IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 29, 2017, accepted October 25, 2017, date of publication November 1, 2017, date of current version November 28, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2768540

Secure Index and Data Symbol Modulation for OFDM-IM

YONGGU LEE[1], HANSEONG JO[1], YOUNGWOOK KO[2], AND JINHO CHOI[1], (Senior Member, IEEE)

[1]School of Electrical Engineering and Computer Science, Gwangju Institute of Science and Technology, Gwangju 61005, South Korea
[2]School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, Belfast BT7 1NN, U.K.

Corresponding author: Jinho Choi (jchoi0114@gist.ac.kr)

This work was supported in part by the Institute for Information and communications Technology Promotion grant through the Korea Government (MSIT) under Grant 2017-0-00413 (Streamlined IoT Communications by Physical Layer Device Identification).

ABSTRACT In this paper, we propose a secure index and data symbol modulation scheme for orthogonal frequency division multiplexing with index modulation (OFDM-IM) systems. By exploiting the notion of the channel reciprocity in time division duplexing mode over wireless channels for shared channel state information as a secret key, we investigate randomized mapping rules for index modulation as well as data symbol modulation. Due to the randomized mapping rules for index and data symbol modulation in OFDM-IM, an eavesdropper is not able to correctly decide message bits even though active subcarriers and their symbols are correctly estimated. In particular, we exploit a characteristic of OFDM-IM which uses a fraction of subcarriers for transmissions to enhance security of data symbol modulation. In addition, to design a set of mapping rules for data symbol modulation, we investigate both a random-selection-based set and a bit-mismatch-based set. Through the analysis and simulation results, we demonstrate that the proposed scheme based on the randomized mapping rules for index modulation and data symbol modulation has a better performance than an existing scheme (modified for OFDM-IM) in terms of bit error rate (BER) and successful attack probability. In particular, we can show that the BER at an eavesdropper is much higher if the bit-mismatch-based set of mapping rules is used.

INDEX TERMS Orthogonal frequency division multiplexing, index modulation, data symbol modulation, physical layer security.

I. INTRODUCTION

Index modulation (IM) is an emerging key technique for 5th generation (5G) wireless networks because of its high spectral and energy efficiency [1]. There are two well-known applications of IM. One is spatial modulation (SM) [2] and the other is orthogonal frequency division multiplexing (OFDM)-IM. Especially, OFDM-IM has been intensively studied in [1], [3]–[11]. Unlike conventional OFDM [12], a fraction of subcarriers are active, and the indices of active subcarriers convey information bits in OFDM-IM. Due to a high spectral efficiency as well as a high energy efficiency, it is considered not only for high speed wireless communications systems but also for machine-type communications (MTC) such as body centric communications (BCC) and smart grid communications [7], [13], where the energy efficiency is important.

Various attractive IM-aided OFDM systems have been studied. In [14] and [15], dual-mode (DM) OFDM-IM that all the subcarriers divided into two groups are modulated by a pair of distinguishable modulation constellations is presented to achieve better performance in terms of reliability. In addition, for 5G wireless networks, multiple-input multiple-output (MIMO) OFDM-IM where IM concept is combined with MIMO transmissions to take advantages of two techniques is proposed as an alternative to classical MIMO-OFDM in [10]. In [11], a transmit diversity scheme for OFDM-IM is presented to obtain diversity gain with low complexity maximum likelihood (ML) detection.

Due to the inherent broadcast nature of wireless communications, it is vulnerable to eavesdropping on confidential data transmitted to a legitimate receiver. Security techniques in upper layers have been used for the transmission of confidential data [16]. However, such security techniques may need a high computational complexity and a large overhead. Furthermore, they may become prone to powerful computing attacks due to emerging powerful computing devices [17].

To overcome those problems, physical layer security has attracted a lot of attentions [18]–[21]. It exploits the dynamic characteristics of wireless communications such as random channel, noise, and interferences for secure transmissions. In [22], the process of generating a key from a wireless channel is introduced and it is demonstrated that a wireless channel can be used as a source of secret private keys for a legitimate transmitter and a legitimate receiver.

For OFDM systems, physical layer security techniques have been studied in [23]–[29]. In [23], a secrecy rate which is a theoretical secrecy metric in physical layer security is derived under various OFDM communication scenarios. It is shown that the power allocation plays a crucial role in improving the secrecy rate. To increase the secrecy rate under an unfavorable channel scenario, a secure beamforming and artificial noise which degrades eavesdropper's channel are used for secure OFDM transmissions based on the channel state information (CSI) in [25]. However, it is necessary to use multiple antennas at a transmitter for secure beamforming and artificial noise. In [28] and [29], chaotic sequences and the CSI based interleaving are used to randomize the modulated signal for secure OFDM systems. Particularly, in [29], the CSI based interleaving scheme has been studied to prevent an eavesdropper from correctly deciding confidential information symbols in OFDM systems. However, there exists a trade-off between reliability and security which is determined by the number of interleaved subcarriers in [29]. In addition, to guarantee high security and reliability, it may require side information transmissions between legitimate transmitter and receiver.

There are physical layer security techniques for SM [30]–[34]. In [30], a jamming signal is used to prevent from eavesdropping in SM. Transmit precoding for secure SM is introduced in [31]. In addition, information theoretical approach for the security of SM is presented in [32] and [33]. In [34], secure IM for a SM based physical layer security is proposed where the channel between a legitimate transmitter and a legitimate receiver is used to randomize a mapping rule for only IM symbols in [34]. However, although the information bits transmitted by IM can be secure, it does not guarantee any security for transmitted data symbols through active subcarriers.

In this paper, we propose a secure IM and data symbol modulation (DSM) scheme to improve the physical layer security in OFDM-IM systems. In particular, based on the channel reciprocity between a legitimate transmitter and a legitimate receiver in time division duplexing (TDD) mode, the CSI based randomized mapping rules for IM and DSM are proposed to confuse an eavesdropper who does not have the CSI. Unlike the conventional schemes for secure OFDM in [29] and SM in [34] where no security for DSM bits are considered, we also ensure secure transmissions of DSM bits. Therefore, all information bits that are transmitted by either IM or DSM can be secure in the proposed secure OFDM-IM without any additional side information. It is noteworthy that we use a characteristic of OFDM-IM that a fraction of subcarriers is used for transmissions to enhance the security of DSM bits. The CSI associated with active subcarriers which are determined by IM bits is used as a secret key in the proposed secure DSM. Then, it can dynamically update the secret key (i.e., CSI) for the coherence time without any side information, while it is necessary to send side information to change the secret key in secure OFDM [29]. Furthermore, we design a set of mapping rules for DSM to improve the security of DSM bits. To this end, we develop a bit-mismatch based set of mapping rules for secure DSM and provide the bit error rate (BER) performance analysis at an eavesdropper. Through a theoretical analysis and numerical simulations, we can show that the proposed set of mapping rules is superior to a random-selection based set of mapping rules in terms of security. In particular, we show that the proposed secure OFDM-IM using the bit-mismatch based set of mapping rules can result in a high BER at an eavesdropper even if an eavesdropper's signal to noise ratio (SNR) is high.

The main contributions of this paper are summarized as follows:

- The secure mapping algorithms to protect both IM and DSM bits are proposed under the OFDM framework for the secure OFDM-IM scheme. To the best of our knowledge, secure DSM for OFDM-IM has not been studied in the literature yet and only the secure IM is studied under the SM framework.
- For the performance analysis, we derive the BER expressions at a legitimate receiver and an eavesdropper, which represent the reliability and the security, respectively. For pragmatic systems, we evaluate the impact of imperfect CSI on the performance. Throughout the paper, as a security metric, we use the BER at an eavesdropper for uncoded systems. Unfortunately, this performance metric is not an information-theoretic security measure [35]. However, as in [29], [34], and [36], it might be used as a pragmatic metric for lightweight secure transmission schemes. In particular, since OFDM-IM might be used in applications where transmitters and receivers have various implementation constraints in terms of complexity (e.g., BCC in [7]), it might be desirable to consider simple, but effective secure OFDM-IM that can securely transmit both IM and DSM bits. Furthermore, we derive a successful attack probability that an eavesdropper estimates secure mapping rules in the proposed secure OFDM-IM. It is shown that if a characteristic of OFDM-IM is employed for secure DSM in the proposed secure OFDM-IM, the successful attack probability can be much lower compared to that of secure OFDM.
- To maximize the security performance in terms of BER at an eavesdropper, we propose the bit-mismatch based set of mapping rules for secure DSM. Employing such set of mapping rules for the secure OFDM-IM is shown to ensure a high BER at the eavesdropper even at high SNR.
- In addition to theoretical and computer simulation results, hardware experiments are performed to

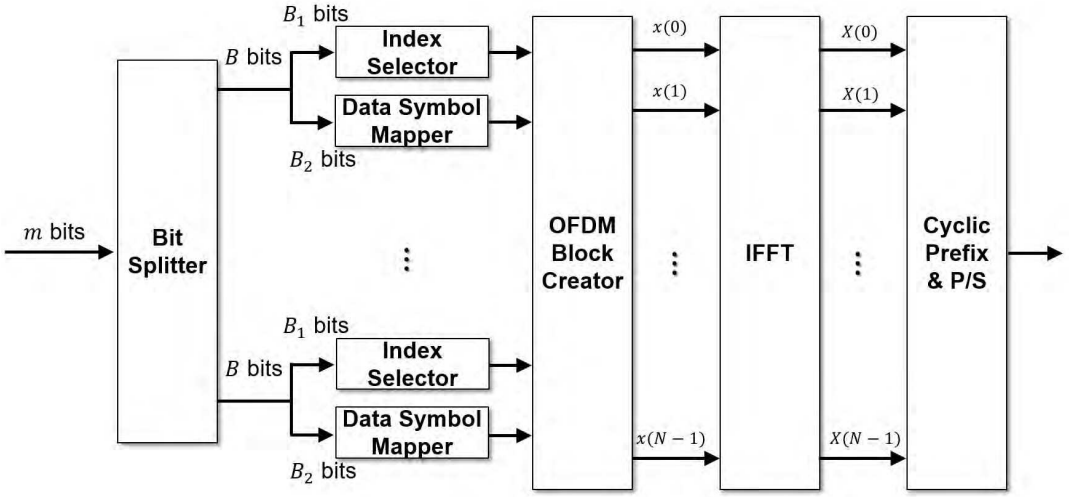


FIGURE 1. The transmitter structure of OFDM-IM [3].

validate the realistic performance of the secure OFDM-IM scheme by using an Universal Software Radio Peripheral (USRP) hardware platform.

The remainder of this paper is organized as follows. Section II presents a background of conventional OFDM-IM and presents a system model for the proposed secure OFDM-IM. We conduct a theoretical analysis for reliability and security of the secure OFDM-IM in Section III and IV. In Section V, we design a bit-mismatch based set of mapping rules for secure DSM. The simulation results to evaluate the performance of the proposed scheme are presented in Section VI. Finally, concluding remarks are given in Section VII.

Notation: Upper-case and lower-case boldface letters are used for matrices and vectors, respectively. The superscripts T and H represent the transpose and Hermitian of a random variable, respectively. Denote by $\mathbf{I}$ the identity matrix. $\mathcal{CN}(\mu, \sigma^2)$ represents the distribution of circularly symmetric complex Gaussian (CSCG) with mean μ and variance σ^2. $\mathbb{E}[\cdot]$ is the statistical expectation.

II. SYSTEM MODEL

A. OFDM-IM

Suppose that a legitimate transmitter, called Alice, sends confidential signals to a legitimate receiver, called Bob, while there exists an eavesdropper, called Eve, in a multicarrier system. In every transmission from Alice to Bob, we consider OFDM-IM system, where N subcarriers are divided into g clusters [3].

Each cluster has n subcarriers so that $N = ng$, which is also the size of fast Fourier transform (FFT) for OFDM-IM. Unlike conventional OFDM, not all the subcarriers are used for transmission in OFDM-IM, where only k out of n subcarriers are active per cluster, where $k \leq n$. The combination of the active subcarriers is referred to as IM symbol and the number of possible IM symbols per cluster is $C(n, k) = \binom{n}{k}$. Thus, the number of bits to be transmitted by IM per cluster is $B_1 = \lfloor \log_2 C(n, k) \rfloor$. The set of k active subcarrier indices in the β-th cluster for $\beta = 0, 1, \cdots, g-1$ is given by

$$I_\beta = \{i_{\beta,0}, \cdots, i_{\beta,k-1}\}, \tag{1}$$

where $i_{\beta,u} \in \{1, 2, \cdots, n\}$ for $u = 0, 1, \cdots, k-1$.

Once the active subcarriers are selected, $B_2 = k \log_2 M$ bits can be conveyed by M-ary modulation, which is referred to as DSM, on the k active subcarriers. The set of k M-ary symbols in the β-th cluster is given by

$$S_\beta = \{s_{\beta,0}, \cdots, s_{\beta,k-1}\}, \tag{2}$$

where $s_{\beta,u} \in \mathcal{S}$. Here, $\mathcal{S}$ represents the constellation of M-ary signals. Thus, $B_1 + B_2$ bits are transmitted per cluster.

Denote by $\mathbf{x}_F = [\mathbf{x}_0^T, \cdots, \mathbf{x}_{g-1}^T]^T$ the OFDM symbol vector in OFDM-IM, where $\mathbf{x}_\beta = [x_\beta(0), \cdots, x_\beta(n-1)]^T$ represents the transmitted symbol vector of the β-th cluster that $x_\beta(i_{\beta,u}-1) \in \mathcal{S}$ for $i_{\beta,u} \in I_\beta$, otherwise $x_\beta(i_{\beta,u}-1) = 0$. For convenience denote by $K = kg$ the total number of active subcarriers. In Fig. 1, an transmitter structure of OFDM-IM is illustrated.

The OFDM-IM signal in the frequency domain is transformed into the time domain for transmissions as follows:

$$\mathbf{x}_T = \frac{1}{\sqrt{K}} \mathbf{F}_N^{\mathrm{H}} \mathbf{x}_F, \tag{3}$$

where $\mathbf{F}_N^{\mathrm{H}}$ denotes the discrete Fourier transform (DFT) matrix and $\mathbb{E}[\mathbf{x}_T^{\mathrm{H}} \mathbf{x}_T] = N$ under the assumption that $\mathbb{E}[|s_{\beta,u}|^2] = 1$ for all β and u. Then, a cyclic prefix (CP) of length N_{cp}, which is $\mathbf{x}_{T,CP} = [x_T(N-N_{cp}+1), \cdots, x_T(N)]^T$, is appended at the beginning of $\mathbf{x}_T$. Note that the CP length, denoted by N_{cp}, has to be longer than the length of the channel impulse response (CIR), denoted by ν, to avoid the inter-block interference [12], [37].

After deleting CP and performing FFT, the received signals in the frequency domain at Bob and Eve, respectively, are

given by

$$\mathbf{y}_b = \mathbf{H}\mathbf{x}_F + \mathbf{n}_b, \tag{4}$$
$$\mathbf{y}_e = \mathbf{G}\mathbf{x}_F + \mathbf{n}_e, \tag{5}$$

where $\mathbf{n}_b \sim \mathcal{CN}(0, \tilde{N}_0\mathbf{I})$ and $\mathbf{n}_e \sim \mathcal{CN}(0, \tilde{N}_0\mathbf{I})$ are independent background noise terms at Bob and Eve, respectively, in the frequency domain. Here, $\tilde{N}_0$ represents the noise spectral density (in the frequency domain). In addition, the diagonal frequency domain channel matrices of Bob and Eve, respectively, are given by

$$\mathbf{H} = diag(H(0), H(1), \cdots, H(N-1)) \tag{6}$$

and

$$\mathbf{G} = diag(G(0), G(1), \cdots, G(N-1)), \tag{7}$$

where $H(i)$ and $G(i)$ are the channel coefficients of the i-th subcarrier in the frequency domain at Bob and Eve, respectively, which can be represented as follows:

$$H(i) = \sum_{q=0}^{\nu-1} h_q e^{-j2\pi\frac{qi}{N}},$$
$$G(i) = \sum_{q=0}^{\nu-1} g_q e^{-j2\pi\frac{qi}{N}}. \tag{8}$$

Here, $h_q \sim \mathcal{CN}(0, \frac{\sigma_H^2}{\nu})$ and $g_q \sim \mathcal{CN}(0, \frac{\sigma_G^2}{\nu})$ are the CIRs at Bob and Eve, respectively, as in [3]. In this case, the channels are multipath Rayleigh fading channels.

B. SECURE OFDM-IM

In this subsection, we first introduce an existing secure OFDM scheme in [29] that exploits the randomness of channels, and then propose a novel approach for secure transmissions in OFDM-IM to compare the secure OFDM-IM with the existing secure OFDM.

In OFDM, the randomness of wireless multipath channels can be exploited for secure transmissions in the physical layer. For example, a dynamic subcarrier interleaving scheme is proposed for secure OFDM by taking advantage of the channel reciprocity in [29]. In this approach, at Alice, P out of the N subcarriers of an OFDM signal are selected and interleaved after the symbol modulation. Here, the selection of P subcarriers and interleaving pattern are determined by the CSI between Alice and Bob, which is assumed to be shared between Alice and Bob based on the channel reciprocity in TDD mode. The indicator of the subcarrier selection is given by

$$I(i) = \begin{cases} 1, & i \in U \\ 0, & \text{otherwise} \end{cases}, \quad i = 0, \cdots, N-1, \tag{9}$$

where U denotes the set of indices of subcarriers included in the interleaving. Following the subcarrier selection, the P selected subcarriers are interleaved in descending order of their channel gains observed at the transmitter. The order of the P subcarrier gains is renamed as follows:

$$[\tilde{S}(0), \cdots, \tilde{S}(P-1)]^{\mathrm{T}}, \tag{10}$$

where $\tilde{S}(p)$ for $p = 0, \cdots, P-1$ becomes the p-th largest $|H(i)|^2$. Then, there is a one-to-one mapping between the descending order of U and the descending order of channel gains. For example, if $P = 3$, $U = \{3, 7, 9\}$ and $|H(7)|^2 > |H(9)|^2 > |H(3)|^2$, the interleaved signals are $\tilde{x}_F^I(3) = \tilde{x}_F(7)$, $\tilde{x}_F^I(7) = \tilde{x}_F(9)$, $\tilde{x}_F^I(9) = \tilde{x}_F(3)$, where $\tilde{x}_F^I(i)$ is a transmitted signal of the i-th subcarrier in the secure OFDM system and the superscript I represents the interleaved symbols. Clearly, Bob can detect the correct symbols by using the deinterleaving based on the CSI knowledge, while Eve could have incorrect symbols due to unknown CSI to Eve.

In conventional OFDM-IM as in [3], B_1 bits are mapped onto the indices of k active subcarriers by a look-up table or combinatorial method, while B_2 bits are mapped onto k symbols by a DSM mapping rule in each cluster. With known mapping rules for IM and DSM, Eve can recover IM bits and DSM bits using the ML detection for active subcarrier indices and their symbols as Bob does [3]. In this case, it is clear that there is no guaranteed secrecy. To overcome this problem, we employ the channel reciprocity to secure OFDM-IM, similar to the SM approach in [34], where the mapping rule for IM can be selected from a set of different mapping rules depending on the CSI between Bob and Alice. To this end, the CSI should change enough to generate randomness of the CSI for secure IM and at the same time the CSI should not quickly vary in order to satisfy the channel reciprocity constraint (i.e., there exists a trade-off). Then, in TDD, the channel reciprocity implies that Alice and Bob have the same CSI which can be used as a shared secret key for a randomized mapping rule in IM. In [34], however, a randomized mapping rule is limited only for IM, without taking into consideration DSM. Unlike [34], we study opportunities to apply a randomized mapping rule to DSM by using a characteristic of OFDM-IM. This forms the main contribution of this work together with a design of DSM mapping rules in order to increase the BER at Eve. Furthermore, a successful attack probability that Eve estimates secure mapping rules can be low by using the CSI associated active subcarriers as a secret key for seucre DSM. Consequently, we aim to transmit more secure bits than the approach in [34] in the context of OFDM-IM. The resulting scheme is called the secure OFDM-IM in this paper, which is illustrated in Fig. 2.

As shown in Fig. 2, we assume that a block of N subcarriers is divided into η subblocks of Wn subcarriers (i.e., $N = \eta Wn$). One subblock includes W clusters and each cluster has n subcarriers. For the secure OFDM-IM, each cluster has individual mapping rule for secure IM, while W clusters included in one subblock share the same mapping rule for secure DSM. It means that there are η mapping rules for secure DSM, while g mapping rules are used for secure IM in the proposed secure OFDM-IM.

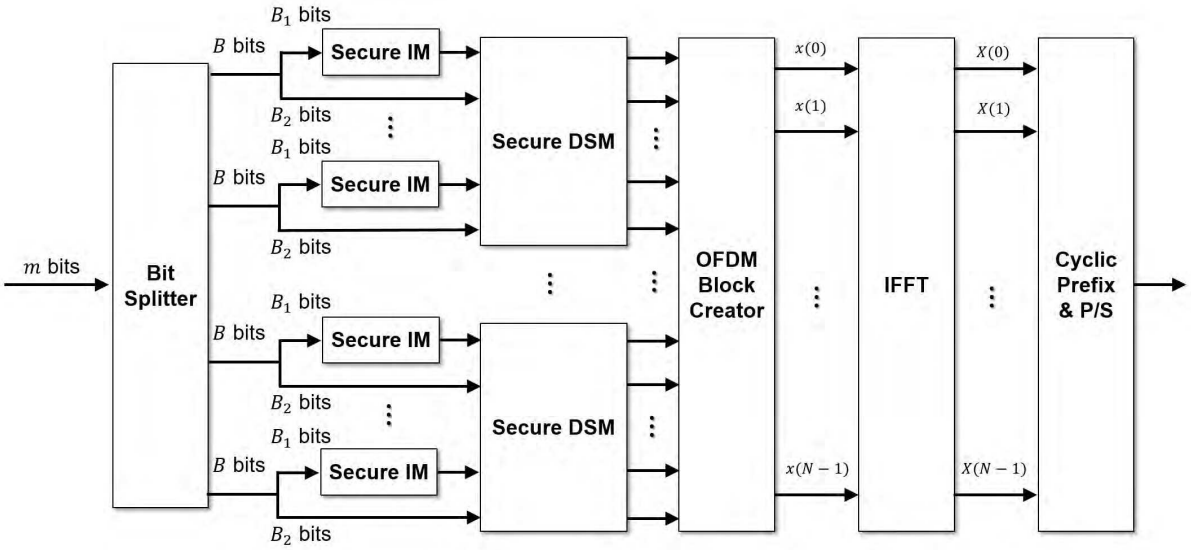


FIGURE 2. The transmitter structure of the proposed secure OFDM-IM.

1) SECURE IM

There are two secrecy mapping parts in the proposed secure OFDM-IM. In the first part, similar to [34], we consider a random mapping rule for IM. In a cluster, before selecting the active subcarriers, Alice estimates $|H(i)|^2$. Then she sorts $|H(i)|^2$ in descending order and renames them as follows:

$$[S(0), \ldots, S(n-1)]^T, \tag{11}$$

where $S(l)$ for $l = 0, \cdots, n-1$ becomes the l-th largest $|H(i)|^2$, i.e., $S(0) \geq \cdots \geq S(n-1)$, and l is the index of $S(l)$ not $H(i)$. There is a one-to-one mapping between $\{|H(i)|^2\}$ and $\{S(l)\}$. In the conventional OFDM-IM, a trivial mapping rule is used. For example, if $n = 4$, $k = 2$, the 0th and 2nd subcarriers are active, then non-zero signals are transmitted through the 0th and 2nd subcarriers. On the other hand, in secure OFDM-IM, the mapping rule for IM is related to $\{S(l)\}$. Thus, if $S(0) = |H(3)|^2$, $S(1) = |H(2)|^2$, $S(2) = |H(1)|^2$, $S(3) = |H(0)|^2$, subcarrier 3 and subcarrier 1 corresponding to $S(0)$ and $S(2)$, respectively, are active. Since $\{S(l)\}$ is unknown to Eve, she does not know the mapping rule, leading to failed recovery of the IM bits.

2) SECURE DSM

The second secrecy part is to ensure secrecy of DSM, which is not considered in [34]. For secure DSM, we also use a randomized mapping rule based on the CSI associated with the active subcarrier indices. A mapping rule for secure DSM in one subblock is determined by channel gains associated with $\kappa = Wk$ active subcarriers in one subblock. For example, if $W = 1$, the number of active subcarriers in each subblock is given by $\kappa = k$. In this case, the possible number of secret keys for secure DSM may be small with a few k. The order of κ channel gains corresponds to the randomized mapping rule in the set of mapping rules. For example, if $\kappa = 2$ and $M = 2$, a mapping rule for secure DSM is selected in accordance with the order of channel gains associated with active subcarrier indices as follows:

$$\{|H(\iota_1)|^2 \leq |H(\iota_2)|^2\} \rightarrow \{\mathcal{M}_1 : [0] \rightarrow -1,\ [1] \rightarrow 1\},$$
$$\{|H(\iota_2)|^2 \leq |H(\iota_1)|^2\} \rightarrow \{\mathcal{M}_2 : [0] \rightarrow 1,\ [1] \rightarrow -1\},$$

where ι_1 and ι_2 are active subcarrier indices in a subblock.

To obtain better security performance in terms of BER at Eve, we design a set of mapping rules. For example, consider a set of mapping rules with 4-QAM. In 4-QAM, there exist $4! = 24$ possible mapping rules. Suppose that Alice uses a certain mapping rule for 4-QAM as follows: $\{\mathcal{M} : [00] \rightarrow 1+j,\ [01] \rightarrow -1+j,\ [10] \rightarrow 1-j,\ [11] \rightarrow -1-j\}$ and the transmitted symbols are perfectly detected at Eve. If Eve chooses the following mapping rule: $\{\mathcal{M}' : [00] \rightarrow -1-j,\ [01] \rightarrow 1-j,\ [10] \rightarrow -1+j,\ [11] \rightarrow 1+j\}$, the BER becomes $\frac{1}{2}$ although the transmitted symbols are correctly recovered. Thus, depending on Eve's selection of the DSM mapping rule, the BER varies and is usually high. In Section V, we will investigate details on the mapping rule for secure DSM.

III. RELIABILITY ANALYSIS

In this section, the BER at Bob is analyzed to evaluate the reliability for the proposed scheme. For pragmatic systems, we assume the presence of channel estimation errors.

The ML detection [38] is performed to jointly find the active subcarrier indices and DSM symbols of the active subcarriers. The ML detection at Bob can be performed as follows:

$$\{\hat{i}_b, \hat{s}_b(i)\} = \arg \min_{i_b \in \mathcal{I},\ s_b(i) \in \mathcal{S}} \|\mathbf{y}_b - \mathbf{H}\mathbf{x}_F\|^2, \tag{12}$$

where $\mathcal{I}$ and $\mathcal{S}$ denote the sets of indices and the constellations, respectively.

Since the detection of the both IM and DSM bits depends on the shared CSI between Alice and Bob, the CSI certainty plays an important role in the proposed scheme. Particularly, the use of CSI ensures to randomize the look-up table for secure IM and DSM. Unlike the conventional OFDM-IM [3], thus, bit errors are induced by not only ML detection errors but also incorrect mapping rules caused by imperfect CSI. The BER can be given by

$$P_e^B = 1 - (1 - P_e^{B_1})(1 - P_e^{B_2}), \tag{13}$$

where $P_e^{B_1}$ and $P_e^{B_2}$ are the bit error probabilities caused by ML detection errors and incorrect selection of mapping rules, respectively.

A. BER AT BOB WITH PERFECT CSI

If the channel is perfectly estimated at Alice and Bob, there are no errors induced by the selection of incorrect IM and DSM mapping rules at Bob (i.e., $P_e^{B_2} = 0$). Then, from (13), P_e^B is determined solely by $P_e^{B_1}$. To compute $P_e^{B_1}$, notice that from $\mathbf{H}$ in (6), the length of the CIR determines the correlation of the channel coefficients matrix as follows:

$$\mathbf{K} = \mathbb{E}[\mathbf{h}\mathbf{h}^{\mathrm{H}}] = \mathbf{F}_N^{\mathrm{H}}\tilde{\mathbf{I}}\mathbf{F}_N, \tag{14}$$

where $\mathbf{h}$ is a diagonal vector of $\mathbf{H}$ and $\tilde{\mathbf{I}} = [\frac{\sigma_H^2}{\nu}\mathbf{I}_{\nu\times\nu}\ \mathbf{0}_{\nu\times(N-\nu)};\ \mathbf{0}_{(N-\nu)\times\nu}\ \mathbf{0}_{(N-\nu)\times(N-\nu)}]$. $\mathbf{K}$ depends on the characteristics of the channel (e.g., the length of CIR). If the length of CIR is N, $\mathbf{K}$ becomes $\sigma_H^2\mathbf{I}_N$, i.e., the correlation of $\{H(i)\}$ is zero. Otherwise, the $H(i)$s are correlated.

The received signal for the β-th cluster at Bob is given by

$$\mathbf{y}_\beta = \mathbf{H}_\beta\mathbf{x}_\beta + \mathbf{n}_\beta, \tag{15}$$

where $\mathbf{x}_\beta$ and $\mathbf{H}_\beta$ represents the transmitted signal vector and channel coefficients matrix corresponding to the β-th cluster, respectively. Let $\mathbf{h}_\beta$ represent the vector containing the diagonal elements of $\mathbf{H}_\beta$. Then, $\mathbf{K}_n = \mathbb{E}[\mathbf{h}_\beta\mathbf{h}_\beta^{\mathrm{H}}]$ is the β-th submatrix of centered along the main diagonal of the matrix $\mathbf{K}$ in (14). As shown in [3], the BER for each cluster is the same as that of OFDM-IM. Then, the unconditional pairwise error probability (UPEP) for the β-th cluster is given by

$$P\left(\mathbf{x}_\beta \to \hat{\mathbf{x}}_\beta\right) \approx \frac{1/12}{\det(\mathbf{I}_n + q_1\mathbf{K}_n\mathbf{A})} + \frac{1/4}{\det(\mathbf{I}_n + q_2\mathbf{K}_n\mathbf{A})}, \tag{16}$$

where $q_1 = \frac{1}{4\tilde{N}_0}$, $q_2 = \frac{1}{3\tilde{N}_0}$, and $\mathbf{A} = \left(\mathbf{x}_\beta - \hat{\mathbf{x}}_\beta\right)^{\mathrm{H}}\left(\mathbf{x}_\beta - \hat{\mathbf{x}}_\beta\right)$. Thus, from (13) and (16), the average BER of the ML detection [3] is given by

$$P_e^{B_1} \approx \frac{1}{Bn_{\mathbf{x}_\beta}}\sum_{\mathbf{x}_\beta}\sum_{\hat{\mathbf{x}}_\beta} P\left(\mathbf{x}_\beta \to \hat{\mathbf{x}}_\beta\right)\mathbf{e}\left(\mathbf{x}_\beta, \hat{\mathbf{x}}_\beta\right), \tag{17}$$

where $n_{\mathbf{x}_\beta}$ is the number of possible realizations of $\mathbf{x}_\beta$ and $\mathbf{e}\left(\mathbf{x}_\beta, \hat{\mathbf{x}}_\beta\right)$ is the number of error bits for the corresponding pairwise error event.

B. BER AT BOB WITH IMPERFECT CSI

Notice that in practice, it is difficult to share identical CSI between Bob and Alice due to channel estimation errors caused by noise, interference and imperfect hardware at each side. From this, it is necessary to take into account imperfect CSI in deriving BER. To this end, the uncertain channel matrices at Alice and Bob, respectively, can be modeled as follows:

$$\begin{aligned}\hat{\mathbf{H}}_T &= \mathbf{H} + \mathbf{\Delta H}_T,\\ \hat{\mathbf{H}}_R &= \mathbf{H} + \mathbf{\Delta H}_R,\end{aligned} \tag{18}$$

where $\mathbf{\Delta H}_T = diag(\Delta H_T(0), \cdots, \Delta H_T(N-1))$ and $\mathbf{\Delta H}_R = diag(\Delta H_R(0), \cdots, \Delta H_R(N-1))$ are the diagonal estimation error matrices at Alice and Bob, respectively. Here, we assume that $\Delta H_T(i) \sim \mathcal{CN}(0, \sigma_T^2)$ and $\Delta H_R(i) \sim \mathcal{CN}(0, \sigma_R^2)$ for $i = 0, \cdots, N-1$ [29].

First, derive $P_e^{B_1}$ with channel estimation errors in order to evaluate the performance of the proposed scheme under a practical scenario. As shown in [3], the upper bound on the UPEP with channel estimation errors is given by

$$P\left(\mathbf{x}_\beta \to \hat{\mathbf{x}}_\beta\right) \le \frac{1/12}{\det(\mathbf{I}_n + \tilde{q}_1\tilde{\mathbf{K}}_n\mathbf{A})} + \frac{1/4}{\det(\mathbf{I}_n + \tilde{q}_2\tilde{\mathbf{K}}_n\mathbf{A})}, \tag{19}$$

where $\tilde{q}_1 = \frac{1}{4\tilde{N}_0+4\sigma_R^2}$, $\tilde{q}_2 = \frac{1}{3\tilde{N}_0+3\sigma_R^2}$ and $\tilde{\mathbf{K}}_n = \mathbf{K}_n + \sigma_R^2\mathbf{I}_n$. Then, using (17) and (19), the upper bound on the BER of ML detection can be found.

Secondly, consider the derivation of $P_e^{B_2}$, which is the BER due to mismatched mapping rules with channel estimation errors. To square mapping rules at Alice with mapping rules at Bob, the order of estimated channel gains at Alice should be the same as that of Bob. The orders of channel gains at Alice and Bob, respectively can be expressed as

$$|\hat{H}_T(\iota_{T,0})|^2 \ge |\hat{H}_T(\iota_{T,1})|^2 \ge \cdots \ge |\hat{H}_T(\iota_{T,N-1})|^2 \tag{20}$$

and

$$|\hat{H}_R(\iota_{R,0})|^2 \ge |\hat{H}_R(\iota_{R,1})|^2 \ge \cdots \ge |\hat{H}_R(\iota_{R,N-1})|^2. \tag{21}$$

If $\iota_{T,l} = \iota_{R,l}$ for $l = 0, 1, \cdots, N-1$, Alice and Bob can use the same mapping rules for IM and DSM. To obtain the probability that Bob has the same order of the channel gains as that of Alice, the correlation between the estimated CSI at Alice and Bob is to be taken into account. Thus, we write the estimated channel matrix at Bob as follows:

$$\hat{\mathbf{H}}_R = \hat{\mathbf{H}}_T + \mathbf{\Delta H}_{TR}, \tag{22}$$

where $\mathbf{\Delta H}_{TR} = \mathbf{\Delta H}_R - \mathbf{\Delta H}_T$ is the error matrix between the estimated channel matrices at Alice and Bob. Here, $\mathbf{\Delta H}_{TR}$ is a diagonal matrix whose diagonal elements follow a zero mean CSCG distribution with variance $\sigma_T^2 + \sigma_R^2$ (i.e., $\Delta H_{TR}(i) \sim \mathcal{CN}(0, \sigma_{TR}^2)$ for $i = 0, 1, \cdots, N-1$).

For simplicity, it is assumed that $\sigma_T^2 = \sigma_R^2$, $\sigma_{TR}^2 = \sigma_T^2 + \sigma_R^2$ and $Q = \frac{\sigma_{TR}^2}{\tilde{N}_0}$ [39]. Then, as mentioned in [29], the estimated

channel gain at Bob follows a noncentral chi-square distribution with 2 degrees of freedom. Let $\hat{\lambda}_{R,i} = |\hat{H}_R(i)|^2$ be the estimated channel gain of subcarrier i at Bob. Then, for a given estimated channel matrix at Alice, the conditional probability density function of the estimated channel gain at Bob is given by

$$f_{R,i}(\hat{\lambda}_{R,i}||\hat{H}_T(i)|^2) = \frac{1}{\sigma_{TR}^2} e^{-\left(\frac{|\hat{H}_T(i)|^2+\hat{\lambda}_{R,i}}{\sigma_{TR}^2}\right)} I_0\left(\Upsilon(\hat{\lambda}_{R,i})\right), \tag{23}$$

where $\Upsilon(\hat{\lambda}_{R,i}) = \frac{\sqrt{\hat{\lambda}_{R,i}|\hat{H}_T(i)|^2}}{2\sigma_{TR}^2}$ and $I_0(x) = \sum_{k=0}^{\infty} \frac{(x/2)^{2k}}{k!\Gamma(k+1)}$ is the modified Bessel function of the first kind. The conditional cumulative distribution function is also given by

$$F_{R,i}(\hat{\lambda}_{R,i}) = 1 - Q_1\left(\frac{\sqrt{2}|\hat{H}_T(i)|}{\sigma_{TR}}, \frac{\sqrt{2\hat{\lambda}_{R,i}}}{\sigma_{TR}}\right), \tag{24}$$

where $Q_\theta(a, b)$ is the Marcum Q-function.

Let $\Phi_T(D)$ and $\Phi_R(D)$ denote a random event for certain orders of D channel gains at Alice and Bob, respectively. Then, from [29], the probability that Bob has the same mapping rules as Alice based on $\hat{\mathbf{H}}_R$ is given by

$$P(\Phi_R(D)|\Phi_T(D)) = \frac{P(\Phi_R(D) \cap \Phi_T(D))}{P(\Phi_T(D))}. \tag{25}$$

For tractable analysis, it is assumed that all channel gains are independent. Then, $P(\Phi_T(D)) = \frac{1}{D!}$. As in [29], the probability of the events that the orders of the channel gains at Alice and Bob are the same can be given by

$$\begin{aligned} P(\Phi_R(D) \cap \Phi_T(D)) = &\int_{-\infty}^{\infty} \cdots \int_{\hat{\lambda}_{T,D-2}}^{\infty} f(\hat{\lambda}_{T,0}) \cdots f(\hat{\lambda}_{T,D-1}) \\ &\{\int_{-\infty}^{\infty} f_{R,0}(\hat{\lambda}_{R,0}) d\hat{\lambda}_{R,0} \cdots \\ &\int_{\hat{\lambda}_{R,D-2}}^{\infty} f_{R,D-1}(\hat{\lambda}_{R,D-1}) d\hat{\lambda}_{R,D-1}\} \\ &d\hat{\lambda}_{T,0} d\hat{\lambda}_{T,1} \cdots d\hat{\lambda}_{T,D-1}, \end{aligned} \tag{26}$$

where $\hat{\lambda}_{T,i} = |\hat{H}_T(i)|^2$ is the i-th estimated channel gain at Alice and follows an exponential distribution with parameter $\sigma_{\hat{H}_T}^2 = \sigma_H^2 + \sigma_T^2$. However, it is difficult to obtain a closed-form of the probability due to Bessel function. Instead, the probability can be obtained by using numerical integrations or Monte Carlo simulations. The numbers of the channel gains used for secure IM in a cluster and DSM in a subblock are n and κ, respectively. Then, the probabilities of the events that orders of the channel gains at Alice and Bob for secure IM and DSM, respectively, are the same can be given by $P_{IM} = P(\Phi_R(n)|\Phi_T(n))$ and $P_{DSM} = P(\Phi_R(\kappa)|\Phi_T(\kappa))$. Finally, the BER induced by mismatched mapping rules is given by

$$P_e^{B_2} = \frac{B_1}{B}(1 - P_{IM})e_{IM} + \frac{B_2}{B}(1 - P_{DSM})e_{DSM}, \tag{27}$$

where e_{IM} and e_{DSM} are the average BERs for IM and DSM, respectively, when Bob selects different mapping rules from those of Alice for IM and DSM with the estimated CSI.

Finally, the upper bound on the BER at Bob with imperfect CSI can be obtained by applying (17) and (27) to (13). Here, $P_e^{B_1}$ is sensitive to the SNR and channel estimation errors, while $P_e^{B_2}$ can be largely influenced by the number of active subcarriers and the channel estimation errors. More importantly, $P_e^{B_2}$ or e_{DSM} depends on the set of mapping rules, which is also true for Eve. Thus, it might be possible to design the set of mapping rules for more secure transmissions, which is studied in Section V.

IV. SECURITY ANALYSIS

In this section, the BER at Eve and a successful attack probability that Eve estimates the secure mapping rules in the proposed scheme, respectively, are analyzed to evaluate the security for the proposed scheme.

A. BIT ERROR RATE AT EVE FOR SECURITY ANALYSIS

In this subsection, for tractable analysis, we assume that for high SNR, the BER at Eve is computed as a security metric. Note that this is a quite favorable assumption for Eve. For high SNR, Eve is able to detect active subcarriers and their symbols with a high probability by the ML detection as follows:

$$\{\hat{i}_e, \hat{s}_e(i)\} = \arg \min_{i_e \in \mathcal{I},\ s_e(i) \in \mathcal{S}} \|\mathbf{y}_e - \mathbf{G}\mathbf{x}_F\|^2. \tag{28}$$

However, since the mapping rules for IM and DSM are not known to Eve, Eve has to choose certain mapping rules at random, which lead to incorrect decisions and a high BER.

1) BER OF SECURE IM

Unlike Bob, even though Eve can correctly detect the indices of active subcarriers and transmitted symbols thanks to a high SNR, Eve cannot correctly recover bits as the IM mapping rule is unknown. Suppose that the channels for Bob and Eve are perfectly independent. Denote by $P_e^{E_1}$ the error probability of IM bits at Eve. Based on the analysis in [34], it can be shown that $P_e^{E_1} = 0.5$. It is noteworthy that unlike the approach in [34], we have secure DSM through active subcarriers. In the next subsection, we study the security of secure DSM in terms of BER.

2) BER OF SECURE DSM

Given M-ary constellation, we can have $M!$ possible different mapping rules for secure DSM. In addition, since the order of the channel power gains is used as a secret key, there are $\kappa!$ possible keys in each subblock. Let L denote the number of symbol mapping rules used for secure DSM. Suppose that Eve knows the set of mapping rules for secure DSM by analyzing the received signals. For example, if Eve performs known plaintext attacks [40], she can easily estimate the set of mapping rules. It is a favorable assumption to Eve. For a given Eve's mapping rule, the BER for the DSM bits at Eve

is simply given by

$$P_e^{E_2} = \sum_{m=1}^{L} p_m P_{e_m}^{E_2}, \tag{29}$$

where $p_m = \frac{1}{L}$ is the probability[1] that the m-th mapping rule is selected for DSM among L mapping rules, $P_{e_m}^{E_2} = \frac{1}{\log_2 M}\rho_e^m$ is the conditional BER on the m-th mapping rule use, and ρ_e^m is the mean value of the number of mismatched bits per symbol between the m-th mapping rule and the mapping rule selected by Eve.

From (29), we can see that the BER at Eve is determined by the average number of mismatched bits. As the number of mismatched bits between the true mapping rule and the mapping rule selected by Eve increases, the BER at Eve should increase.

Denote by Λ the bit-mismatch matrix for a set of mapping rules, whose element is the number of mismatched bits between the m-th mapping rule and the p-th mapping rule which is denoted by $\Lambda_{m,p}$ for $m, p = 1, 2, \cdots, L$. Here, $\Lambda_{m,m} = 0$ and $\Lambda_{m,p} = \Lambda_{p,m}$. Then, we can represent the BER of DSM bits at Eve for a given set of mapping rules as follows:

$$P_e^{E_2} = \frac{1}{L^2 \log_2 M} \sum_{m=1}^{L} \sum_{p=1}^{L} \Lambda_{m,p}. \tag{30}$$

In (30), to obtain a high BER at Eve, we have to find the set of DSM mapping rules that have large $\Lambda_{m,p}$ for $m \neq p$.

In summary, from the analysis, we find the average BER for both IM and DSM bits at Eve as follows:

$$P_e^{E} = \left(\frac{B_1}{B_1 + B_2}\right) P_e^{E_1} + \left(\frac{B_2}{B_1 + B_2}\right) P_e^{E_2}, \tag{31}$$

where $P_e^{E_1}$ and $P_e^{E_2}$ are the BERs for the IM bits and the DSM bits, respectively. The BER of IM bits at Eve can converge to 0.5 under the independent channel scenario. However, the BER of DSM bits at Eve depends on the set of mapping rules which determines the values of $\Lambda_{m,p}$. Thus, it is important to design a set of mapping rules for secure DSM which is discussed in Section V.

B. SUCCESSFUL ATTACK PROBABILITY FOR SECURITY ANALYSIS

In this subsection, we analyze the successful attack probability that Eve estimates the secure mapping rules in the proposed OFDM-IM.

As mentioned earlier, although Eve can obtain correct indices and symbols by using ML detection with high computing power in the secure OFDM-IM, Eve cannot recover IM and DSM bits without secure mapping rules. So, Eve can attempt to perform attacks that Eve estimates the secure mapping rules. If the IM and DSM bits are unknown to Eve, the probabilities that Eve chooses the mapping rules for secure IM in one cluster and for secure DSM in one subblock, respectively, are given by $\frac{1}{2^{B_1}}$ and $\frac{1}{L}$. For example, if $N = 128, n = 4, \eta = 16, L = 2$ and $B_1 = 2$, the successful attack probability is given by $P_{S,A} = \left(\frac{1}{2^{B_1}}\right)^{\frac{N}{n}} \times \left(\frac{1}{L}\right)^{\eta} \approx 8 \times 10^{-25}$. It is negligibly small. However, if Eve knows the transmitted IM and DSM bits, Eve can perform known plaintext attacks which make the successful attack probability high. In particular, if IM bits are known to Eve, the mapping rule for secure IM can easily be estimated by Eve.

On the other hand, the proposed secure DSM can protect the attacks by exploiting a characteristic of OFDM-IM which uses a fraction of subcarriers for transmissions. Due to the change of active subcarrier indices, the mapping rules for secure DSM which are determined by the CSI of the active subcarriers can change for the coherence time. As mentioned earlier, if the CSI quickly changes with short coherence time, it can frequently update a secret key that it makes Eve's attacks difficult, while the channel reciprocity constraint may invalid with short coherence time. The proposed secure DSM scheme can make the CSI used as a secret key change dynamically for coherence time because the secret key is associated with the CSI of multiple active subcarriers that change in accordance with IM bit stream. This leads us to improve the above trade-off and makes the Eve's attack difficult.

To perform the successful attack in the proposed secure OFDM-IM, Eve has to estimate the secure mapping rules for all secret key changes which are determined with the active subcarrier indices in the proposed secure OFDM-IM. Then, for tractable analysis, we assume that the active subcarrier indices in one subblock are disjoint (i.e., there are disjoint 2^{WB_1} indices). It means that the possible number of secret key regeneration for the coherence time is 2^{WB_1}. In addition, Eve may need at least $\lceil \frac{M-1}{\kappa} \rceil$ disjoint constellations to estimate the mapping rule for secure DSM in one subblock. Thus, for a secure DSM mapping rule in one subblock, at least $\lceil \frac{M-1}{\kappa} \rceil 2^{WB_1}$ observations are required for the Eve's attack. On the other hand, if the secure DSM is applied to OFDM systems with η mapping rules for secure DSM, at least $\lceil \frac{M-1}{Wn} \rceil$ observations (i.e., only $\lceil \frac{M-1}{Wn} \rceil$ disjoint constellations) are required for the Eve's attack.

The average data symbol error probability [41] of classical M-ary PSK under perfect CSI is approximated by

$$P_M \approx \frac{\varsigma}{12}\left[\frac{1}{1 + \frac{nE_s\rho}{k\tilde{N}_0}} + \frac{3}{1 + \frac{4nE_s\rho}{3k\tilde{N}_0}}\right], \tag{32}$$

where $\rho = \sin^2(\frac{\pi}{M})$, $\varsigma = 1, 2$ for $M = 2$ and $M > 2$, respectively, and E_s is symbol energy. In this paper, we assume $E_s = 1$. Then, as shown in [41], an index error probability and a data symbol error probability at Eve caused by ML detection errors in the proposed secure OFDM-IM are

[1] We assume that Eve knows the set of mapping rules, but does not know which one is used for the DSM of a given subblock. Thus, we assume that Eve chooses one randomly and uniformly among L mapping rules.

approximated as follows:

$$P_I \approx \frac{\varphi}{12}\left\{\left[1+\frac{nE_s}{4k\tilde{N}_0}\right]^{-2}+3\left[1+\frac{nE_s}{3k\tilde{N}_0}\right]^{-2}\right\} \quad (33)$$

and

$$P_D = \left(1-\frac{1}{M}\right)P_I + P_M - P_I P_M, \quad (34)$$

where $\varphi = k(n-k)$. Then, the probability that Eve detects incorrect indices or data symbols in each cluster is approximated by

$$P_S \approx 1-(1-P_I)(1-P_D)^k. \quad (35)$$

From (35), the probability that Eve estimates a secure DSM mapping rule for each subblock with $\lceil\frac{M-1}{\kappa}\rceil 2^{WB_1}$ observations is approximated by

$$P_A \approx (1-P_S)^{W\lceil\frac{M-1}{\kappa}\rceil 2^{WB_1}}. \quad (36)$$

The independent $\eta(=\frac{N}{Wn})$ mapping rules are used for secure DSM in the proposed secure OFDM-IM. Then, from (36), the successful attack probability for all subblocks is approximated by

$$P_{S,A} \approx (1-P_S)^{\frac{N\lceil\frac{M-1}{\kappa}\rceil}{n}2^{WB_1}}. \quad (37)$$

From (37), we can find that the successful attack probability can significantly decrease with a large $\frac{N\lceil\frac{M-1}{\kappa}\rceil}{n}2^{WB_1}$. From this, although the modulation order is small (e.g., $M=2,4$), we can obtain low successful attack probability with large W (or B_1). However, note that from (27), the BER at Bob can be high with a large W due to channel estimation errors. Therefore, to make the Eve's attack difficult with reasonable reliability, it is desirable to have large N and B_1.

V. BIT-MISMATCH BASED SET OF MAPPING RULES FOR SECURE DSM SCHEME

In this section, we focus on developing a set of DSM mapping rules. In particular, to maximize the security performance, we intend to maximize the BER at Eve, and the performance criterion for the randomized DSM is derived in this section. We develop a bit-mismatch based set and a random-selection based set of mapping rules for secure DSM. Particularly, the bit-mismatch based set is designed to maximize the performance criterion and compared with the random-selection[2] based set.

[2]The performance of the random-selection based set will provide an average performance that can be achieved without any optimal design of the set of mapping rules for secure DSM. Thus, the performance of the random-selection based set can be used as a baseline performance to see the performance improvement by the bit-mismatch based set of mapping rules.

A. BIT-MISMATCH BASED SET

From (30), to obtain a high BER at Eve, we have to find the set of DSM mapping rules that have large $\Lambda_{m,p}$ for $m \neq p$. To this end, the mean of the elements, which is given by

$$\xi = \frac{1}{L^2}\sum_{m=1}^{L}\sum_{p=1}^{L}\Lambda_{m,p}, \quad (38)$$

is employed as the performance criterion for secure DSM in this subsection.

In the bit-mismatch based set of mapping rules, we choose the L best DSM mapping rules that maximize ξ among all possible $M!$ DSM mapping rules. Let $\mathbf{\Psi}$ denote the bit-mismatch matrix for all possible mapping rules whose element is the number of mismatched bits per symbol denoted by $\psi_{s,q}$ for $s,q = 1,2,\cdots,M!$. Let $\mathcal{A}$ denote the set of possible numbers of the mismatched bits between two different mapping rules. Then, the set of possible numbers of mismatched bits between two different mapping rules is given by

$$\mathcal{A} = \left\{\frac{2}{M},\cdots,\log_2 M\right\}. \quad (39)$$

Clearly, $\psi_{s,p} \in \mathcal{A}$ for $s \neq p$. The cardinality of the set for the possible number of mismatched bits is given by $|\mathcal{A}| = \frac{M}{2}\log_2 M$. From (39), $\Lambda_{m,p} \leq \log_2 M$ and $\Lambda_{m,p}+\Lambda_{m,a}+\Lambda_{a,p} \leq 2\log_2 M$ for $a = 1,\cdots,L$ due to the symmetric relationship between mapping rules. Then, the sum of the elements in the m-th row and the p-th column in Λ can be bounded as follows:

$$\Theta_{m,p} = \sum_{a=1}^{L}\Lambda_{m,a}+\sum_{b=1}^{L}\Lambda_{b,p} \leq L\log_2 M. \quad (40)$$

In (40), when $\Lambda_{m,p} = \log_2 M$, $\Lambda_{m,a}+\Lambda_{a,p} = \log_2 M$ due to the symmetric property of mapping rules. Then, if $\Lambda_{m,p} = \log_2 M$, $\Theta_{m,p} = L\log_2 M$ can be maximized. From this, we design the bit-mismatch based set of mapping rules whose each mapping rule has the complementary mapping rule in the set.

Let $\mathcal{M}_m^{\circ}$ denote the complementary mapping rule of the m-th mapping rule which has the largest mismatched bits (i.e., $\log_2 M$) with the m-th mapping rule among $M!$ possible mapping rules. For example, for 4-QAM, the m-th mapping rule and its complementary mapping rule, respectively, are given by $\mathcal{M}_m$: $[00] \rightarrow 1+j$, $[01] \rightarrow -1+j$, $[10] \rightarrow 1-j$, $[11] \rightarrow -1-j$ and $\mathcal{M}_m^{\circ}$: $[00] \rightarrow -1-j$, $[01] \rightarrow 1-j$, $[10] \rightarrow -1+j$, $[11] \rightarrow 1+j$. Each mapping rule among $M!$ possible mapping rules surely has one complementary mapping rule among them. Then, if L is an even number, there exist $\frac{L}{2}$ pairs of mapping rules in the bit-mismatch based set with $L \leq M!$. On the other hand, if L is an odd number, there exist $\frac{L-1}{2}$ pairs of mapping rules and one mapping rule without its the complementary mapping rule in the bit-mismatch based set. Then,

the bit-mismatch based set of mapping rule can maximize ξ as follows:

$$\xi = \frac{1}{2L^2}\sum_{m=1}^{L}\Theta_{m,L-m+1} \leq \begin{cases} \dfrac{\log_2 M}{2} & \text{if } L = 2l \\ \dfrac{\log_2 M}{2} - \dfrac{\log_2 M}{2L^2} & \text{if } L = 2l+1, \end{cases} \tag{41}$$

where the complementary mapping rule of the m-th mapping rule is the $(L-m+1)$-th mapping rule in the bit-mismatch set. As shown in (41), if L is an odd number, there might be a slight performance degradation due to one unpaired mapping rule. However, if L is not small, the performance degradation is negligible. Nevertheless, it is desirable to have an even L. From (30) and (41), when the bit-mismatch based set of mapping rules is used, the BER of DSM bits at Eve is given by

$$P_{e,b}^{E_2} = \begin{cases} \dfrac{1}{2} & \text{if } L = 2l \\ \dfrac{1}{2} - \dfrac{1}{2L^2} & \text{if } L = 2l+1. \end{cases} \tag{42}$$

Let us consider a simple example with 4-QAM, where $\mathcal{S} = \{\pm 1 \pm j\}$. If $L = 4$, there are $C(4!, 4)$ sets for the mapping rules. Among them, a set of mapping rules which maximizes the mean value of $\Lambda_{m,p}$ is as follows:

$$\begin{aligned} \mathcal{M}_1 &: [00] \to 1+j, [01] \to -1+j, [10] \\ &\quad \to 1-j, [11] \to -1-j, \\ \mathcal{M}_2 &: [00] \to -1+j, [01] \to 1+j, [10] \\ &\quad \to -1-j, [11] \to 1-j, \\ \mathcal{M}_3 &: [00] \to 1-j, [01] \to -1-j, [10] \\ &\quad \to 1+j, [11] \to -1+j, \\ \mathcal{M}_4 &: [00] \to -1-j, [01] \to 1-j, [10] \\ &\quad \to -1+j, [11] \to 1+j, \end{aligned}$$

where $\mathcal{M}_3 = \mathcal{M}_2^{\circ}$ and $\mathcal{M}_4 = \mathcal{M}_1^{\circ}$. Then, for this set of mapping rules, the bit-mismatch matrix is given by

$$\Lambda = \begin{bmatrix} 0 & 1 & 1 & 2 \\ 1 & 0 & 2 & 1 \\ 1 & 2 & 0 & 1 \\ 2 & 1 & 1 & 0 \end{bmatrix} \tag{43}$$

with $\xi = 1$. From (30), we can obtain $P_{e,b}^{E_2} = 0.5$. Thus, although Eve can detect the transmitted symbols and know the set of the selected mapping rules, the BER at Eve can be high as she does not know which DSM mapping rule is actually used by Alice.

B. RANDOM-SELECTION BASED SET

It is also possible to consider a set of mapping rules that are randomly selected. This may provide an average performance without any optimal design for the set of mapping rules for secure DSM (e.g., the bit-mismatch based set). In the random-selection based set of mapping rules, we randomly select L mapping rules among all $M!$ possible DSM mapping rules regardless of the number of mismatched bits. Thus, Λ is random and we have to find the mean of Λ for all different mapping rules. Then, the mean of $\mathbf{\Lambda}$ is given by

$$\mathbb{E}[\Lambda_{m,p}] = \begin{cases} 0, & \text{if } m = p, \\ \omega, & \text{otherwise.} \end{cases} \tag{44}$$

To find ω, we select a certain mapping rule and compute the number of mismatched bits with all other mapping rules. As mentioned earlier, $\mathbf{\Psi}$ is considered to compute the number of mismatched bits for all possible mapping rules. For example, for 4-QAM, $\mathcal{A} = \{0.5, 1, 1.5, 2\}$, as shown in TABLE 1. Due to the symmetric property of $\psi_{s,q}$, the mean of the number of mismatched bits is given by

$$\mathbb{E}[\psi_{s,q}] = \frac{\log_2 M}{2}. \tag{45}$$

From (45), for given s, $\sum_{q=1}^{M!}\psi_{s,q} = \frac{M!\log_2 M}{2}$. Then, ω can be found as

$$\omega = \frac{1}{M!-1}\sum_{q\neq s}\psi_{s,q} = \frac{M!\log_2 M}{2(M!-1)}, \tag{46}$$

where $\sum_{q\neq s}\psi_{s,q} = \sum_{q=1}^{M!}\psi_{s,q}$ because of $\psi_{s,s} = 0$. Then, from (44) and (46), the sum of all elements of $\mathbb{E}[\Lambda]$ becomes

$$\sum_{m=1}^{L}\sum_{p=1}^{L}\mathbb{E}\left[\Lambda_{m,p}\right] = \frac{L(L-1)M!\log_2 M}{2(M!-1)}. \tag{47}$$

Thus, from (30), the BER at Eve with the random-selection based set of mapping rules is given by

$$P_{e,r}^{E_2} = \frac{(L-1)M!}{2L(M!-1)}. \tag{48}$$

TABLE 1. The number of mapping rules denoted by Ω for different number of mismatched bits among all possible mapping rules, when $M = 4$.

$\psi_{s,q}$	0	0.5	1	1.5	2
Ω	1	4	13	4	1

TABLE 2. The number of mapping rules denoted by Ω for different number of mismatched bits among all possible mapping rules, when $M = 8$.

$\psi_{s,q}$	0	0.25	0.5	0.75	1
Ω	1	12	114	876	3,855
$\psi_{s,q}$	1.25	1.5	1.75	2	2.25
Ω	9,096	12,412	9,096	3,855	876
$\psi_{s,q}$	2.5	2.75	3		
Ω	114	12	1		

For example, for 4-QAM, the BER at Eve with the random-selection based mapping rules becomes $P_{e,r}^{E_2} = \frac{12(L-1)}{23L}$. On the other hand, if M, which is a power of 2, is high (e.g., 8, 16 and so on), the BER at Eve can be represented as follows:

$$P_{e,r}^{E_2} = \frac{1}{2} - \frac{1}{2L}. \tag{49}$$

From (48) and (49), it can be found that as the size of the random-selection based set of mapping rules, L increases, the BER at Eve increases. This implies that with the larger set of DSM mapping rules, the better security for DSM Alice and Bob can have. In addition, from (48), if $L = M!$, then it is shown that $P_{e,r}^{E_2} = 0.5$.

In summary, we design the bit-mismatch based set of mapping rules for secure DSM which maximizes the performance criterion, ξ. From (42) and (49), we can see that the bit-mismatch based set of mapping rules can provide an improved performance compared with the average performance that can be obtained by the random-selection based set of mapping rules.

VI. SIMULATION RESULTS

In this section, we present simulation results with two different channels: one is the channel where all the frequency-domain channel coefficients are independent and the other is a more realistic one, where the frequency-domain channel coefficients are correlated as the length of CIR, ν, is shorter than the number of subcarriers, N. The former channel is ideal as the equivocation of the secret key from the CSI between Alice and Bob can be maximized. In addition, we show experimental results obtained using a software defined radio (SDR) platform.

A. COMPUTER SIMULATION RESULTS

In this subsection, we present simulation results to see the performance of the proposed secure OFDM-IM system in terms of BER. For simulations, we assume that $n = 4$, $k = 2$, $N = 128$, $N_{cp} = \nu + 6$ and $\sigma_H^2 = \sigma_G^2 = 1$. In addition, the SNR is defined as follows: $SNR = \frac{E_b}{N_0}$, where $E_b = (N + N_{cp})/m$ denotes the bit energy and N_0 represents the noise variance in the time domain, which is given by $N_0 = \left(\frac{N}{K}\right)\tilde{N}_0$.

Fig. 3 shows the BER of DSM bits at Eve with respect to SNR when $W = 2$ and $L = 2$. In this figure, as the SNR increases, the BER of the conventional scheme in [34], which only has secure IM, rapidly decreases, while the proposed scheme can maintain a high BER at Eve regardless of SNR because of the bit-mismatch between randomized mapping rule at Alice and an arbitrarily selected mapping rule at Eve for the secure DSM. According to (48), if the channels are independent, the BERs associated with the random-selection based set of mapping rules for $M = 4$ and $M = 8$ converge to 0.2609 and 0.25, respectively, as SNR $\rightarrow \infty$. This can be confirmed by the simulation results in Fig. 3. In addition, from (42), the BERs associated with the bit-mismatch based

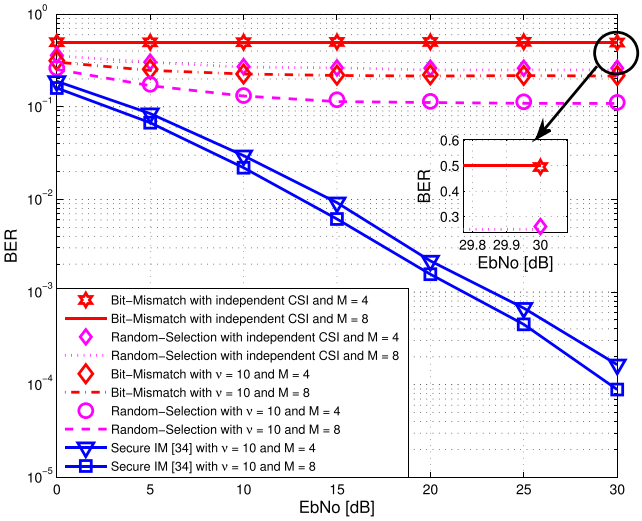


FIGURE 3. BER of DSM bits at Eve for different SNR with perfect CSI, where $W = 2$ and $L = 2$.

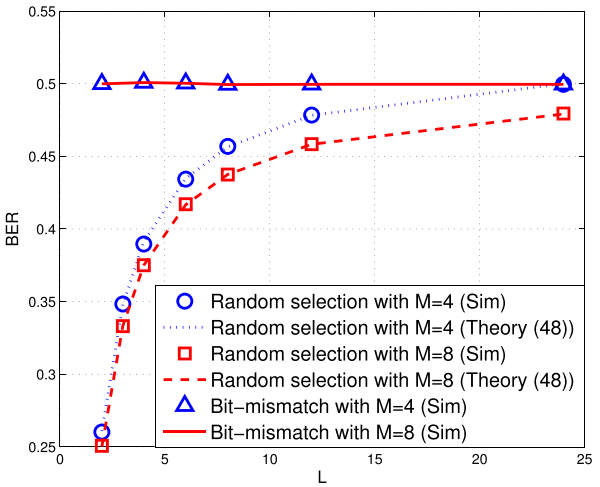


FIGURE 4. BER of DSM bits at Eve for different size of set of mapping rules denoted by L with perfect CSI where $W = 2$, $M = 4$ and SNR = 30dB.

set of mapping rules are always 0.5 with $L = 2$. However, in a practical case where $\nu = 10$, as shown in the figure, slightly lower BERs at Eve than theoretical results which are obtained with independent channels can be obtained. This shows that the channel correlation degrades the performance of secure OFDM-IM.

In Fig. 4, we show the simulation results for the BERs of DSM bits at Eve for different values of L when $W = 2$, $M = 4$ and SNR = 30dB. To see the impact of L on the BER, it is assumed that the channel coefficients are independent in this simulation. As the size of the set of mapping rules, L, increases, the BER at Eve increases for the random-selection based set of mapping rules. Furthermore, for a smaller M, a higher BER at Eve can be obtained for a fixed L in the random-selection based set of mapping rules. As shown in (48), if $L = M!$, the random-selection based

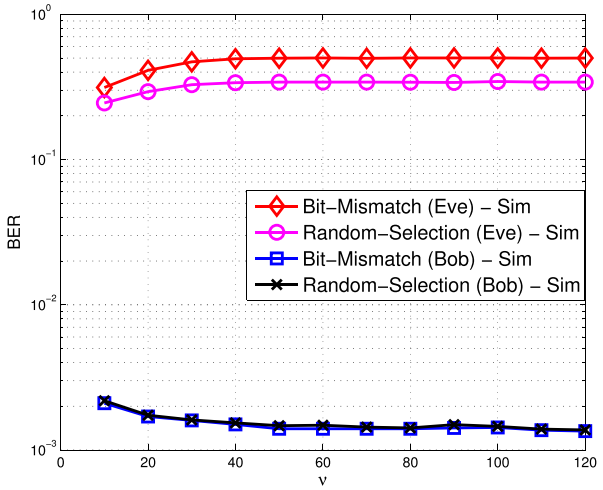


FIGURE 5. BER of both IM bits and DSM bits at Bob and Eve for different number of taps denoted by ν with perfect CSI, where $W = 2$, $M = 4$, $L = 2$ and SNR = 20dB.

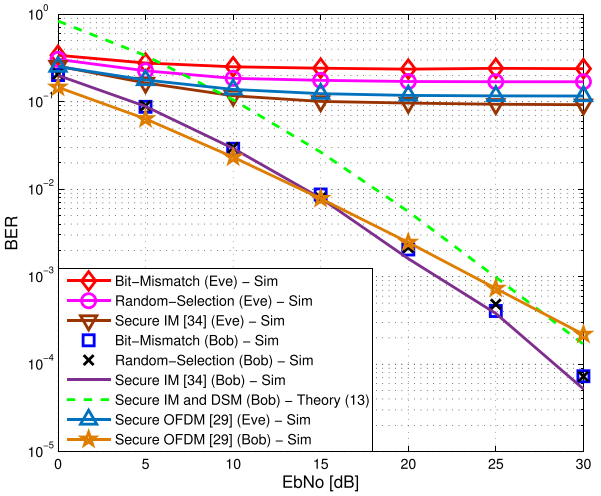


FIGURE 6. BER of both IM bits and DSM bits at Bob and Eve for different SNR with perfect CSI, where $W = 2$, $M = 4$, $\nu = 10$, $P = 16$ and $L = 2$.

set results in a BER of 0.5 at Eve as explained in Section V. But, L should be less than or equal to the length of the secret key, $\kappa!$. In the proposed OFDM-IM, the number of active subcarriers in a subblock, κ, may be small. Thus, we may have $\kappa! < M!$. In this case, the random-selection based set does not allow us to achieve a high BER at Eve. On the other hand, the bit-mismatch based set of mapping rules can maintain a high BER (i.e., 0.5) when L is an even number as shown in Fig. 4. Consequently, it is necessary to use the proposed bit-mismatch based set of mapping rules for secure OFDM-IM.

In Fig. 5, we display the BER of both IM bits and DSM bits at Bob and Eve for different values of ν in order to see the impact of the length of CIR, ν, on the secrecy in terms of the BER at Eve when $W = 2$, $M = 4$, $L = 2$ and SNR = 20dB. Particularly, the proposed scheme that uses the channels in the frequency domain as a secret key is influenced by the length of CIR in terms of security. In addition, as shown in [3], it can also affect the reliability which is evaluated in terms of the BER at Bob. Since the ordering pattern of the channel gains is diversified with the independence of the channels, it increases the probability that Eve chooses an incorrect mapping rule in the proposed scheme. In OFDM-IM, the performance gap caused by a low ν may be small because it only uses a subset of subcarriers. In this figure, it can be found that as the length of CIR increases, the BER at Eve slightly increases, while the BER at Bob decreases, which demonstrates that a large ν is desirable.

In Fig. 6, we show the simulation results for the BER of both IM and DSM bits at Bob and Eve for various values of SNR when perfect CSI is assumed with $W = 2$, $M = 4$, $\nu = 10$, $P = 16$ and $L = 2$. As shown in this figure, the BER at Bob of the proposed scheme is slightly higher than that of the conventional OFDM-IM because the set of mapping rules in the proposed scheme cannot always use the gray mapping. In addition, the BER of the OFDM-IM scheme is lower than or equal to that of the OFDM with the same spectral efficiency (1.7778 bits/s/Hz). However, the proposed scheme has a significant performance improvement in terms of the BER at Eve while the conventional secure schemes in [29] and [34] can have a relatively low BER at Eve. Especially, the bit-mismatch based set which is designed to maximize the bit mismatch in secure DSM has a remarkable performance improvement in terms of the BER at Eve. In detail, the BERs at Eve with the random-selection and the bit-mismatch based sets converge to about 0.16 and 0.23 as SNR $\rightarrow \infty$, respectively (which are lower than theoretical values (0.34 and 0.5) from (31) due to the correlation of frequency domain channel coefficients). Consequently, we observe the secure IM and DSM with perfect CSI has a better performance than the conventional schemes [29] and [34] in terms of security while maintaining almost the same reliability.

Fig. 7 shows the BER of both IM and DSM bits at Bob and Eve with respect to SNR with imperfect CSI when $W = 2$, $M = 4$, $\nu = 10$, $Q = 1/2$, $P = 16$ and $L = 2$. Under a practical channel estimation scenario, the proposed scheme is evaluated in this simulation to see BER. In addition, we compare the BERs at Bob and Eve of the proposed scheme with the secure OFDM approach in [29]. In the secure OFDM, both Alice and Bob select not only the indices of the interleaved subcarriers but also the interleaved pattern with imperfect CSI. Obviously, the BER at Bob increases due to the channel estimation errors. Especially, the BER at Bob of the secure OFDM is slightly lower than that at Eve due to mismatched indices of interleaved subcarriers and wrong interleaved patterns caused by channel estimation errors. Similarly, the BER at Bob of the proposed scheme also increases because of mismatched mapping rules due to channel estimation errors. Meanwhile, the BER at Eve of the proposed scheme is still higher than that of the secure OFDM scheme in [29]. Thus, the proposed scheme has a better performance than the secure OFDM scheme in terms of security under practical channel estimation scenarios with similar reliability.

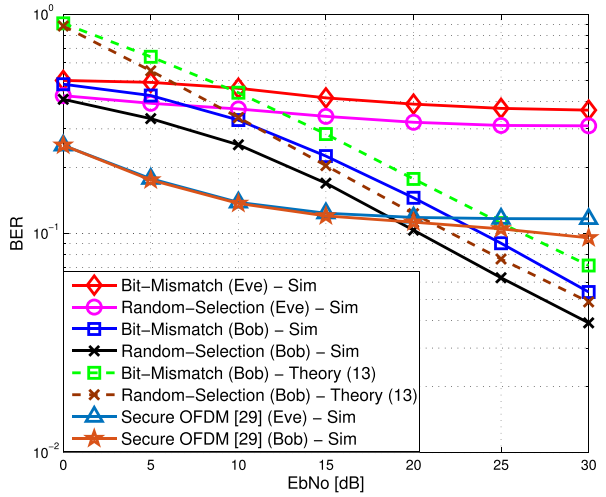
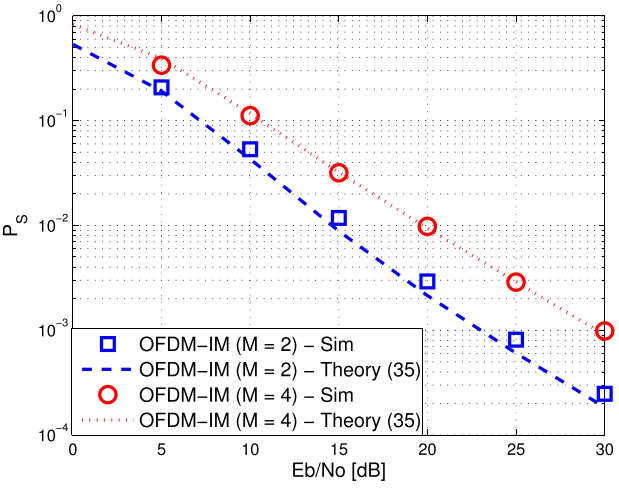


FIGURE 7. BER of both IM bits and DSM bits at Bob and Eve for different SNR with imperfect CSI, where $W = 2$, $M = 4$, $\nu = 10$, $Q = 1/2$, $P = 16$ and $L = 2$.

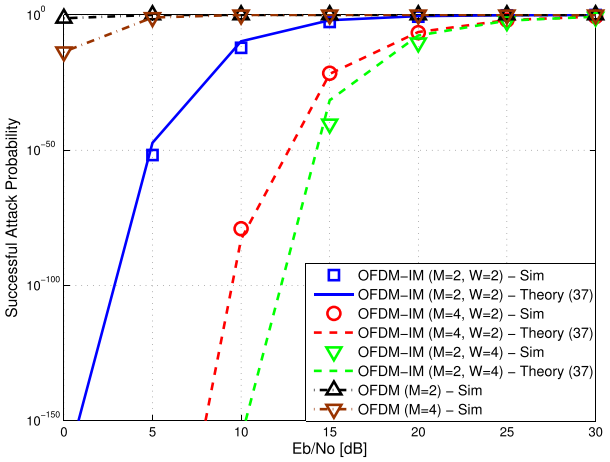
In Fig. 8, we show the impact of various parameters (i.e., M, W and SNR) on the successful attack probability when $L = M!$. In Fig. 8 (a), the probability that Eve detects incorrect indices or data symbols in one cluster is shown for various SNR. As shown in this figure, a high modulation order and a low SNR make the probability high. From (37), the probability significantly influences to the successful attack probability because Eve should detect the correct indices and symbols to estimate secure mapping rules. In Fig. 8 (b), we show the simulation results for the successful attack probability for various SNR. We compare the successful attack probability of the secure OFDM-IM with that of the secure OFDM with the secure DSM scheme. As mentioned in subsection IV.B, at least $\lceil \frac{M-1}{\kappa} \rceil 2^{WB_1}$ observations are required for the Eve's attack in the secure OFDM-IM, while at least $\lceil \frac{M-1}{Wn} \rceil$ observations are required for the attack in the secure OFDM. Due to the large number of observations, the secure OFDM-IM can obtain a much lower successful attack probability than that of the secure OFDM. Furthermore, in the secure OFDM-IM, the successful attack probability can be reduced with large W and M. In particular, as shown in this figure, W has a significant impact on the successful attack probability. That is, although the modulation order is small (e.g, $M = 2$), a large W results in a low successful attack probability.

B. EXPERIMENTAL RESULTS

In this subsection, experimental results are provided to validate the proposed secure OFDM-IM scheme by using the USRP which is a SDR hardware platform. The USRP is a flexible and low cost platform developed by National Instruments (NI). We have used two NI USRPs whose model is the USRP-2943R and a vector signal analyzer (VSA) which plays a role as a computer to control the USRPs, as shown in Fig. 9. In addition, we use channel simulator which simulates



(a)



(b)

FIGURE 8. Performances for various values of SNR, where $L = M!$; (a) the probability of incorrect indices or data symbols in one cluster; (b) the probability of successful attack by Eve.

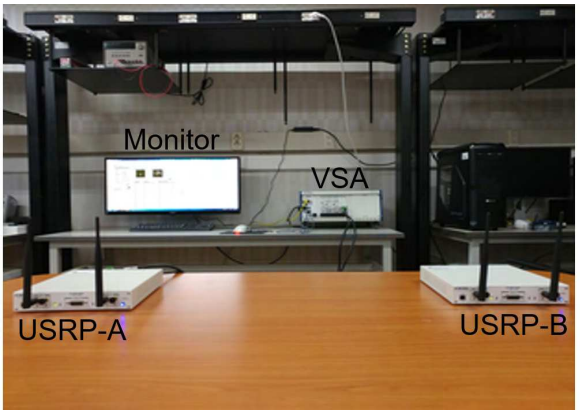


FIGURE 9. USRP experiment environment for the secure OFDM-IM.

outdoor channels from the USRP because an indoor channel in our experimental environment which is similar to a flat channel (i.e., $\nu = 1$ or 2) cannot be used as a secret key in

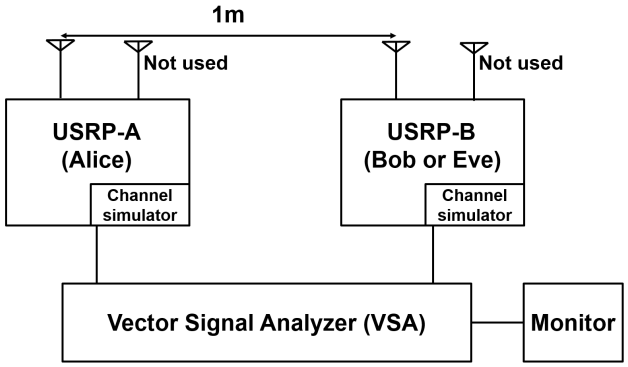


FIGURE 10. Block diagram of the USRP experiment for the secure OFDM-IM.

TABLE 3. Simulation parameters.

Number of total subcarriers (N)	128
Receiver power gain	2dB
IQ rate	390 kHz
Number of subcarriers in a cluster (n)	4
Number of active subcarriers in a cluster (k)	2
Number of clusters in a subblock (W)	2
Number of mapping rules in a set (L)	2
Modulation order (M)	4
Communication distance	1m
Subcarrier spacing	1.52 kHz
Carrier Frequency	1.5 GHz

the secure OFDM-IM. In addition, we assume that channel coefficients which are generated by the channel simulator are perfectly shared between Alice and Bob. As shown in Fig. 10, USRP-A and USRP-B play roles as Alice and Bob (or Eve), respectively. In experimental simulations, simulation parameters are given in Table. 3.

In Figs. 11 and 12, the experimental results by using the USRPs are shown to validate the proposed secure OFDM-IM. Fig. 11 shows the BER of IM and DSM bits at Bob and Eve with respect to a transmission power gain in the

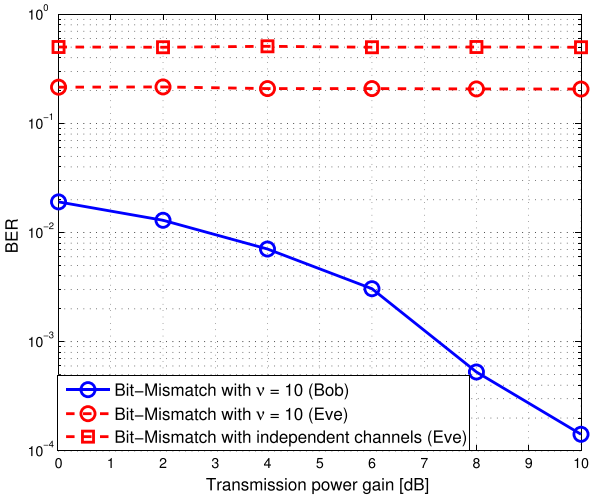


FIGURE 11. BER of both IM bits and DSM bits at Bob and Eve for different transmission power gain in the USRP experiment.

USRP-A when the bit-mismatch based set is used. As shown in this figure, under the ideal channel condition (i.e., all the channel coefficients are independent) which are generated by the channel simulator, the BER at Eve can be maximized (i.e., 0.5) regardless of the transmission power gain. In addition, under the practical channel condition with $\nu = 10$, as the transmission power gain increases, the BER at Eve is kept to about 0.2 regardless of the transmission power gain while the BER at Bob decreases. Consequently, the experimental results confirm the validation of the secure OFDM-IM.

In Fig. 12, we depict the transmitted thermal infrared image [42] whose size is 256 × 256 pixels from Alice and recovered thermal infrared images at Bob and Eve, respectively, when the transmission power gain is 4dB and $\nu = 10$. As mentioned earlier, the OFDM-IM can be suitable for applications where transmitters and receivers have various implementation constraints in terms of complexity. In the simulation, we assume that the infrared sensor (Alice) which is a small device with low complexity transmits an infrared image to an access point (Bob) with the secure OFDM-IM in the presence of an eavesdropper (Eve). From the figure, we can find that the recovered image at Bob is almost same with that of Alice although the negligible noise exists. On the

FIGURE 12. Thermal infrared images at Alice, Bob and Eve, respectively, where the transmission power gain is 4dB.

other hand, the recovered image at Eve is very noisy. In summary, we can see that under the thermal infrared transmission scenario, Bob can correctly detect the confidential data (i.e., the infrared image) from the received signal with the secure OFDM-IM, while Eve obtains almost useless data from the received signal.

VII. CONCLUSION

We have proposed the secure IM and DSM for OFDM-IM systems. Unlike the conventional scheme which only has secure IM, the proposed scheme was able to protect DSM bits as well as IM bits based on the randomized mapping rule with the use of the CSI between Alice and Bob. Most remarkably, the CSI associated with active subcarriers can be used as a secret key to enhance the security of DSM in the proposed secure OFDM-IM. It makes the Eve's attack difficult by changing the secret key for the coherence time. In addition, to design a set of mapping rules for secure DSM, we studied the random-selection based set of mapping rules and the bit-mismatch based set of mapping rules. In the bit-mismatch based set of mapping rules, we proposed a performance criterion to choose the mapping rules that can increase the BER at Eve. Eventually, it was ensured to make the BER at Eve the worst (i.e., 0.5). From the analysis and simulation results, we have shown that the proposed secure IM and DSM scheme for OFDM-IM systems outperforms the conventional scheme in terms of security.

REFERENCES

[1] E. Ba ar, "Index modulation techniques for 5G wireless networks," *IEEE Commun. Mag.*, vol. 54, no. 7, pp. 168–175, Jul. 2016.

[2] R. Y. Mesleh, H. Haas, S. Sinanovic, C. W. Ahn, and S. Yun, "Spatial modulation," *IEEE Trans. Veh. Technol.*, vol. 57, no. 4, pp. 2228–2241, Jul. 2008.

[3] E. Ba ar, Ü. Aygölü, E. Panayırci, and H. V. Poor, "Orthogonal frequency division multiplexing with index modulation," *IEEE Trans. Signal Process.*, vol. 61, no. 22, pp. 5536–5549, Nov. 2013.

[4] R. Abu-Alhiga and H. Haas, "Subcarrier-index modulation OFDM," in *Proc. IEEE 20th Int. Symp. Pers., Indoor Mobile Radio Commun.*, Sep. 2009, pp. 177–181.

[5] D. Tsonev, S. Sinanovic, and H. Haas, "Enhanced subcarrier index modulation (SIM) OFDM," in *Proc. IEEE GLOBECOM Workshops (GC Wkshps)*, Dec. 2011, pp. 728–732.

[6] N. Ishikawa, S. Sugiura, and L. Hanzo, "Subcarrier-index modulation aided OFDM—Will it work?" *IEEE Access*, vol. 4, pp. 2580–2593, 2016.

[7] J. Crawford and Y. Ko, "Low complexity greedy detection method with generalized multicarrier index keying OFDM," in *Proc. IEEE 26th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Aug./Sep. 2015, pp. 688–693.

[8] J. Zheng and R. Chen, "Achieving transmit diversity in OFDM-IM by utilizing multiple signal constellations," *IEEE Access*, vol. 5, pp. 8978–8988, 2017.

[9] S. G. Domouchtsidis, G. D. Ntouni, V. M. Kapinas, and G. K. Karagiannidis, "OFDM-IM vs FQAM: A comparative analysis," in *Proc. IEEE 23rd Int. Conf. Telecommun. (ICT)*, May 2016, pp. 1–5.

[10] E. Ba ar, "On multiple-input multiple-output OFDM with index modulation for next generation wireless networks," *IEEE Trans. Signal Process.*, vol. 64, no. 15, pp. 3868–3878, Aug. 2016.

[11] J. Choi, "Coded OFDM-IM with transmit diversity," *IEEE Trans. Commun.*, vol. 65, no. 7, pp. 3164–3171, Jul. 2017.

[12] J. Choi, *Adaptive and Iterative Signal Processing in Communications*. Cambridge, U.K.: Cambridge Univ. Press, 2006.

[13] Y. Ko, "A tight upper bound on bit error rate of joint OFDM and multicarrier index keying," *IEEE Commun. Lett.*, vol. 18, no. 10, pp. 1763–1766, Oct. 2014.

[14] T. Mao, Z. Wang, Q. Wang, S. Chen, and L. Hanzo, "Dual-mode index modulation aided OFDM," *IEEE Access*, vol. 5, pp. 50–60, 2017.

[15] T. Mao, Q. Wang, and Z. Wang, "Generalized dual-mode index modulation aided OFDM," *IEEE Commun. Lett.*, vol. 21, no. 4, pp. 761–764, Apr. 2017.

[16] W. Stallings and M. P. Tahiliani, *Cryptography and Network Security: Principles and Practice*, vol. 6. London, U.K.: Pearson, 2014.

[17] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[18] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[19] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[20] A. Mukherjee, "Physical-layer security in the Internet of Things: Sensing and communication confidentiality under resource constraints," *Proc. IEEE*, vol. 103, no. 10, pp. 1747–1761, Oct. 2015.

[21] J. Choi, J. Ha, and H. Jeon, "Physical layer security for wireless sensor networks," in *Proc. IEEE 24th Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2013, pp. 1–6.

[22] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Commun.*, vol. 18, no. 4, pp. 6–12, Aug. 2011.

[23] F. Renna, N. Laurenti, and H. V. Poor, "Physical-layer secrecy for OFDM transmissions over fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 4, pp. 1354–1367, Aug. 2012.

[24] C.-Y. Wu, P.-C. Lan, P.-C. Yeh, C.-H. Lee, and C.-M. Cheng, "Practical physical layer security schemes for MIMO-OFDM systems using precoding matrix indices," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1687–1700, Sep. 2013.

[25] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Physical layer security of MIMO–OFDM systems by beamforming and artificial noise generation," *Phys. Commun.*, vol. 4, no. 4, pp. 313–321, 2011.

[26] X. Wang, M. Tao, J. Mo, and Y. Xu, "Power and subcarrier allocation for physical-layer security in OFDMA-based broadband wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 693–702, Sep. 2011.

[27] M. Bouanen, F. Gagnon, G. Kaddoum, D. Couillard, and C. Thibeault, "An LPI design for secure OFDM systems," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, Oct./Nov. 2012, pp. 1–6.

[28] D. Luengo and I. Santamaria, "Secure communications using OFDM with chaotic modulation in the subcarriers," in *Proc. IEEE 61st Veh. Technol. Conf. (VTC-Spring)*, vol. 2. May 2005, pp. 1022–1026.

[29] H. Li, X. Wang, and J. Y. Chouinard, "Eavesdropping-resilient OFDM system using sorted subcarrier interleaving," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 1155–1165, Feb. 2015.

[30] L. Wang, S. Bashar, Y. Wei, and R. Li, "Secrecy enhancement analysis against unknown eavesdropping in spatial modulation," *IEEE Commun. Lett.*, vol. 19, no. 8, pp. 1351–1354, Aug. 2015.

[31] F. Wu, R. Zhang, L.-L. Yang, and W. Wang, "Transmitter precoding-aided spatial modulation for secrecy communications," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 467–471, Jan. 2016.

[32] X. Guan, Y. Cai, and W. Yang, "On the secrecy mutual information of spatial modulation with finite alphabet," in *Proc. IEEE Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Oct. 2012, pp. 1–4.

[33] S. R. Aghdam, T. M. Duman, and M. Di Renzo, "On secrecy rate analysis of spatial modulation and space shift keying," in *Proc. IEEE Int. Black Sea Conf. Commun. Netw. (BlackSeaCom)*, May 2015, pp. 63–67.

[34] X. Wang, X. Wang, and L. Sun, "Spatial modulation aided physical layer security enhancement for fading wiretap channels," in *Proc. IEEE 8th Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Oct. 2016, pp. 1–5.

[35] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[36] M. Baldi, M. Bianchi, and F. Chiaraluce, "Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: A security gap analysis," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 883–894, Jun. 2012.

[37] Y. S. Cho, J. Kim, W. Y. Yang, and C. G. Kang, *MIMO-OFDM Wireless Communications With MATLAB*. Hoboken, NJ, USA: Wiley, 2010.

[38] J. Choi, *Optimal Combining and Detection: Statistical Signal Processing for Communications*. Cambridge, U.K.: Cambridge Univ. Press, 2010.
[39] P. Sure and C. M. Bhuma, "A survey on OFDM channel estimation techniques based on denoising strategies," *Eng. Sci. Technol., Int. J.*, vol. 20, no. 2, pp. 629–636, 2017.
[40] Y. Zheng, M. Schulz, W. Lou, Y. T. Hou, and M. Hollick, "Highly efficient known-plaintext attacks against orthogonal blinding based physical layer security," *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, pp. 34–37, Feb. 2015.
[41] T. Van Luong and Y. Ko, "Impact of CSI uncertainty on MCIK-OFDM: Tight, closed-form symbol error probability analysis," *IEEE Trans. Veh. Technol.*, to be published.
[42] J. Portmann, S. Lynen, M. Chli, and R. Siegwart, "People detection and tracking from aerial thermal views," in *Proc. IEEE Int. Conf. Robot. Autom. (ICRA)*, May/Jun. 2014, pp. 1794–1800.

YONGGU LEE received the B.E. degree in electronics engineering from Kyungpook National University, Daegu, South Korea, and the M.S. degree in electrical engineering and computer science from the Gwangju Institute of Science and Technology, Gwangju, South Korea, in 2016, where he is currently pursuing the Ph.D. degree with the School of Electrical Engineering and Computer Science. His research interests include the areas of communications and signal processing, with emphasis on physical layer security, 5G communication systems, and machine type communications.

HANSEONG JO received the B.E. degree in electronic communication engineering from Hanyang University, Ansan, South Korea, in 2016. He is currently pursuing the M.S. degree with the School of Electrical Engineering and Computer Science, Gwangju Institute of Science and Technology. His research interests include the areas of communications and signal processing, with emphasis on physical layer security, 5G communication systems, and machine type communications.

YOUNGWOOK KO received the B.S.E. degree in information and communications engineering from Hannam University, South Korea, and the M.S. and Ph.D. degrees in electrical engineering from Arizona State University, Tempe, AZ, USA, in 2002 and 2006, respectively. He was a Senior Researcher with Samsung for two years. In 2008, he was with the Electrical and Computer Engineering Department, University of Alberta, Canada. From 2010 to 2013, he was a Senior Research Fellow with CCSR, University of Surrey, U.K. Since 2013, he has been with the ECIT Institute, Queen's University of Belfast, as a Lecturer. He is a pioneer of index modulation techniques, and his current research is in the areas of index modulation OFDM, sporadic machine type communications, physical wireless security, and the next generation wireless manufacturing systems. He has authored over 40 publications in major IEEE international journals, and peer-reviewed international conferences. He is a member of the EPSRC Peer-Review Associate College and on the Editorial Board of the *Elsevier Journal on Physical Communications*. He was a recipient of several EPSRC and Newton projects, such as the EPSRC First Grant Award and the EPSRC IDS.

JINHO CHOI (SM'02) was born in Seoul, South Korea. He received the B.E. degree *(magna cum laude)* in electronics engineering from Sogang University, Seoul, in 1989, and the M.S.E. and Ph.D. degrees in electrical engineering from the Korea Advanced Institute of Science and Technology in 1991 and 1994, respectively. He was with the College of Engineering, Swansea University, U.K., as a Professor/Chair in wireless. He is with the Gwangju Institute of Science and Technology as a Professor. He has authored two books published by Cambridge University Press in 2006 and 2010. His research interests include wireless communications and array/statistical signal processing. He received the 1999 Best Paper Award for Signal Processing from EURASIP, the 2009 Best Paper Award from WPMC (Conference). He is currently an Editor of the IEEE TRANSACTIONS COMMUNICATIONS and the IEEE WIRELESS COMMUNICATIONS LETTERS and had served as an Associate Editor or Editor of other journals including the IEEE COMMUNICATIONS LETTERS, the *Journal of Communications and Networks*, the IEEE TRANSACTIONS VEHICULAR TECHNOLOGY, and the ETRI journal.