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 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 can be sent to 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 \( X^H \) be the Hermitian of matrix \( X \). \( \| \cdot \| \) represents the Euclidean norm. \( \text{Re}(\cdot) \) and \( \text{Im}(\cdot) \) 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 \( N_{Ti} \) and \( N_{To} \) antennas, while macro user equipment (MUE\(_1\)) and pico user equipment (PUE\(_0\)) have \( N_{Rh} \) and \( N_{Ro} \) antennas, respectively. The eavesdropper (PUE\(_e\)) located in the coverage of pico-cell is equipped with \( N_{Re} \) antennas. Let \( P_{Ti} \) and \( P_{To} \) denote the transmit power of MBS\(_1\) and PBS\(_0\), respectively. Let \( H_{0} \in \mathbb{C}^{N_{Rh} \times N_{To}} \), \( H_{1} \in \mathbb{C}^{N_{Rh} \times N_{Ti}} \), and \( H_{0e} \in \mathbb{C}^{N_{Ro} \times N_{Re}} \) 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 \( H_{10} \in \mathbb{C}^{N_{Rh} \times N_{Ti}} \) and \( H_{1e} \in \mathbb{C}^{N_{Ro} \times N_{Re}} \), 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, \( H_{0} \) and \( H_{0e} \) 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.

![System model](image)

We let \( x_1 \) and \( x_0 \) denote the desired data vectors from MBS\(_1\) and PBS\(_0\) to their serving subscribers. \( \mathbb{E}(\|x_1\|^2) = \mathbb{E}(\|x_0\|^2) = 1 \) 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, \( x_1 \) and \( x_0 \) 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 \( x_0^i \) can be generated at, and sent by PBS\(_0\). Since the transmission from MBS\(_1\) to MUE\(_1\) only depends on \( H_{1} \) 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:

\[
y_0 = \sqrt{P_{T_{0}} H_{0} p_{0} x_{0}^i} + \sqrt{P_{T_{1}} H_{10} p_{1} x_{1}} + z_0
\]  

(1)

where \( p_{0} \) represents the precoding vector for the iCoded data \( x_{0}^i \) at PBS\(_0\) and \( p_{1} \) 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\(_1\). \( z_0 \) denotes the additive white Gaussian noise (AWGN) vector whose elements have zero-mean and variance \( \sigma^2_n \). Note that in Eq. (1), PBS\(_0\) sends an iCoded signal (carrying \( x_{0}^i \)) instead of its desired signal (carrying data \( x_0 \)).

PUE\(_0\) employs filter vector \( w_{0} \) to obtain the estimated signal \( \hat{x}_{0} \) as:

\[
\hat{x}_{0} = \sqrt{P_{T_{0}} w_{0}^{H} H_{0} p_{0}} x_{0}^i + \sqrt{P_{T_{1}} w_{0}^{H} H_{10} p_{1}} x_{1} + w_{0}^{H} z_0.
\]  

(2)
We adopt the singular value decomposition (SVD) based precoding and receive filtering as an example, i.e., we apply SVD to \( H_0 \) to obtain \( H_0 = U_0 \Lambda_0 V_0^H \). Then, we employ \( p_0 = v_0(1) \) and \( w_0 = u_0(1) \) at PBS0 and PUE0, respectively, where \( v_0(1) \) and \( u_0(1) \) represent the first column vectors of the right and left singular matrices \( V_0 \) and \( U_0 \). \( \Lambda_0 \) is a diagonal matrix whose main diagonal elements are non-zero singular values of \( H_0 \), denoting the amplitude gain of spatial sub-channels determined by \( V_0 \) and \( U_0 \) cooperatively. In practice, there are other signal processing options which can be used for designing \( p_0 \) and \( w_0 \).

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 \( p_0 = v_0(1) \), \( w_0 = u_0(1) \) and Eq. (3) into Eq. (2), we have:

\[
\hat{s}_0 = \sqrt{P_{T_0}} \lambda_0(1) x_0 + \sqrt{P_{T_1}} |u_0(1)|^H H_{10} p_1 x_1 + [u_0(1)]^H z_0 \tag{4}
\]

where \( \lambda_0(1) \) is the largest singular value of \( H_0 \), indicating the amplitude gain of the principal eigenmode (i.e., spatial sub-channel) of \( H_0 \). The first term on the RHS of Eq. (4) contains PUE0’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 PUE0, the second and third terms on the RHS of Eq. (4) must satisfy:

\[
\sqrt{P_{T_0}} \lambda_0(1) x_c + \sqrt{P_{T_1}} |u_0(1)|^H H_{10} p_1 x_1 = 0. \tag{5}
\]

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

\[
x_c = -\sqrt{P_{T_1}/P_{T_0}} \lambda_0(1)^{-1} |u_0(1)|^H H_{10} p_1 x_1. \tag{6}
\]

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:

\[
\hat{s}_0 = \sqrt{P_{T_0}} \lambda_0(1) x_0 + [u_0(1)]^H z_0. \tag{7}
\]

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 PUE0 can be calculated as:

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

where \( \sigma_n^2 \) 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 \( s_0 = \sqrt{P_{T_0}} \lambda_0(1) x_0 \), the immunizing signal as \( s_c = \sqrt{P_{T_0}} \lambda_0(1) x_c \), the received signal component from PBS0 as \( \hat{s}_0 = \sqrt{P_{T_0}} \lambda_0(1) x_0 + \sqrt{P_{T_0}} \lambda_0(1) x_c \), and the interference from MBS1 as \( s_1 = \sqrt{P_{T_1}} |u_0(1)|^H H_{10} p_1 x_1 \), respectively. Then, the estimated/filtered signal in Eq. (4) (ignoring noise) can be rewritten as \( \hat{s}_0 = \hat{s}_0^* + s_1 \). Similarly, the iCoded signal sent by PBS0 is expressed as \( s_0^* = \sqrt{P_{T_0}} p_0 x_0^* \).

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 PBS0 and PUE0 as \( \mathcal{J}_T(\cdot) = 1/\sqrt{P_{T_0}} p_0 \) and \( \mathcal{J}_R(\cdot) = 1/\sqrt{P_{T_0}} \lambda_0(1) \), respectively. Then, we can have \( \mathcal{J}_T(s_0) = x_0^* \), \( \mathcal{J}_R(s_0) = x_0 \), \( \mathcal{J}_R(s_c) = x_c \), \( \mathcal{J}_R(s_0^*) = x_0^* \) and \( \mathcal{J}_R(s_1) = x_0 \). As for \( \mathcal{J}_R(s_1) \), it should be noticed that \( \mathcal{J}_R(s_1) = \frac{s_1}{\sqrt{P_{T_0}} \lambda_0(1)} \). 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.

As Fig. 2 shows, PBS0 first calculates the immunizing data \( x_c (\mathcal{J}_R(s_c)) \) according to interference \( s_1 \) 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 \( x_0^* (\mathcal{J}_R(s_0^*)) \), point B. Next, PBS0 sends the iCoded signal \( s_0^* \) to PUE0. Likewise, PUE0 applies \( w_0 = u_0(1) \) to the received mixed signal \( y_0 \) and extracts the estimated data symbol, denoted as \( \mathcal{J}_R(s_0) \), from the post-processed signal \( \hat{s}_0 \). \( \mathcal{J}_R(s_0) = \mathcal{J}_R(s_0^* + s_1) \) holds. According to Eq. (7), \( \mathcal{J}_R(s_0) \) is the same as \( \mathcal{J}_R(s_0) \) (point A), i.e., PUE0 can accurately recover original desired data \( x_0 \) from \( s_0^* + s_1 \). Based on the above discussion, iCoding can mitigate the interference \( s_1 \) at PUE0, hence realizing immunity to interference. Moreover, since \( \mathcal{J}_T(s_0^*) \neq x_0 \), PUE0’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, PBS0’s power range needs to be extended; this will not only incur more transmit power consumption, but also increase PBS0’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-\( M \)-QAM where \( M \) represents for the modulation order, as an example to illustrate the principle of
directions determined by \( \theta \). Next, we copy the original constellation along the other four directions determined by phase angle \( \Delta \). The center of the duplicated constellation is \( [\sqrt{M}]\Delta \) away from the origin (i.e., the center of original constellation). \( \Delta \) represents the horizontal (or vertical) distance between two adjacent constellation points. The notation \([\cdot]\) 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 \( \theta_{II} \in \{ \pi, \frac{3\pi}{2}, \frac{\pi}{2}, \frac{2\pi}{2} \} \). The center of the duplicated constellation is \( \sqrt{2}[\sqrt{M}]\Delta \) 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 1st round extended constellation.

Note, in practice, that the iCoded symbol may still be out of the range of the 1st 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 distance \( 3^k \sqrt{2}[\sqrt{M}]\Delta \) and \( 3^k \sqrt{2}[\sqrt{M}]\Delta \) from the origin along the directions determined by \( \theta_I \) and \( \theta_{II} \), 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 1st round extended square-16QAM constellation where the 8-shaped mapping rule is applied. At the Tx-side, PBS0 calculates \( x_c \) (\( J_T(s_0^*) \)) according to \( s_1 \) and then encodes \( x_0 \) (point A in Fig. 4) with it so as to obtain \( x_0^* \). When \( x_0^* (J_T(s_0^*)) \), point B) exceeds the range of original constellation, \( J_T(s_0^*) \) is mapped back to \( x_0^* \) (\( J_T(s_0^*) \), point C), \( s_0^* \) is the actual transmitted signal of PBS0. \( J_T(s_0^*) = x_0^* \) indicates removing \( \sqrt{P_T} \) from \( x_0^* \) in the expression of \( s_0^* \). As Fig. 4 shows, the relative position of \( J_T(s_0^*) \) in constellation 0 is the same as that of \( J_T(s_0^*) \) in constellation 3. In this way, an arbitrary iCoded symbol can be limited to the range of original constellation. Then, \( J_T(s_0^*) \) is sent by PBS0.

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

\[
\begin{align*}
\text{Re}(\hat{x}_0^*) &= \rho_0 \cos \phi_0 - \text{Drd}\left(\frac{\rho_0 \cos \phi_0}{D}\right) \\
\text{Im}(\hat{x}_0^*) &= \rho_0 \sin \phi_0 - \text{Drd}\left(\frac{\rho_0 \sin \phi_0}{D}\right)
\end{align*}
\]

where \( \text{Drd}(\cdot) \) denotes the rounding-off operation. \( D \) is the horizontal mapping distance between \( J_T(s_0^*) \) (point B) and \( J_T(s_0^*) \) (point C), \( D = 3^{k-1} \sqrt{2}[\sqrt{M}]\Delta \) 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 \( \text{Rsd}(\cdot) \) to denote the 8-shaped mapping operation, by substituting \( D = 8 \), \( \text{Re}(x_0^*) = 9 \) and \( \text{Im}(x_0^*) = 7 \) into Eq. (9), we can see that \( \text{Rsd}(x_0^*) = \hat{x}_0^* \) holds.

At the Rx-side, PUE0 extracts \( J_R(s_0^* + s_1) \) (point D) from the post-processed mixed signal \( s_0^* + s_1 \), and then inversely maps \( J_R(s_0^* + s_1) \) to obtain the estimated data \( J_R(s_0^*) \) in the original constellation. As the figure shows, \( J_R(s_0^*) = J_R(s_0^*) = x_0^* \) holds; that is, \( x_0^* \) is accurately decoded. The expression of inverse mapping rule at PUE0 is the same as that at PBS0, we only need to substitute the amplitude and phase of \( J_R(s_0^* + s_1) \) instead of \( \rho_0^* \) and \( \phi_0^* \), into Eq. (9).

In Fig. 4, we use yellow arrowed arcs to depict the 8-shaped mapping at PBS0 and PUE0. Specifically, start from \( x_0^* \) (point A) to \( J_T(s_0^*) \) (point B) via arc AB; next, along BC to \( J_T(s_0^*) = x_0^* \) (point C); and then, from point C via CD to \( J_R(s_0^* + s_1) \) (point D); finally, along DA to \( J_R(s_0^*) \) (point
A). Since the shape of $\text{ABCD}$A 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 $N_T = N_{R_1} = N_{R_2} = 2$ 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 $5 \times 10^4$ 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$_e$, as well as their joint distribution function $p(x_0, \hat{x}_0)$, respectively, so that $c_0$ can be calculated as:

$$c_0 = \max_{p(x_0)} \left\{ \sum_{x \in X} \sum_{\hat{x} \in \hat{X}_0} p(x_0, \hat{x}_0) \log_2 \frac{p(x_0, \hat{x}_0)}{p(x_0)p(\hat{x}_0)} \right\}$$  \hspace{1cm} (10)

where $X$ and $\hat{X}_0$ denote the symbol sets at PBS$_0$ and PUE$_0$, respectively, $x_0 \in X$ and $\hat{x}_0 \in \hat{X}_0$, $I(X_0; \hat{X}_0)$ 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 $P_T$ and $P_0$ 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 $\zeta_1 = 10 \log \frac{P_T}{\sigma_n^2}$ and $\zeta_0 = 10 \log \frac{P_0}{\sigma_n^2}$, respectively. We also use $\gamma$ to denote the ratio of $P_T$ to $P_0$, i.e., $\gamma = \frac{P_T}{P_0}$. We set $\gamma \in \{0, 1\}$ in the simulation.

Fig. 5 shows the variation of $c_0$ and $c_e$ along with $\eta$ under different $\zeta_0$s. As the figure shows, since PUE$_0$ is subject to the interference from MBS$_1$ whereas PUE$_e$ 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 $\zeta_0$, $c_0$ is independent of $\eta$; while under medium to high $\eta$, $c_e$ is independent of $\eta$. This is because SINR at PUE$_0$ and PUE$_e$ can be expressed as $\gamma_0 = \frac{P_T}{\sigma_n^2} = 10^{0.1 \zeta_0}$ and $\gamma_e = \frac{P_0}{P_T + \sigma_n^2} = \frac{1}{\eta(10^{-0.1 \zeta_0} + 1)}$, respectively. Then, one can see from the expression of $\gamma_0$ that $c_0$ is independent of $\eta$ and increases as $\zeta_0$ grows. As for $c_e$, we can see that when $\eta$ is quite small, $\zeta_0$ dominates both $\gamma_e$ and $c_e$, and $c_e$ slightly increases as $\zeta_0$ grows; while as $\eta$ grows larger, $\gamma$ becomes dominant compared to $10^{-0.1 \zeta_0}$ in calculating $\gamma_e$, so that $c_e$ becomes less dependent on the variation of $\zeta_0$.

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 $\eta$, the probability that IoE is lost is negligible, yielding a slightly better $c_e$ than 0.25bit/symbol.

Fig. 6 plots the variation of $c_0$ and $c_e$ along with $\eta$ under different $\zeta_0$s. Given fixed $\zeta_0$, $c_0$ is shown to decrease as $\eta$ grows; while for $c_e$, it decreases with an increase of $\eta$ when $\eta$ is low and becomes invariant under medium to high $\eta$. This is because SINR at PUE$_0$ and PUE$_e$ can be computed as $\gamma_0 = \frac{P_T}{\sigma_n^2} = 10^{0.1 \zeta_0}$ and $\gamma_e = \frac{P_0}{P_T + \sigma_n^2} = \frac{1}{\eta(10^{-0.1 \zeta_0} + 1)}$, respectively. Then, one can see from the expression of $\gamma_0$ that $c_0$ is in inverse proportional to $\eta$, so that $\gamma_0$ and $c_0$ reduce as $\eta$ grows. Given fixed $\eta$, since higher $\zeta_1$ yields larger $10^{0.1 \zeta_1}$, $c_0$ enhances as $\zeta_1$ grows. As for $c_e$, it decreases as $\zeta_1$ grows under fixed and small $\eta$. This is because when $\eta$ is quite small, $\eta$ can dominate and yield a large $\gamma_e$, making $c_e$ slightly better than 0.25bit/symbol; while as $\eta$ grows larger, $\gamma_e$ degenerates obviously, incurring $c_e$ being as small as 0.25bit/symbol.
s-1

PUE

higher SE.

not incur any desired signal’s power loss, and hence yielding

under

is consumed for generating the steering signal. Hence, ZF

Fig. 7. PUE

ζ

transmission of PUE

η

interference-free desired transmission. Moreover, since the

information carried in the interference, an iCoded signal

security simultaneously. By exploiting both CSI and data

narrowing coding


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

Fig. 7 plots the variation of PUE0’s average SE along with η under C1 = 10dB and different IM schemes. Given fixed C1, P̂ T1 decreases as η grows, hence decreasing PUE0’s SE. Since both iCoding and 2pMIMO realize interference-free data reception at PUE0, they can achieve the highest SE. Under C1 = 10dB, the strength of interference is relatively stronger than that of the noise. So, IM can contribute more to PUE0’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 PUE0; whereas for IS, only the effective portion of interference imposing on the desired transmission of PUE0 is mitigated, thus decreasing IM cost and preserving the performance of intended transmission. As η grows larger, P̂ T1 becomes strong relative to P̂ T0, thus ZF can mitigate more interference with the same desired signal’s power loss, whereas for IS, more transmit power at PBS0 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 PBS0, thus outperforming IS in PUE0’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 evaluation have shown that the proposed scheme can effectively improve a legitimate user’s transmission efficiency and secrecy.