Physical Layer Security Increased by Perfect Scrambling in COFDM Multipath Fading Transmission Systems

Baojian Gao, Yucheng Zhang, Qiang Liu* and Xingyuan Liu
Information Technology of Northwest University, Xi’an, Shaanxi, China

*Corresponding author

Abstract. With the deeper research on the theory of physical layer security, the method of reducing the security gap through information scrambling has received extensive attention. This method can lower the security gap of the wireless communication systems, thereby reducing the implementation cost of physical layer security. In this paper, a more rigorous definition of perfect scrambling and the complete conditions which should be satisfied by perfect scrambling matrix are presented. On this basis, we proved that with the increase of the size of the perfect scrambling matrix, the perfect scrambling can be asymptotically achieved, and the 0dB security gap can be asymptotically achieved for systems with closed-form expression of bit error rate. Finally, in this paper, a COFDM multi-channel secure transmission scheme is presented by apply perfect information scrambling to the LDPC-OFDM system. Security gaps of the scheme under Gaussian channel and multipath fading channel are simulated, and obtains good results. Our analysis indicates that in the multipath transmission and multipath fading environment, the security gap close to 0dB can be achieved by combining information perfect scrambling and error correction coding with good performance.

Keywords: Security gap; physical layer security; perfect scrambling; COFDM.

1. Introduction

1.1. Background and Related Works

In the mid-20th century, after Shannon proposed the concept of ‘perfect secrecy’, Wyner and others proposed the eavesdropping channel model depicted in Figure 1, and the concept of secrecy capacity was proposed[1-3]. In this model, it is assumed that Eve is an eavesdropper between Alice and Bob. In addition to the different channel conditions, Eve and Bob share other information, and they have the same receiving, demodulating and decoding capabilities. The secrecy capacity equals the difference between the secrecy capacity of the legitimate channel capacity and the wiretap channel capacity. When the quality of the legitimate channel is better than that of the wiretap channel, the difference can be positive by using secret coding, making secure transmission possible. The secrecy capacity is the maximum communication rate for such secure transmissions. With the introduction of the concept of secrecy capacity, more scholars have begun to focus research on physical layer security technologies that aim to increase secrecy capacity and good research achievements has been acquired[3,4,5].

However, as secrecy capacity is a safety measure that is based in information theory, obtaining the secrecy capacity of an actual wireless channel requires knowledge of more complete information source distribution and channel parameters, this is relatively difficult; secrecy capacity uses the equivocation of information as the basis by which it measures secrecy, and it is not suitable for analyzing the secrecy of specific data blocks. For these reasons, in the early 21st century, based on the eavesdropping channel model shown in Figure 1, in [6], scholars such as Kline used the bit error rate (BER) as a measure for
secrecy of the physical layer, converting the difference between different channels into the difference in BER between an eavesdropper and the legitimate receiver, and proposing the concept of the security gap, as is shown in Figure 2. The curve in Figure 2 is the received bit error rate curve of Alice and Bob session. If the SNR at Bob's receiver is greater than or equal to $SNR_{C_1,Min}$ and $BER \leq BER_{B,Max} = 10^{-5}$, at the same time, Eve's receiving SNR is less than or equal to $SNR_{C_2,Max}$ and $BER \geq BER_{E,Min}$, then the formula (1) is defined as the security gap. The security levels of the security gap at $BER_{E,Min} = 0.4 / 0.45 / 0.49$ is corresponding to low, middle and high-level, which are respectively indicated as $SG(0.4,10^{-5})$, $SG(0.45,10^{-5})$ and $SG(0.49,10^{-5})$ with dB as the unit. The smaller the security gap, the lower the cost of implementing physical layer security.

$$SG(BER_{E, Min} \times 10^{-5}) = SNR_{C_1,Min}(dB) - SNR_{C_2,Max}(dB)$$  \hspace{1cm} (1)

Figure 1. The wire-tap channel model.

Figure 2. The security gap.

At the same time, scholars such as Kliner introduced a calculation method that uses LDPC code puncturing to reduce the security gap. This method utilizes the ambiguity of the puncturing position at a low SNR to increase the BER of an eavesdropper, and reinstates the puncturing position under high SNR conditions with the mutual relationship between the coding structures, meanwhile decreasing the legal user’s bit error rate, thereby effectively reducing the security gap. In [7], under a Gaussian multiple access wiretap channel (The multiple access channel consists of two or more sources which send messages to a common receiver), a secure coding scheme which utilizes low-density parity-check (LDPC) codes by employing random bit insertion and puncturing techniques is proposed, which can achieve $SG(0.4,10^{-5}) \approx 1.35dB$.

In order to reduce the security gap, a method of information scrambling is proposed by Baldi M. et al., which is to perform special reversible transformation on the source information, and then coding transmission, and recover information by decoding and inverse transformation at the receiving end. This method achieves error bit transfer, which can lower the security gap and make the physical layer security implementation less cost. Therefore, it has received extensive attention.
In [8], the method that combines information scrambling and error correcting coding (LDPC, BCH codes) is proposed. This method achieves error bit transfer, causing a large increase in the BER of low SNR region. The speed at which the BER increases in high SNR region is smaller than the speed at which it slows down due to the channel code. With this, $SG(0.4,10^{-5})$ can fall to around 1.4dB. Meanwhile, [9] uses a scrambling matrix, but concurrently introduces an Automatic Repeat Request (ARQ) protocol with authentication that reduces $SG(0.4,10^{-5})$ to around 1dB. And [10] introduces the use of HARQ in conjunction with concatenated scrambling, which can achieve $SG(0.4,10^{-5}) \leq 0dB$ with increase the node authentication and feedback function. Recently, [11] combines information scrambling with randomized serially concatenated convolutional codes (RSCCCS), when RSCCCS's code length is $n=8004$ and the information bit length is $k=2000$, $SG(0.4,10^{-5})$ can be reduced to as low as 0.63dB. And [12] consider several LDPC coded transmissions and compare their security gap performance, when QC-LDPC code with $n = 1024$ and code rate $R = \frac{3}{4}$, the security gap with perfect scrambling over the flat AWGN channel can be reduced to 1.66dB. Then [13] improves security performance through the pre-coding of the feed-forward (FF) structure, and propose the joint iterative decoding method between LDPC ($k=480$, $n=960$) and FF codes, the simulation results suggest that the security gap over the AWGN channel can be reduced to 2.26dB.

1.2. Motivation and our Contributions

By analyzing and comparing the above schemes and results, we can see that most of the schemes adopt information scrambling, the combination scheme of information scrambling and error correction coding can achieve the lower security gap. For all that, this scheme still has the following problems:

- Can the perfect information scrambling be achieved? What conditions should be satisfied by the binary perfect scrambling matrix? What the theoretical relationship is between the size of the scrambling matrix and the security gap? These problems have not been solved at present.
- The existing literature mainly focuses on the security gap of single path wireless transmission systems based on modulation of BPSK under Gaussian channel. There are few studies on the security gap of multipath fading channel and the multi-channel wireless transmission systems, so the conclusions are not conducive to application in the actual wireless communication systems.

This paper focuses on the theoretical and applied research of the security gap of point-to-point simplex wireless communication systems. Such wireless communication systems with a small resource consuming have no feedback channel, and it is a basic component of other complex communication systems. In this type of wireless communication systems, the bit error rate curves of the legitimate users and the eavesdropper have the same decreasing trend as in Figure 2, so the minimum security gap of the system is 0dB. Therefore, when the system reaches 0dB security gap, the critical region is small as well, and the transition from the region reserved to legitimate receivers to the region where eavesdroppers should stay becomes sharper[12]. On this occasion, the secure and reliable communication can be realized as long as the signal to noise ratio of the legal channel is slightly higher than eavesdropping channel. Our main contributions are summarized below.

- In this paper, a more rigorous definition of perfect scrambling, and the complete conditions which should be satisfied by perfect scrambling matrix are given. Based on that, we proved that with the increase of the size of the perfect scrambling matrix, the perfect scrambling can be asymptotically achieved. Simulation and analysis of the approximation error of different matrix sizes, the results show that the maximum error would less than $10^{-3}$ when the matrix size is greater than 1000.
- For point-to-point simplex wireless communication systems (without feedback channel) which adopts BPSK modulation and incoherent demodulation, we prove that the 0dB security gap can be asymptotically achieved by perfect scrambling under Gaussian noise.
- Most channels in practice are multipath fading channels, and the widely used broadband wireless communication technologies are the multi-carrier and the multi-channel technique represented by OFDM. In order to verify the practical effect of security gap, a multi-channel
secure transmission scheme based on perfect scrambling and LDPC coding is proposed in COFDM system. The security gap of the scheme under Gaussian channel and multipath fading channel are simulated, the simulation results show that the scheme can achieve a security gap close to 0dB.

The remainder of the paper is organized as follows. In section II, the asymptotically realize methods of perfect scrambling and 0dB security gap are described in detail; Section III provides the multi-channel security transmission scheme based on LDPC-OFDM, and simulation and analysis of security gap of the scheme under Gaussian and multipath noise. Section IV draws conclusions.

2. The Asymptotically Realization Methods of Perfect Scrambling and 0dB Security Gap

The simplex point to point wireless communication systems (without feedback channel) which using BPSK modulation and non-coherent demodulation has the closed-form expression of bit error rate under Gaussian channel, and its ideal security gap is 0dB. In this section, the research is carried out under this system model.

**Definition 1: Perfect scrambling.** If $M$ transformation is applied to $k$ bits information on the sending side which aims to realize information scrambling, and then $M^{-1}$ transformation is carried out on the received information at the receiver’s end therefore reinstating the information, the bit error rate before the $M^{-1}$ transformation is $P_e$ and the bit error rate after the $M^{-1}$ transformation is as indicated in (2), we define the $M$ transformation as perfect scrambling.

$$P_e' = \frac{1}{2} \left(1 - (1 - P_e)^k\right)$$

(2)

From (2), it is easy to see that under perfect scrambling, once there are bit errors in the received $k$ bits information, no matter what the error bit is one or more, the BER will be half of the original frame error rate after descrambling. If there are no error codes inside the received $k$-bit information, there will be no error codes after descrambling. Furthermore, since the first derivative of (2) with respect to $P_e$ is satisfied with $1(1 - P_e)^{k-1} > 0$, so we can draw a conclusion that as $P_e$ increases, the value of $P_e'$ also increases.

Assuming that we already know that at $GF(2)$, scrambling matrix $M = [m_{i,q}]_{k \times k}$ and its inverse matrix is $M^{-1} = [m'_{i,q}]_{k \times k}$. M scrambles the transmitted $k$ long information sequence $v = (v_1, v_2, \ldots, v_k)$ at the sender’s end, achieves $u = vM = (u_1, u_2, \ldots, u_k)$, and then perform non-coded BPSK modulation and non-coherent demodulation on $u$, the demodulated output obtained at the receiver’s end is $u_B = u \oplus e = (u_1 \oplus e_1, u_2 \oplus e_2, \ldots, u_k \oplus e_k)$ ($e = (e_1, e_2, \ldots, e_k)$ is an error pattern). Ultimately, the descrambling matrix $M^{-1} = [m'_{i,q}]_{k \times k}$ is used to de-scramble $u_B$, we get:

$$v_B = u_B M^{-1} = u M^{-1} \oplus e M^{-1} = v \oplus e M^{-1}$$

$$e M^{-1} = (e', e'_2, \ldots, e'_k)$$

$$e'_i = e_i m_{i,q} \oplus e_{2,i} m'_{2,i} \oplus \cdots \oplus e_{k,i} m'_{k,i}$$

(3)

**Theorem 1:** If all columns of the inverse $M^{-1}$ of an invertible matrix $M_{k \times k}$ (where $k$ is an even number) are randomized sequences (and all elements of the sequence are independent and identically-distributed random variables), and the density is 0.5, then transformation of the matrix can asymptotically achieve perfect scrambling.
Proof: Let’s assume that \( P_j \) indicates the probability when the number of “1” is \( j \) in the error pattern vector \( e = (e_1, e_2, \ldots, e_k) \) before descrambling, and that equation (4) is easily achievable. If \( P_{ij}^q \) indicates that when sequential descrambling is carried out on error pattern \( e = (e_1, e_2, \ldots, e_k) \) containing \( j \) number of “1”, \( e_{m_{ij}} \) \((l = 1, 2, \ldots, k)\) in equation (3) contains \( i \) probability of “1”, \( q \) indicates the sequence number of the descrambling matrix, noting that all of the index such as \( i \) and \( j \) in this paper are non-negative integer. As all columns with \( M^{-1}_{ij} \) are random sequences of \( k \) length and all sequences have \( k/2 \) number of “1” (column density 0.5), we arrive at equation (5), from which we can then arrive at \( P_e^{ns} \), the BER function after descrambling (as is shown in equation (6)). \( P_e \) represents the system BER before descrambling, and \( k \) represents the length of information packets.

\[
P_j = \binom{k}{j} P_e^j (1-P_e)^{k-j}
\]

\[
P_{ij}^q = P_{ij} = \frac{\binom{j}{i} \binom{k-j}{k/2-i}}{\binom{q}{k/2}} \quad q = 1, 2, \ldots, k
\]

\[
P_e^{ns} = \sum_{j=1}^{k} \binom{k}{j} P_e^j (1-P_e)^{k-j} \sum_{\min\{\frac{j}{2}\}}^{\min\{\frac{k}{2}\}} P_{ij}
\]

If

\[
p_{od}(j) = \frac{\sum_{i=0}^{\min\{\frac{j}{2}\}} \binom{j}{i} \binom{k-j}{k/2-i}}{\binom{k}{k/2}}, \quad p_{oe}(j) = \frac{\sum_{i=0}^{\min\{\frac{j}{2}\}} \binom{j}{i} \binom{k-j}{k/2-i}}{\binom{k}{k/2}}
\]

Then combine with (5), it is easy to obtain:

\[
\sum_{i=0}^{\min\{\frac{j}{2}\}} P_{ij} = p_{od}(j) + p_{oe}(j) = 1
\]

As \( j \) is a fixed timing, the integer collection obtainable by \( i \) is \( G = \{0,1,2,\ldots,j\} \) (where \( i \) and \( j \) always satisfied with \( i \leq j \)), which makes it easy to see that the number of even and odd numbers in the collection change depending on whether \( j \) is an odd or even number. Therefore, the probability that \( i \) takes an even number (\( p_{oe} \)), and the probability that it takes an odd number (\( p_{od} \)) also changes accordingly, and this determines how \( P_{od}(j) \) and \( P_{oe}(j) \) change. We shall discuss the two cases respectively.

1) When \( j \) is an odd number,

\[
p_{oe} = p_{od} = \frac{1}{2}
\]

And it is easy to achieve the following via combination formula:
And \( j - i \) is an odd number if \( i \) is an even number while being an even number if \( i \) is an odd number, we can therefore get the following result through (7), (8) and (10):

\[
D(j) = |p_{od}(j) - p_{ev}(j)| = 0
\]

(11)

\[
p_{od}(j) = p_{ev}(j) = \frac{1}{2}
\]

(12)

2) When \( j \) is a non-zero even number,

It is easy to obtain:

\[
p_{od} = \begin{cases} \frac{j + 1}{j + 1}, & j \text{ is odd} \\ \frac{j}{j + 1}, & j \text{ is even} \end{cases}
\]

(13)

\[
p_{od} + p_{od} = 1
\]

(14)

\[
|p_{od} - p_{od}| = \frac{1}{j + 1}
\]

(15)

According (15), we can draw a conclusion that as \( j \) increases, the absolute value of the difference between the probabilities that \( i \) is an odd number and \( i \) is an even number decreases to zero. Therefore, the absolute value of the difference between \( p_{od}(j) \) and \( p_{od}(j) \) determined by (15) will also decrease as \( j \) increases. To put it simply, \( D(j) = |p_{od}(j) - p_{od}(j)| \) will decreases as \( j \) increases.

As it is easy to calculate \( D(j) = \frac{1}{k - 1} \) when \( j = 2 \), so we can determine that when \( j \) takes any non-zero even number, the following formula stands:

\[
D(j) \leq \frac{1}{k - 1}
\]

(16)

\[
\lim_{k \to \infty} D(j) = \lim_{k \to \infty} |p_{od}(j) - p_{od}(j)| = 0
\]

(17)

From the outcomes of 1) and 2) above, as \( k \) goes to infinity, we can deduce the following:

\[
P_{od} = \sum_{j=1}^{k} \left( \begin{array}{c} k \\ j \end{array} \right) Pe^{(1 - Pe)^{j+j}} p_{od}(j) = \frac{1}{2} \sum_{j=1}^{k} \left( \begin{array}{c} k \\ j \end{array} \right) Pe^{(1 - Pe)^{j-j}} = \frac{1}{2} \left( 1 - (1 - Pe)^{k} \right)
\]

(18)

Theorem 1 provides us a way to achieve perfect scrambling. The method is to construct a perfect scrambling matrix \( M^{-1} = [m_{i,j}]_{1 \times k} \) as a descrambling matrix, and its inverse matrix \( M = [m_{i,j}]_{1 \times k} \) as a scrambling matrix. In order to achieve good scrambling effects in practical applications, it is necessary to construct a pseudo-random scrambling matrix that satisfies the above conditions. The scrambling matrix used in the later chapters is a perfect scrambling matrix constructed in a pseudo-random manner.
Lemma 1: The 0dB security gap can be asymptotically achieved by perfect scrambling.

3. Security Gap Analysis of COFDM with Perfect Scrambling under Multipath Channel

3.1. Baseband Transmission Model of OFDM System under Multipath Fading Channel

LDPC-OFDM is a wideband wireless communication technology commonly used in 4G and 5G, which belongs to multi-carrier and multi-channel parallel transmission technology. There is little research on the security gap of such communication systems in existing literature. This section focuses on the security gap of perfect scrambling based on LDPC-OFDM system under the condition of Gaussian and multipath fading channels. We can get the baseband model of perfect scrambling based on LDPC-OFDM system under the condition of Gaussian and multipath fading channels, as shown in Figure 3. We refer to the system that contains the perfect information scrambling module as scrambled system, and the system that does not contain the perfect information scrambling module is called the unscrambled system.

![Figure 3. Scrambled/unscrambled COFDM system digital baseband model.](image)

In the eavesdropping channel model (see Figure 1), we assume that the same transmission system as shown in Figure 3 is used between Alice and Bob, and between Alice and Eve. Since Bob's channel parameters $H(i)$ and $W(i)$ are different from Eve's, their SNR and BER are also different. Under this hypothesis, we use the baseband model to simulate and analyze the security gap of the system under different channels.

In the simulation, 100 sets of 3367 bits of information are generated as a source in a pseudo-random manner, and ensure that the probability of occurrence of "0" and "1" in $3367 \times 100$ bits of information is close to 0.5. In order to eliminate the influence of random noise, the above 100 sets of source information are simulated respectively, and the average value of the simulation results as the final simulation result. With a pseudo-random matrix produced through pseudo-randomization as a descrambling matrix. Its column density is extremely close to 0.5 and it uses 16QAM Gray mapping for constellation mapping; for coding, it uses the Euclidean $(4095, 3367)$ EG-LDPC code $^{14}$. It achieves high-order constellation soft demodulation through (19) and takes initialized log-likelihood ratio $L_k(0)$. Substituting the latter into the Log-BP decoding algorithm $^{15}$, the maximum decoding iterations is 30. And set $\Delta f = 15$ kHz, $N=1024$.

$$L_{k,m}(0) = \log \frac{p_k}{p_{\bar{k}}} = \log \frac{\sum \exp \left( \frac{R(k) - U_{m}^{(i)}}{2\sigma} \right)}{\sum \exp \left( \frac{R(k) - U_{m}^{(i)}}{2\sigma} \right)}, \quad 0 \leq k \leq N-1, 1 \leq i \leq 4 \quad (19)$$

Especially, $U_{m}, m=1,2L$ 16 represent the complex symbols corresponding to the constellation point, $Z_{(i)}^{(0)}$ (or $Z_{(i)}^{(1)}$) represent the set of complex symbols corresponding to the constellation points with the first bit as 0 (or 1) in the 4 binary bits corresponding to $U_{m}$.

3.2. Improvements in the Definition of the Security Gap
The security gap defined by (1) is only suitable for the case where the bit error rate curve has an analytical expression, but it is often difficult to satisfy in practical applications. This is because after using error correction coding, the actual bit error rate jumps to zero with the increase of signal to noise ratio, and the bit error rate of $10^{-5}$ does not appear. The corresponding different levels of security gap is $SG(0.4,0)$, $SG(0.45,0)$ and $SG(0.49,0)$, with dB as the unit. This improvement does not change the size of the secure region shown in Figure 2, and the size of the reliable region is reduced, so the legitimate users have higher receiving reliability.

$$SG(BER_{E,Min},0)=SNR_{C_1,Min}(dB) - SNR_{C_2,Max}(dB)$$ (20)

3.3. Security Gap in the Gaussian Channel

In the baseband simulation model shown in Figure 3, we take $H(i)=1, i=0,1,2,L N-1$, which is degraded to base band model in Gaussian noise environment. In this model, we respectively simulate the security gap of scrambled system and unscrambled system, and compare the simulation results. Figure 4 shows the $SG(BER, 0)$ vs. BER curves under Gaussian noise. These curves are also known as the system's security gap curves. The security gap curve is transformed from the error rate curve by formula (20), where the BER is the bit error rate of the eavesdropper, and the bit error rate of the legitimate users is always 0. From this figure, the security gap curves of the scrambled system are upward rapidly, that is, with a slightly increase in the security gap, the bit error rate of the eavesdropper will quickly reach 0.4 or more. Meanwhile the security gap curves of unscrambled system are slow upward. Table 1 shows the values for typical security gap from Figure 4. From the trend of the above curves and the specific data of Table 1, we can get the following conclusions:

- The data in Table 1 indicate that the security gap of the scrambled system is significantly lower than the security gap of the unscrambled system. For example, the 0.4 level security gap from 20.58 dB to 0.34dB. The result shows that for unscrambled system, when the received SNR of the legitimate users is higher than the eavesdropper’s 20.58 dB, the legitimate users can to achieve secure and reliable communication (That is, the legitimate users realizes reliable data reception at the bit error rate of 0, and the eavesdropper receives data at the bit error rate of 0.4 or more). Obviously, this is almost impossible in the actual communication systems. But for scrambled system, this kind of difference (security gap) reduced to 0.34 dB, and therefore a dramatic increase in the ability of legitimate users to achieve secure communication at the physical layer.

- The above results show that the scrambled system can obtain $SG(0.4,0)=0.34dB$ when $k=3367$, this result is closer to the ideal security gap (0dB). It is easy to see that the scrambled system with the above configuration of simulation parameters can achieve the fast approximation of the ideal security gap.

**Figure 4.** The BER vs. SG (BER, 0) curves under Gaussian channel. The red line coordinate point (0.34, 0.4) indicates the 0.4-level security gap in scrambled system. And the blue line coordinate point (20.58, 0.4) indicates the 0.4-level security gap in unscrambled system.
3.4. The Security Gap under Multipath Channel

In the actual wireless communication systems, there are various multipath fading channels. In order to facilitate the study of the security gap of the system shown in Figure 3 under multipath channel, we selected three extended model scenarios defined in the 3G LTE protocol\cite{15}, namely Extended Pedestrian A (EPA), Extended Vehicular A (EVA) and Extended Typical Urban (ETU). Using its parameters, we can obtain the channel impulse response parameters \( H(i), (i = 0, 1, \cdots, N - 1) \) in different multipath scenarios. According to these parameters, the simulation is carried out under different multipath channel models.

Figure 5 shows the security gap curves of the scrambled system in three multipath scenarios: EPA, EVA, and ETU. From these curves we can see that the security gaps of the scrambled system in the multipath scenarios are reduced to around 0.6 dB, and thus secure communication of legitimate users is easier to achieve. Combining the trend of the curves above with security gaps in Table 2, we can get the following conclusions:

- The scrambled system can get the very low security gap in Gaussian (SG (0.4, 0) = 0.34dB) and multipath scenarios (SG (0.4, 0) ≤ 0.83dB). This result shows that the scrambled system (see Figure 3) is easier to ensure the physical layer security in the actual communication, and it has good practical value.

- Comparing the security gap of the scrambled system in EPA, EVA, and ETU, it can easily be seen that the smallest security gap (SG (0.4, 0) =0.53dB) is EPA multipath scenario, which is 0.2dB higher than the security gap of Gaussian. The second is the security gap of ETU, the biggest is the security gap of EVA. Since the number of paths of the EPA is 7, the EVA and the ETU are 9. In addition, the relative power of the ETU is smaller than that of the EVA. Therefore, the smaller the number of multipath paths, the lower the security gap. And when the number of paths is the same, the smaller the relative power, the lower the safety gap.

\[\text{Table 1. The security gap under Gaussian channel.}\]

| system      | SG(0.4,0) | SG(0.45,0) | SG(0.49,0) |
|-------------|-----------|------------|------------|
| unscrambled | 20.58     | 26.18      | 38.94      |
| scrambled   | 0.34      | 0.35       | 0.45       |

\[\text{Table 2. The security gap of different channels.}\]

| System | channel   | SG(0.4,0) | SG(0.45,0) | SG(0.49,0) |
|--------|-----------|-----------|------------|------------|
| scrambled | ETU | 0.62 | 0.69 | 0.78 |
|         | EPA     | 0.53     | 0.58       | 0.68       |
|         | EVA     | 0.83     | 0.89       | 1.03       |

\[\text{Figure 5. The BER vs. SG (BER, 0) curves under ETU, EVA and EPA in scrambled system.}\]
3.5. Comparing Performance

Literature [7], [8], [11], [12] and [13] proposed different methods to reduce the security gap under the non-feedback eavesdropping channel model. Since the specific parameters and application scenarios of these methods are different from this paper, it is difficult to make a fair comparison. However, these methods obtain the minimum security gap that can be achieved by them, so we only compare the minimum security gap that can be achieved by different methods, and the results are shown in Table 3.

| methods          | AWGN-SG(0.4,0) | ETU-SG(0.4,0) | EVA-SG(0.4,0) | EPA-SG(0.4,0) |
|------------------|----------------|--------------|--------------|--------------|
| [7]              | 1.35           | /            | /            | /            |
| [13]             | 2.26           | /            | /            | /            |
| [12]             | 1.66           | /            | /            | /            |
| [8]              | 1.4            | /            | /            | /            |
| [11]             | 0.63           | /            | /            | /            |
| scrambled COFDM system | 0.34     | 0.62         | 0.83         | 0.53         |

The comparison results in Table 3 show that the scrambled COFDM system designed in this paper can obtain the minimum security gap (0.34dB) under Gaussian channel, and obtain the smaller security gap (SG (0.4,0) = 0.53 dB) in multipath scenarios, which is even lower than security gaps of other related literatures under Gaussian channel.

4. Conclusion

In this paper, it is proved that with the increase of the size of perfect scrambling matrix, not only perfect scrambling can be asymptotically achieved, but also the 0 dB security gap can be asymptotically achieved through perfect scrambling. In particular, we propose the scrambled COFDM system. We illustrate our findings via numerical results which demonstrate that this system can quickly close to the 0 dB security gap under Gaussian channel, and can achieve very low security gap under the multipath fading channel. At the same time, the above results also indicate that in the point-to-point simplex wireless communication systems under Gaussian channel, as well as in the multi-carrier and multi-channel wireless communication systems under the multipath fading channel, the low security gap can be achieved.

Acknowledgments

Thanks to the National Natural Science Foundation of China (Grant No.61501372) and the Shaanxi Provincial Natural Science Foundation of China (Grant No.2017JM6012) for funding this study, and thanks to those who provide helping for the research and publication in this paper.

References

[1] Shannon C E. Communication theory of secrecy systems. 1945. Bell System Technical Journal, 2014, 28(4) pp 656-715.

[2] Wyner A D. The wire-tap channel. Bell System Technical Journal, 1975, 54(8) pp 1355-1387

[3] Liang Y and Poor H V, Shamai S. Secure Communication Over Fading Channels. IEEE Transactions on Information Theory, 2008, 54(6) pp 2470-2492

[4] Valliappan N, Lozano A and Heath R W. Antenna Subset Modulation for Secure Millimeter-Wave Wireless Communication. IEEE Transactions on Communications, 2013, 61(8) pp 3231-3245

[5] Goel S and Negi R. Guaranteeing Secrecy using Artificial Noise. IEEE Transactions on Wireless Communications, 2008, 7(6) pp 2180-2189

[6] Klinc D, Ha J and Mclaughlin S W, et al. LDPC for Physical Layer Security. Global Telecommunications Conference, 2009. GLOBECOM. IEEE Xplore, 2010 pp 1-6

[7] Shahbaz S, Akhbari B and Asvadi R. LDPC codes over Gaussian multiple access wiretap channel. Iet Communications, 2018, 12(8) pp 962-969.

[8] Baldi M, Bianchi M and Chiaraluce F. Non-systematic Codes for Physical Layer Security.
Information Theory Workshop. IEEE, 2010 pp 1-5
[9] Baldi M, Bianchi M and Chiaraluce F. Increasing Physical Layer Security through Scrambled Codes and ARQ. IEEE International Conference on Communications Workshops. IEEE, 2011 pp 1-5
[10] Baldi M, Bianchi M and Chiaraluce F. Coding With Scrambling, Concatenation, and HARQ for the AWGN Wire-Tap Channel: A Security Gap Analysis. IEEE Transactions on Information Forensics & Security, 2012, 7(3) pp 883-894
[11] Alireza Nooraiepour and Tolga M. Duman. Randomized Convolutional Codes for the Wiretap Channel. IEEE Transactions on Communications, VOL. 65, NO. 8, AUGUST 2017
[12] Baldi M, Maturo N and Ricciutelli G, et al. Security gap analysis of some LDPC coded transmission schemes over the flat and fast fading Gaussian wire-tap channels. Eurasip Journal on Wireless Communications and Networking, 2015, 2015(1) pp 1-12.
[13] Kwon K, Kim T and Heo J. Pre-coded LDPC coding for physical layer security. Eurasip Journal on Wireless Communications & Networking, 2016, 2016(1) pp 283.
[14] Yu Kou, Shu Lin, and Marc P C. Fossorier. Low-Density Parity-Check Codes Based on Finite Geometries: A Rediscovery and New Results, IEEE Transactions on Information Theory VOL. 47, NO. 7, November 2001
[15] 3GPP TS 36.101 V9.0.0. Evoled Universal Terrestrial Radio Access (E-UTRA). 3GPP:2009