sensors

MDPI

Article

A Random Subcarrier-Selection Method Based on Index Modulation for Secure Transmission

Tao Zhan [1], Jiangong Chen [1], Shan Luan [2] and Xia Lei [1,*]

[1] National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China (UESTC), Chengdu 611731, China; ztzs1998@163.com (T.Z.); jg_chen1997@163.com (J.C.)
[2] China Academy of Space Technology (CAST), Beijing 100192, China; luanshanhrb@163.com
* Correspondence: leixia@uestc.edu.cn

Abstract: Recently, a frequency diverse array (FDA) has been employed in an orthogonal frequency division multiplexing (OFDM) transmitter to achieve secure wireless communication without mathematical encryption. However, an insecure coupling effect arises if the frequency increments are linearly assigned to all antenna elements. To solve this problem, random subcarrier-selection methods are proposed; however, the challenge lies in the random selection of subcarriers. Inspired by the randomness of index modulation (IM), this paper proposes a low complexity random subcarrier-selection method based on index modulation (RSCS-IM). Specifically, this work conducted analysis on the spectral efficiency (SE) of our system and the computational complexity of RSCS-IM, which works out a closed-form expression of the BER performance of a desired position and validates the theoretical outcomes through simulation.

Keywords: FDA; OFDM; random subcarrier-selection; secure communication; index modulation

Citation: Zhan, T.; Chen, J.; Luan, S.; Lei, X. A Random Subcarrier-Selection Method Based on Index Modulation for Secure Transmission. *Sensors* **2022**, *22*, 2676. https://doi.org/10.3390/s22072676

Academic Editor: Michael Cheffena

Received: 19 January 2022
Accepted: 21 March 2022
Published: 31 March 2022

1. Introduction

1.1. Problem Formulation

Wireless communication plays an important role in today's communication systems. However, since the open nature of the environment allows illegal users to eavesdrop confidential messages, the security of wireless communication is urgently needed and therefore has attracted extensive attention and research [1–3].

1.2. Current Literature

A conventional technique for wireless-communication security is mathematical encryption [4]. Nevertheless, it suffers from heavy system overhead and computational complexity. In contrast to mathematical encryption, directional modulation (DM) is a key-less physical-layer security (PLS) transmission technique, which uses an antenna array to transmit signal only along the desired direction or even only in the desired position [5]. In the past few decades, the implementation of DM was mainly based on a phased array (PA) [6]. However, the transmit beam pattern is only angle-dependent if employing PA, and it cannot guarantee the security of the transmission when eavesdroppers share the same direction with the legitimate user.

To address such a problem, another antenna array model, a frequency diverse array (FDA), was proposed in [7]. The authors in [7] pointed out an extra range-dependent property of the FDA by introducing a frequency offset between adjacent antenna elements. Benefiting from this feature, an FDA has the range-angle dependent property and delivers potential applications in PLS. In order to generate the required beam patterns, a number of researchers have conducted investigations on the design of frequency offset [8–12]. Moreover, Gao et al. proposed a multi-carrier FDA scheme in [13] to improve the performance.

The carriers assigned to all antenna elements can be mutually orthogonal by designing a proper frequency offset. Thus, Ding et al. [14] constructed an orthogonal frequency

division multiplexing (OFDM) system with an FDA for secure transmission. Unfortunately, as the result of the coupling effect, there were positions besides the legitimate receiver where the BER was low as well. If eavesdroppers were located at these positions, the transmission was not secure. In order to mitigate the coupling effect of a conventional FDA, the authors of [15] proposed a random FDA (RFDA) by employing random frequency increments across the array elements. Furthermore, a multi-beam wireless communication scheme was proposed in [16] with RFDA, which was security-enhanced, spectrum-efficient and power-efficient.

However, for medium-scale and large-scale DM systems, the receiver structure of RFDA dramatically increases the circuit cost, motivating the authors of [17] to propose a random subcarrier-selection array based using the OFDM technique instead of RFDA. Additionally, Shen et al. [18] gave two practical random subcarrier-selection methods: a quadratic subcarrier set plus randomization procedure (QSS Plus RP) and a prime subcarrier set plus randomization procedure (PSS Plus RP), both of which could select the subcarriers randomly and achieve secure precise wireless transmission.

1.3. Motivation and Related Work

It can be derived from [17,18] that the key of combining FDA with OFDM, while mitigating the coupling effect, was to randomly distribute a set of orthogonal subcarriers to each antenna array element. The authors of [18] gave two practical random subcarrier-selection methods: QSS Plus RP and PSS Plus RP. The QSS was defined as a set whose subcarrier index along the antenna array is a non-linear function of the corresponding antenna element index. The PSS was defined as a set whose subcarrier index is prime. Moreover, in order to destroy the regular order and produce a more random subcarrier index distribution over the transmitting antennas, the authors designed a block interleaving randomization procedure and repeated it until the randomization metric was larger than the predefined threshold.

However, this method brought about new problems. First, the repetition of the block interleaving operation increased system complexity, and it was hard to obtain a proper predefined threshold. Also, it generated a large number of unused subcarriers that greatly wasted spectrum.

To alleviate the above problems, this paper proposed a random subcarrier-selection method based on index modulation. On one hand, the bitstream was a random binary sequence, which could guarantee the randomness of the selected subcarriers; on the other hand, similar to IM [19], the indices of the subcarriers could also carry the information, which mitigated the waste of subcarriers. Moreover, our proposed scheme avoided the repeated block interleaving, achieving lower complexity. The proposed scheme could be used in wireless communications where the FDA is required to provide secure transmission.

1.4. Benefits and Challenges

The main benefits are summarized as follows:

- A new random subcarrier-selection method was proposed to guarantee the randomness of the selected subcarriers. In contrast to the scheme proposed in [18], RSCS-IM avoids the randomization procedure while the selected subcarriers are more random.
- IM is combined with subcarrier selection. By employing IM, the information was conveyed not only by MQAM modulation but also by the indices of the activated subcarriers, which improved the SE. Operating at the same SE, the BER performance was promoted by employing our scheme.
- The secure precise transmission via computer simulation was demonstrated and derived the closed-form expression of BER for the desired position. The theoretical outcomes were validated by simulation results as well.

- The main challenges are summarized as follows: in order to achieve precise and secure wireless communication, the randomness of the selected subcarriers must be guaranteed; the system complexity must be reduced and SE must be improved.

The rest of the paper can be summarized as follows. In Section 2, the system model is presented, including the conventional random subcarrier-selection method and the proposed random subcarrier-selection method based on IM. Performance analysis is depicted in Section 3. The computer simulation results are given in Sections 4 and 5 draws the conclusion.

The notations used in this manuscript are shown in Table 1.

Table 1. Notations used in this manuscript.

Notation	Description
$\sum$	Sum.
$X \sim \mathcal{CN}(0, \sigma^2)$	The distribution of a circularly symmetric complex Gaussian.
$\binom{n}{k}$	The binomial coefficient.

2. System Model

2.1. Conventional Random Subcarrier-Selection Method

The frequency increments of the conventional uniform FDA are linearly assigned to all antenna elements, resulting in an insecure coupling effect [7]. For mitigating this problem, a random subcarrier-selection method was proposed in [18], where a N_T-element antenna array was employed at the transmit side and each element transmitted the same subcarrier symbol. The used subcarriers were randomly selected from the all-subcarrier set of OFDM. Assuming that the number of total subcarriers is N_s, then we have the following:

$$S_{sub} = \{f_m | f_m = f_c + m\Delta f, (m = 0, 1, \ldots, N_s - 1)\}, \tag{1}$$

where f_c is the reference frequency, m denotes the subcarrier index, and Δf stands for the sub-channel bandwidth. The random subcarrier-selection method PSS Plus RP is described below. Firstly, the authors constructed a random subcarrier index set defined as

$$S_p = \{k_p | k_p \textit{ is a prime number}, k_p \in (0, 1, 2, \ldots, N_s - 1)\}. \tag{2}$$

In order to make a more random subcarrier index distribution over the transmit antennas, the authors proposed a random procedure (RP) by prime modulo operation and block interleaving. A constant p was chosen, which was the largest prime less than $\sqrt{N_T}$. Then, the set S_p was partitioned into p subsets by taking all set elements modulo p, which is represented as

$$K = K_0 \cup K_1 \cup \cdots \cup K_{p-1}. \tag{3}$$

Finally, the authors permuted the element order in the set K by block interleaving [18], which is depicted in Figure 1. In addition, the values of I and J should satisfy the inequality

$$(J - 1)I < N_T < JI. \tag{4}$$

It is worth pointing out that the block interleaving would be repeated until the randomness of the subcarrier index was greater than a certain threshold. To measure the random degree of the selected subcarriers, a random metric (RM) δ_I was defined in [18]. Suppose that the indices of the selected subcarriers are represented as

$$\eta = \{\eta(1), \eta(2), \cdots, \eta(N_T)\}. \tag{5}$$

The subcarrier index spacing vector can be derived as

$$\Delta\eta = [|\eta(1) - \eta(2)|, |\eta(2) - \eta(3)|, \cdots, |\eta(N_T - 1) - \eta(N_T)|]. \tag{6}$$

Then, δ_I can be expressed as

$$\delta_I = \frac{1}{N_T - 1} \sum_{i=1}^{N_T - 1} (\Delta\eta(i) - \bar{\Delta}\eta)^2, \tag{7}$$

where $\Delta\eta(i)$ is the i-th element of $\Delta\eta$. In addition, $\bar{\Delta}\eta$ denotes the average value of $\Delta\eta$, which is given by

$$\bar{\Delta}\eta = \frac{1}{N_T - 1} \sum_{i=1}^{N_T - 1} \Delta\eta(i), \tag{8}$$

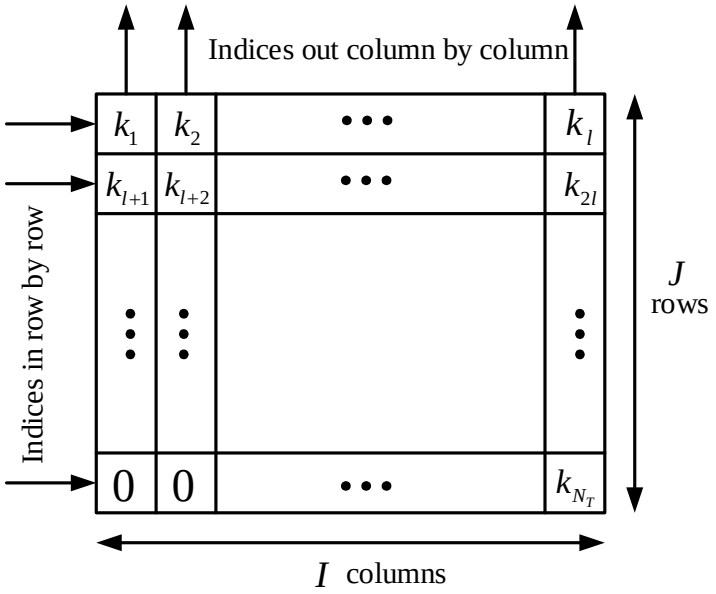


Figure 1. The principle of block interleaving.

Figure 2 draws the flow chart of PSS Plus RP. As shown in Figure 2, firstly, N_T subcarriers were selected whose index was a prime number from the given subcarrier set in (1). Next, a prime number p was chosen, which was the largest prime less than $\sqrt{N_T}$. Then, these N_T indices were partitioned into p groups using the modulo-p operation. Finally, the block interleaving operation was performed, as shown in Figure 1, on this p-group index and the RM was computed. If RM was larger than the predefined threshold, the index output after block interleaving was the desired index. Otherwise, the block interleaving operation was repeated until RM was larger than the predefined threshold. We could see that there were a number of unused subcarriers causing the waste of spectrum. Additionally, a proper threshold was hard to obtain and the repeated block interleaving operation increased the computational complexity.

2.2. The Proposed Random Subcarrier-Selection Method Based on Index Modulation

It could be seen from the description of the conventional scheme in Section 2.1 that the complexity of PSS Plus RP mainly resulted from block interleaving, which was repeated until the random degree was greater than the predefined value. Meanwhile, the spectrum was wasted since a large number of subcarriers were unused. For alleviating this problem, this paper proposed a novel random subcarrier-selection method based on index modulation (RSCS-IM) under a new FDA OFDM communication architecture. The array structure of the proposed FDA OFDM transmitter based on IM is shown in Figure 3, where the legitimate transmitter Alice equipped a N_T-element linear antenna array with

element space d. The legitimate receiver Bob and N eavesdroppers Eve all employed a single antenna. In the conventional scheme [18], all antennas of Alice transmitted the same subcarrier symbol per OFDM symbol. While in our scheme, all antennas of Alice transmitted different subcarrier symbols per OFDM symbol to Bob by selecting multiple subcarriers from the subcarrier set using IM. If the first antenna was taken as the reference, Bob was located at (θ_0, R_0), which was represented as the red star. The positions of the N eavesdroppers were $(\theta_1, R_1), (\theta_2, R_2), \cdots, (\theta_n, R_n)$ respectively, which were represented as the black stars. Suppose there were N_s orthogonal subcarriers in our FDA OFDM-IM system and the set of subcarriers was

$$S_{sub} = \{f_m | f_m = f_c + m\Delta f, m = 0, 1, \cdots, N_s - 1\}, \tag{9}$$

where f_c is the reference frequency, m denotes the subcarrier index, and Δf stands for the subchannel bandwidth, $T_s = 1/\Delta f$ denotes the period of an OFDM symbol. It was assumed that $N_s\Delta f \ll f_c$ and $d = \lambda/2$, where $\lambda = c/f_c$ denotes the wave length and c is the light speed. The subcarrier frequency assigned to the n-th antenna was $f_{\eta(n)}$, where $f_{\eta(n)} \in S_{sub}$ and $\eta(n) \in \{0, 1, \cdots, N_s - 1\}$. $\eta(n)$ was determined by the bits used for index selection. It is worth pointing out that for different n_1, n_2, $\eta(n_1) \neq \eta(n_2)$. In a far-field scenario, the received signal at (θ_0, R_0) could be represented by

$$s(t) = \sum_{k=1}^{N_T} x_k e^{j\varphi_k} e^{j2\pi f_{\eta(k)}(t - \frac{R_k}{c})} + \sum_{k=1}^{N_T} n_k, \tag{10}$$

where $f_{\eta(k)} = f_c + \eta(k)\Delta f$, $R_k = R_0 - (k-1)d\sin\theta_0$. φ_k denotes the initial phase of the k-th antenna and n_k is the received additive white Gaussian noise (AWGN) of the k-th antenna with the distribution of $n_k \sim \mathcal{CN}(0, \sigma^2)$. So, we can rewrite (10) as

$$\begin{aligned} s(t) &= \sum_{k=1}^{N_T} x_k e^{j\varphi_k} e^{j2\pi(f_c + \eta(k)\Delta f)(t - \frac{R_k}{c})} + \sum_{k=1}^{N_T} n_k \\ &= \sum_{k=1}^{N_T} x_k e^{j\varphi_k} e^{j2\pi f_c t} e^{j2\pi\eta(k)\Delta f t} e^{-j2\pi f_{\eta(k)}\frac{R_k}{c}} + \sum_{k=1}^{N_T} n_k \\ &= e^{j2\pi f_c t} \sum_{k=1}^{N_T} x_k e^{j(\varphi_k - 2\pi f_{\eta(k)}\frac{R_k}{c})} e^{j2\pi\eta(k)\Delta f t} + \sum_{k=1}^{N_T} n_k. \end{aligned} \tag{11}$$

After receiving the signal in (11), it was firstly down-converted to baseband by multiplying by $e^{-j2\pi f_c t}$. Then, the baseband signal was sampled at $t = n/N_s\Delta f$ $(n = 0, 1, \cdots, N_s - 1)$ and we obtained

$$s(n) = \sum_{k=1}^{N_T} x_k e^{j(\varphi_k - 2\pi f_{\eta(k)}\frac{R_k}{c})} e^{j2\pi n\eta(k)/N_s} + \sum_{k=1}^{N_T} n_k. \tag{12}$$

Observing Equation (12), if the symbols corresponding to the inactive subcarriers were set to zero and the noise was ignored, $s(n)$ was the inverse fast Fourier transform (IFFT) of $x_k e^{j(\varphi_k - 2\pi f_{\eta(k)}\frac{R_k}{c})}$. For the sake of demodulating the original signal correctly, the initial phase of antenna k should satisfy the following identity [14]

$$\varphi_k - 2\pi f_{\eta(k)}\frac{R_k}{c} = \varphi_0, \tag{13}$$

where φ_0 is a constant. So, by taking the fast Fourier transform (FFT) for $s(n)$ and multiplying by $e^{-j\varphi_0}$, the original signal x_k could be restored.

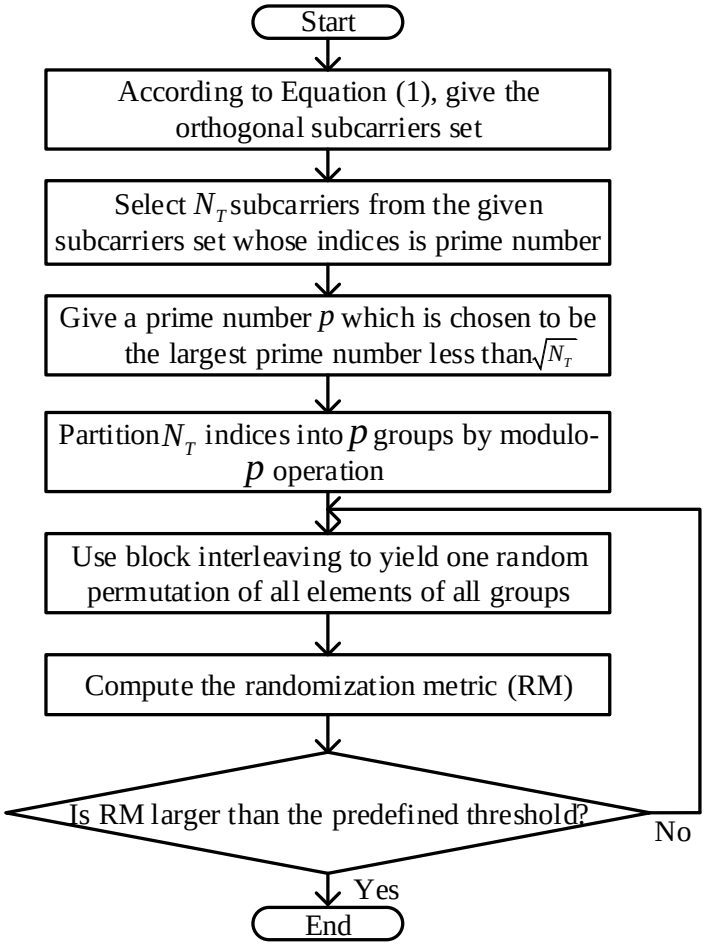


Figure 2. Flow chart of PSS Plus RP.

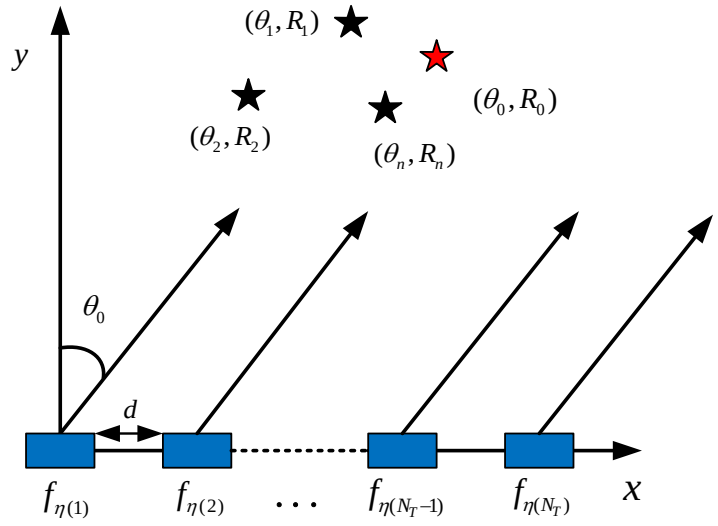


Figure 3. Array Structure of the FDA OFDM-IM Transmitter.

The concrete random subcarrier-selection method based on index modulation (RSCS-IM) will be described in this part. It was assumed that the number of total orthogonal subcarriers and antenna array elements were N_s and N_T, respectively. For convenience, suppose $N_s = 2^{m_1}$ and $N_T = 2^{m_2}$, where both m_1 and m_2 are positive integers and $m_1 > m_2$.

Firstly, the index of all the orthogonal subcarriers was divided into a matrix whose dimension was $N_T \times \frac{N_s}{N_T}$, i.e.,

$$I_{sub} = \begin{pmatrix} 1 & N_T+1 & \cdots & N_s-N_T+1 \\ 2 & N_T+2 & \cdots & N_s-N_T+2 \\ \vdots & \vdots & \ddots & \vdots \\ N_T & 2N_T & \cdots & N_s \end{pmatrix}. \tag{14}$$

Next, a subcarrier was selected from every row of I_{sub}, respectively. For every row, p bits were used to select the subcarrier, where

$$p = log_2 \frac{N_s}{N_T} = m_1 - m_2. \tag{15}$$

Figure 4 depicts the flow chart of the proposed scheme, RSCS-IM. As shown in Figure 4, firstly, all the indices from the orthogonal subcarrier set in (9) were divided into the matrix in (14). Next, $p \times N_T$ bits were generated and each p-bit of binary data was converted to a decimal, according to the data bits generated by the source, where $p = log_2 \frac{N_s}{N_T}$. Finally, one index from every row of matrix (14) was picked in turn using these N_T decimal data as columns and we obtained the N_T desired indices. So, we could see that the proposed scheme avoided the repeated block interleaving operation and guaranteed the randomness of the selected subcarriers. Moreover, the indices of the activated subcarriers could transmit extra data bits, mitigating the waste of spectrum.

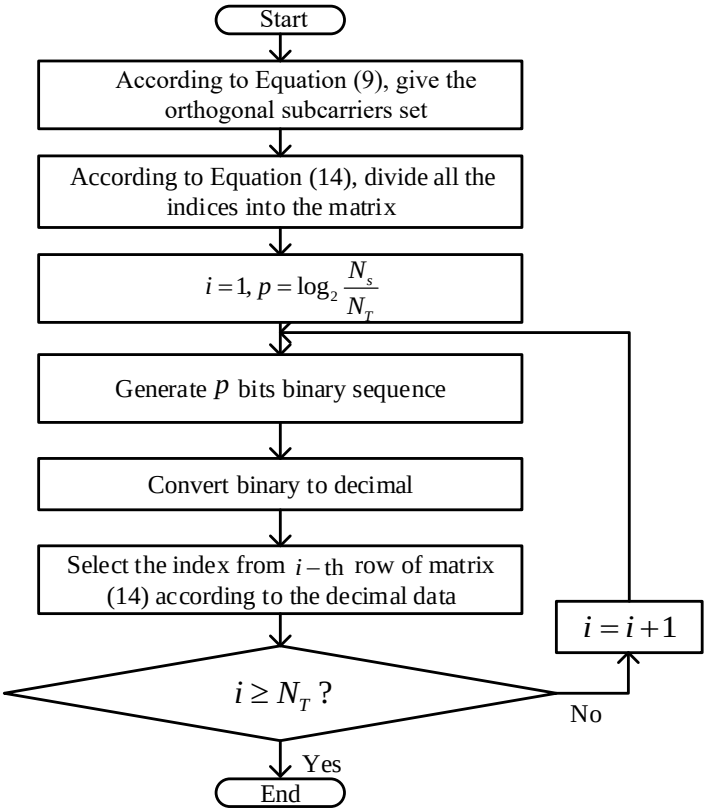


Figure 4. Flow chart of RSCS-IM.

Hence, the whole block diagram of FDA OFDM-IM system is described in Figure 5, where $m = (p+q)N_T, p = m_1 - m_2, q = log_2 M$ and M is the order of modulation.

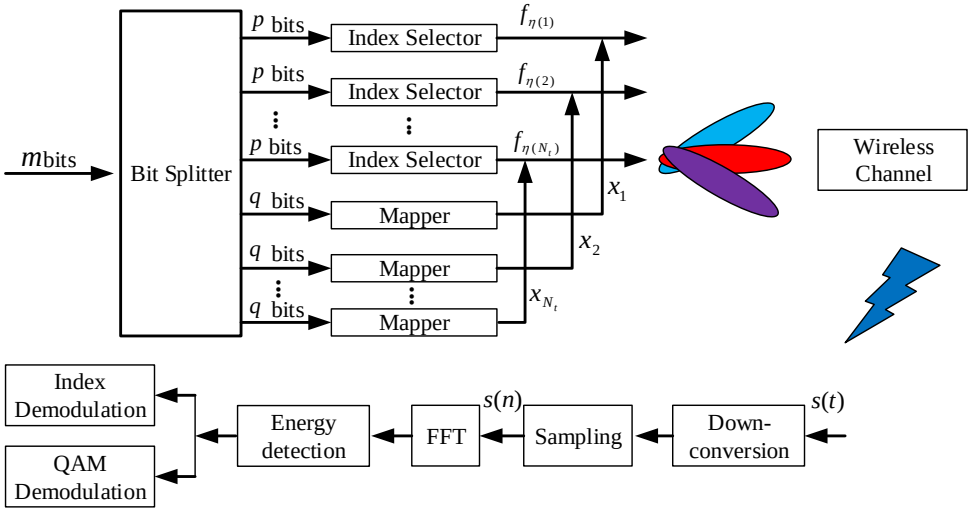


Figure 5. Block diagram of the FDA OFDM-IM system.

As shown in Figure 5, a total of m information bits entered the bit splitter. These m bits were split into $2N_T$ groups. For the first N_T groups, each group contained p bits for index-selection while the other N_T groups each contained q bits for mapping. After that, the signal was conveyed by the FDA OFDM-IM system in the far-field scenario and Bob received the signal $s(t)$ in (10). Just as depicted above, taking down-conversion and sampling for $s(t)$ in turn, we could obtain $s(n)$ in (12). Next, an N_s-point FFT was obtained for $s(n)$. Then, in order to detect the activated subcarriers, we adopted the scheme of greedy detection and determined the location of maximum energy for every row in (14) as the index of the activated subcarrier. Finally, the index demodulation and QAM demodulation were obtained, respectively, and the original data could be restored. As for the eavesdroppers, assuming that they were consistent with the demodulation method used by the legitimate receiver, from (13) we could see that there was a phase offset between the received data and original data. So they could not restore the original data correctly.

In summary, the proposed scheme could guarantee the randomness of the selected subcarriers because of the randomness of the information bits. Moreover, the indices of the activated subcarriers could transmit extra data bits, improving the SE. In Section 3, we will analyse the performance of RSCS-IM and PSS Plus RP in detail.

3. Performance Analysis

In this section, we analyse some important factors of the proposed scheme RSCS-IM, including the SE, complexity and BER performance of the desired position. Meanwhile, the factors mentioned above of the scheme's "prime subcarrier set plus randomization procedure (PSS Plus RP)" proposed in [18] were also analyzed for comparison.

3.1. Spectral Efficiency and Computational Complexity Analysis

- Spectral Efficiency Analysis
  One OFDM symbol was taken for reference. According to the principle of RSCS-IM, an OFDM symbol included N_1 bits information, which was defined as

$$N_1 = N_T log_2 \frac{N_s}{N_T} + N_T log_2 M, \tag{16}$$

  where N_T is the number of antennas, N_s represents the number of total subcarriers and M is the modulation order. While for PSS Plus RP, the counterpart was

$$N_2 = N_T log_2 M. \tag{17}$$

It was obvious that $N_1 - N_2 = N_T log_2 \frac{N_s}{N_T} > 0$, so RSCS-IM promoted the spectrum efficiency. Meanwhile, we could see that a large N_s implied a higher spectrum efficiency; however, larger N_s also implied higher computational complexity. We could select the value of N_s and N_T to meet our requirement in a certain scenario.

- Computational Complexity Analysis
  According to the principles of PSS Plus RP and RSCS-IM shown in Figures 2 and 4, respectively, we analyze the computational complexity of these two schemes in this subsection. The computational complexity was evaluated in terms of the real-valued operations, including real-valued multiplication, real-valued additions, and real-valued modulo operations. According to the principles, we gave the complexity of these two methods shown in Table 2, where N_s and N_T denote the number of total subcarriers and antennas, respectively, and N is the number of loops of block interleaving.

Table 2. Complexity of PSS Plus RP and RSCS-IM.

Scheme	Complexity		
	Addition	**Multiplication**	**Modulo**
RSCS-IM	$N_T(log_2 \frac{N_s}{N_T} - 1)$	$\frac{N_T log_2 \frac{N_s}{N_T} (log_2 \frac{N_s}{N_T} - 1)}{2} + N_T$	—
PSS Plus RP	$4N(N_T - 1)$	$N(N_T - 1)$	N_T

From Table 2 we could clearly see that the number of modulo operations in RSCS-IM was less than that of PSS Plus RP. As for the addition operation, in general, $N_T < 4N$ and $log_2 \frac{N_s}{N_T} < N_T$, so $N_T(log_2 \frac{N_s}{N_T} - 1) < 4N(N_T - 1)$. Moreover, $log_2 \frac{N_s}{N_T} < 10$ in most cases. $log_2 \frac{N_s}{N_T}(log_2 \frac{N_s}{N_T} - 1)/2$ and N had the same order of magnitude. Thus, we could see that the number of multiplications in these two schemes were basically equal. Overall, the complexity of RSCS-IM was lower.

3.2. BER Performance Analysis of the Desired Position

In what follows, the average BER of the desired position is analyzed. As shown in Figure 5, demodulation includes index demodulation and QAM demodulation, both of which need to know the index of the activated subcarriers. For all alternative orthogonal subcarriers, we could consider that the activated subcarriers conveyed the QAM symbol plus noise while the inactivated subcarriers just conveyed the noise. As a result, we adopted greedy detection to determine the index of activated subcarriers. Suppose that $y_i(\alpha)$ denotes the symbol whose index is α of the i-th row in (14), then,

$$\hat{\alpha} = \arg\max_{\alpha} |y_i(\alpha)|^2. \tag{18}$$

After determining the index of the activated subcarriers, ML detection was adopted to determine the constellation symbols, which was similar to the classical QAM demodulation, i.e.,

$$\hat{s}(\hat{\alpha}) = \arg\min_{x(\hat{\alpha}) \in S} |y(\hat{\alpha}) - x(\hat{\alpha})|^2. \tag{19}$$

where S is the set of standard constellation symbols and $y(\hat{\alpha})$ denotes the received symbol.

According to the analysis above, average BER could be represented as

$$P_s = \frac{n_i + n_Q}{n_t}, \tag{20}$$

where n_i and n_Q denote the number of wrong bits of index demodulation and QAM demodulation, respectively. n_t denotes the total bits of an OFDM symbol, including the

bits of index selection. As the index selection of each group, i.e., each row in (14) did not affect each other, taking an arbitrary group for example, we could get

$$n_t = log_2(\frac{N_s}{N_T}) + log_2 M. \tag{21}$$

It was assumed that P_g denoted the error probability of greedy detection. When greedy detection was wrong, the bit error rate of index was P_i and the counterpart of QAM modulation was P_{Q1}. Otherwise, the bit error rate of QAM modulation was P_{Q2}. So, n_i could be written as

$$n_i = P_g P_i log_2(\frac{N_s}{N_T}), \tag{22}$$

and n_Q as

$$n_Q = P_g P_{Q1} log_2 M + (1 - P_g) P_{Q2} log_2 M. \tag{23}$$

From the principal of greedy detection, when greedy detection was wrong, i.e., $max\{|n(\hat{\alpha})|^2\} > |x(\alpha) + n(\alpha)|^2$, we have

$$P_g = P(max\{|n(\hat{\alpha})|^2\} > |x(\alpha) + n(\alpha)|^2). \tag{24}$$

In line with [20], a closed-form expression of (24) is

$$P_g = 1 - \sum_{k=0}^{\frac{N_s}{N_T}-1} \begin{pmatrix} N_s/N_T - 1 \\ k \end{pmatrix} \frac{(-1)^k}{k+1} e^{\gamma_\alpha (\frac{1}{k+1} - 1)}, \tag{25}$$

where γ_α denotes the SNR of activated subcarriers and $\begin{pmatrix} N_s/N_T - 1 \\ k \end{pmatrix}$ is the binomial coefficient. When it came to P_i, we knew that the index demodulation was turning the decimal index into a binary bit stream and the index met $I \in [0, \frac{N_s}{N_T} - 1]$. The essence of wrong greedy detection was detecting the correct index as one of the other $\frac{N_s}{N_T} - 1$ wrong indexes. Meanwhile, the probability of detecting the correct index as any other wrong index was the same. So,

$$P_i = \frac{\frac{1}{2} log_2(\frac{N_s}{N_T}) \frac{N_s}{N_T}}{(\frac{N_s}{N_T} - 1) log_2(\frac{N_s}{N_T})} = \frac{\frac{N_s}{N_T}}{2(\frac{N_s}{N_T} - 1)}. \tag{26}$$

As for P_{Q1} and P_{Q2}, after a brief analysis, we could get

$$P_{Q1} = \frac{1}{2}, \tag{27}$$

and

$$P_{Q2} = P_{QAM}, \tag{28}$$

where P_{QAM} denotes the BER of classical QAM modulation. Hence, substituting (25)–(28) into (22) and (23) we could obtain n_i and n_Q. Finally, P_s could be derived by substituting (21)–(23) into (20).

In terms of PSS Plus RP, it did not include the index demodulation and its BER performance was similar to the classical OFDM system in the Gaussian channel, which could be represented as

$$P = P_{QAM}. \tag{29}$$

From (28) and (29) we could see that P_s was equal to P when the greedy detection was always right, i.e., $P_i = 0$, which was in line with the analysis.

In terms of Eve, it is worth pointing out that, when employing an RSCS-IM scheme,

the bits transmitted by te index could be demodulated correctly when SNR was high enough i.e.,

$$P_{e1} = \frac{\frac{1}{2} log_2 M}{log_2(\frac{N_s}{N_T}) + log_2 M}, \tag{30}$$

where P_{e1} represents the BER of Eve when SNR was high enough for RSCS-IM. While for PSS Plus RP, assuming P_{e2} represents the BER of Eve, regardless of the value of SNR,

$$P_{e2} = \frac{1}{2} \tag{31}$$

since it did not include the index modulation.

4. Simulation Results

In this section, the simulation results of the random degree, the computational complexity, and the BER performance are depicted to describe the performance of RSCS-IM. In this simulation, system parameters were chosen as follows: reference frequency $f_c = 2.404$ GHz [14], signal bandwidth $B = 20$ MHz, the number of total subcarriers $N_s = 512$ or 1024, $E_b/N_0 = 9$ dB, the number of antenna array elements $N_T = 64$, the legitimate receiver Bob was located at $(30^\circ, 100$ m), and we employed a QPSK constellation. The constant $\varphi_0 = 0$ in (13). These parameters are listed in Table 3.

Table 3. The system parameters in our simulation.

Parameter	Value	Description
f_c	2.404 GHz	Reference frequency.
B	20 MHz	Signal bandwidth.
N_s	512/1024	The number of total subcarriers.
N_T	64	The number of antenna array elements.
E_b/N_0	9 dB	Average bit energy to noise power ratio.
(θ_0, R_0)	$(30^\circ, 100$ m)	The desired position.
φ_0	0	The constant of Equation (13).

4.1. The Simulation Results of Random Degree

To measure the random degree of the selected subcarriers of the proposed RSCS-IM and the PSS Plus RP [18], we calculated δ_I in (7) of the two random subcarrier-selection methods many times. The results are presented in Figure 6. As shown in Figure 6, the random degree of the proposed scheme RSCS-IM was always larger than that of PSS Plus RP in ten thousand simulations, meaning that the selected subcarriers employing RSCS-IM were more random. Additionally, comparing Figure 6a with Figure 6b, we could see that when $N_s = 1024$, the random degree was improved using both methods because the number of available subcarriers increased. Moreover, the increase in random degree was greater when employing RSCS-IM rather than employing PSS Plus RP since the number of increased subcarriers employing RSCS-IM was more than the number of increased primes employing PSS Plus RP.

4.2. The Simulation Results of Computational Complexity

To visualize the computational complexity of the two schemes, we simulated the number of addition, multiplication, and modulo operations and selected $N_s = 512/1024$ and $N_T = 64$. When δ_I firstly reached 95% of the maximum random degree, the number of loops $N = 23/22$. The concrete computational complexity is depicted in Figure 7. Hence, we could see that the number of additions, multiplications, and modulo operations in RSCS-IM were all less than that of PSS Plus RP. The complexity of RSCS-IM was lower. Comparing Figure 7a with Figure 7b, when $N_s = 1024$, the complexity of PSS Plus RP was basically unchanged since the number of loops was basically independent of N_s, while the complexity increased slightly, when employing RSCS-IM, in addition and multiplication

operations. However, the complexity of RSCS-IM was still substantially lower than that of PSS Plus RP when N_s was not particularly large.

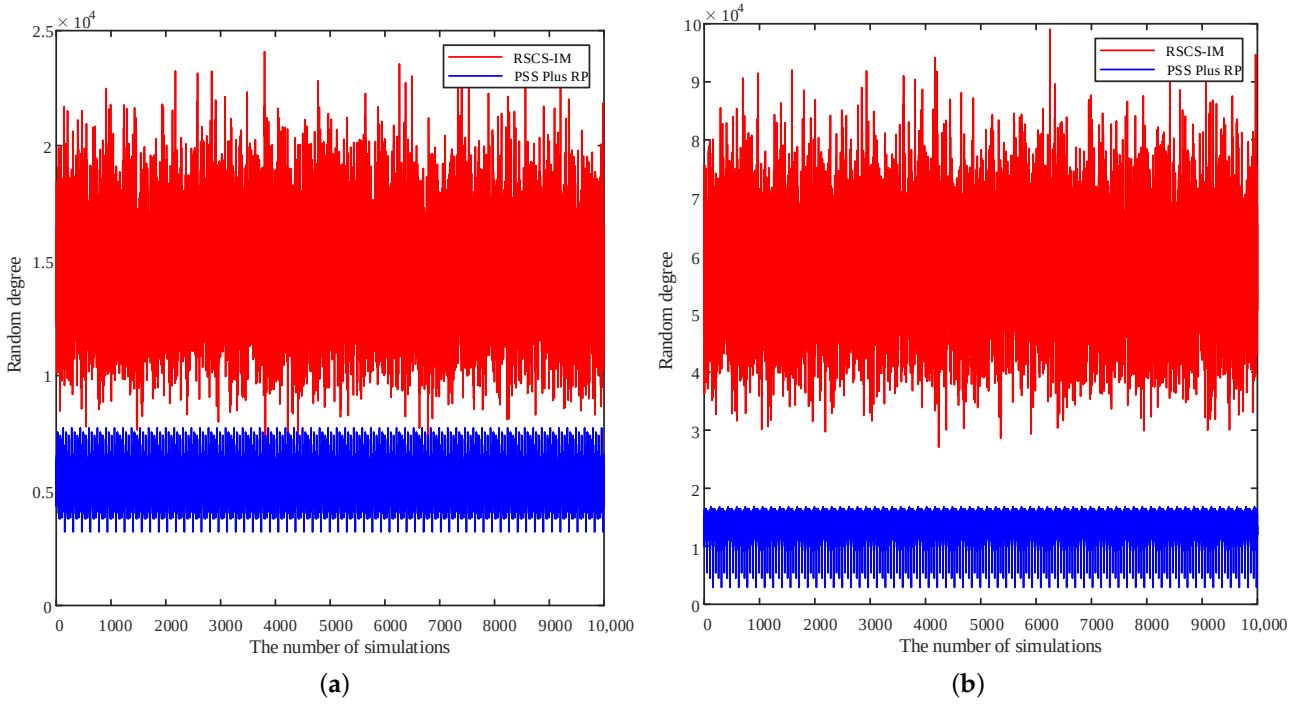


Figure 6. Simulation comparison of the random degree. (**a**) $N_s = 512$. (**b**) $N_s = 1024$.

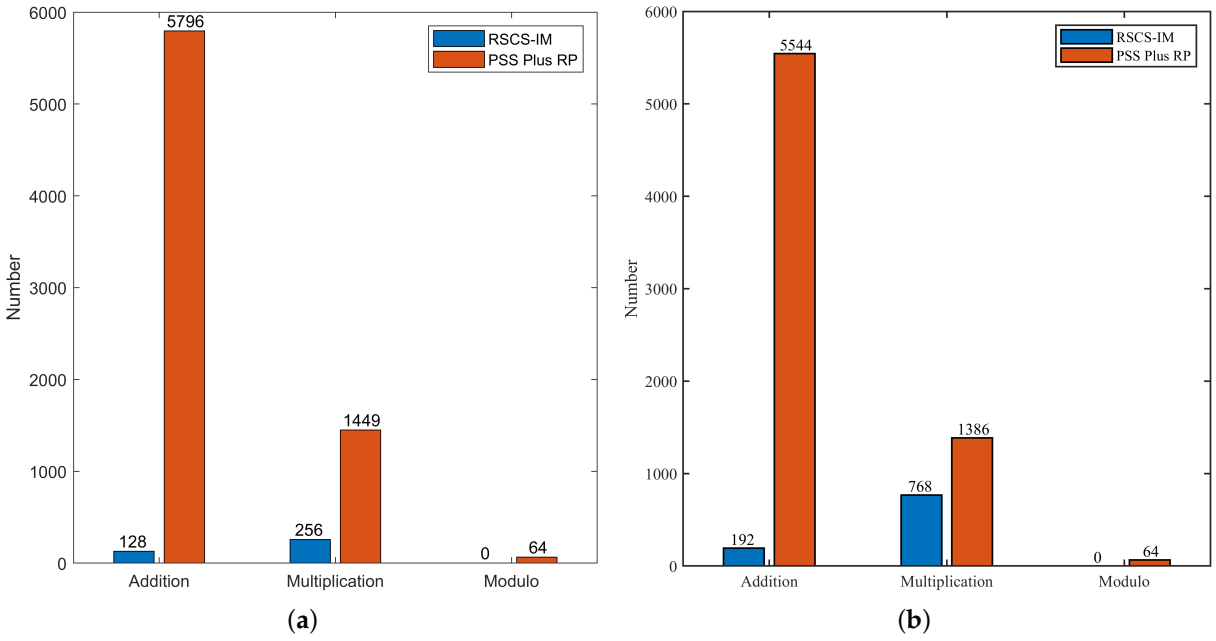


Figure 7. The computational complexity of RSCS-IM and PSS Plus RP. (**a**) $N_s = 512$. (**b**) $N_s = 1024$.

4.3. The Simulation Results of BER Performance

In order to evaluate the secure performance of the proposed scheme RSCS-IM, the 3-D performance surface of BER versus the direction angle and distance was simulated. Furthermore, we simulated the performance of PSS Plus RP to make a comparison with our scheme. Meanwhile, in order to illustrate the coupling effect of a uniform FDA, and to further illustrate the importance of randomly selecting subcarriers, this paper also

simulated the 3-D performance surface of BER versus the direction angle and distance of uniform FDA [7].

Figure 8 is the 3-D performance surface of BER versus the direction angle and distance of a uniform FDA. As shown in Figure 8, besides the desired position, there were other positions where the BER was low as well. If eavesdroppers were located at these positions, the transmission was not secure. This phenomenon is known as the coupling effect of a uniform FDA.

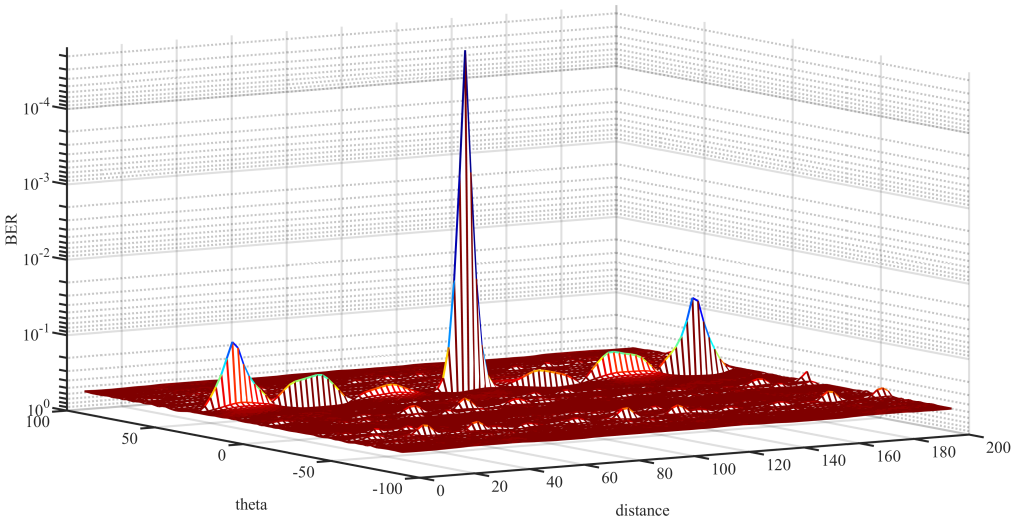


Figure 8. 3-D performance surface of a uniform FDA.

Figure 9 depicts the 3-D BER performance surface versus the direction angle and distance when the number of total subcarriers $N_s = 512$. Compared with Figure 8, Figure 9 depicts that low bit error rate occurred only in a small area around the desired position. The other positions could not restore the original signal correctly. Therefore, the random selection of subcarriers was important for weakening the coupling effect and, thus, achieving safe and accurate wireless transmission.

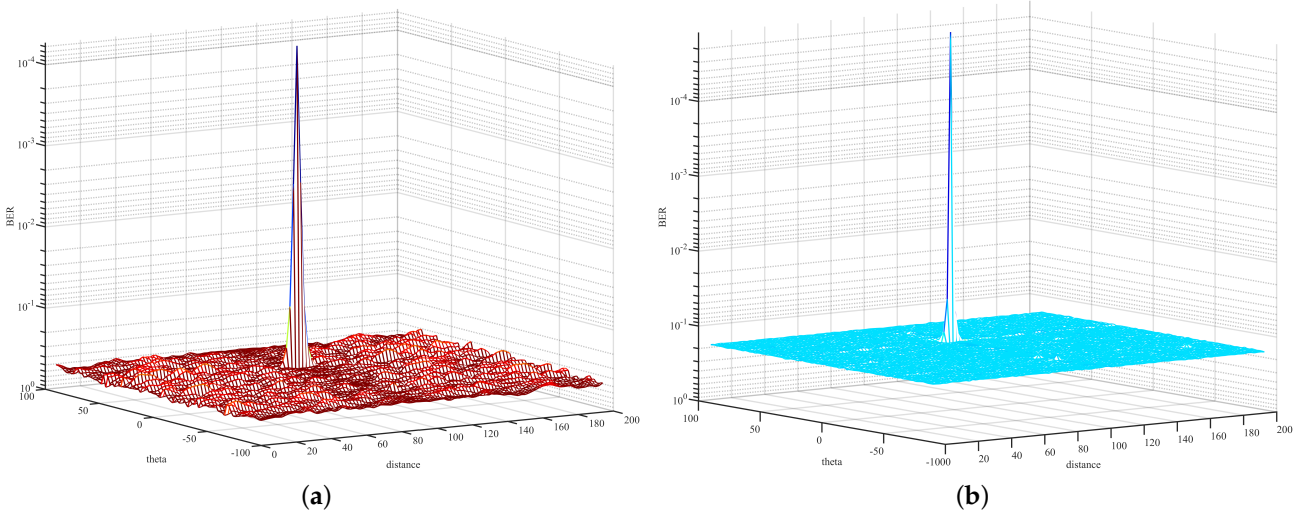
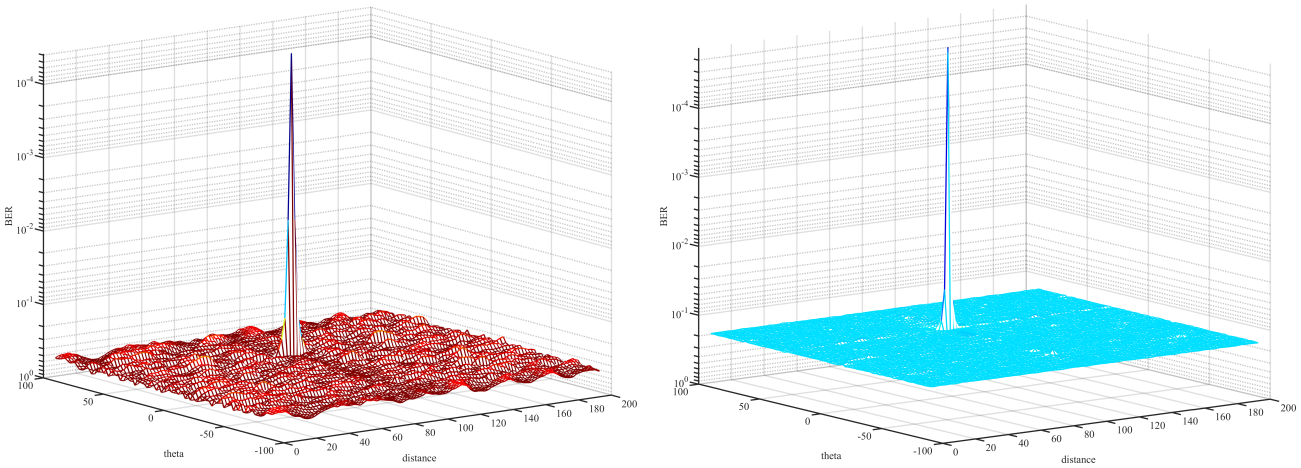


Figure 9. 3-D performance surface of BER versus the direction angle and distance ($N_s = 512$). (**a**) 3-D performance surface of BER using PSS Plus RP; (**b**) 3-D performance surface of BER using RSCS-IM.

When $N_s = 1024$, Figure 10 depicts the 3-D BER performance surface versus the direction angle and distance. Figure 10a is similar to Figure 9a. Comparing Figure 10b with Figure 9b, the BER performance at Eve was slightly improved because of the increased

weight of bits used for index selection. In terms of the desired position, there was a certain BER gain when employing RSCS-IM, comparing Figure 10b with Figure 10a.



(**a**) (**b**)

Figure 10. 3-D performance surface of BER versus the direction angle and distance ($N_s = 1024$). (**a**) 3-D performance surface of BER using PSS Plus RP; (**b**) 3-D performance surface of BER using RSCS-IM.

Figure 11 depicts the BER performance versus E_b/N_0 of Bob. As shown in Figure 11, the theoretical and simulation curves were basically consistent. Specifically, regardless of $N_s = 512$ or $N_s = 1024$, the BER performance of Bob was consistent when employing PSS Plus RP since it did not include IM. The BER performance of Bob was only related to the symbol modulation method. Additionally, when $N_s = 512$ and BER was 10^{-2}, there was more than 1dB gain when employing RSCS-IM rather than PSS Plus RP. When $N_s = 1024$, there was an extra gain in the BER performance of Bob compared with $N_s = 512$ in high E_b/N_0, since SE was improved. While in low E_b/N_0, there was a distinct degradation in the error probability of greedy detection. So the BER performance of Bob was basically consistent in low E_b/N_0 when $N_s = 512$ and $N_s = 1024$. Likewise, since the error probability of greedy detection was very high in low E_b/N_0, the BER performance of Bob employing RSCS-IM was worse than employing PSS Plus RP.

From Figure 9 we can see that the BER performance of the other positions, other than the desired position, was of small variation. So, when taking an arbitrary position (60°, 50 m) as an eavesdropper (Eve), the BER performance versus SNR using RSCS-IM with different N_T is shown in Figure 12. The number of total subcarriers $N_s = 512$. As for Eve, the BER performance versus SNR was always about $\frac{1}{2}$ when employing PSS Plus RP. As the other positions could demodulate the index bits correctly, the BER performance employing RSCS-IM was less than $\frac{1}{2}$. Specifically, the bigger $\frac{N_s}{N_T}$ was, the lower the BER was in high SNRs. In other words, the less bits used in IM, the higher the BER was in high SNRs. Thus, we could control the BER performance in other positions by selecting a proper value of $\frac{N_s}{N_T}$ so that Eve could not restore the original signal correctly, even if error correction coding was employed.

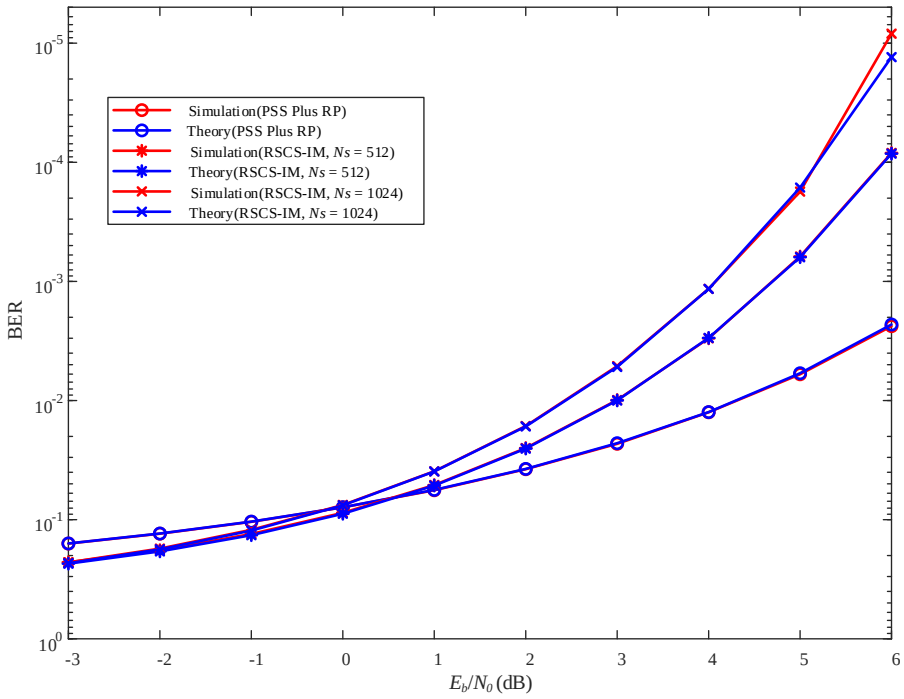


Figure 11. BER performance versus E_b/N_0 of Bob.

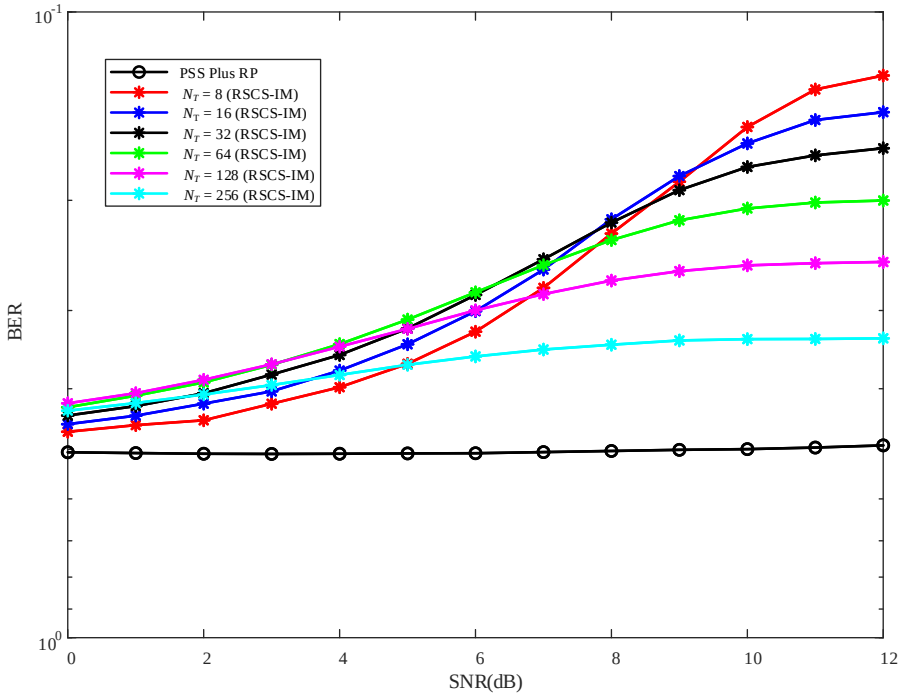


Figure 12. BER performance versus SNR of Eve under RSCS-IM and PSS Plus RP schemes with different N_T.

5. Conclusions

Based on IM, this paper proposed a new random subcarrier-selection method, RSCS-IM, which achieved secure and precise wireless transmission. Compared to PSS Plus RP, which was proposed in [18], RSCS-IM not only enhanced the SE but also reduced complexity. At the same SE, the proposed RSCS-IM scheme featured better BER performance. Moreover, the BER performance of an eavesdropper could be limited by selecting a proper value of

N_s/N_T. Finally, we derived the closed-form expression of BER for the desired position and demonstrated the performance of our scheme via numerical simulation.

Author Contributions: Conceptualization, X.L.; methodology, X.L., J.C. and T.Z.; software, T.Z. and J.C.; validation, T.Z.; formal analysis, T.Z.; investigation, T.Z.; resources, T.Z.; data curation, T.Z.; writing—original draft preparation, T.Z.; writing—review and editing, X.L. and J.C.; visualization, T.Z.; supervision, X.L. and S.L.; project administration, X.L. and S.L.; funding acquisition, X.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by National Key R&D Program of China (2020YFB1806607) and the Foundation of stability support plan for National Key Lab (IFN2020104).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

FDA	Frequency diverse array
OFDM	Orthogonal frequency division multiplexing
RSCS-IM	Random subcarrier-selection method based on index modulation
BER	Bit error rate
SE	Spectral efficiency
PLS	Physical-layer security
DM	Directional modulation
PA	Phased array
RFDA	Random frequency diverse array
IM	Index modulation
MQAM	Multiple Quadrature Amplitude Modulation
FDA OFDM-IM	FDA OFDM transmitter based on index modulation
AWGN	Additive white Gaussian noise
PSS Plus RP	Prime subcarrier set plus randomization procedure
IFFT	Inverse fast Fourier transform
FFT	Fast Fourier transform
RM	Random metric

References

1. Yang, N.; Wang, L.; Geraci, G.; Elkashlan, M.; Yuan, J.; Di Renzo, M. Safeguarding 5G wireless communication networks using physical layer security. *IEEE Commun. Mag.* **2015**, *53*, 20–27. [CrossRef]
2. Zhao, N.; Yu, F.R.; Li, M.; Yan, Q.; Leung, V.C. Physical layer security issues in interference-alignment-based wireless networks. *IEEE Commun. Mag.* **2016**, *54*, 162–168. [CrossRef]
3. Zou, Y.L.; Zhu, J.; Wang, X.; Leung, V. Improving physical-layer security in wireless communications using diversity techniques. *IEEE Netw.* **2015**, *29*, 42–48. [CrossRef]
4. Xie, N.; Zhang, S. Blind Authentication at the Physical Layer Under Time-Varying Fading Channels. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 1465–1479. [CrossRef]
5. Kalantari, A.; Soltanalian, M. Directional Modulation via Symbol-Level Precoding: A Way to Enhance Security. *IEEE J. Sel. Top. Signal Process* **2016**, *10*, 1478–1493. [CrossRef]
6. Daly, M.P.; Bernhard, J.T. Directional Modulation Technique for Phased Arrays. *IEEE Trans. Antennas Propag.* **2009**, *57*, 2640–2663. [CrossRef]
7. Antonik, P.; Wicks, M.C.; Griffiths, H.D.; Baker, C.J. Frequency diverse array radars. In Proceedings of the 2006 IEEE Conference on Radar, Verona, NY, USA, 24–27 April 2006; p. 3.
8. Khan, W.; Qureshi, I.M.; Saeed, S. Frequency Diverse Array Radar with Logarithmically Increasing Frequency Offset. *IEEE Antennas Wirel. Propag. Lett.* **2015**, *14*, 499–502. [CrossRef]
9. Xu, Y.; Shi, X.; Li, W.; Xu, J. Flat-Top Beampattern Synthesis in Range and Angle Domains for Frequency Diverse Array via Second-Order Cone Programming. *IEEE Antennas Wirel. Propag. Lett.* **2016**, *15*, 1479–1482. [CrossRef]

10. Xiong, J.; Wang, W.Q.; Shao, H.; Chen, H. Frequency Diverse Array Transmit Beampattern Optimization with Genetic Algorithm. *IEEE Antennas Wirel. Propag. Lett.* **2017**, *16*, 469–472. [CrossRef]
11. Xu, Y.; Luk, K.M. Enhanced Transmit—Receive Beamforming for Frequency Diverse Array. *IEEE Trans. Antennas Propag.* **2020**, *68*, 5344–5352. [CrossRef]
12. Liao, Y.; Wang, J.; Liu, Q.H. Transmit Beampattern Synthesis for Frequency Diverse Array with Particle Swarm Frequency Offset Optimization. *IEEE Trans. Antennas Propag.* **2021**, *69*, 892–901. [CrossRef]
13. Gao, K.; Wang, W.Q.; Chen, H.; Cai, J. Transmit Beamspace Design for Multi-Carrier Frequency Diverse Array Sensor. *IEEE Sens. J.* **2016**, *16*, 5709–5714. [CrossRef]
14. Ding, Y.; Zhang, J.; Fusco, V. Frequency diverse array OFDM transmitter for secure communication. *Electron. Lett.* **2015**, *51*, 1374–1375. [CrossRef]
15. Liu, Y.; Ruan, H.; Wang, L.; Nehorai, A. The random frequency diverse array: A new antenna structure for uncoupled direction-range indication in active sensing. *IEEE J. Sel. Top. Signal Process* **2017**, *11*, 295–308. [CrossRef]
16. Gao, J.; Qiu, B.; Zhou, J. Spatial Modulation and MP-WFRFT-Aided Multi-Beam Wireless Communication Scheme Based on Random Frequency Diverse Array. *Sensors* **2020**, *20*, 5298. [CrossRef] [PubMed]
17. Shu, F.; Wu, X.; Li, J.; Chen, R.; Wang, J. Secure and precise wireless transmission for random-subcarrier-selection based directional modulation transmit antenna array. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 890–904. [CrossRef]
18. Shen, T.; Zhang, S.; Chen, R.; Wang, J.; Hu, J.; Shu, F.; Wang, J. Two practical random-subcarrier-selection methods for secure precise wireless transmissions. *IEEE Trans. Veh. Technol.* **2019**, *68*, 9018–9028. [CrossRef]
19. Basar, E.; Aygolu, U.; Panayirci, E.; Poor, H.V. Orthogonal frequency division multiplexing with index modulation. In Proceedings of the IEEE GLOBECOM, Anaheim, CA, USA, 3–7 December 2012; pp. 4741–4746.
20. Crawford, J.; Ko, Y. Low complexity greedy detection method with generalized multicarrier index keying ofdm. In Proceedings of the 2015 IEEE 26th Annual International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), Hong Kong, China, 30 August–2 September 2015; pp. 688–693.