iCoding: Countermeasure Against Interference and Eavesdropping in Wireless Communications

Zhao Li
School of Cyber Engineering
Xidian University
Xi'an, China
zli@xidian.edu.cn

Yanyan Zhu
School of Cyber Engineering
Xidian University
Xi'an, China
zyy970616@163.com

Kang G. Shin
Dept. of Electrical Engineering and Computer Science
The University of Michigan
Ann Arbor, USA
kgshin@umich.edu

***Abstract*—With the rapid development of wireless communication technologies, interference management (IM) and security/privacy in data transmission have become critically important. On one hand, due to the broadcast nature of wireless medium, the interference superimposed on the desired signal can destroy the integrity of data transmission. On the other hand, malicious receivers (Rxs) may eavesdrop a legitimate user's transmission and thus breach the confidentiality of communication. To counter these threats, we propose a novel encoding method, called *immunizing coding* (iCoding), which handles both IM and physical-layer security simultaneously. By exploiting both channel state information (CSI) and data carried in the interference, an iCoded signal is generated and sent by the legitimate transmitter (Tx). The iCoded signal interacts with the interference at the desired/legitimate Rx, so that the intended data can be recovered without the influence of disturbance, i.e., immunity to interference is achieved. In addition, since the data carried in the iCoded signal which is obtained via encoding the desired data and interference cooperatively, is different from the original desired data, the eavesdropper cannot access legitimate information by wiretapping the desired signal. Therefore, immunity to eavesdropping is achieved. Our theoretical analysis and in-depth simulation have shown iCoding to effectively manage interference while preventing potential eavesdropping, hence enhancing the legitimate user's data transmission and secrecy thereof.**

***Index Terms*—interference, secure communication, coding, interference management, channel capacity, spectral efficiency**

I. INTRODUCTION

Due to the broadcast nature of wireless channels, wirelessly transmitted signals overlap with each other [1], risking the integrity and confidentiality of wireless transmissions compared to wired communication [2]. On one hand, interference is superimposed on the desired signal at the intended receiver (Rx), impeding the recovery of the user's data and hence risking the integrity of communication [3]. On the other hand, owing to the broadcast nature of wireless medium, eavesdroppers within the coverage area of the legitimate transmission can hear and decode the signal to get the transmitted information, thus risking the confidentiality of communication. To mitigate/counter the above-mentioned threats, techniques such as interference management (IM) [4-9], secure communication (SC) [10-13], and mechanisms incorporating both together [14,15] have been proposed and receiving an increasing attention in recent years.

There have been numerous IM methods, including zero-forcing beamforming (ZFBF) [4], ZF reception [5] and interference alignment (IA) [6], which exploit channel state information (CSI); physical-layer network coding (PNC) [7], which utilizes the information carried in the interfering signal; and interference neutralization (IN) [8] and interference steering (IS) [9], which exploit both CSI and data of the interference. Aiming to defend against the breach of confidentiality from potential eavesdroppers in wireless communication systems, traditional SC addresses the security at upper layers of the protocol stack by using secret keys. With the increasing compute power of eavesdroppers, the effectiveness of traditional SC is facing a great challenge, yielding physical-layer security technologies, such as key encryption [10], artificial noise (AN) [11], cooperative jamming (CJ) [12] and beamforming (BF) [13], receiving widespread attention in recent years.

The above-mentioned IM and SC schemes are designed to address the risk of interference or eavesdropping. In practice, however, both risks may exist simultaneously. Therefore, it is important to design a comprehensive solution by integrating countermeasures of both IM and eavesdropping together. In [14], an IA-aided SC method was proposed. It lets the legitimate Tx send AN, so as to disrupt ZF-reception-based eavesdropping. However, this scheme degrades legitimate data rate and cannot guarantee security when the eavesdropper is equipped with multiple antennas. The authors of [15] combined IA with CJ, in which AN is generated not only by the legitimate destination, but also the legitimate source and relay, thus degrading eavesdroppers' signal-to-interference-plus-noise ratio (SINR) severely. By carefully designing the precoding matrices, interferences from different Txs can be aligned within the same subspace at the legitimate destination, but not aligned at the eavesdroppers due to the randomness of wireless channels. However, this method incurs high cooperation overhead. Based on the above descriptions, to the best of our knowledge, the existing integration of IM and eavesdropping prevention [14,15] always eliminates the risks of interference and eavesdropping separately via two independent operations, i.e., no real integration is available.

To mitigate/overcome the above-mentioned deficiencies of existing schemes, we propose a novel scheme, called *immunizing coding* (iCoding), to achieve IM and SC in one operation. With this scheme, the original desired data is encoded at the legitimate Tx based on CSI and data information carried in the interference; the encoded data (i.e., iCoded data) is then sent to the desired/legitimate Rx. On one hand, the iCoded data is different from the original data, hence achieving the confidentiality of communication. On the other hand, the iCoded data interacts with interference at the legitimate Rx, so that the impact of interference on the desired transmission can be eliminated. In the design of iCoding, we present an 8-shaped mapping rule to meet the power constraint at the legitimate Tx. According to this rule, the iCoded data symbols to be sent can be confined to the original standard constellation map.

Throughout this paper, we use the following notations. The set of complex numbers is denoted as $\mathbb{C}$, while vectors and matrices are represented by bold lower-case and upper-case letters, respectively. Let $\mathbf{X}^H$ be the Hermitian of matrix $\mathbf{X}$. $\|\cdot\|$ represents the Euclidean norm. $\mathbb{E}(\cdot)$ denotes statistical expectation. $\mathrm{Re}(\cdot)$ and $\mathrm{Im}(\cdot)$ represent taking the real and imaginary part of a complex number.

II. System Model

We consider downlink transmission in heterogeneous cellular networks (HCNs) composed of overlapping macro and pico cells. As Fig. 1 shows, both macro BS (MBS_1) and pico BS (PBS_0) are equipped with N_{T_1} and N_{T_0} antennas, while macro user equipment (MUE_1) and pico user equipment (PUE_0) have N_{R_1} and N_{R_0} antennas, respectively. The eavesdropper (PUE_e) located in the coverage of pico-cell is equipped with N_{R_e} antennas. Let P_{T_1} and P_{T_0} denote the transmit power of MBS_1 and PBS_0, respectively. Let $\mathbf{H}_0 \in \mathbb{C}^{N_{R_0}\times N_{T_0}}$, $\mathbf{H}_1 \in \mathbb{C}^{N_{R_1}\times N_{T_1}}$, and $\mathbf{H}_{0e} \in \mathbb{C}^{N_{R_e}\times N_{T_0}}$ be the channel matrices from PBS_0 to PUE_0, MBS_1 to MUE_1, and PBS_0 to PUE_e, while CSI from MBS_1 to PUE_0 and PUE_e are denoted as $\mathbf{H}_{10} \in \mathbb{C}^{N_{R_0}\times N_{T_1}}$ and $\mathbf{H}_{1e} \in \mathbb{C}^{N_{R_e}\times N_{T_1}}$, respectively. We assume PBS_0 operates in an open mode [16], i.e., users in the coverage of PBS_0 can access it, so that users' traffic can be offloaded from a heavily-loaded macro-cell to a pico-cell. Therefore, PUE_e may act as a legitimate user of PBS_0 to eavesdrop on the information transmitted from PBS_0 to PUE_0. Since PUE_0 and PUE_e are usually not at the same location, $\mathbf{H}_0$ and $\mathbf{H}_{0e}$ are statistically independent of each other [17]. We adopt a spatially uncorrelated Rayleigh flat fading channel to model the elements of the above channel matrices as independent and identically distributed (i.i.d.) zero-mean unit-variance complex Gaussian random variables. We assume that all Rxs experience block fading, i.e., channel parameters remain constant in a block consisting of several successive time slots and vary randomly between successive blocks. MUE_1 and PUE_0 can accurately estimate CSI from MBS_1 and PBS_0 to them, respectively, and feed it back to their associated BS via a low-rate, error-free link (e.g., X2 interface [18]). We assume reliable links for the delivery of CSI and signaling. The delivery delay is negligible relative to the time scale at which the channel state varies.

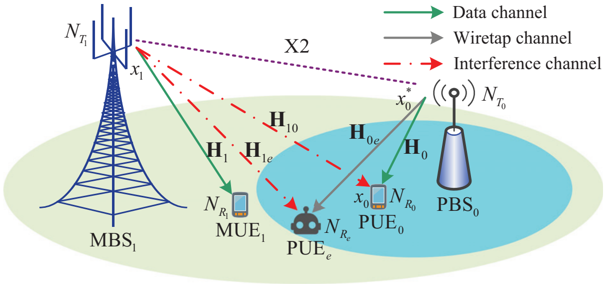


Fig. 1. System model.

We let $\mathbf{x}_1$ and $\mathbf{x}_0$ denote the desired data vectors from MBS_1 and PBS_0 to their serving subscribers. $\mathbb{E}(\|\mathbf{x}_1\|^2) = \mathbb{E}(\|\mathbf{x}_0\|^2) = 1$ holds. For clarity of presentation, we assume both macro- and pico-transmissions employ beamforming (BF), i.e., only one data stream is sent from MBS_1 to MUE_1, and PBS_0 to PUE_0, respectively. Then, $\mathbf{x}_1$ and $\mathbf{x}_0$ become scalars x_1 and x_0. According to Fig. 1, transmission from MBS_1 to MUE_1 interferes with that from PBS_0 to PUE_0. Nevertheless, due to the limited coverage of pico-cell, PBS_0 will not cause too much interference to MUE_1, and thus the disturbance from PBS_0 to MUE_1 will be omitted in the rest of this paper. Since pico-cells are deployed to improve the capacity and coverage of existing cellular systems, each pico-cell, unlike the macro-cell, has subordinate features, and hence the transmission in the macro-cell is given priority over that in the pico-cell. Specifically, MBS_1 will not adjust its transmission for the pico-users. However, we assume that PBS_0 can acquire the information of x_1 via inter-BS collaboration; this assumption is easy to be met because PBS_0 and MBS_1 are deployed by the same operator [19]. With the above CSI and data information, iCoded data x_0^* can be generated at, and sent by PBS_0. Since the transmission from MBS_1 to MUE_1 only depends on $\mathbf{H}_1$ and is free from interference, we mainly focus on the pico user's transmission performance (including its secure capacity).

III. Design of Immunizing Coding

The received signal at PUE_0 is expressed as:

$$\mathbf{y}_0 = \sqrt{P_{T_0}}\mathbf{H}_0\mathbf{p}_0 x_0^* + \sqrt{P_{T_1}}\mathbf{H}_{10}\mathbf{p}_1 x_1 + \mathbf{z}_0 \quad (1)$$

where $\mathbf{p}_0$ represents the precoding vector for the iCoded data x_0^* at PBS_0 and $\mathbf{p}_1$ is the precoder for the interfering data x_1 at MBS_1. The first term on the right-hand side (RHS) of Eq. (1) denotes the iCoded signal sent from PBS_0 and the second term is the interference from MBS_1. $\mathbf{z}_0$ denotes the additive white Gaussian noise (AWGN) vector whose elements have zero-mean and variance σ_n^2. Note that in Eq. (1), PBS_0 sends an iCoded signal (carrying x_0^*) instead of its desired signal (carrying data x_0).

PUE_0 employs filter vector $\mathbf{w}_0$ to obtain the estimated signal $\hat{\mathrm{s}}_0$ as:

$$\hat{\mathrm{s}}_0 = \sqrt{P_{T_0}}\mathbf{w}_0^H\mathbf{H}_0\mathbf{p}_0 x_0^* + \sqrt{P_{T_1}}\mathbf{w}_0^H\mathbf{H}_{10}\mathbf{p}_1 x_1 + \mathbf{w}_0^H\mathbf{z}_0. \quad (2)$$

We adopt the singular value decomposition (SVD) based precoding and receive filtering as an example, i.e., we apply SVD to $\mathbf{H}_0$ to obtain $\mathbf{H}_0 = \mathbf{U}_0\mathbf{\Lambda}_0\mathbf{V}_0^H$. Then, we employ $\mathbf{p}_0 = \mathbf{v}_0^{(1)}$ and $\mathbf{w}_0 = \mathbf{u}_0^{(1)}$ at PBS$_0$ and PUE$_0$, respectively, where $\mathbf{v}_0^{(1)}$ and $\mathbf{u}_0^{(1)}$ represent the first column vectors of the right and left singular matrices $\mathbf{V}_0$ and $\mathbf{U}_0$. $\mathbf{\Lambda}_0$ is a diagonal matrix whose main diagonal elements are non-zero singular values of $\mathbf{H}_0$, denoting the amplitude gain of spatial sub-channels determined by $\mathbf{V}_0$ and $\mathbf{U}_0$ cooperatively. In practice, there are other signal processing options which can be used for designing $\mathbf{p}_0$ and $\mathbf{w}_0$.

Let the iCoded data x_0^* be determined by the original desired data x_0 and x_c where x_c indicates virtual immunizing data. Then, Eq. (3) can be obtained as:

$$x_0^* = x_0 + x_c. \tag{3}$$

Substituting $\mathbf{p}_0 = \mathbf{v}_0^{(1)}$, $\mathbf{w}_0 = \mathbf{u}_0^{(1)}$ and Eq. (3) into Eq. (2), we have:

$$\begin{aligned}\hat{\mathbf{s}}_0 = \sqrt{P_{T_0}}\lambda_0^{(1)}x_0 + \sqrt{P_{T_0}}\lambda_0^{(1)}x_c + \sqrt{P_{T_1}}[\mathbf{u}_0^{(1)}]^H\mathbf{H}_{10}\mathbf{p}_1 x_1 \\ + [\mathbf{u}_0^{(1)}]^H\mathbf{z}_0\end{aligned} \tag{4}$$

where $\lambda_0^{(1)}$ is the largest singular value of $\mathbf{H}_0$, indicating the amplitude gain of the principal eigenmode (i.e., spatial sub-channel) of $\mathbf{H}_0$. The first term on the RHS of Eq. (4) contains PUE$_0$'s desired data x_0 and the second term has the immunizing data x_c.

For accurate recovery of the desired data x_0 at PUE$_0$, the second and third terms on the RHS of Eq. (4) must satisfy:

$$\sqrt{P_{T_0}}\lambda_0^{(1)}x_c + \sqrt{P_{T_1}}[\mathbf{u}_0^{(1)}]^H\mathbf{H}_{10}\mathbf{p}_1 x_1 = 0. \tag{5}$$

From Eq. (5) we can get Eq. (6) as:

$$x_c = -\sqrt{P_{T_1}/P_{T_0}}[\lambda_0^{(1)}]^{-1}[\mathbf{u}_0^{(1)}]^H\mathbf{H}_{10}\mathbf{p}_1 x_1. \tag{6}$$

Note that in Eq. (6) x_c is related to the interfering data x_1, but not to x_0. By substituting Eq. (6) into Eq. (4), we can get:

$$\hat{\mathbf{s}}_0 = \sqrt{P_{T_0}}\lambda_0^{(1)}x_0 + [\mathbf{u}_0^{(1)}]^H\mathbf{z}_0. \tag{7}$$

Therefore, according to Eq. (7), the interference is eliminated, thus leaving only the desired signal and noise. Based on the above analysis, the average spectral efficiency (SE) of PUE$_0$ can be calculated as:

$$\mathbb{E}(r_0) = \mathbb{E}\left\{\log_2\left\{1 + P_{T_0}[\lambda_0^{(1)}]^2/\sigma_n^2\right\}\right\} \tag{8}$$

where σ_n^2 denotes the noise power.

For clarity of presentation, we take square-16QAM (Quadrature Amplitude Modulation) as an example to illustrate the basic principle of iCoding, as shown in Fig. 2. We denote the desired signal component as $\mathbf{s}_0 = \sqrt{P_{T_0}}\lambda_0^{(1)}x_0$, the immunizing signal as $\mathbf{s}_c = \sqrt{P_{T_0}}\lambda_0^{(1)}x_c$, the received signal component from PBS$_0$ as $\tilde{\mathbf{s}}_0^* = \sqrt{P_{T_0}}\lambda_0^{(1)}x_0^*$, and the interference from MBS$_1$ as $\mathbf{s}_1 = \sqrt{P_{T_1}}[\mathbf{u}_0^{(1)}]^H\mathbf{H}_{10}\mathbf{p}_1 x_1$, respectively. Then, the estimated/filtered signal in Eq. (4) (ignoring noise) can be rewritten as $\hat{\mathbf{s}}_0 = \tilde{\mathbf{s}}_0^* + \mathbf{s}_1$. Similarly, the iCoded signal sent by PBS$_0$ is expressed as $\mathbf{s}_0^* = \sqrt{P_{T_0}}\mathbf{p}_0 x_0^*$. According to Eqs. (2)–(4), we define operator $\mathcal{J}(\cdot)$ to represent extraction of the effective portion of a signal component, i.e., equivalent data symbol carried in the signal. By applying $\mathcal{J}(\cdot)$ to various signals, the inter-signal relationship can be mapped into the constellation map and represented by inter-equivalent-symbol relationship. It should be noted that $\mathcal{J}(\cdot)$ may involve different signal processing for various signal components. Specifically, we define the operators at PBS$_0$ and PUE$_0$ as $\mathcal{J}_T(\cdot) = 1/\sqrt{P_{T_0}}\mathbf{p}_0$ and $\mathcal{J}_R(\cdot) = 1/\sqrt{P_{T_0}}\lambda_0^{(1)}$, respectively. Then, we can have $\mathcal{J}_T(\mathbf{s}_0^*) = x_0^*$, $\mathcal{J}_R(\mathbf{s}_0) = x_0$, $\mathcal{J}_R(\mathbf{s}_c) = x_c$, $\mathcal{J}_R(\tilde{\mathbf{s}}_0^*) = x_0^*$ and $\mathcal{J}_R(\hat{\mathbf{s}}_0) = x_0$. As for $\mathcal{J}_R(\mathbf{s}_1)$, it should be noticed that $\mathcal{J}_R(\mathbf{s}_1) = \frac{\mathbf{s}_1}{\sqrt{P_{T_0}}\lambda_0^{(1)}} = \frac{\sqrt{P_{T_1}}[\mathbf{u}_0^{(1)}]^H\mathbf{H}_{10}\mathbf{p}_1}{\sqrt{P_{T_0}}\lambda_0^{(1)}}x_1$, i.e., $\mathcal{J}_R(\mathbf{s}_1) \neq x_1$. Based on the above discussion, we can use a two-dimensional vector to express the equivalent data symbol carried in a signal in the constellation map, the vector starts at the origin and ends at the constellation point corresponding to the equivalent data symbol.

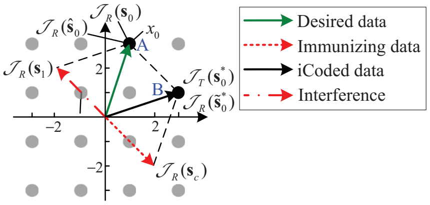

$\mathcal{J}_R(\mathbf{s}_0)$
$\mathcal{J}_R(\hat{\mathbf{s}}_0)$
x_0
A
$\mathcal{J}_R(\mathbf{s}_1)$
2
$\mathcal{J}_T(\mathbf{s}_0^*)$
B
$\mathcal{J}_R(\tilde{\mathbf{s}}_0^*)$
−2
2
−2
$\mathcal{J}_R(\mathbf{s}_c)$
Desired data
Immunizing data
iCoded data
Interference

Fig. 2. Illustration of the basic principle of iCoding.

As Fig. 2 shows, PBS$_0$ first calculates the immunizing data x_c ($\mathcal{J}_R(\mathbf{s}_c)$) according to interference $\mathbf{s}_1$ in terms of Eq. (6), and then encodes the original desired data x_0 (point A in Fig. 2) with x_c to obtain the iCoded data x_0^* ($\mathcal{J}_T(\mathbf{s}_0^*)$, point B). Next, PBS$_0$ sends the iCoded signal $\mathbf{s}_0^*$ to PUE$_0$. Likewise, PUE$_0$ applies $\mathbf{w}_0 = \mathbf{u}_0^{(1)}$ to the received mixed signal $\mathbf{y}_0$ and extracts the estimated data symbol, denoted as $\mathcal{J}_R(\hat{\mathbf{s}}_0)$, from the post-processed signal $\hat{\mathbf{s}}_0$. $\mathcal{J}_R(\hat{\mathbf{s}}_0) = \mathcal{J}_R(\tilde{\mathbf{s}}_0^* + \mathbf{s}_1)$ holds. According to Eq. (7), $\mathcal{J}_R(\hat{\mathbf{s}}_0)$ is the same as $\mathcal{J}_R(\mathbf{s}_0)$ (point A), i.e., PUE$_0$ can accurately recover original desired data x_0 from $\tilde{\mathbf{s}}_0^* + \mathbf{s}_1$. Based on the above discussion, iCoding can mitigate the interference $\mathbf{s}_1$ at PUE$_0$, hence realizing immunity to interference. Moreover, since $\mathcal{J}_T(\mathbf{s}_0^*) \neq x_0$, PUE$_e$'s eavesdropping on x_0 is crippled.

IV. Constellation Extension and 8-Shaped Mapping

A. Constellation Extension

Due to the randomness of interference, the iCoded data x_0^* may be out of the range of the original constellation map. In such a case, if x_0^* is directly sent, PBS$_0$'s power range needs to be extended; this will not only incur more transmit power consumption, but also increase PBS$_0$'s hardware cost. In what follows, we will first present the constellation extension so that the iCoded symbol exceeding the original constellation can be represented.

Next, we take square-MQAM where M represents for the modulation order, as an example to illustrate the principle of

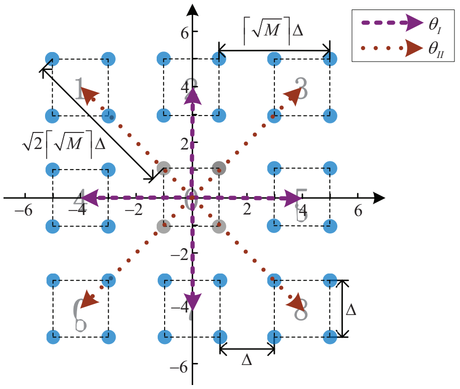


Fig. 3. Illustration of constellation extension.

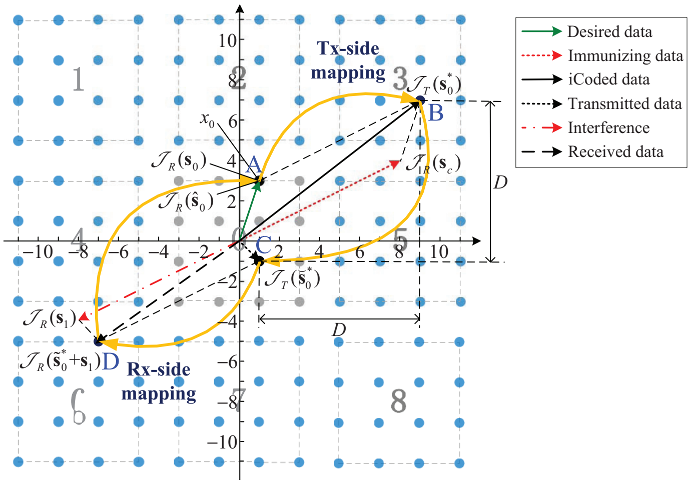
constellation extension. It should be noted that other types of modulation are also applicable. Fig. 3 plots the extension of square-4QAM. As the figure shows, we index the original constellation map with 0, then we duplicate the original constellation along four directions determined by phase angle $\theta_I \in \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$. The center of the duplicated constellation is $\lceil\sqrt{M}\rceil\Delta$ away from the origin (i.e., the center of original constellation). Δ represents the horizontal (or vertical) distance between two adjacent constellation points. The notation $\lceil\cdot\rceil$ denotes rounding up to the nearest integer. We can thus obtain the first-stage duplicated constellation map by adding four constellations indexed with 5, 2, 4 and 7, respectively, to 0. Next, we copy the original constellation along the other four directions determined by $\theta_{II} \in \{\frac{\pi}{4}, \frac{3\pi}{4}, \frac{5\pi}{4}, \frac{7\pi}{4}\}$. The center of the duplicated constellation is $\sqrt{2}\lceil\sqrt{M}\rceil\Delta$ away from the origin. Then, four constellations indexed with 3, 1, 6 and 8 are added to the first-stage duplicated constellation map, so that we can get the second-stage duplicated constellation. We refer the whole of the original constellation and the duplicated 8 constellations as the 1^{st} round extended constellation.

Note, in practice, that the iCoded symbol may still be out of the range of the 1^{st} round extended constellation. In such a case, we can get the k^{th} round extended constellation by duplicating the $(k-1)^{th}$ round extended constellation distancing $3^{k-1}\lceil\sqrt{M}\rceil\Delta$ and $3^{k-1}\sqrt{2}\lceil\sqrt{M}\rceil\Delta$ from the origin along the directions determined by θ_I and θ_{II}, respectively.

B. 8-Shaped Mapping

Based on the above discussion, the iCoded data can be represented by the constellation point in the extended constellation map. However, direct transmission of such an extended symbol requires a high dynamic range of transmit power at the Tx, incurring an increase of equipment's complexity and cost. To solve this problem, we propose an 8-shaped mapping rule which is applied to the Tx and Rx, respectively. For simplicity, we consider the case of iCoded symbol coinciding with standard constellation point.

Fig. 4 shows the realization of iCoding in the 1^{st} round extended square-16QAM constellation where the 8-shaped mapping rule is applied. At the Tx-side, PBS$_0$ calculates x_c ($\mathcal{J}_R(\mathbf{s}_c)$) according to $\mathbf{s}_1$ and then encodes x_0 (point A in Fig. 4) with it so as to obtain x_0^*. When x_0^* ($\mathcal{J}_T(\mathbf{s}_0^*)$, point B)



Desired data
Immunizing data
iCoded data
Transmitted data
Interference
Received data
Tx-side mapping
Rx-side mapping
1
2
3
4
5
6
7
8
$\mathcal{J}_T(\mathbf{s}_0^*)$
B
A
C
D
x_0
$\mathcal{J}_R(\mathbf{s}_0)$
$\mathcal{J}_R(\hat{\mathbf{s}}_0)$
$\mathcal{J}_R(\mathbf{s}_c)$
$\mathcal{J}_T(\breve{\mathbf{s}}_0^*)$
$\mathcal{J}_R(\mathbf{s}_1)$
$\mathcal{J}_R(\tilde{\mathbf{s}}_0^*+\mathbf{s}_1)$
D
D
10
8
6
4
2
−2
−4
−6
−8
−10
−10
−8
−6
−4
−2
2
4
6
8
10

Fig. 4. Realization of iCoding in extended constellation and with 8-shaped mapping rule.

exceeds the range of original constellation, $\mathcal{J}_T(\mathbf{s}_0^*)$ is mapped back to $\breve{x}_0^*$ ($\mathcal{J}_T(\breve{\mathbf{s}}_0^*)$, point C), $\breve{\mathbf{s}}_0^*$ is the actual transmitted signal of PBS$_0$. $\mathcal{J}_T(\mathbf{s}_0^*) = \breve{x}_0^*$ indicates removing $\sqrt{P_{T_0}}\mathbf{p}_0$ in the expression of $\breve{\mathbf{s}}_0^*$. As Fig. 4 shows, the relative position of $\mathcal{J}_T(\breve{\mathbf{s}}_0^*)$ in constellation 0 is the same as that of $\mathcal{J}_T(\mathbf{s}_0^*)$ in constellation 3. In this way, an arbitrary iCoded symbol can be limited to the range of original constellation. Then, $\mathcal{J}_T(\breve{\mathbf{s}}_0^*)$ is sent by PBS$_0$.

Noting that an arbitrary symbol can be represented by its amplitude (ρ) and phase (ϕ), an iCoded data x_0^* can be expressed as $x_0^* = \rho_0^* e^{j\phi_0^*}$. Then, we can get $\mathrm{Re}(x_0^*) = \rho_0^* \cos\phi_0^*$ and $\mathrm{Im}(x_0^*) = \rho_0^* \sin\phi_0^*$. So, the 8-shaped mapping rule can be expressed as:

$$\begin{cases} \mathrm{Re}(\breve{x}_0^*) = \rho_0^* \cos\phi_0^* - D\mathrm{Rd}\left(\frac{\rho_0^* \cos\phi_0^*}{D}\right) \\ \mathrm{Im}(\breve{x}_0^*) = \rho_0^* \sin\phi_0^* - D\mathrm{Rd}\left(\frac{\rho_0^* \sin\phi_0^*}{D}\right) \end{cases} \tag{9}$$

where $\mathrm{Rd}(\cdot)$ denotes the rounding-off operation. D is the horizontal mapping distance between $\mathcal{J}_T(\mathbf{s}_0^*)$ (point B) and $\mathcal{J}_T(\breve{\mathbf{s}}_0^*)$ (point C). $D = 3^{k-1}\lceil\sqrt{M}\rceil\Delta$ holds. Consider Fig. 4 as an example, in which $k = 1$, $M = 16$ and $\Delta = 2$, so that we can get $D = 8$. We use $\mathcal{R}_8(\cdot)$ to denote the 8-shaped mapping operation, by substituting $D = 8$, $\mathrm{Re}(x_0^*) = 9$ and $\mathrm{Im}(x_0^*) = 7$ into Eq. (9), we can see that $\mathcal{R}_8(x_0^*) = \breve{x}_0^*$ holds.

At the Rx-side, PUE$_0$ extracts $\mathcal{J}_R(\tilde{\mathbf{s}}_0^* + \mathbf{s}_1)$ (point D) from the post-processed mixed signal $\tilde{\mathbf{s}}_0^* + \mathbf{s}_1$, and then inversely maps $\mathcal{J}_R(\tilde{\mathbf{s}}_0^* + \mathbf{s}_1)$ to obtain the estimated data $\mathcal{J}_R(\hat{\mathbf{s}}_0)$ in the original constellation. As the figure shows, $\mathcal{J}_R(\hat{\mathbf{s}}_0) = \mathcal{J}_R(\mathbf{s}_0) = x_0$ holds; that is, x_0 is accurately decoded. The expression of inverse mapping rule at PUE$_0$ is the same as that at PBS$_0$, we only need to substitute the amplitude and phase of $\mathcal{J}_R(\tilde{\mathbf{s}}_0^* + \mathbf{s}_1)$ instead of ρ_0^* and ϕ_0^*, into Eq. (9).

In Fig. 4, we use yellow arrowed arcs to depict the 8-shaped mapping at PBS$_0$ and PUE$_0$. Specifically, start from x_0 (point A) to $\mathcal{J}_T(\mathbf{s}_0^*)$ (point B) via arc $\overset{\frown}{\mathrm{AB}}$; next, along $\overset{\frown}{\mathrm{BC}}$ to $\mathcal{J}_T(\breve{\mathbf{s}}_0^*) = x_0^*$ (point C); and then, from point C via $\overset{\frown}{\mathrm{CD}}$ to $\mathcal{J}_R(\tilde{\mathbf{s}}_0^* + \mathbf{s}_1)$ (point D); finally, along $\overset{\frown}{\mathrm{DA}}$ to $\mathcal{J}_R(\hat{\mathbf{s}}_0)$ (point

A). Since the shape of $\widehat{ABCDA}$ is similar to that of number 8, we call the proposed mapping rule as 8-shaped mapping.

V. Evaluation

We now evaluate the performance of iCoding using MATLAB simulation. We employ channel capacity to demonstrate the efficiency and secrecy of the proposed method. According to information theory, channel capacity of PUE$_0$ and PUE$_e$, denoted as c_0 and c_e, respectively, are the maximum amount of mutual information that can be achieved in the communications from PBS$_0$ to them. Besides iCoding, we also simulate some other typical methods, including IS, IN, ZF reception, point-to-point multiple-input multiple-output (p2pMIMO) and non-interference management (non-IM) (i.e., the PUE$_0$ employs matched filtering (MF) to decode its desired data while leaving the interference un-managed) for comparison.

We set $N_{T_i} = N_{R_i} = N_{R_e} = 2$ where $i \in \{0, 1\}$ and assume SVD based precoding and receive filtering is employed. We let both MBS$_1$ and PBS$_0$ adopt square-16QAM to generate 10^3 symbols i.e., x_1 and x_0, in each sample. We obtain the simulation results by averaging over 5×10^4 samples. We can obtain the marginal distribution functions of x_0 as $p(x_0)$ at PBS$_0$ and the estimated $\hat{x}_0$ as $p(\hat{x}_0)$ at PUE$_0$, as well as their joint distribution function $p(x_0, \hat{x}_0)$, respectively, so that c_0 can be calculated as:

$$\begin{aligned} c_0 &= \max_{p(x_0)} \{I(X_0; \hat{X}_0)\} \\ &= \max_{p(x_0)} \left\{ \sum_{x_0 \in X} \sum_{\hat{x}_0 \in \hat{X}_0} p(x_0, \hat{x}_0) \log_2 \frac{p(x_0, \hat{x}_0)}{p(x_0) p(\hat{x}_0)} \right\} \end{aligned} \tag{10}$$

where X and $\hat{X}_0$ denote the symbol sets at PBS$_0$ and PUE$_0$, respectively, $x_0 \in X_0$ and $\hat{x}_0 \in \hat{X}_0$ hold, $I(X_0; \hat{X}_0)$ represents the average mutual information. Similarly, PUE$_e$'s eavesdropping capacity c_e is computed as $c_e = \max I(X_0; \hat{X}_e)$ where $\hat{X}_e$ is the estimated symbol set at PUE$_e$.

We use $\bar{P}_{T_1}$ and $\bar{P}_{T_0}$ to denote the effective power of received signals sent from MBS$_1$ and PBS$_0$, at PUE$_0$ [8]. Then, we define the transmit power of MBS$_1$ and PBS$_0$ normalized by noise power as $\zeta_1 = 10 \lg \frac{\bar{P}_{T_1}}{\sigma_n^2}$ and $\zeta_0 = 10 \lg \frac{\bar{P}_{T_0}}{\sigma_n^2}$, respectively. We also use η to denote the ratio of $\bar{P}_{T_1}$ to $\bar{P}_{T_0}$, i.e., $\eta = \frac{\bar{P}_{T_1}}{\bar{P}_{T_0}}$. We set $\eta \in [0.1, 5]$ in the simulation.

Fig. 5 shows the variation of c_0 and c_e along with η under different ζ_0s. As the figure shows, since PUE$_e$ is subject to the interference from MBS$_1$ whereas PUE$_0$ is free from interference due to the use of iCoding, clearly c_0 outperforms c_e. When $\zeta_0 = 10$dB, c_0 can be as high as 4bit/symbol, i.e., reaching the upper bound of the channel capacity of 16QAM-based transmission [20]. In addition, given fixed ζ_0, c_0 is independent of η; while under medium to high η, c_e is independent of η. This is because SINR at PUE$_0$ and PUE$_e$ can be expressed as $\gamma_0 = \frac{\bar{P}_{T_0}}{\sigma_n^2} = 10^{0.1\zeta_0}$ and $\gamma_e = \frac{\bar{P}_{T_0}}{\bar{P}_{T_1} + \sigma_n^2} = \frac{1}{\eta + 10^{-0.1\zeta_0}}$, respectively. Then, we can see from the expression of γ_0 that c_0 is independent of η and increases as ζ_0 grows. As for c_e, we can see that when η is quite small, ζ_0 dominates both γ_e and c_e, and c_e slightly increases as ζ_0 grows; while as η grows larger, η becomes dominant compared to $10^{-0.1\zeta_0}$ in calculating γ_e, so that c_e becomes less dependent on the variation of ζ_0. Moreover, since iCoding can realize immunity-to-eavesdropping (IoE), PUE$_e$'s eavesdropping is further destroyed, incurring c_e as low as 0.25bit/symbol, i.e., the lower bound of the channel capacity of 16QAM-based transmission. Under very small η, the probability that IoE is lost is inegligible, yielding a slightly better c_e than 0.25bit/symbol.

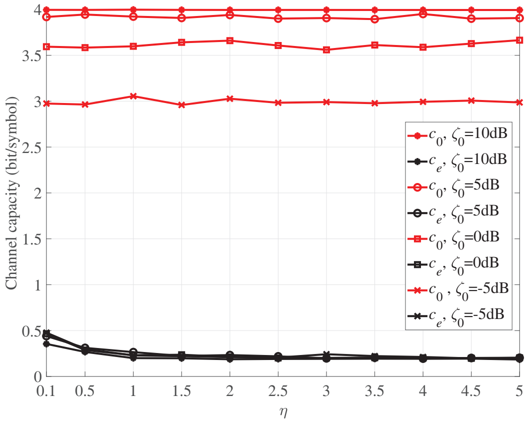


Fig. 5. Variation of c_0 and c_e vs. η under different ζ_0s.

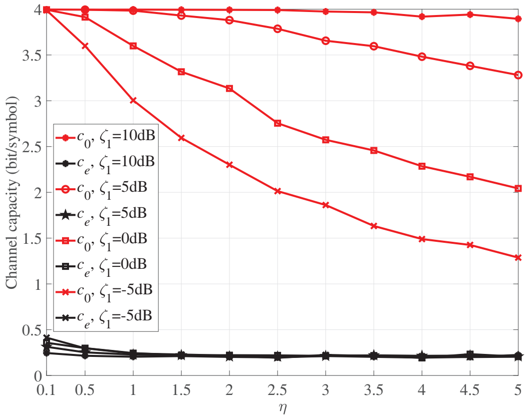


Fig. 6. Variation of c_0 and c_e vs. η under different ζ_1s.

Fig. 6 plots the variation of c_0 and c_e along with η under different ζ_1s. Given fixed ζ_1, c_0 is shown to decrease as η grows; while for c_e, it decreases with an increase of η when η is low and becomes invariant under medium to high η. This is because SINR at PUE$_0$ and PUE$_e$ can be computed as $\gamma_0 = \frac{\bar{P}_{T_0}}{\sigma_n^2} = \frac{10^{0.1\zeta_0}}{\eta}$ and $\gamma_e = \frac{\bar{P}_{T_0}}{\bar{P}_{T_1} + \sigma_n^2} = \frac{1}{\eta(1 + 10^{-0.1\zeta_1})}$, respectively. Then, one can see from the expression of γ_0 that c_0 is in inverse proportional to η, so that γ_0 and c_0 reduce as η grows. Given fixed η, since higher ζ_1 yields larger $10^{0.1\zeta_1}$, c_0 enhances as ζ_1 grows. As for c_e, it decreases as ζ_1 grows under fixed and small η. This is because when η is quite small, η can dominate and yield a large γ_e, making c_e slightly better than 0.25bit/symbol; while as η grows larger, γ_e degenerates obviously, incurring c_e being as small as 0.25bit/symbol.

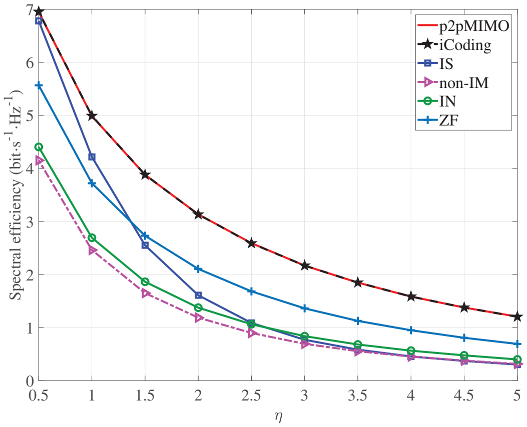


Fig. 7. PUE$_0$'s average SE vs. η with various IM schemes under $\zeta_1 = 10$dB.

Fig. 7 plots the variation of PUE$_0$'s average SE along with η under $\zeta_1 = 10$dB and different IM schemes. Given fixed ζ_1, $\bar{P}_{T_0}$ decreases as η grows, hence decreasing PUE$_0$'s SE. Since both iCoding and p2pMIMO realize interference-free data reception at PUE$_0$, they can achieve the highest SE. Under $\zeta_1 = 10$dB, the strength of interference is relatively stronger than that of the noise. So, IM can contribute more to PUE$_0$'s SE, yielding SE of IS, IN and ZF reception higher than that of non-IM. When η is small, IS outperforms ZF. This is because ZF reception incurs more desired signal's power loss while nullifying interference at PUE$_0$; whereas for IS, only the effective portion of interference imposing on the desired transmission of PUE$_0$ is mitigated, thus decreasing IM cost and preserving the performance of intended transmission. As η grows larger, $\bar{P}_{T_1}$ becomes strong relative to $\bar{P}_{T_0}$, thus ZF can mitigate more interference with the same desired signal's power loss, whereas for IS, more transmit power at PBS$_0$ is consumed for generating the steering signal. Hence, ZF outperforms IS as η increases. Compared to IS, iCoding does not incur transmit power cost at PBS$_0$, thus outperforming IS in PUE$_0$'s SE. Compared to ZF reception, iCoding does not incur any desired signal's power loss, and hence yielding higher SE.

VI. Conclusion

In this paper, we proposed a novel method, called *immunizing coding* (iCoding), to achieve IM and physical-layer security simultaneously. By exploiting both CSI and data information carried in the interference, an iCoded signal is generated and sent by the legitimate/desired Tx. Such a signal interacts with the interference at the intended Rx and can mitigate the effect of disturbance, hence achieving interference-free desired transmission. Moreover, since the iCoded data differs from the original desired data, the eavesdropper cannot access legitimate information via wiretapping the desired signal, achieving immunity to eavesdropping. Our theoretical analysis and numerical evaulation have shown that the proposed scheme can effectively improve a legitimate user's transmission efficiency and secrecy.

Acknowledgment

This work was supported in part by NSF of Shaanxi Province under Grant 2021JM-143; the Fundamental Research Funds for the Central Universities under Grant Number JB211502; the Project of Key Laboratory of Science and Technology on Communication Network under Grant Number 6142104200412; and the U.S. National Science Foundation under Grant 1317411.

References

[1] Z. Li, J. Ding, X. Dai, et al., "Exploiting interactions among signals to decode interfering transmissions with fewer receiving antennas," Computer Commun., vol. 136, pp. 63-75, Feb. 2019.

[2] Y. Zou, Z. Jia, X. Wang, et al., "A survey on wireless security: technical challenges, recent advances, and future trends," Proc. of the IEEE, vol. 104, no. 9, pp. 1727-1765, Aug. 2016.

[3] N. Zhao, F. U. Yu, M. Li, et al., "Physical layer security issues in interference-alignment-based wireless networks," IEEE Commun. Mag., vol. 54, no.8, pp. 162-168, Aug. 2016.

[4] D. Tse and P. Viswanath, Fundamentals of Wireless Communication. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[5] T. Yoo and A. Goldsmith, "On the optimality of multiantenna broadcast scheduling using zero-forcing beamforming," IEEE J. Sel. Areas Commun., vol. 24, no. 3, pp. 528-541, Mar. 2006.

[6] V. Ntranos, M. A. Maddah-Ali, and G. Caire, "Cellular interference alignment," IEEE Trans. Inf. Theory, vol. 61, no. 3, pp. 1194-1217, Mar. 2015.

[7] S. Zhang, S. C. Liew, and P. P. Lam, "Hot topic: physical layer network coding," in *Proc. of ACM Annual Intl. Conf. Mobile Computing and Networking (MOBICOM)*, pp. 358-365, Sept. 2006.

[8] Z. Li, K. G. Shin, and L. Zhen, "When and how much to neutralize interference?" in *Proc. of IEEE Intl. Conf. Comput. Commun. (INFOCOM)*, pp. 1-9, May 2017.

[9] Z. Li, Y. Liu, K. G. Shin, et al., "Interference steering to manage interference in IoT," IEEE Internet Things J., vol. 6, no. 6, pp. 10458-10471, Dec. 2019.

[10] K. Zeng, "Physical layer key generation in wireless networks: challenges and opportunities," IEEE Commun. Mag., vol. 53, pp. 33-39, Jun. 2015.

[11] A. Mukherjee and A. L. Swindlehurst, "Fixed-rate power allocation strategies for enhanced secrecy in MIMO wiretap channels," in *Proc. IEEE Intl. Workshop on Sig. Process. Advances for Wireless Commun. (SPAWC)*, pp. 344-348, Jun. 2009.

[12] 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. of IEEE Intl. Conf. Computer Commun. (INFOCOM)*, pp. 1-9, Apr. 2016.

[13] B. Chen, C. Zhu, W. Li, et al., "Original symbol phase rotated secure transmission against powerful massive MIMO eavesdropper," IEEE Access, vol. 4, pp.3016-3025, Jun. 2016.

[14] 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, Aug. 2016.

[15] Z. Ding, M. Peng, and H. H. Chen, "A general relaying transmission protocol for MIMO secrecy communications," IEEE Trans. Commun., vol. 60, no. 11, pp. 3461-3471, Nov. 2012.

[16] T. Quek, D. Guillaume, I. Guvenc, et al., Small cell networks: Deployment, PHY technologies, and resource management, Cambridge, U.K.: Cambridge Univ. Press, 2013.

[17] Y. C. Tung, S. Han, D. Chen, and K. G. Shin, "Vulnerability and protection of channel state information in multiuser MIMO networks," in *Proc. of ACM SIGSAC Conf. Comput. & Commun. Security (CCS)*, pp. 775-786, Nov. 2014.

[18] Z. Li, S. Cui, K. G. Shin, et al., "Coordinated multi-point transmissions based on interference alignment and neutralization," in *Proc. of IEEE Intl. Conf. on Computer Commun. (INFOCOM)*, pp. 370-378, Apr. 2016.

[19] F. Pantisano, M. Bennis, W. Saad, et al., "Interference alignment for cooperative femtocell networks: a game-theoretic approach," IEEE Trans. Mobile Computing, vol. 12, no. 11, pp. 2233-2246, Nov. 2013.

[20] B. Liu, Y. Zhang, K. Wang, et al., "Performance comparison of PS star-16QAM and PS square-shaped 16QAM (square-16QAM)," IEEE Photon. J., vol. 9, no. 6, pp. 1-8, Dec. 2017.