulation 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 distributed 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, which is expensive or even impossible in practice, thus the secrecy of legitimate transmission is guaranteed.

In 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 $\mathbf{X}$. $\|\cdot\|$ and $|\cdot|$ indicate the Euclidean norm and the absolute value, respectively.

II. System Model

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

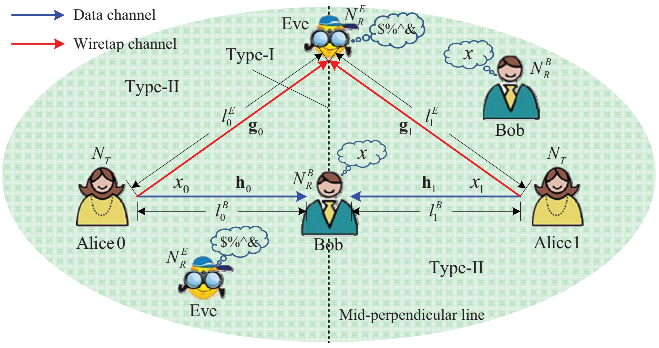


Fig. 1. System model.

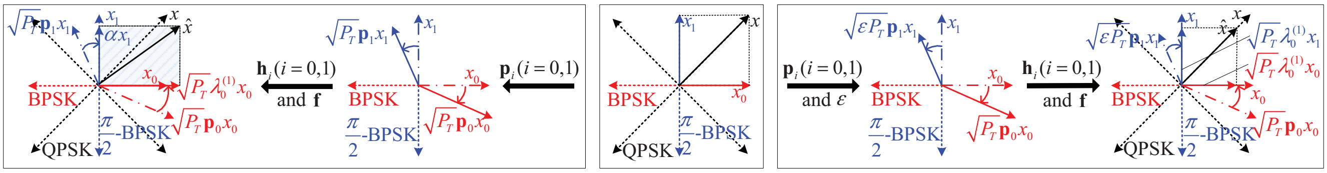
We use $\mathbf{h}_i \in \mathbb{C}^{N_R^B \times N_T}$ $(i \in \{0,1\})$ to denote the channel matrix from Alice i to Bob, while the channel matrix from Alice i to Eve is denoted by $\mathbf{g}_i \in \mathbb{C}^{N_R^E \times N_T}$. We adopt a spatially uncorrelated [4] Rayleigh flat fading channel to 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 and feed it back to the two Alices via a low-rate 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 $\delta_t^B = |l_1^B - l_0^B|/c$ and $\delta_t^E = |l_1^E - l_0^E|/c$, respectively. We use x to denote a QPSK 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.

III. Design of DDM-Sec

We take QPSK as an example to show the realization of DDM-Sec as plotted in Fig. 2. The input bipolar data sequence is denoted as $s(t)$. 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 $x_1(t) = s_1(t)\sin(\omega_c t)$. 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. In the DDM-Sec, $x_0(t)$ and $x_1(t)$ are precoded and transmitted by two collaborated Txs. These two transmissions arrive at Bob through various wireless channels. Bob receives a mixed signal, and then post-processes it to obtain $\hat{x}(t)$. In the end, we employ the maximum likelihood (ML) detection so that the data information $\hat{s}(t)$ is recovered from $\hat{x}(t)$.

In what follows, we will detail the distributed implementation of QPSK using two collaborative Txs. For clarity of exposition and without ambiguity, we omit the time index t in the following discussion. Without loss of generality, we assume Alice 0 employs BPSK and Alice 1 adopts BPSK



$\sqrt{P_T}\mathbf{p}_1x_1$
x_1
αx_1
x
$\hat{x}$
x_0
$\sqrt{P_T}\lambda_0^{(1)}x_0$
BPSK
$\frac{\pi}{2}$-BPSK
QPSK
$\sqrt{P_T}\mathbf{p}_0x_0$
$\mathbf{h}_i(i=0,1)$ and $\mathbf{f}$
$\mathbf{p}_i(i=0,1)$
$\mathbf{p}_i(i=0,1)$ and ε
$\sqrt{\varepsilon P_T}\mathbf{p}_1x_1$
$\sqrt{P_T}\lambda_0^{(1)}x_1$

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

Fig. 3. An illustration of Pw/oPC and Pw/PC based DDM-Sec .

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 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:

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

where $\mathbf{z}$ represents for the additive white Gaussian noise (AWGN) vector whose elements have zero-mean and variance σ_n^2. Note that what we are interested is the overall effect of the two signal terms on the right-hand side of Eq. (1), not the individual components.

Note that x_i ($i \in \{0,1\}$) 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. 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 $\rho_i = 1$. As $\mathbf{h}_0$ and $\mathbf{h}_1$ are random and independent from each other, $\hat{x}$ will be an attenuated QPSK symbol/waveform. Fig. 2(c) shows three typical attenuation cases. We can see that the estimated $\hat{x}$ 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 well-shaped QPSK waveform from which Rx recovers its desired information.

Next, we will first present the Pw/oPC based DDM-Sec under QPSK, and then discuss the Pw/PC based DDM-Sec suitable for more general modulation schemes. We take the singular value decomposition (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 $\mathbf{p}_0 = \mathbf{v}_0^{(1)}$ as the precoder at Alice 0 (design of $\mathbf{p}_1$ will be elaborated later) and $\mathbf{f} = \mathbf{u}_0^{(1)}$ as the filter at Bob. $\mathbf{v}_i^{(1)}$ 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:

$$\hat{x} = \sqrt{P_T}[\mathbf{u}_0^{(1)}]^H\mathbf{h}_1\mathbf{p}_1x_1 + \sqrt{P_T}\lambda_0^{(1)}x_0 + [\mathbf{u}_0^{(1)}]^H\mathbf{z}. \qquad (2)$$

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

To obtain a correct QPSK symbol via the combination of the two signals from Alice 0 and 1, Eq. (3) should hold.

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

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 Eq. (3), $\mathbf{p}_1$ can be obtained as:

$$\mathbf{p}_1 = \{[\mathbf{u}_0^{(1)}]^H\mathbf{h}_1\}^\dagger/\|\{[\mathbf{u}_0^{(1)}]^H\mathbf{h}_1\}^\dagger\|. \qquad (4)$$

So, the estimated signal at Bob becomes:

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

Fig. 3 illustrates the basic principle of Pw/oPC and Pw/PC based DDM-Sec. In subfigure (b), a QPSK symbol x is decomposed into two BPSK symbols, i.e., x_0 and x_1. The leftmost subplot of subfigure (a) shows Pw/oPC based DDM-Sec, 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 Fig. 3(a), although the combined $\hat{x}$ is away from the desired QPSK symbol x, according to the ML criterion, Bob can still correctly recover $\hat{s}$ from $\hat{x}$.

As for Pw/PC based DDM-Sec, we employ a power control factor, ε_1, at Alice 1, to make the following equation hold.

$$\sqrt{\varepsilon_1 P_T}[\mathbf{u}_0^{(1)}]^H\mathbf{h}_1\mathbf{p}_1 = \sqrt{P_T}\lambda_0^{(1)}. \qquad (6)$$

Then, Alice 1 can calculate $\mathbf{p}_1$ according to Eq. (4) and compute ε_1 in terms of Eq. (6), respectively, while Alice 0 and Bob perform signal processing in the same way as they do in Pw/oPC based DDM-Sec. Fig. 3(c) illustrates Pw/PC based DDM-Sec. The rightmost subplot of Fig. 3(c) plots the post-processed signals at Bob. Since we have properly designed $\mathbf{p}_1$ and ε_1, 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.

Based on the design of DDM-Sec, one can see that no extra processing is imposed on Bob. That is, DDM-Sec is transparent to the Rx. Moreover, DDM-Sec doesn't incur any additional power cost (compared to, e.g., AN-based method, etc). These characteristics can facilitate its application.

IV. Performance Analysis of DDM-Sec

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-Sec's performance.

A. Calculation of Secrecy Capacity

In the wiretap channel, 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 the Shannon capacity of the eavesdropper's channel, $\mathcal{C}_E$, from Bob's capacity, $\mathcal{C}_B$, as:

$$\mathcal{C}_S = \max_{P(x)} \{\mathcal{C}_B - \mathcal{C}_E, 0\}. \tag{7}$$

$\mathcal{C}_E$ 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 $P(x, \hat{x})$, the maximum average mutual information can be computed as:

$$\mathcal{C}_E = \max_{P(x)} \sum_{x \in X} \sum_{\hat{x} \in \hat{X}} P(x, \hat{x}) \log_2 \{P(x, \hat{x})/[P(x)P(\hat{x})]\} \tag{8}$$

where X and $\hat{X}$ denote the transmit and receive symbol sets, respectively, $x \in X$ and $\hat{x} \in \hat{X}$. Note that Eq. (8) can also be used for calculating $\mathcal{C}_B$.

B. The Impact of Large- and Small-scale Fading on DDM-Sec

In DDM−Sec, the reception performance of both legitimate Rx and eavesdropper is sensitive to the delay/phase difference of two signal components. Such a difference also affects the physical-layer security of DDM−Sec. 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 difference incurred by LSF, it depends on the propagation paths' length difference of two signals, while the phase difference yielded by SSF results from the difference between $\mathbf{h}_0$ and $\mathbf{h}_1$. We take the Rx employing coherent detection as an example, and for simplicity omit the noise term in the derivation. Recall that the modulated symbols x_0 and x_1 can be represented as signals $x_0 = s_0 \cos(\omega_c t)$ and $x_1 = s_1 \sin(\omega_c t)$, we can rewrite Eq. (1) as:

$$\hat{x} = \sqrt{P_T} \mathbf{f}^H \{\mathbf{h}_1 \mathbf{p}_1 s_1 \sin(\omega_c t) + \mathbf{h}_0 \mathbf{p}_0 s_0 \cos[\omega_c (t + t_\triangle)]\} \tag{9}$$

where $t_\triangle$ denotes the delay difference incurred by LSF.

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 estimated base-band signals $\hat{x}_0$ and $\hat{x}_1$ as:

$$\hat{x}_0 = \{\sqrt{P_T} \mathbf{f}^H \mathbf{h}_0 \mathbf{p}_0 s_0 \cos(\omega_c t_\triangle)\}/2, \tag{10}$$

$$\hat{x}_1 = \{\sqrt{P_T} \mathbf{f}^H \mathbf{h}_1 \mathbf{p}_1 s_1 [1 - \sin(\omega_c t_\triangle)]\}/2. \tag{11}$$

The coordinates of the base-band data obtained by the Rx can be expressed by $(\hat{x}_0, \hat{x}_1)$ in a constellation map. So, we can 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 $\hat{s}$. Due to LSF and SSF, $(\hat{x}_0, \hat{x}_1)$ deviates from the original desired data point x (see in Fig. 3(b)) whose coordinates are (s_0, s_1). Such deviation will affect Rx's reception accuracy. In Eqs. (10) and (11), the SSF, indicated by $\frac{1}{2}\sqrt{P_T} \mathbf{f}^H \mathbf{h}_0 \mathbf{p}_0$ and $\frac{1}{2}\sqrt{P_T} \mathbf{f}^H \mathbf{h}_1 \mathbf{p}_1$, 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 $\cos(\omega_c t_\triangle)$ and $1 - \sin(\omega_c t_\triangle)$. When $\omega_c t_\triangle \neq 2k\pi$ where $k \in \mathbb{Z}$ and $\mathbb{Z}$ denotes integer set, $(\hat{x}_0, \hat{x}_1)$ is different from (s_0, s_1).

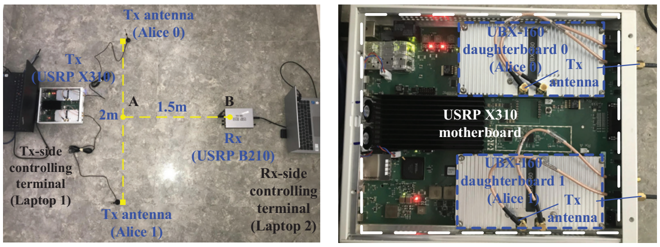
For the phase difference incurred by SSF, we can use the methods proposed in Section III to design $\mathbf{p}_0$ and $\mathbf{p}_1$ based on CSI estimation, so as to let $\sqrt{P_T} \mathbf{f}^H \mathbf{h}_0 \mathbf{p}_0 = \sqrt{P_T} \mathbf{f}^H \mathbf{h}_1 \mathbf{p}_1$ hold. As for $t_\triangle$ 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 $t_\triangle = 0$, then we can have $\cos(\omega_c t_\triangle) = 1 - \sin(\omega_c t_\triangle) = 1$. It should be noticed that when $\omega_c t_\triangle = 2k\pi$ $(k \neq 0)$, although $\cos(\omega_c t_\triangle) = 1 - \sin(\omega_c t_\triangle) = 1$ can hold, there is still a non-zero $t_\triangle$ in integer multiples of carrier periods. When $t_\triangle < T_s$ 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 in partial errors in the superimposed QPSK waveform for that symbol period and incorrect demodulation. When $t_\triangle > T_s$, 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 should make $t_\triangle$ as close to 0 as possible.

V. Evaluation

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

A. Hardware Implementation of DDM-Sec

We employ a USRP X310 equipped with two UBX-160 radio frequency (RF) daughterboards as the Txs, and a USRP B210 as the Rx, to implement DDM−Sec. For simplicity, we let the two UBX-160 daughterboards and B210 be equipped with a single antenna. As Fig. 4(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 acts as the legitimate Rx (i.e., Bob) to detect the received mixed signal. The X310 connects to a terminal (laptop 1), which controls the two RF daughterboards to realize the BPSK modulations, and further transmit the modulated signals. The B210 is connected to another terminal (laptop 2), which controls the signal detection and data demodulation.



(a) Experimental setup

(b) Internal structure of USRP X310

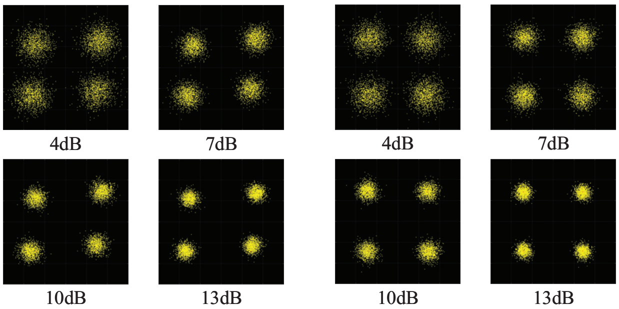
Fig. 4. Hardware implementation of DDM−Sec.

In the experiment, all devices are deployed in a 3m×3m plane. The two transmit antennas are approximately 2m apart,

TABLE I
PARAMETER SETTINGS OF DDM-Sec.

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]

and the Rx (point B) is located on the perpendicular bisector (i.e., AB) of the line connecting the transmit antennas, approximately 1.5m away from point A. The main parameters used in the experiment are shown in Table I. According to the experimental setup shown in Fig. 4(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 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. Fig. 4(b) shows the two UBX-160 daughterboards installed on an X310 motherboard, which provides a unified clock reference to the dautherboards for generating carrier signals of the same frequency. The synchronization between the B210 and the X310 is realized by laptop 2 controlling the B210 to implement processing such as phase-locked loop (PLL)-based fine frequency compensation, etc [9].


4dB 7dB 4dB 7dB
10dB 13dB 10dB 13dB

(a) DDM-Sec (b) CM

Fig. 5. Comparison of QPSK constellations at Bob under DDM-Sec and CM.

Fig. 5 compares the QPSK constellations of the demodulated data at the legitimate Rx with DDM-Sec and conventional centralized modulation (CM) under various transmit gains. With CM, a single Tx (implemented by a UBX-160 daughterboard) employs QPSK modulation to transmit, while Bob (implemented by a B210 device) adopts QPSK demodulation to decode the data. We can see from Fig. 5 that with the increase of the transmit gain, both DDM-Sec and CM can output more concentrated and clearer QPSK constellation points at Bob. Given the same transmit gain, there is a minor distortion between the constellations of DDM-Sec and CM. This is because the received QPSK waveform under DDM-Sec is obtained by superimposing two BPSK signals over the air interface at the Rx, and the experimental setup shown in Fig. 4(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. 5 that legitimate transmission using DDM-Sec can achieve comparable performance to that with CM.

B. MATLAB Simulation of DDM-Sec

We now use MATLAB simulations to evaluate the proposed scheme's performance. We will show Bob's capacity and Eve's eavesdropping performance under symbol rate $R_s = 1.2 \times 10^8$Baud and carrier frequency 2.4GHz [10]. In this simulation, both Alice 0 and 1 are equipped with $N_T = 2$ antennas, while Bob and Eve have a single antenna.

In what follows, we will simulate Bob and Eve's capacity as well as secrecy capacity under the proposed DDM-Sec and conventional CM, respectively. As for Eve, a delay difference of $0.3T_s$ exists and full inter-symbol interference (ISI[1]) 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-Sec, the ratio of transmit power at each Alice to noise power, i.e., $\gamma_{DDM-Sec} = \lg(P_T/\sigma_n^2)$, is set to be from 0dB to 20dB. For fairness, the ratio of transmit power at Alice 0 to noise power under CM, i.e., $\gamma_{CM} = \lg(2P_T/\sigma_n^2)$, varies from 3dB to 23dB. We will study two typical adversary models, denoted as I and II, respectively, in evaluating Eve's capacity and the secrecy capacity. Under adversary model I, 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 II, 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 I as *medium* while under model II as *strong*. As for model II, 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:

$$\hat{\mathbf{h}}_i = \eta \mathbf{h}_i + \sqrt{1-\eta^2}\,\mathbf{\Xi} \tag{12}$$

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 $\mathbf{\Xi}$ is an $N_R^B \times N_T$ diagonal complex Gaussian matrix with zero mean and unit variance. In the following evaluation, we will adopt $\eta \in \{0.7, 0.9, 1\}$.

Fig. 6 shows Bob's capacity with DDM-Sec and CM, respectively, where a dual x-axis is used. Specifically, under the total transmit power constraint, $\gamma_{CM} = \gamma_{DDM-Sec} + 3$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-Sec) under various adversary models is identical. As the figure shows, given low $\gamma_{DDM-Sec}(\gamma_{CM})$, DDM-Sec yields smaller $\mathcal{C}_B$ than CM. This is because although Pw/PC based DDM-Sec can output a well-shaped QPSK waveform, a de-

[1] When there is non-zero $t_\triangle$ but insufficient guard interval between adjacent symbols, a symbol of one signal component will interfere with both its prior and subsequent symbols of the other component. We call this full ISI.

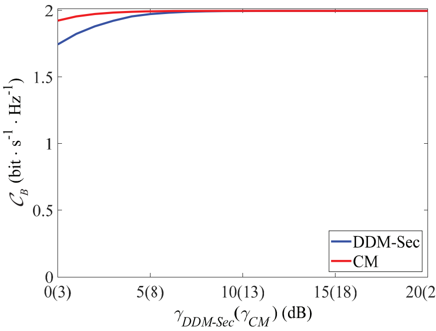


Fig. 6. Bob's capacity under DDM−Sec and CM.

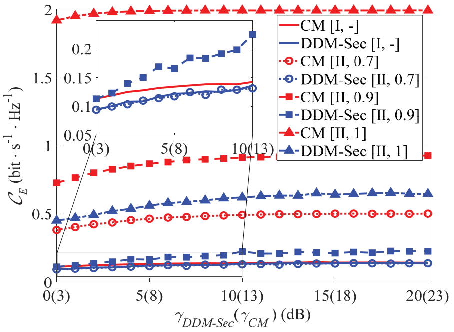


Fig. 7. Eve's capacity under DDM−Sec and CM.

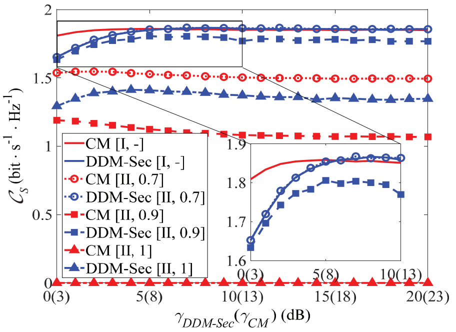


Fig. 8. Secrecy capacity under DDM−Sec and CM.

sired signal power loss may occur (see in Fig. 3(c)), thus impairing DDM−Sec's $\mathcal{C}_B$. Under low $\gamma_{DDM-Sec}(\gamma_{CM})$, noise dominates Bob's capacity, yielding $\mathcal{C}_B$ of DDM−Sec inferior to that of CM. As $\gamma_{DDM-Sec}(\gamma_{CM})$ grows, the influence of noise decreases, incurring $\mathcal{C}_B$ of both schemes increases and approaches 2bps/Hz[2]. Therefore, the capacity is upper bounded by 2bps/Hz.

Fig. 7 shows Eve's capacity of DDM−Sec and CM under various adversary models and ηs. For simplicity, we employ the vector $[\mathcal{M}, \eta]$ where $\mathcal{M} \in \{\mathrm{I}, \mathrm{II}\}$ 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 $\mathcal{M} = \mathrm{I}$. Under adversary model I, Eve only knows $\mathbf{g}_i$, due to the exploitation of channel randomness (CM and DDM−Sec) and delay difference (DDM−Sec), both DDM−Sec and CM yield very low $\mathcal{C}_E$. In the case of adversary model II, Eve acquires $\mathbf{g}_i$ and estimates $\mathbf{h}_i$ with accuracy coefficient η. Due to the enhanced capability of eavesdropper, $\mathcal{C}_E$ of CM under adversary model II is clearly improved over that under model I. 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, $\mathcal{C}_E$ grows with an increase of η under model II. Furthermore, $\mathcal{C}_E$ of CM under $\eta = 1$ equals $\mathcal{C}_B$ of CM in Fig. 6, 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−Sec, both channel randomness (under $\eta < 1$) and delay difference are exploited for secure transmission, so $\mathcal{C}_E$ of DDM−Sec under model II is slightly improved over that under model I. Moreover, given the same η, DDM−Sec's $\mathcal{C}_E$ is much lower than CM's under model II. Although $\mathcal{C}_E$ increases as η grows under model II, $\mathcal{C}_E$ of DDM−Sec with $\eta = 1$ is still inferior to that of CM under $\eta = 0.9$. That is, DDM−Sec exhibits good secrecy performance when the eavesdropper's capability is strong.

Fig. 8 plots the secrecy capacity of DDM−Sec and CM under various adversary models and ηs. As the figure shows, $\mathcal{C}_S$ of CM is higher than that of DDM with small $\gamma_{DDM-Sec}(\gamma_{CM})$ under adversary model I. As $\gamma_{DDM-Sec}(\gamma_{CM})$ grows, the influence of noise decreases, incurring $\mathcal{C}_S$ of DDM−Sec approaches that of CM in a high $\gamma_{DDM-Sec}(\gamma_{CM})$ region under adversary model I. In the case of model II, $\mathcal{C}_S$ of CM decreases with an increase of η, while $\mathcal{C}_S$ of DDM−Sec decreases slightly compared to that under model I.

VI. Conclusion

In this paper, we have proposed a novel physical-layer secure transmission scheme, called DDM−Sec. We have shown that traditional QPSK modulation can be realized by two cooperative Txs, each generating a BPSK signal — and the two BPSK components are orthogonal to each other, in a distributed manner. The legitimate Rx can then decode the desired information from the mixed received signal. Our theoretical analysis, hardware experiment, 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.

References

[1] Y. Zou, J. Zhu, X. Wang, et al., "A Survey on Wireless Security: Technical Challenges, Recent Advances and Future Trends," Proceedings of the IEEE, vol. 104, no. 9, pp. 1727-1765, 2016.

[2] K. Zeng, "Physical Layer Key Generation in Wireless Networks: Challenges and Opportunities," IEEE Commun. Mag., vol. 53, no. 6, pp. 33-39, 2015.

[3] T. Wang, Y. Liu, and J. Ligatti, "Fingerprinting Far Proximity From Radio Emissions," in Proc. of European Symp. on Research in Computer Security (ESORICS), pp. 508-525, 2014.

[4] Y. Tung, S. Han, D. Chen, et al., "Vulnerability and Protection of Channel State Information in Multiuser MIMO Networks," in Proc. of ACM SIGSAC Conf. Comput. & Commun. Security (CCS), pp. 775-786, 2014.

[5] S. Goel and R. Negi, "Guaranteeing Secrecy using Artificial Noise," IEEE Trans. Wireless Commun., vol. 7, no. 6, pp. 2180-2189, 2008.

[6] N. Zhao, F. R. Yu, M. Li, et al., "Anti-Eavesdropping Schemes for Interference Alignment (IA)-Based Wireless Networks," IEEE Trans. Wireless Commun., vol. 15, no. 8, pp. 5719-5732, 2016.

[7] J. Liu, Z. Liu, Y. Zeng, et al., "Cooperative Jammer Placement for Physical Layer Security Enhancement," IEEE Network, vol. 30, no. 6, pp. 56-61, 2016.

[8] Z. Li, J. Chen, K. G. Shin, et al., "Interference Recycling: Exploiting Interfering Signals to Enhance Data Transmission," in Proc. of IEEE Intl. Conf. Computer Commun. (INFOCOM), pp. 100-108, 2019.

[9] MathWorks: QPSK Receiver with USRP™ Hardware in Simulink - MATLAB & Simulink Example, https://ww2.mathworks.cn/help/supportpkg/usrpradio/ug/qpsk-receiver-with-usrp-hardware-in-simulink.html?s_tid=srchtitle_USRP%20QPSK_3, 2022.

[10] IEEE Std. 802.11n-2009: Enhancements for Higher Throughput, http://www.ieee802.org, 2009.

[2] Since a QPSK modulated signal is decomposed into two BPSK signal components, each of them carries 1-bit information per symbol. Moreover, according to the Nyquist Criterion, 2Baud/Hz is the highest possible unit bandwidth symbol rate, which is also called the *Nyquist rate*.