sensors

MDPI

Article

# A Secure Transmission Scheme Based on Artificial Fading for Wireless CrowdSensing Networks

**Zhi-Jiang Xu [1,2,3], Fang-Ni Chen [3,4], Yuan Wu [2] and Yi Gong [3,*]**

1 Zhijiang College, Zhejiang University of Technology, Shaoxing 312030, China; zyfxzj@zjut.edu.cn
2 College of Information Engineering, Zhejiang University of Technology, Hangzhou 310023, China; iewuy@zjut.edu.cn
3 Department of Electrical and Electronic Engineering, Southern University of Science and Technology, Shenzhen 518055, China; cfnini@163.com
4 School of Information and Electronic Engineering, Zhejiang University of Science and Technology, Hangzhou 310023, China
* Correspondence: gongy@sustc.edu.cn; Tel.: +86-0755-8801-8518

Received: 29 August 2018; Accepted: 10 October 2018; Published: 17 October 2018


**Abstract:** For secure transmission of low cost single antenna communication nodes in wireless crowdsensing networks under static channel, a physical layer communication scheme is proposed, where each digital modulated symbol is encrypted by a random key at the transmitter and decrypted with the same key at the receiver. The legal users exploit the synchronized chaotic sequence and the two-stage block interleaver to generate a complex random variable (random key), whereby its envelope obeys the Rayleigh distribution and its phase obeys the uniformly distribution. The modulated symbol is multiplied by the complex random variable (encryption) to imitate the Rayleigh fading of the channel at the transmitting end. The received symbol is divided by the identical complex random variable (decryption) to recover the transmitted message before the digital demodulation at the receiving end. Simulation results show that the bit error ratio (BER) performance of the legitimate users is consistent with the theoretical value of the Rayleigh fading channel, while the corresponding BER of the eavesdropper is too high (about 0.5) to intercept any information.

**Keywords:** chaotic sequence; artificial fading; physical layer security; wireless crowdsensing networks

## 1. Introduction

With the rapid development during the past decades, wireless communication networks have been applied in many fields [1,2]. However, due to the broadcast nature, information is vulnerable to be intercepted by the eavesdroppers which are in the coverage area of the transmission. Security is an important factor in modern wireless communication networks. For the secure transmission of IoT (Internet of Things) [3–5] and crowdsensing [6,7] networks, conventional schemes based on computational complexity are to encrypt the data at the data link layer or the application layer, such as reputation management schemes [8] and privacy-preserving participant selection scheme [9]. Unfortunately, these schemes neither can prevent transmitted information from being cracked nor are suitable for power-constraint sensor devices in crowdsensing networks. At present, physical layer security provides a new paradigm that can effectively protect information from being eavesdropped by exploiting stochastic characteristics of wireless channels [10,11].

Maurer firstly put forward the idea that legitimate parties can extract secret key by exploiting channel characteristics in [12]. Subsequently, Hershey et al. [13] proposed that legitimate parties could use the reciprocity of the wireless channel to generate the secret key in Time Division Duplexing (TDD) systems. The independence and randomness of the reciprocal channel guarantee the security of

the key. At present, most of the key-extracting methods are based on time-varying channels [14,15]. However, the wireless channel in some application scenarios is static or quasi-static, and the key generated with such methods is not suitable for encryption, because the key entropy or the key generation rate is too low. To improve the security performance, diversity technology based on multi-antenna system and relay system has attracted more and more attention [16–20]. However, a device in a low-cost wireless network, e.g., the sensor node in WSN (Wireless Sensor Network), is usually equipped with only one antenna. Furthermore, the physical-layer key generation method assumes that the eavesdropping device is placed outside the half-a-wavelength range of the legitimate receiver. However, this assumption has not been rigorously evaluated in the open literature, and it might be invalid in some practical scenarios [21], which do not experience extensive multi-path scattering. It is shown in [22] that in reality a strong correlation may be encountered between the main channel and the wiretap channel, even when the eavesdropper is located significantly more than half-a-wavelength away from the legitimate receiver.

Recently, the use of digital modulation encryption as a new physical layer security technology has attracted lots of attention. Because its security does not depend on the channel characteristics, this kind of physical layer encryption technology has inherent advantages in the communication security aspect under the static or quasi-static channel environment. In [23], Zang et al. proposed an encrypting scheme based on MSK (Minimum Shift Keying) modulator which possesses eight different structures. In this scheme, the legitimate transceiver and receiver synchronously change the structure of the modulator according to a set of random numbers generated from the $m$ sequence. The eavesdropper cannot demodulate the received signal correctly without knowing the structure of the modulator. However, considering the high standardization of modern communication protocols, when the eavesdropper knows the modulator structure and part of the original text, the $m$ sequence used to control the modulator structure may be deciphered by the eavesdropper. In [24], Husain et al. proposed a physical layer encryption scheme based on the diversity of 16QAM (Quadrature Amplitude Modulation) constellation mapping which was regarded as secret key and unavailable for eavesdroppers. This scheme can achieve the perfect secret proposed by Shannon and provide a promising prospect in the military area. However, this scheme is not suitable for highly standardized civilian communications. Ma et al. [25] proposed a scheme to secure communication with the aid of symbol rotation and artificial noise. Wang proposed to secure OFDM (Orthogonal Frequency Division Multiplexing) by two-stage chaos mapping and symbol rotation [26]. However, in those two schemes, only the phase of the constellation is changed, and the eavesdropper can obtain transmitting data by cryptanalysis.

Because chaotic signals have impulse-like auto-correlation and low cross-correlation values, many DCSK (differential Chaos Shift Keying) modulation technique for secure multi-user communication systems have been studied and evaluated [27,28]. Cooperative relaying and friendly jamming schemes have been recognized as a promising approach to enhancing the security. A comprehensive survey of the recent works on cooperative relaying and jamming techniques for securing wireless transmissions is provided in [29]. Artificial noise (AN) transmission is another effective approach to enhancing security provided that the instantaneous CSI (Channel State Information) of each eavesdropper is not available. A secrecy beamforming scheme, which exploits AN-aided to secure multiple-input single-output non-orthogonal multiple access (MISO-NOMA) transmission, is proposed in [19]. The secrecy capacities under various channel fading with AN are analyzed in [20,30,31]. Furthermore, Atallah et al. [32] proposed different protocols to foil the eavesdropper. Most of the recently proposed AN schemes are based on a hypothesis that the number of transmit antennas is larger than that of the receive antennas [20]. This strategy might fail when both legitimate parties are equipped with single antennas in some scenarios.

In this paper, a physical layer encryption technique based on artificial Rayleigh fading is proposed for the security of digital transmission of low cost single antenna wireless nodes in a static or quasi-static channels. The main idea of the proposed scheme is as follows. For the transmitter, each digitally

modulated symbol is multiplied by a complex random variable used to imitate channel fading in wireless communications. For legitimate recipients, the identical complex random variable can be generated synchronously so that the transmitted information can be recovered correctly. For eavesdroppers, if they could not acquire synchronously the complex random variable, no information can be obtained. In this paper, a synchronous chaotic sequence generator is used to generate an uniformly distribution random sequence, and then a complex random variable whose envelope is Rayleigh distribution and whose phase is an uniformly distributed is generated by the transformation of the uniformly distribution.

The main contributions of this paper are as follows. (1) A physical layer encryption method is proposed. The legitimate parties in a static or quasi-static channel generate complex random variables (key) with a synchronous chaotic sequence, which is used to simulate the static or quasi-static channel into a Rayleigh fading channel. (2) A two-stage interleaver is introduced to make a synchronous chaotic sequence divided into four groups of irrelevant sequences. (3) The scrambling of chaotic sequences by the introduced two-stage interleaver significantly increases the difficulty of the eavesdropper's cracking.

The rest of this paper is organized as follows. The proposed physical layer encryption scheme, including the structure of the two-stage interleaver and the generation process of complex Gauss random variables, is elaborated in Section 2. We derive the theoretical BER (bit error ratio) for the proposed communication system, and verify it by MATLAB in Section 3. The simulation results show that eavesdroppers cannot intercept any effective information under the condition of unknown (or unsynchronized) chaotic sequence and/or the structure of the two-stage interleaver. Finally, a summary is made in Section 4.

## 2. Secure Communication Scheme

In this paper, we assume that both legitimate parties are equipped with single antenna, and their communication protocols are open and standardized. We consider the secure transmission of the communication between the two parties in a static/quasi-static channel. In wireless communication, the amplitude and phase of the signal sent by the sender are randomly faded or fluctuated due to the random characteristics of the channel. If the channel estimation is not accurate enough, the SNR (signal-to-noise ratio) of the receiver may deteriorate dramatically and the demodulator cannot work properly, which results in a high BER. The most serious consequence is the inability to communicate, that means the receiver fails to obtain any information. Inspired by this, we propose the following encryption communication scheme. The training sequence used for channel estimation is sent according to the communication protocol, and the legitimate users or eavesdroppers can estimate the CSI accurately. For binary bitstreams that represent confidential information, the legitimate parties need to be encrypted and decrypted to prevent interception by the eavesdroppers. We emphasize here that both encryption process and decryption process are implemented in the physical layer. A synchronous chaotic generator is employed to generate random complex variables (also called the secret key) $h_k$, whose magnitude follows Rayleigh distribution and the phase follows an uniformly distribution within $(-\pi, \pi)$, respectively. The binary bitstream to be transmitted is mapped into symbols $\{s_k\}$ after a digital modulator (e.g., 16QAM). Then, $s_k$ is multiplied by a random complex variable $h_k$ (also called encryption), which imitates the random fading in wireless communication. The legitimate receiver generates a secret key that is completely synchronized and consistent with that of the transmitter. The received symbol is divided by the key to recover the encrypted symbol (also called decryption). Thus, the digital demodulator can work properly. On the contrary, the eavesdropper uses the channel estimation of the training sequence in the static channel to demodulate the received symbols that have experienced the artificial random fading channel. Obviously, its demodulator cannot work properly, which results in high BER. Therefore, the secret information is hard to intercept.

This section mainly introduces the baseband communication system with the secure transmission shown in Figure 1, including the chaotic sequence generator, the process of generating the complex

random variable, and the structure and working mode of the two-stage block interleaver. The "key" in Figure 1 is composed of the mapping equation of chaotic sequence, the initial value and the number of iterations before chaotic generator enters into chaotic period. Furthermore, we assume that the chaotic generator of legitimate receiver is perfectly synchronized with that of the transmitter.

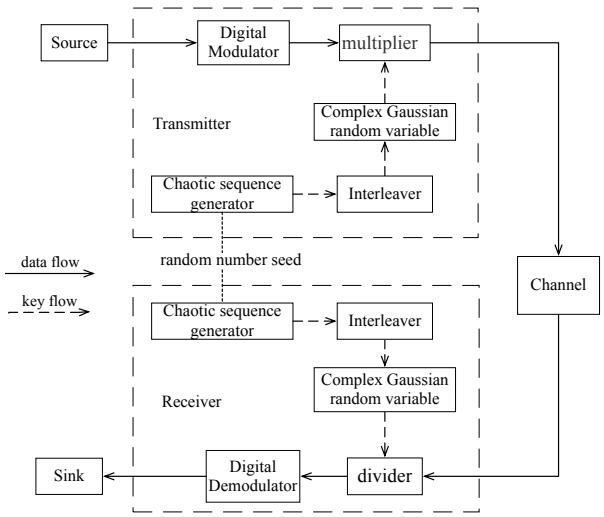



**Figure 1.** Block diagram of the proposed secure communication system with artificial Rayleigh fading and two-stage block interleaver (baseband only).

### *2.1. Generation of Random Complex Variables (Secret Key)*

In wireless communications, Rayleigh [33] is the most common statistical model to describe the time-varying characteristics of the received envelope statistics of flat fading signals or independent multi-path components. In this paper, an artificial Rayleigh model is used to imitate channel fading. The fading coefficient, $h_k$, can be expressed as

$$h_k = h_{k,R} + \imath h_{k,I} = \mu_k e^{\imath\theta_k} , \tag{1}$$

where $h_{k,R}$ and $h_{k,I}$ are two independent random variables of normal distribution with a mean value of 0 and a variance of $\frac{1}{2}$, respectively, such that the power of $h_k$ is equal to 1, i.e., $h_{k,R}, h_{k,I} \sim \mathcal{N}(0, \frac{1}{2})$ and $\mathbb{E}[|h_k|^2] = 1$. In Equation (1), $\mu_k$ and $\theta_k$ are the envelope and phase of $h_k$ respectively. Thus, $\mu_k$ obeys Rayleigh distribution, and $\theta_k$ obeys the uniformly distribution within $(-\pi, \pi)$. The mean value of $h_k$ is 0, which means $\mathbb{E}[h_k] = \mathbb{E}[h_{k,R} + h_{k,I}] = 0$. To increase the randomness of secret keys, the keys should be independent with each other, i.e.,

$$\mathbb{E}[h_k h_l^*] = \mathbb{E}[(h_{k,R} + \imath h_{k,I})(h_{l,R} - \imath h_{l,I})] = \mathbb{E}[h_{k,R}h_{l,R} + h_{k,I}h_{l,I}] + \imath\mathbb{E}[h_{k,I}h_{l,R} - h_{k,R}h_{l,I}] = \delta_{kl} , \tag{2}$$

where $\mathbb{E}[\cdot]$ denotes expected operator, and $(\cdot)^*$ denotes conjugate operator.

To make it harder for eavesdropper to decipher, a complex random variable, $h_k$, is generated to change the envelope and phase of a digital modulated symbol $s_k$. Thus, the transmitted symbol, $x_k$, can be given by

$$x_k = s_k h_k = s_k \mu_k e^{\imath\theta_k}, \ 1 \le k \le N , \tag{3}$$

where $N$ represents the number of symbols to be transmitted. It is reasonable to assume that both $s_k$ and $h_k$ are independent with each other because they come from different sources. Moreover, due to the normalized fading power, $\mathbb{E}[|h_k|^2] = 1$, the power of the transmitted symbols, $\mathbb{E}[|x_k|^2]$, can be expressed as

$$\mathbb{E}\left[|x_k|^2\right] = \mathbb{E}\left[|s_k|^2\right]\mathbb{E}\left[|h_k|^2\right] = \mathbb{E}\left[|s_k|^2\right] . \tag{4}$$

This means that the encryption operation does not introduce additional power consumption.

We note that $h_k$ in Equation (1) is composed of two independent normal distribution random variables. It is well known that a standard normal distributed random variable can be transformed by two independent uniformly distribution random variables through the classic Box–Muller equation [34]. Let $x, y \sim \mathcal{U}(0,1)$ and $z \sim \mathcal{N}(0,1)$; the expression of Box–Muller equation is written as

$$z = \sqrt{-2\ln x}\cos(2\pi y)\,. \tag{5}$$

Chaos is a deterministic pseudorandom process that occurs in nonlinear dynamic systems. This process is aperiodic, non-convergent and highly sensitive to initial values [35]. Owing to the sensitive dependence on initial conditions, it allows generating an infinite number of uncorrelated signals. In this paper, a Tent mapping [36] is chose to generate the uniformly distributed chaotic sequence $\{b_i\}$. The Tent mapping equation is written as

$$b_{i+1} = 2\beta(1- \mid b_i \mid) - 1, \;\; i = 1, 2, \cdots \tag{6}$$

An appropriate parameter $\beta$ in Equation (6) can guarantee that $\{b_i\}$ is a uniformly distributed in the range of $(-1, 1)$, and be set to 0.999 throughout this paper. A sampled chaotic sequence with length $L = 1000$, and the initial seed $b_1 \in (-1, 1)$ is generated randomly. As we known, an ECDF (Empirical Cumulative Distribution Function) is the distribution function associated with the empirical measure of a sample in statistics. Therefore, an ECDF is introduced to measure the distribution of random sequences. Let $(x_1, \cdots, x_n)$ be IID (Independent, Identically Distributed) real random variables with the common cumulative distribution function $F(t)$, then the ECDF is defined as

$$\widehat{F}_n(t) = \frac{\text{number of elements in the sample} \leq t}{n} = \frac{1}{n}\sum_{i=1}^{n} \mathbf{1}_{x_i \leq t}\,, \tag{7}$$

where $\mathbf{1}_A$ is the indicator of event $A$.

As shown in Figure 2, ECDF of a sampled chaotic sequence is a straight line with slope 0.5. It indicates that $\{b_i\} \in [-1, 1]$ obeys uniformly distribution. Furthermore, to verify its correlation, the autocorrelation coefficient is introduced and defined as [37]

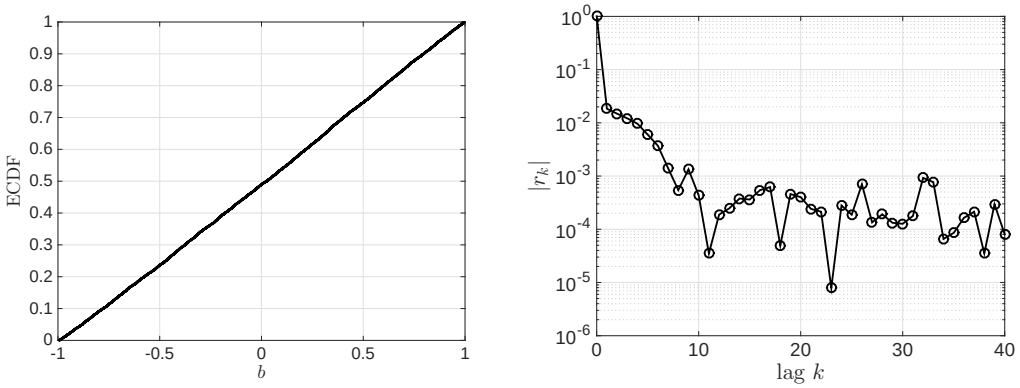
$$r_k = \frac{c_k}{c_0}\,, c_k = \frac{1}{L-k}\sum_{i=1}^{L-k}(b_i - \bar{b})(b_{i+k} - \bar{b})\,, \bar{b} = \frac{1}{L}\sum_{i=1}^{L} b_i\,. \tag{8}$$

Absolute autocorrelation coefficients of the first 41 lags of a sampled chaotic sequence, $|r_k|$ $(k = 0, 1, \cdots, 40)$, are calculated and shown in Figure 2. It is noted that when the lag is greater than 1, $|r_k|$ is close to 0.01, and it stays around 0.001 when the lags are greater than 10. Therefore, it is reasonable to assume that uniformly distribution sequence $\{b_i\}$ is IID.

A new chaotic sequence $a_i \sim \mathcal{U}(0,1)$, which satisfies the condition of Box–Muller transformation, is obtained through a simple linear transformation defined as

$$a_i = \frac{b_i + 1}{2}\,. \tag{9}$$

According to Equations (1) and (5), we note that four independent and uniformly distributed random variables are required to generate a complex normal distribution random variable through Box–Muller transformation. Intuitively, four chaotic generators should be employed in a legitimate user. This greatly increases the complexity of both parties. To simplify the structure of the system, a two-stage block interleaver is introduced in our proposed secure scheme. With the aid of the interleaver, only one chaotic sequence generator is needed to produce four uniformly distribution random variables that satisfies the requirement of Equation (1), i.e., $h_{k,R}$ and $h_{k,I}$ are two independent random variables.

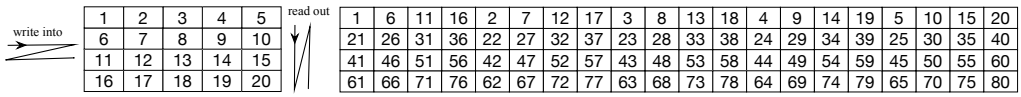



(**a**) ECDF (**b**) Autocorrelation

**Figure 2.** Empirical cumulative distribution function and absolute autocorrelation coefficient of a sampled chaotic sequence $\{b_i\}$ using Tent mapping equation, where functions cdfplot() and xcorr() in MATLAB are used to calculate ECDF and $r_k$, respectively.

### *2.2. Two-Stage Block Interleaver*

As mentioned in Section 2.1, the chaotic generator shown in Equation (6) could generate an uniformly distributed chaotic sequence $\{b_i\}$. Two subsets extracted from the chaotic sequence $\{b_i, i = 1, 2, \cdots, \}$, e.g., $\{b_1, b_9, b_{17}, b_{25}, b_{33}, \cdots\}$ and $\{b_5, b_{13}, b_{21}, b_{29}, b_{37} \cdots\}$, can be considered as independent with each other if their cross-correlation is small enough. To generate four independent chaotic sequences from a chaotic generator, a two-stage block interleaver is proposed, and its structure is shown as Figure 3.




| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 |
| 16 | 17 | 18 | 19 | 20 |

(**a**) first-stage

| 1 | 6 | 11 | 16 | 2 | 7 | 12 | 17 | 3 | 8 | 13 | 18 | 4 | 9 | 14 | 19 | 5 | 10 | 15 | 20 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 21 | 26 | 31 | 36 | 22 | 27 | 32 | 37 | 23 | 28 | 33 | 38 | 24 | 29 | 34 | 39 | 25 | 30 | 35 | 40 |
| 41 | 46 | 51 | 56 | 42 | 47 | 52 | 57 | 43 | 48 | 53 | 58 | 44 | 49 | 54 | 59 | 45 | 50 | 55 | 60 |
| 61 | 66 | 71 | 76 | 62 | 67 | 72 | 77 | 63 | 68 | 73 | 78 | 64 | 69 | 74 | 79 | 65 | 70 | 75 | 80 |

(**b**) second-stage

**Figure 3.** Two-stage block interleaver.

The numbers in Figure 3 represent the original order of chaotic sequence generated by the chaotic generator. The work mode of those two block interleavers is written in column-wise and read in line-wise. The output of the first-stage block interleaver is the input of the second-stage block interleaver. Thus, four independent chaotic sequences are obtained via the scrambling by the two-stage block interleaver, respectively, i.e.,

$$x_1 = \{b_1, b_{21}, b_{41}, b_{61}, b_6, b_{26}, b_{46}, b_{66}, \cdots, b_2, b_{22}, b_{42}, b_{62}\}, \tag{10a}$$

$$x_2 = \{b_7, b_{27}, b_{47}, b_{67}, b_{12}, b_{32}, b_{52}, b_{72}, \cdots, b_8, b_{28}, b_{48}, b_{68}\}, \tag{10b}$$

$$y_1 = \{b_{13}, b_{33}, b_{53}, b_{73}, b_{18}, b_{38}, b_{58}, b_{78}, \cdots, b_{14}, b_{34}, b_{54}, b_{74}\}, \tag{10c}$$

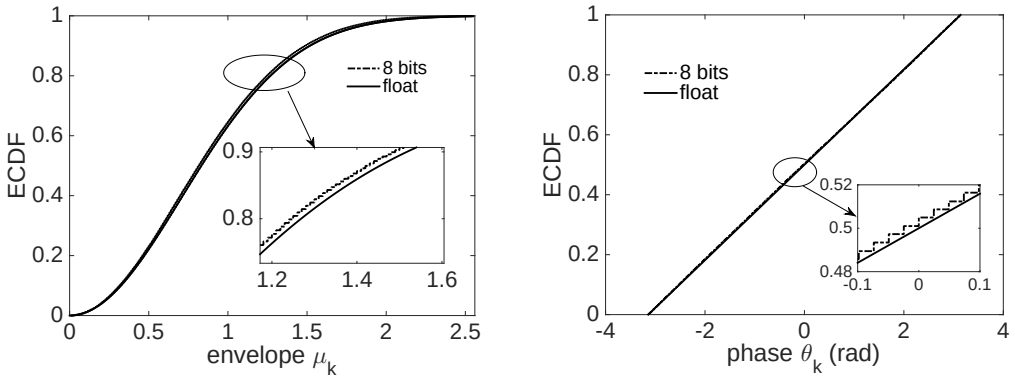
$$y_2 = \{b_{19}, b_{39}, b_{59}, b_{79}, b_5, b_{25}, b_{45}, b_{65}, \cdots, b_{20}, b_{40}, b_{60}, b_{80}\}. \tag{10d}$$

For each chaotic sequence in Equation (10), the adjacent offset is greater than 20. Hence, as can be seen in Figure 2, the absolute autocorrelation coefficient is less than 0.001. Similarly, for each pair of chaotic sequences $(x_i, y_i), i \in \{1, 2\}$, the offset is 12, thus its corresponding absolute cross-correlation coefficient is also less than 0.001. Therefore, four chaotic sequences via the proposed two-stage block interleaver meet the requirements of independence to generate a complex random key.

To improve the efficiency of generating random keys, two two-stage block interleavers, as shown in Figure 3, are introduced to perform read/write operations on those two interleavers in turn. When 80 chaotic numbers are written to the first Interleaver A, the subsequent 80 chaotic numbers are written to the second Interleaver B. When Interleaver A reads empty, Interleaver B must have been filled, and Interleavers A and B exchange read/write operation in turn. For each digital modulated symbol, four chaotic numbers are generated by the chaotic generator. Four independent chaotic numbers are outputted by the proposed two-stage interleaver, and then transformed by Equation (5), a complex random variable shown in Equation (1) is generated. Furthermore, another benefit of the introduced interleaver is that even if the eavesdropper synchronizes with the transmitter's chaotic generator by some means, but if the structure of the interleaver is unknown, the eavesdropper still fails to generate a random key which is consistent with that of the transmitter. The consequence is that the eavesdropper cannot correctly demodulate the received symbols. Therefore, the introduced interleaver increases the difficulty of key cracking and further improves the security of communication.

### *2.3. Quantization of Complex Random Variables*

The initial seed $b_1 \in (-1, 1)$ is randomly generated, the parameter $\beta$ is set to 0.999 and a chaotic sequence of length 800,000 is generated, then its corresponding complex Gauss random variable sequence of length 200,000, $\{h_k\}$, is also generated via the proposed interleaver and the Box–Muller transformation. It is easy to calculate its magnitude $\{\mu_k\}$ and phase $\{\theta_k\}$, and their corresponding ECDFs are shown in Figure 4.




(**a**) Envelope (**b**) Phase

**Figure 4.** Empirical cumulative distribution function diagram of normalize complex Gauss random variable, in which solid line represents floating point operations, and dashed line represents 8-bit quantization operations.

It can be seen in Figure 4 that the magnitude obeys the Rayleigh distribution and the phase obeys the uniformly distribution on $(-\pi, \pi)$, which are completely consistent with the theory. In practical engineering, there is a quantitative problem because of the limitation of the finite word length of the digital-to-analog conversion device. Note that the aforementioned envelope of complex Gauss random variable obeys the Rayleigh distribution, and the power of $h_k$ is normalized to 1. Thus, the PDF (Probability Density Function) of the envelope, $f_\mu(x)$, is given by

$$f_\mu(x) = 2xe^{-x^2}, \tag{11}$$

and its cumulative distribution function (CDF) is written as

$$\Pr(\mu \le x) = \int_0^x f_\mu(t)\mathrm{d}t = 1 - e^{-x^2}. \tag{12}$$

According to Equation (12), it is easy to know that the probability of envelope greater than 2.55 is 0.14%. Thus, a $n = 8$ quantized bits are used to represent size of envelope, whose range is $[0, 2.55]$, i.e., the envelope amplitude of the corresponding 1 bits is 0.01. In Addition, for envelope amplitude greater than 2.55, it is truncated to 2.55. Similarly, an 8-bit quantization is also used in the phase on $(-\pi, \pi)$, and the corresponding phase of one bit is $\frac{\pi}{128}$ radians. Whether the quantified complex Gaussian random variable as a key satisfies the one-time pad depends on the analysis of the key characteristics. Here, whether the quantified complex Gauss random variable obeys strictly IID is analyzed. For complex Gauss variables, satisfying the correlation shown in Equation (2) means they are independent with each other. We use the simulation to verify the correlation of quantified random variable. In this simulation, 200,000 samples of complex gaussian random variables $\{h_k\}$ are generated, whose envelope and phase are quantified by 8-bit, as shown in Figure 4. It can be seen that the 8-bit quantization is close enough to the floating point operations.

Furthermore, to verify the independent expression in Equation (2), a normalized correlation coefficient is introduced and defined as:

$$r_{q,k} = \frac{\sum_{i=1}^{L-k}(h_{q,i} - \overline{h_q})(h_{q,i+k} - \overline{h_q})^*}{\sum_{i=1}^{L}(h_{q,i} - \overline{h_q})(h_{q,i} - \overline{h_q})^*}, \overline{h_q} = \frac{1}{L}\sum_{i=1}^{L} h_{q,i}, \tag{13}$$

where $\{h_{q,i}\}$ is a quantized complex Gaussian random variable with length of $L$, the superscript $(\cdot)^*$ denotes complex conjugate operator, and $k$ is the lag.

In this simulation, the absolute value of normalized correlation coefficient with lags $k$, $|r_{q,k}|$, are calculated and shown in Figure 5. It can be seen that $|r_{q,k}|$ is less than 0.01 when the offset is greater than 1, which means that the quantified complex random variables are IID. Furthermore, it is noted that the chaotic sequence has a strong sensitivity to the initial seed, and the imperceptible changes of the initial seed will make the chaotic sequence to change greatly. Therefore, legitimate parties can simultaneously change the initial seed to increase difficulty of deciphering the chaotic sequence by eavesdroppers. The analysis of key space and decoding time based on the two-stage chaotic map OFDM security transmission are presented in [38]. Similar to this literature, our proposed secure transmission scheme also has a large key space and long crack time.

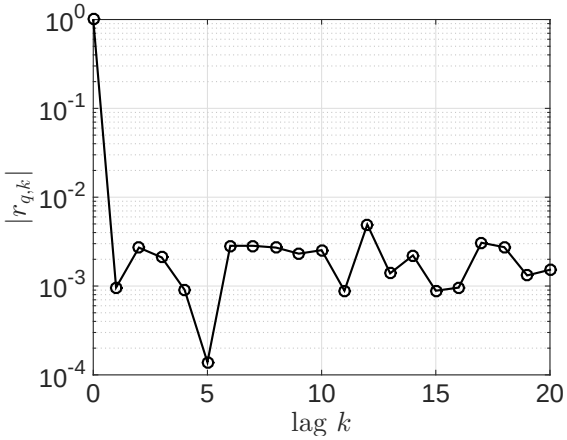



**Figure 5.** Absolute value of normalized correlation coefficient of complex Gauss random variables with 8-bit quantization.

## 3. Performance Analysis and Simulation

### *3.1. Theoretical BER*

Assuming that the power spectral density of white noise $n(t)$ is $\frac{N_0}{2}$, the bandwidth of signal is $B$ and the interval of symbol is $T_s$. $E_b$ denotes the bit energy and $E_s$ represents the symbol energy. If shape filter satisfies $T_s = \frac{1}{B}$, and Gray code mapping is used in digital modulation, then the relationship between bit signal to noise ratio $\gamma_b$ and symbol signal to noise ration $\gamma_s$, BER (Bit Error Ratio) $P_b$ and SER (Symbol Error Ratio) $P_s$ are give by

$$\begin{cases} \gamma_b = \dfrac{E_b}{N_o} = \dfrac{E_s}{N_o \log_2 M} = \dfrac{\gamma_s}{\log_2 M}, \\ P_b \cong \dfrac{P_s}{\log_2 M}. \end{cases} \tag{14}$$

Table 6.1 in [33] lists the common digital modulations and their corresponding SER/BER when coherent demodulation is used, e.g., SER of the correlated demodulation under AWGN for rectangular $M$QAM($M > 4$) is

$$P_s(\gamma_s) = 1 - \left(1 - \frac{2(\sqrt{M}-1)}{\sqrt{M}} Q\left(\sqrt{\frac{3\gamma_s}{M-1}}\right)\right)^2 \tag{15}$$

and BER is

$$P_b(\gamma_b) \simeq \frac{4}{\log_2 M} Q\left(\sqrt{\frac{3\gamma_b \log_2 M}{M-1}}\right), \tag{16}$$

where $\mathcal{Q}(x)$ function is defined as

$$\mathcal{Q}(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}} e^{-\frac{t^2}{2}} \mathrm{d}t = \frac{1}{2}\mathrm{erfc}\left(\frac{x}{\sqrt{2}}\right), \tag{17}$$

and $\mathrm{erfc}(x)$ is the complementary error function.

Next, we derive the theoretical BER expression of the legitimate receiver under Rayleigh fading channel. As mentioned above, the envelope of complex Gauss random variable, $\mu_k$, obeys Rayleigh distribution and its power $\mathbb{E}[\mu_k^2] = 1$. Thus, $\lambda_k = \mu_k^2$ obeys the exponential distribution with a parameter of 1, i.e., its PDF is given by

$$f_\lambda(\lambda_k) = e^{-\lambda_k}. \tag{18}$$

In the static additive white Gaussian noise (AWGN) channel, the symbol received by the legitimate user is

$$r_k = s_k h_k + n_k, \tag{19}$$

where complex Gaussian white noise $n_k \sim \mathcal{CN}(0, N_0)$. After the symbol is encrypted, its instantaneous SER (or BER) is $\lambda_k \gamma_s$ ($\lambda_k \gamma_b$), and the average SER (or BER) is obtained by statistical averaging, i.e.,

$$\overline{P_s}(\gamma_s) = \int_0^\infty P_s(\lambda\gamma_s) e^{-\lambda} d\lambda \tag{20a}$$

$$\overline{P_b}(\gamma_b) = \int_0^\infty P_b(\lambda\gamma_b) e^{-\lambda} d\lambda \tag{20b}$$

Combining Equation (20) and Table 6.1 in [33], the BER expressions of BPSK, 4QAM and 16QAM with proposed encryption scheme are given by

$$\overline{P_b}(\gamma_b) = \begin{cases} \frac{1}{2}\left(1 - \sqrt{\frac{\gamma_b}{1+\gamma_b}}\right) & \text{BPSK/QPSK/4QAM} \\ \frac{1}{\log_2 M}\left(1 - \sqrt{\frac{\gamma_b \log_2 M}{\csc^2\left(\frac{\pi}{M}\right) + \gamma_b \log_2 M}}\right) & M\text{PSK}(M > 4) \\ \frac{2}{\log_2 M}\left(1 - \sqrt{\frac{3\gamma_b \log_2 M}{2(M-1) + 3\gamma_b \log_2 M}}\right) & \text{Rectangular } M\text{QAM}(M > 4) \end{cases} \quad (21)$$

### 3.2. Simulations and Analysis

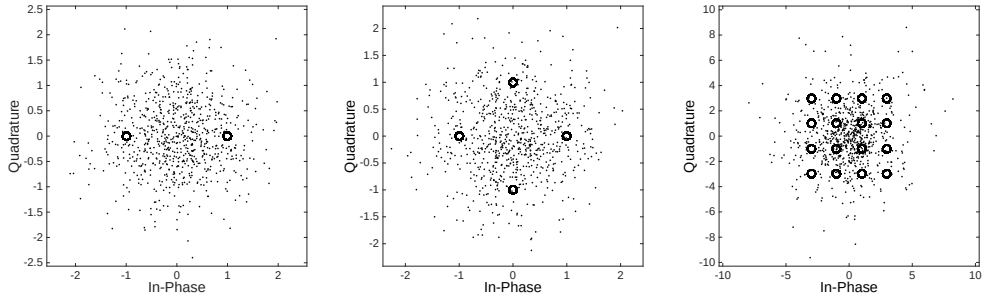
In this section, we carry out Matlab (ver. R2014b) simulation on the system shown in Figure 1 to verify the BER performance of legal user and eavesdropper, respectively. The channel is assumed to be static AWGN channel and is invariant in the whole simulation. The parameter in the Tent mapping $\beta$ is set to 0.999, and initial seed of chaotic sequence $b_1$ is a random number in $(-1, 1)$. Figure 6 shows the encrypted constellation of BPSK, QPSK, and 16QAM, respectively, when $\gamma_b = 20$ dB. It can be seen that the random variation of its phase and amplitude leads to the random distribution of the digital modulated symbol. AMC (Automatic Modulation Classification) [39] and DMC (Digital Modulation Classification) [40] technologies for modulation recognition based on time periodicity of constellation change are bound to fail because their constellation does not show periodic changes in time. Therefore, the proposed transmission scheme has good security.

The chaotic generator at the legitimate receiver is assumed to be synchronized perfectly, i.e., the generated complex random variables are identical with that of the transmitter. Based on Equation (19), the legitimate user decrypts the received symbol $r_k$ before demodulation, i.e., the decrypted symbol $\widehat{s_k}$ is given by

$$\widehat{s_k} = \frac{r_k}{h_k} = s_k + \frac{n_k}{h_k}. \quad (22)$$

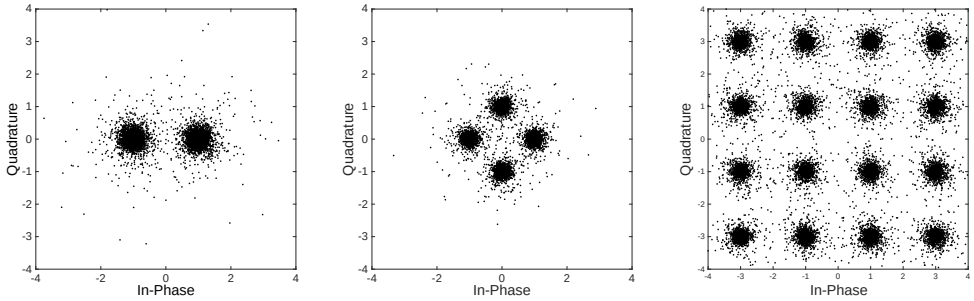
Figure 7 shows the decrypted constellation of the received symbols (10,000 symbols) with $\gamma_b =$ 20 dB. Because the envelope of the complex normal random variable obeys Rayleigh distribution, there are lots of very small envelope amplitude values, i.e., there are many symbols near the $0 + 0\imath$ neighborhood, as shown in Figure 6. The term $n_k/h_k$ in Equation (22) produces a relatively large value, i.e., the decryption operation amplifies significantly the complex Gauss noise $n_k$. Figure 7 shows the constellation of 10,000 decrypted symbols (the range of quadrature and in-phase components is limited to (−4,4)), and there are many symbols of magnitude far exceeding that of the corresponding digitally modulated constellation. In Figure 7, it can be seen that the influence of noise amplification is obviously messy in the vicinity of the digital modulation constellation. However, it is still possible to distinguish the type of its modulation, and most of the symbols are able to be demodulated correctly. BER will be further decreased if the constellation after decryption is clearer. Otherwise, it will be more indistinct. Meanwhile, if the eavesdropper does not get the secret key, its constellation is very indistinct and the demodulator cannot work properly.

Figure 8 shows the BER performances of the legitimate receiver and eavesdropper, respectively. As shown in Figure 8, BER of the legitimate receiver decreases with the increase of bit SNR $E_b/N_0$, and the simulation results fully conform to the theoretical derivation colorred in Equation (21). Meanwhile, because the eavesdropper does not recover the key consistent with the sender, its BER will not decrease with the increase of the bit SNR, which is about 0.5. As a result, the eavesdropper does not intercept any effective information.




(**a**) BPSK (**b**) QPSK (**c**) 16QAM

**Figure 6.** Constellations of the received 800 symbols with bit signal to noise ratio $\gamma_b = 20$ dB, where its corresponding digital modulation constellation is represented by the marker "o".




(**a**) BPSK (**b**) QPSK (**c**) 16QAM

**Figure 7.** Constellation (10,000 symbols) after demodulation of the legitimate user with $\gamma_b = 20$ dB.

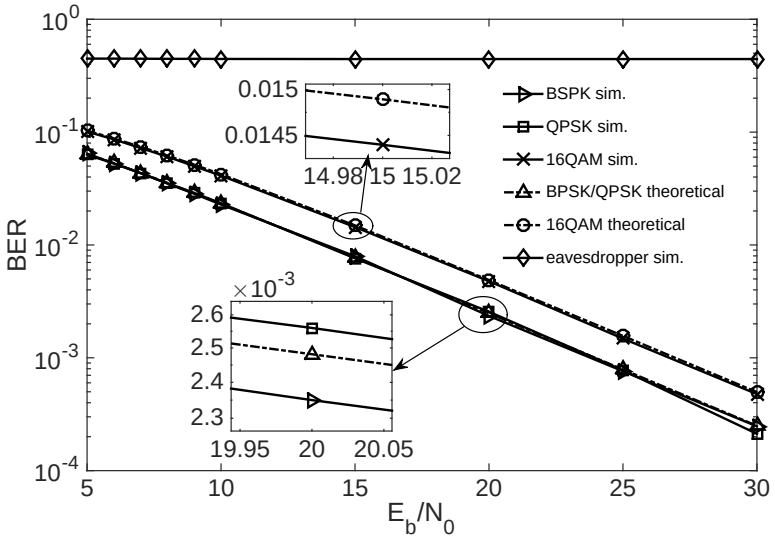



**Figure 8.** BER of the legal user and eavesdropper with various digital modulations.

### *3.3. Secrecy Capacity*

Considering the case of a complex, flat-fading channel with the receiver having perfect knowledge of the channel state, the ergodic capacity of such a channel is given by [41]:

$$C = \mathbb{E}\left[\log_2\left(1 + \frac{|h|^2 P}{\sigma_w^2}\right)\right], \tag{23}$$

where $\mathbb{E}(\cdot)$ denotes the expectation operation, $P$ is a fixed transmit power, $\sigma_w^2$ is the noise variance, $P/\sigma_w^2$ is called SNR, and the expectation is taken over the gain $h$ of the channel. In this paper, the AWGN channel is stationary and ergodic, and bit SNR is denoted as $\gamma_b$. As described in Section 3.1, the power of a complex Gaussian random variable obeys the exponential distribution, and its PDF, $f(\lambda)$, is given by Equation (18). Therefore, the capacity is calculated as follows.

$$C = \int_0^{+\infty} \log_2(1 + \lambda\gamma_b) f(\lambda) \mathrm{d}\lambda = \int_0^{+\infty} \log_2(1 + \lambda\gamma_b) e^{-\lambda} \mathrm{d}\lambda = -\frac{1}{\ln 2} \mathrm{Ei}\left(-\frac{1}{\gamma_b}\right) e^{\frac{1}{\gamma_b}}. \tag{24}$$

In Equation (24), the exponential integral function, $\mathrm{Ei}(z)$, is defined as $\mathrm{Ei}(z) = \int_{-\infty}^{z} e^t/t \mathrm{d}t$, where the principal value of the integral is taken [42].

At the same time, we can see from the simulations in Section 3.2 that the eavesdropper's error rate is close to 0.5, as shown in Figure 8. This implies that the eavesdropper's channel capacity is close to 0. The secrecy capacity is the channel capacity between Alice and Bob (legitimate users), minus the channel capacity between Alice and Eve (eavesdropper). Therefore, the secrecy capacity is obtained and given by

$$C_s = C_{AB} - C_{AE} = -\frac{1}{\ln 2} \mathrm{Ei}\left(-\frac{1}{\gamma_b}\right) e^{\frac{1}{\gamma_b}}. \tag{25}$$

## 4. Conclusions

In this paper, we have proposed a scheme for physical layer security transmission of single antenna node in wireless crowdsensing networks under static channel. In our scheme, the chaotic sequence generator with Tent mapping is used to generate random complex variables. The modulated symbol is multiplied by the complex random variable (encryption) to imitate the Rayleigh fading of the channel at the transmitting end. The received symbol is divided by the identical complex random variable (decryption) to recover the transmitted message before the digital demodulation at the receiving end. The eavesdropper is unable to intercept any effective information in the case of the unsynchronized the chaotic sequence and/or the unknown structure of the two-stage block interleaver, while the legitimate user can still transmit in security under a certain BER. With the introduction of artificial fading, the phase random rotation of the complex random variable does not cause the increase of BER. However, the variation of the modulated symbol power caused by the envelope fluctuation of the complex random variable , makes the symbol SNR fluctuate. When the envelope is less than 1, the power of the modulation symbol sent to the channel is reduced, that is, the signal-to-noise ratio is reduced, leading to the increase of the bit error ratio. This means reducing reliability to improve safety. Rayleigh fading is one of the worst fading channels. If we want to reduce BER while keeping security, we can also consider $m$-Nakagami fading. It is well known that Nakagami fading degenerates to Rayleigh fading when $m = 1$, and degenerates to no fading channel when $m = \infty$. Therefore, it is possible to choose an appropriate $m$ value to take both reliability and security into account.

**Author Contributions:** Writing—Original Draft Preparation, Z.-J.X. and Y.W.; Writing—Review & Editing, all co-authors; Visualization, all co-authors; Supervision, Not applicable; Project Administration, F.-N.C., Y.W. and Y.G.; Funding Acquisition, F.-N.C.,Y.W. and Y.G.

**Funding:** This work was funded in part by National Natural Science Foundation of China under Projects 61601409 and 61471322; in part by Shenzhen Science and Technology Program under Project JCYJ20170817110410346;

and in part by the Zhejiang Provincial Natural Science Foundation of China under Projects LR16F010003 and LR17F010002.

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

## References

1. Qian, L.; Wu, Y.; Zhou, H.; Shen, X. Joint Uplink Base Station Association and Power Control for Small-cell Networks with Non-orthogonal Multiple Access. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 5567–5582. [CrossRef]
2. Wu, Y.; Qian, L.; Mao, H.; Yang, X.; Zhou, H. Optimal Power Allocation and Scheduling for Non-Orthogonal Multiple Access Relay-Assisted Networks. *IEEE Trans. Mob. Comput.* **2018**, *17*, 2591–2606. [CrossRef]
3. Yang, G.; He, S.; Shi, Z. Leveraging Crowdsourcing for Efficient Malicious Users Detection in Large-Scale Social Networks. *IEEE Internet Things J.* **2017**, *4*, 330–339. [CrossRef]
4. Yang, X.; Wang, X.; Wu, Y.; Qian, L.; Lu, W.; Zhou, H. Small-Cell Assisted Secure Traffic Offloading for Narrow-Band Internet of Thing (NB-IoT) Systems. *IEEE Internet Things J.* **2018**, *5*, 1516–1526. [CrossRef]
5. Pechetti, S.; Jindal, A.; Bose, R. Exploiting Mapping Diversity for Enhancing Security at Physical Layer in the Internet of Things. *IEEE Internet Things J.* **2018**. [CrossRef]
6. Li, X.; Wang, Q.; Dai, H.-N.; Wang, H. A Novel Friendly Jamming Scheme in Industrial Crowdsensing Networks against Eavesdropping Attack. *Sensors* **2018**, *18*. [CrossRef] [PubMed]
7. Yang, G.; He, S.; Shi, Z.; Chen, J. Promoting Cooperation by Social Incentive Mechanism in Mobile Crowdsensing. *IEEE Commun. Mag.* **2017**, 55, 86–92. [CrossRef]
8. Ma, L.; Liu, X.; Pei, Q.; Xiang, Y. Privacy-Preserving Reputation Management for Edge Computing Enhanced Mobile Crowdsensing. *IEEE Trans. Serv. Comput.* **2018**. [CrossRef]
9. Li, T.; Jung, T.; Qiu, Z.; Li, H.; Cao, L.; Wang, Y. Scalable Privacy-Preserving Participant Selection for Mobile Crowdsensing Systems: Participant Grouping and Secure Group Bidding. *IEEE Trans. Netw. Sci. Eng.* **2018**. [CrossRef]
10. Chen, X.; Derrick, W.; Wolfgang, H.; Chen, H. A Survey on Multiple-Antenna Techniques for Physical Layer Security. *IEEE Commun. Surv. Tutor.* **2016**, *99*, 1027–1053. [CrossRef]
11. Wu, Y.; Qian, L.; Mao, H.; Yang, X.; Zhou, H.; Tan, X. Secrecy-Driven Resource Management for Vehicular Computation Offloading Networks. *IEEE Netw.* **2018**, *32*, 84–91. [CrossRef]
12. Maurer, U.M. Secret Key Agreement by Public Discussion from Common Information. *IEEE Trans. Inf. Theory* **1993**, *39*, 733–742. [CrossRef]
13. Hershey, J.; Hassan, A.; Ryarlagadda, R. Unconventional Cryptographic Keying Variable Management. *IEEE Trans. Commun.* **1995**, *43*, 3–6. [CrossRef]
14. Gungor, O.; Chen, F.; Koksal, C. Secret Key Generation via Localization and Mobility. *IEEE Trans. Veh. Technol.* **2015**, *64*, 2214–2230. [CrossRef]
15. Thai, C.T.T.; Lee, J.; Quek, T.Q.S. Physical-Layer Secret Key Generation with Colluding Untrusted Relays. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 1517–1530. [CrossRef]
16. Quist, B.T.; Jensen, M.A. Maximization of the Channel-Based Key Establishment Rate in MIMO Systems. *IEEE Trans. Wirel. Commun.* **2015**, *14*, 5565–5573. [CrossRef]
17. Zhao, H.; Pan, G. Analysis of Secure Communications for A DF and RF Relaying SIMO System with Gauss Errors. *Sci. Sin. Inform.* **2016**, *46*, 350–360. [CrossRef]
18. Song, C. Achievable Secrecy Rate of Artificial Fast-fading Techniques and Secret-key Assisted Design for MIMO Wiretap Channels with Multi-antenna Passive Eavesdropper. *IEEE Trans. Veh. Technol.* **2018**. [CrossRef]
19. Lv, L.; Ding, Z.; Ni, Q.; Chen, J. Secure MISO-NOMA Transmission With Artificial Noise. *IEEE Trans. Veh. Technol.* **2018**, *67*, 6700–6705. [CrossRef]
20. Ahmed, M.; Bai, L. Secrecy Capacity of Artificial Noise Aided Secure Communication in MIMO Rician Channels. *IEEE Access* **2018**, *6*, 7921–7929. [CrossRef]
21. Zou, Y.; Zhu, J.; Wang, X.; Hanzo, L. A Survey on Wireless Security: Technical Challenges, Recent Advances and Future Trends. *Proc. IEEE* **2016**, *104*, 1727–1765. [CrossRef]
22. Edman, M.; Kiayias, A.; Yener, B. On Passive Inference Attacks Against Physical-Layer Key Extraction? In Proceedings of the 4th European Workshop on System Security, Salzburg, Austria, 10 April 2011; pp. 1–6. [CrossRef]

23. Zang, G.; Huang, B.; Chen L.; Gao, Y. One Transmission Scheme Based on Variable MSK Modulator for Wireless Physical Layer Security. In Proceedings of the IEEE International Conference on Wireless Communications & Signal (WCSP), Nanjing, China, 15–17 October 2015; pp. 1–5. [CrossRef]
24. Husain, M.; Mahant, S.; Sridhar, R. CD-PHY: Physical Layer Security in Wireless Networks Through Constellation Diversity. In Proceedings of the IEEE Military Communications Conference (MILCOM), Orlando, FL, USA, 29 October–1 November 2012; pp. 1–9. [CrossRef]
25. Ma, R.; Dai, L.; Wang, Z.; Wang, J. Secure Communication in TDS-OFDM System Using Constellation Rotation and Noise Insertion. *IEEE Trans. Consum. Electron.* **2010**, *56*, 1328–1332. [CrossRef]
26. Li, H.; Wang, X.; Hou, W. Secure Transmission in OFDM Systems by Using Time Domain Scrambling. In Proceedings of the IEEE 77th Vehicular Technology Conference (VTC Spring), Dresden, Germany, 2–5 June 2013; pp. 1–5. [CrossRef]
27. Kaddoum, G.; Gagnon, F.; Richardson, F. Design of a Secure Multi-Carrier DCSK System. In Proceedings of the International Symposium on Wireless Communication Systems (ISWCS), Pairs, France, 28–31 August 2012; pp. 964–968. [CrossRef]
28. Herceg, M.; Kaddoum, G.; Vranjes, D.; Soujeri, E. Permutation Index DCSK Modulation Technique for Secure Multi-User High-Data-Rate Communication System. *IEEE Trans. Veh. Technol.* **2017**, *67*, 2997–3011. [CrossRef]
29. Jameel, F.; Kaddoum, G.; Trung, Q. A Comprehensive Survey on Cooperative Relaying and Jamming Strategies for Physical Layer Security. *IEEE Commun. Surv. Turtor.* **2018**. [CrossRef]
30. Vuppala, S.; Tolossa, Y.J.; Kaddoum, G.; Abreu, G. On the Physical Layer Security Analysis of Hybrid Millimeter Wave Networks. *IEEE Trans. Commun.* **2018**, *66*, 1139–1152. [CrossRef]
31. Tolossa, Y.J.; Vuppala, S.; Kaddoum, G.; Abreu, G. On the Uplink Secrecy Capacity Analysis in D2D-Enabled Cellular Network. *IEEE J. Syst.* **2018**, *12*, 2297–2307. [CrossRef]
32. Atallah, M.; Kaddoum, G. Secrecy Analysis of Cooperative Network with Untrustworthy Relays Using Location-Based Multicasting Technique. In Proceedins of the IEEE 5th International Conference on Future Internet of Things and Cloud, Prague, Czech Republic, 21–27 August 2017; pp. 206–210. [CrossRef]
33. Goldsmith, A. *Wireless Communications*; Cambridge University Press: New York, NY, USA, 2005; pp. 71–167, ISBN 978-0521837163.
34. Box, G.; Muller, M. A Note on the Generation of Random Normal Deviates. In *The Annals of Mathematical Statistics*; Institute of Mathematical Statistics: Rockville Pike, MD, USA, 1958; Volume 29, pp. 610–611, ISSN 00034851.
35. Hilborn, R. *Chaos and Nonlinear Dynamics: An Introduction for Scientists and Engineers*; Oxford University Press: Oxford, UK, 2001; p. 6, ISBN 0198507232.
36. Sedaghatnejad, S.; Farhang, M. Detectability of Chaotic Direct-Sequence Spread-Spectrum Signals. *IEEE Wirel. Commun. Lett.* **2015**, *4*, 589–592. [CrossRef]
37. Box, G.E.P.; Jenkins, G.M.; Reinsel, G.C.; Ljung, G.M. *Time Series Analysis: Forecasting and Control*, 5rd ed.; Wiley: Hoboken, NJ, USA, 2015; p. 32, ISBN 978-1-11867502-1.
38. Wang, Y.; Zhang, X.-Z.; Zeng, J.; Wang, Y.-M. Secure OFDM Transmission Scheme Based on Two-Stage Chaos Mapping. *J. Commun.* **2016**, *37*, 132–129. (In Chinese) [CrossRef]
39. Ramkumar, B. Automatic Modulation Classification for Cognitive Radios Using Cyclic Feature Detection. *IEEE Circuits Syst. Mag.* **2009**, *9*, 27–45. [CrossRef]
40. Mobasseri, B.G. Digital Modulation Classification Using Constellation Shape. *Signal Process.* **2000**, *80*, 251–277. [CrossRef]
41. Simon, H.; Michael, M. *Modern Wireless Communications*; Pearson Prentice Hall: Upper Saddle River, NJ, USA, 2004; p. 364, ISBN 0130224723.
42. Abramowitz, M. *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*; Dover Publications, Inc.: New York, NY, USA, 1974; p. 228, ISBN 0486612724.