Hindawi
Journal of Sensors
Volume 2021, Article ID 9007071, 11 pages
https://doi.org/10.1155/2021/9007071

Research Article

Wireless Communication Physical Layer Sensing Antenna Array Construction and Information Security Analysis

Xiaolong Zhang[1,2,3] **and Wei Wu**[2]

[1]*The 54th Research Institute of China Electronics Technology Group Corporation, Hebei, Shijiazhuang 050002, China*
[2]*China Academic of Electronics and Information Technology, Beijing 100041, China*
[3]*Suzhou Tongyuan Software & Control Technology Co., Ltd., Jiangsu, Suzhou 215125, China*

Correspondence should be addressed to Xiaolong Zhang; zhangxl@tongyuan.cc

Received 8 September 2021; Revised 25 September 2021; Accepted 27 September 2021; Published 25 October 2021

Academic Editor: Guolong Shi

Due to the complexity of wireless communication networks and the open nature of wireless links, complex upper layer network encryption cryptographic algorithms are also difficult to implement effectively in complex mobile wireless communication and interconnection networks, and traditional cryptography-based security policies are gradually not well able to meet the security management needs of today's mobile Internet information era. In this paper, the physical characteristics of the channel in the wireless channel are extracted and used to generate keys, and then, the keys are negotiated so that the keys generated by the two communicating parties are identical. Then, the generated keys are used by the communicating parties to design the interleaving matrix for encryption of the message. The false bit rate of the system is investigated for the case of an interleaving matrix generated using different quantization methods of keys. The problem of characterizing the encoding and encryption techniques for interleaving keys for the physical layer sensing antenna arrays of wireless channels is studied in depth. The physical layer wireless channel interleaving technique and the wireless channel physical layer encryption technique are organically combined, and a joint interleaving encryption method based on the physical layer key of the wireless channel is designed and used to encrypt and randomize the physical layer data information of the OFDM (Orthogonal Frequency Division Multiplexing) system, which improves the security and reliability of the wireless channel information transmission. The effect of physical layer keys under different physical layer quantization methods on the performance of the wireless channel interleaving encryption algorithm is studied, and the quantization methods of pure amplitude, pure phase, and joint amplitude phase are investigated for the characteristics of wireless physical layer channels.

1. Introduction

The Internet has developed rapidly in just a few decades, and in recent years, the emergence of various wireless devices has also driven the development of wireless communication. In this information age, where interdisciplinary science and technology are the main focus and multiplatform technologies are developing rapidly at cross purposes, wireless communication technology will usher in new challenges and opportunities. On the one hand, the rapid development of wireless communication technology makes some wireless energy devices have higher and higher energy demands. Considering from the perspective of energy, in the traditional wireless communication system, the wireless signal generally only carries out wireless information transmission, mainly through the power grid transmission of electricity or with battery power supply for communication equipment to provide stable energy with a stable energy supply system. Some relevant research scholars want to obtain the maximum efficiency of energy conversion by building on the existing energy base or minimizing the energy consumption while satisfying a specific condition [1]. Mainly because of the open nature of wireless broadcasting, resulting in a great security problem of user information, all devices can cross the authorized users directly into the existence of vulnerability of the wireless network or directly on the user information

eavesdropping and cracking, causing a great threat to the security of information. But with the emergence of new networks, some devices consume a lot of energy even when they are in an idle state, for example, some network terminals in sensor networks still consume energy when they are idle and often replace the batteries at a great cost. Based on the above actual situation and application, a new energy collection method is hotly pursued by researchers, this energy collection method can solve the terminal energy limitation problem and its signal itself in the transmission of energy at the same time also carries information, to achieve wireless information to complete the transmission and at the same time can also transmit energy. This new wireless communication method is based on the existing wireless communication technology, and by changing the design of the transmitter and the design of the receiver, it can realize the transmission of wireless information and the transmission of energy at the same time. Wireless energy-carrying technology brings a great change to the development of new wireless communication.

On the other hand, with the increasing popularity of the Internet and mobile devices, the use of mobile devices (especially the popularity of mobile devices) on the Internet is very extensive. In the future, mobile devices will further be involved in all aspects of our life. However, some destructive software can control that software through the vulnerability on the software and steal and damage the information on the software, so the user's information is not safe and can be stolen and tampered with by the destructors at any time [2]. Mainly because of the open nature of wireless broadcasting, resulting in a great security problem of the user's information, all devices can cross the authorized user directly into the existence of vulnerabilities in the wireless network or directly to the user's information eavesdropping and cracking, causing a great threat to the security of information. For information security processing methods, the traditional encryption method is to use a specific password to encrypt text information; the most common algorithms used in data communication include the DES algorithm, RSA algorithm, and PGP algorithm, but also through the encryption algorithm and effective key method to make the encrypted legitimate information not be eavesdropped on by eavesdroppers. The secure transmission of legitimate information is effectively ensured to some extent, but an attacker using the new generation of cryptanalysis techniques can break the cryptosystem by obtaining the key even with access to the carrier on which the cryptographic algorithm operates (computer, secrecy machine, encryption box, IC card, etc.). So the method of encrypting the information only by passwords does not guarantee that the eavesdropper will not tap the secret key, and if the eavesdropper steals the secret key, the user's information security is very threatening [3].

2. Related Works

Unlike the encryption algorithm in traditional wireless communication technology, the physical layer key technology of the wireless channel still has many features and advantages in its application. First, high security, the security of the physical layer key is calculated by the information of the extracted features in the wireless channel after quantization; due to its location in the wireless communication environment and the receiver only when the receiver is within one-half of the wavelength difference, the wireless channel may have great relevance to the receiver. Second, it realizes the effective distribution and management of keys and reduces the difficulty of key sending and receiving management. In the network of traditional wireless communication, the distribution of keys is required before the wireless communication sender and receiver connect to send data, which is used to encrypt the sent data. Third, it is possible to use the technique of real-time generation of physical layer keys for the upper layer or network layer of the data link of the system, where the node and the data center are encrypted at the upper layer. This can realize the matching joint of different security management techniques in the physical layer with each other and can effectively improve the data security of the physical layer wireless communication system. The physical layer security technology at the current stage of research has the following two main aspects.

One is the physical layer key technology based on the characteristics of wireless channels; based on Shannon's information theory, the literature [4] shows that the characteristics unique to wireless communication channels are reciprocity, time varying, and spatial uniqueness, and the physical layer security about wireless channels is mainly studied using these characteristics. The basic idea of using correlated source channels to extract keys is then proposed in the literature [5], i.e., using two discrete correlated random variables with common randomness. The literature [6] provides a rigorous theoretical definition of key extraction using correlated sources of wireless channels and points out the idea of key extraction based on wireless channel features. Assuming that the random sources observed by the legitimate communicating parties are correlated (the eavesdropping party cannot receive the random sources), then it is theoretically possible to use the public channel eigenvalues to extract a sequence of key features that is available only to the legitimate communicating parties. Maurer, after giving the theoretical justification, also gives specific steps: dominance extraction, key negotiation, and secrecy enhancement. In the literature [7], it is proposed that in TDD (Time Division Duplexing) systems, the communicating parties can have relatively consistent reciprocal channel characteristics for the wireless channel, thereby enabling the sharing of relevant sources and the generation of characteristic keys. After that, some key generation schemes have been proposed in the literature [8]. In this literature, the key generation methods were gradually evolved into 4 major steps: (1) channel estimation, (2) quantization, (3) key negotiation, and (4) secrecy enhancement. The paper [9] verifies the reciprocity as well as spatial uniqueness of wireless channels through theoretical derivation and practical simulation, but the influence of environmental factors such as noise and signal measurement delay also causes that the measurements are not perfectly correlated although there is reciprocity. To address this noncorrelation caused by the environment, the literature [10] proposes that the correlation between the measurements can be enhanced using differential

filtering and channel gain compensation. Moreover, the wireless channel feature parameters are diverse and these feature parameters can be extracted to generate the key. The paper [11] uses not only the received signal strength (RSS) to extract the generated key on the ZigBee platform but also the constrained waveform technique of the antenna to enhance the randomness of the key. The paper [12] is also is using extracted RSS to generate keys. The paper [13] further improves the key generation rate by obtaining channel estimates with a higher agreement rate through Channel Impulse Response (CIR). The literature [14] uses the received signal Paul information of the UWB channel as a characteristic parameter to generate keys; the literature [15] proposes to use the reciprocity of the channel response phase information to generate keys. The literature [16] proposes setting the quantization threshold by dynamic negotiation based on double-gated quantization. The literature [17] proposes a multibit quantization approach where the number of quantization bits is determined by the statistics of the channel eigenvalues.

3. Wireless Communication Physical Layer Sensing Antenna Array Construction and Information Security Analysis

3.1. Model of Sensing Antenna Arrays in the Physical Layer of Wireless Communications. Multiantenna systems can use the spatial freedom provided by their multiple antennas to exponentially increase the capacity and spectrum utilization of communication systems under the same bandwidth conditions, which is one of the core technologies of wireless communication. Compared with the traditional single-antenna system, the multiantenna technology can greatly improve spectrum utilization, enabling the system to support higher-speed data services with limited band resources and certain anti-interference performance. Multiantenna systems can use the spatial freedom provided by their multiple antennas to exponentially increase the capacity and spectrum utilization of the communication system under the same bandwidth conditions, which is one of the core technologies of wireless communication. Compared with the traditional single-antenna system, multiantenna technology can greatly improve spectrum utilization, making the system support higher-speed data services with limited frequency band resources and certain antijamming performance. In a multiantenna system, multiple antennas are used on the transmitter side, and the core idea is to use the airspace freedom provided by multiple transmitting antennas to effectively improve the spectrum efficiency of the wireless communication system and achieve a significant increase in data transmission rate as well as a great improvement in communication quality. In a multiantenna system, the transmitter uses multiple antennas, and the core idea is to use the airspace freedom provided by multiple transmitting antennas to effectively improve the spectrum efficiency of the wireless communication system and achieve a significant increase in data transmission rate as well as a great improvement in communication quality. Multiantenna communication systems can send multiple data streams to increase the information transmission rate, use airspace diversity techniques to improve reliability, or use beamforming to improve the signal-to-noise ratio at the receiving end.

Millimeter wave operates in the 30 G-300 GHz band, and the higher frequency band makes it different from systems operating in the conventional band in many ways and therefore poses many implementation challenges. The biggest implementation challenge for millimeter-wave communications is the severe path loss due to the high-frequency band, which is due to the high atmospheric absorption of millimeter waves and their vulnerability to rain absorption and low penetration, but due to the small wavelength of millimeter waves, the problem of high path loss can be solved by using large-scale antenna arrays and beamforming techniques. Another characteristic of millimeter-wave signals is that they are not diffractive, and therefore, millimeter-wave signals tend to break the link when they encounter occlusion. Also, due to its narrow beam, the millimeter-wave channel can be described using the standard multipath model in the low-frequency band, and for the two-dimensional channel model, the antenna arrays at the transmitter and receiver can be described by their respective antenna response vectors, i.e., θ_T and θ_R, which represent the angles a_T and a_R leaving and arriving at the wavefront, respectively, as a function of the phase information about the array as a variable. Due to the use of large-scale antenna arrays and beamforming techniques, millimeter-wave MIMO (multiple-in multiple-out) channels are usually considered to be sparse, i.e., the number of AoD and AoA is small. Because millimeter-wave beams are very narrow, millimeter-wave systems are often considered to be more secure than conventional communications as long as the directions in which the eavesdropper and the legitimate receiver are located in the system do not overlap very much [18]. However, millimeter-wave signals produce a reflective diffusion effect when confronted with hard surfaces and narrow building cracks, and this diffusion effect increases as the signal wavelength decrease. In real urban environments, where communication scenarios are often complex, where line-of-sight communication links are not only often impossible to establish but also where there are many potential scatterers, the reflection-diffusion effect of the signal is often more pronounced and complex, which means that there is a high probability that the signal received by the legitimate receiver and the eavesdropper is received by the same scatterer through different diffusion paths. The biggest implementation challenge for millimeter-wave communication is the severe path loss due to the high-frequency band, which is due to the high atmospheric absorption of millimeter waves and the low penetration rate due to the easy absorption by rain, but the problem of high path loss can be solved by using large-scale antenna arrays and beamforming techniques due to the small wavelength of millimeter waves. Another characteristic of millimeter-wave signals is that the diffraction effect is not obvious; therefore, millimeter-wave signals tend to break the link when they encounter occlusion. Also, due to its narrow beam, the millimeter-wave channel can be described using the standard multipath

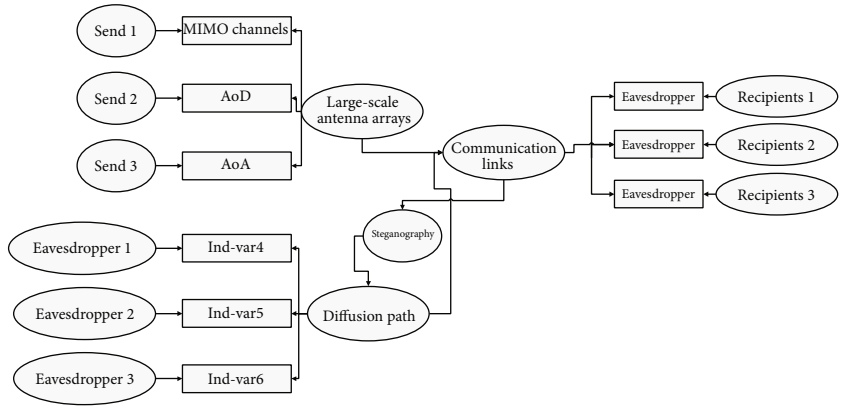

Figure 1: mm-wave shared scatterer multipath channel model.

model in the low-frequency band, that is, there is a high probability that the legitimate receiver's channel and the eavesdropper's channel have similar angles of departure (AoD), and thus, there is a high probability that the encrypted message will be received by the eavesdropper. This channel model is called a shared scatterer multipath channel and is illustrated in Figure 1.

Information entropy is a basis for Shannon's quantification of information in information theory and is primarily related to probability theory; mathematical statistics are closely related. Suppose that the probability density function of the discrete random variable X, when it takes values in the interval $p(x)$ (i.e., self-information), $x \in \chi$, then its entropy (entropy is also known as the average amount of self-information) can be expressed as

$$M(x) = \varphi \sum_{x \in \chi} \left[p^2(x) \cdot \ln p(x) \right] + Ax. \tag{1}$$

The above equation is a generalized function of the message probability $p(x)$, i.e., a statistically weighted function of the logarithm function. The entropy value entropy is a measure of the average uncertainty of a random variable when the entropy value of the random variable is higher, i.e., the more information the event contains [19]. In the case of the existence of an uncertain variable, when there are two uncertain variables (X, Y), its entropy can be expressed as follows, assuming that there exist two random discrete variables X, Y with a range space of values of χ, γ, respectively, and the joint probability distribution of the two is $p(x, y)$, then the joint entropy of the two, $H(x, y)$, can be expressed as follows.

$$H(x, y) = \varphi \sum_{y \in \gamma} \sum_{x \in \chi} [p(x, y) \cdot \ln p(x, y) + Ax + Cy] + \lambda. \tag{2}$$

The information entropy is the amount of information that is output by the source, but the amount of information that is received by the receiver is the mutual information. Let there exist two random discrete variables X, Y taking values in the range space of χ, γ, respectively, and the joint probability distribution of the two is $p(x, y)$, then the mutual information $I(X; Y)$ of the two can be expressed as

$$\begin{aligned} I(X; Y) &= \frac{H(x, y)}{M(x)} \\ &= \frac{\varphi \sum_{y \in \gamma} \sum_{x \in \chi} [p(x, y) \cdot \ln p(x, y) + Ax + Cy] + \lambda}{M(x) = \varphi \sum_{x \in \chi} [p^2(x) \cdot \ln p(x)] + Ax}. \end{aligned} \tag{3}$$

Reciprocal information is the amount of information that can be obtained about X by looking at Y in it.

Channel capacity is a parameter that measures the channel and reflects the maximum amount of the channel that can be transmitted per unit of time and amount of information. From Equations (2) and (3), it can be seen that the rate of information transmission of the channel is related to the distribution probability of the symbols (distribution probability is also called self-information) and that the information Y received at the receiving end depends entirely on the information X sent at the sending end when the channel characteristics are known. Also, since the mutual information $I(X; Y)$ is a concave function about $p(x)$, there must exist $p(x)$ that maximizes $I(X; Y)$. When the condition $p(x) =$ is satisfied, the channel capacity C is denoted as

$$C = P(x) \cdot \max_x^y I(X; Y). \tag{4}$$

The above equation does not give a specific expression, because the specific expressions are different for different channels. In this paper, a Gaussian additive channel is used and P_t in the following equation denotes the transmit power at the transmitter and P_r the received power. So the expression is

$$C = P_r{}^{\gamma} \cdot P_t{}^{\chi} + \varphi H(x, y). \tag{5}$$

The key technology for realizing wireless energy-carrying communication systems is that the communication between the two is realized by encoding and decoding information from the aspect of digital communication. From the perspective of wireless information transmission by electromagnetic

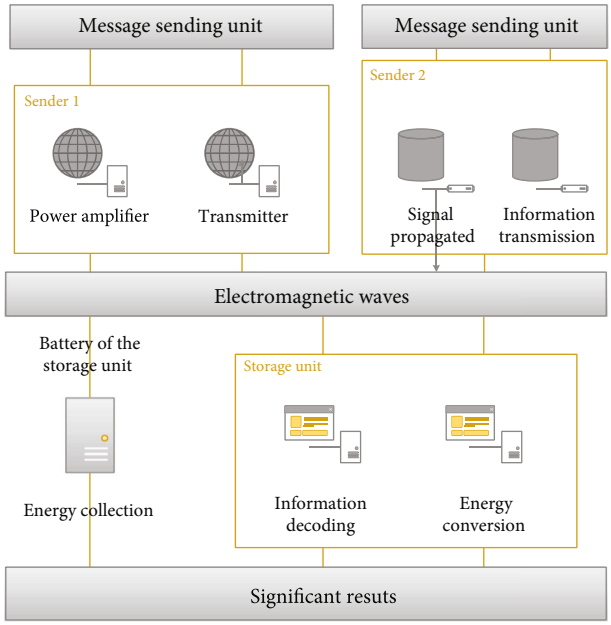

Figure 2: Transmission diagram of the wireless energy-carrying system.

waves, wireless information transmission in space is carried by electromagnetic, so the key to the research of wireless energy-carrying communication technology is to transmit energy signals along with electromagnetic information signals from space [20]. Figure 2 shows the schematic diagram of the wireless energy-carrying communication system to realize the wireless information and energy synergistic transmission; at the transmitting end, the power amplifier amplifies the signal processed by the transmitter and then propagates in space in the form of electromagnetic waves for a distance to the receiving end; the signal propagated in space carries both information transmission and energy transmission, and at the receiving end, specific techniques are used to realize enough power distribution. Traditional cryptography-based secrecy techniques require the communication parties to share keys, and the security of this secrecy mechanism depends on the structure of key generation, the complexity of the encryption algorithm, and the mechanism of key distribution. However, in huge wireless communication networks, the movement of nodes and changes in the network can make the distribution of keys difficult. Physical layer key technology refers to the generation of keys using physical layer characteristics in wireless communication, such as the magnitude and phase of wireless fading. It shows the total power is divided into two parts; part of the power is used for information decoding, and the remaining power is used for energy collection; and the energy collected at the receiving end is stored in the battery of the storage unit through the relevant technology. Nowadays, the research on wireless portable energy cotransmission technology has achieved significant results.

3.2. Information Security Techniques for Physical Layer Sensing Antenna Arrays for Wire Communications. Since wireless communication is vulnerable to malicious attacks or eavesdropping due to its exposure within the air and its broadcast nature, UAV communication is vulnerable to malicious attacks or eavesdropping. To avoid eavesdropping attacks on the system and to ensure secure communication of the system, generally, the system adopts encryption. But the premise of using encryption is that the eavesdropper has limited computing power and cannot or will not be able to crack the key in a short time. But as the computing power of computers continues to increase, this premise gradually disappears and the usefulness of such existing encryption techniques is threatened.

Traditional security techniques use upper layer encryption techniques, while physical layer security techniques can be seen as a complement to traditional security techniques through the study of physical layer characteristics. Physical layer security techniques are based on information theory and use the physical characteristics of the wireless channel to enhance security for the system. As it fully exploits the interference noise and multipath characteristics of the channel, it is not affected by the complexity of the eavesdropper's eavesdropping algorithm and can make the eavesdropper's information acquisition rate to zero [21]. This means that in 5G networks, where there are many end-user accesses and data transmissions, physical layer security techniques can provide a strong complementary guarantee to traditional security techniques. The current physical layer security techniques can be classified as follows.

3.2.1. Physical Layer Security Technology Based on Information Theory. In information theory, the message output by the source is regarded as random, that is, the receiver cannot know with certainty what the message sent by the source is until it receives the message. And after the receiver receives the message, a certain amount of uncertainty is removed from the message sent by the source, and uncertainty is defined in information theory as the huge number of information, which is what is conveyed in the communication. The concept of information theory was first introduced by Shannon and developed based on mathematics the basic concept of secrecy system. By converting each set of plaintext messages, encrypted by a key, into a set of ciphers, Shannon's idea of such a secrecy system is based on key design. The performance of a discrete memoryless eavesdropping channel consisting of a sender, a receiver, and an eavesdropper is investigated by channel conditions without the use of a key. When the channel conditions from the sender to the legitimate receiver are better than the channel conditions from the sender to the eavesdropper, the rate at which the sender and the legitimate receiver can reliably and securely send and receive letters can be found. The concept of confidential capacity, which is the difference between the channel capacity of the legitimate link and the channel capacity of the eavesdropping link, is defined in the literature and it is also the upper limit of the guaranteed secure transmission rate; that is, by applying a transmission rate below the secrecy capacity, data can be guaranteed to be transmitted securely from the source to the receiver without being eavesdropped on by an eavesdropper. However, due to the time-varying fading effect of the wireless channel, the fading

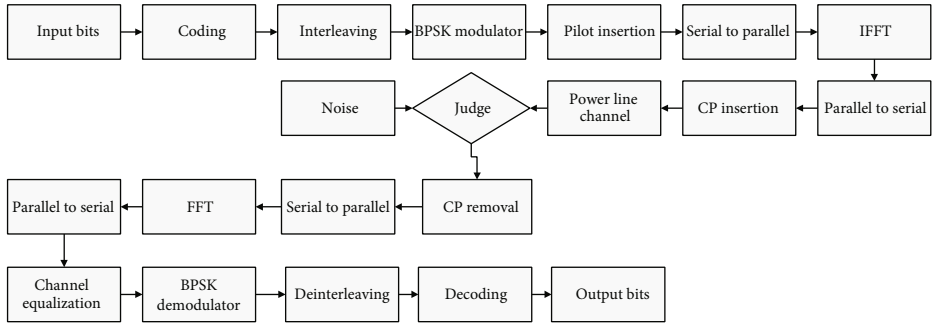

Figure 3: Block diagram of the transceiver of OFDM system.

of the signal sent from the source to the receiver causes a reduction in the channel capacity of the legitimate link, thus reducing the secrecy capacity.

3.2.2. Artificial Interference Noise-Assisted Techniques. Artificial interference noise assisted means that the sender sends communication information along with artificial interference noise to affect the eavesdropper's eavesdropping, but the receiver does not receive this noise low impact so that the secrecy capacity of the system can be increased by reducing the channel capacity of the link from the sender to the eavesdropper. In the literature [22], a portion of the transmit power at the sender is allocated to generate artificial noise to reduce the channel capacity of the eavesdropping link to increase the security of the system. Although this artificial noise ensures the security of wireless transmission, it comes at the cost of resource loss in transmit power, which is to be considered in practical situations depending on the adequacy of such resources.

3.2.3. Beamforming Technology. Beamforming is a technique that uses multiple antennas at the transmitter's end, combined with digital signal processing techniques, to direct the signal to be sent and received. The transmitter can be designed to send a specific directional signal to the legitimate receiver, while if the eavesdropper and receiver are not in the same direction, the signal received by the eavesdropper becomes weak and thus avoids being eavesdropped on. The essence of this technique is to increase the strength of the signal received by the legitimate receiver thereby increasing the channel capacity of the legitimate channel, while decreasing the strength of the signal received by the eavesdropper to reduce the channel capacity of the eavesdropping channel, thereby increasing the security performance of the system.

3.2.4. Physical Layer Key Technology. Conventional cryptography-based secrecy techniques require shared keys between the communicating parties, and the security of this secrecy mechanism depends on the structure of the key generation, the complexity of the encryption algorithm, and the mechanism of key distribution. But in huge wireless communication networks, the movement of nodes and changes in the network can make the distribution of keys difficult. Physical layer key technique refers to the generation of keys using physical layer characteristics in wireless communication, such as the magnitude and phase of wireless fading. There are three main types of such physical layer key generation techniques: key generation based on received signal strength, key generation based on channel impact response, and key generation by a hybrid mechanism. Key establishment at the time of linking two terminals, with keys generated using the randomness of the wireless channel, is a promising technique that has been used in different scenarios.

Figure 3 shows the block diagram of the transmitter and receiver of the OFDM system, where the upper part is the transmitter block diagram and the lower part is the receiver block diagram. On the transmitter side, the transmitted bitstream needs to be coded and interleaved to improve the transmission performance. After that, the bitstream is digitally modulated as well as serial-parallel transformed to map the bitstream to the individual subcarriers, during which the pilot frequency needs to be inserted for phase tracking. Then, a fast Fourier inverse transform is performed and a cyclic prefix of length greater than the maximum transmission delay is inserted as a guard interval to eliminate intersymbol interference. The resulting digital signal is converted to an analog signal by a digital-to-analog converter and then sent out through the RF transmitter module. The operation of the receiver is the inverse of that of the transmitter: the received RF signal is first converted into a digital signal by an analog-to-digital converter, then the cyclic prefix is removed with the help of synchronization techniques, and the signal is restored after serial-parallel conversion, fast Fourier transform, parallel-serial conversion, demodulation, deinterleaving, and decoding. The BER performance of the original scheme and the improved scheme is almost the same when the SNR of the system is 0 dB, and the advantage of the improved scheme becomes more and more obvious as the SNR of the system increases.

Through wireless communication physical layer sensing antenna array encryption technology, the energy receiver receives the signal from the legitimate message sender for dynamic power allocation; part of the signal power is used for energy harvesting and part of the power is used for message decoding, as the energy receiver may be a potential eavesdropper to ensure the secure transmission of the communication system, a friendly jammer is added to the system; the jammer uses one of the antennae to receive the

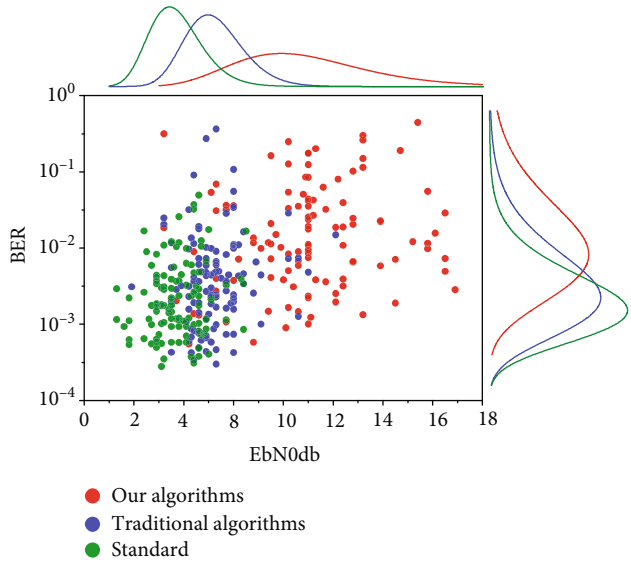

Figure 4: BER comparison with a conventional algorithm for same bit phase and bit amplitude.

signal from the message sender and convert it into electrical power to store in the battery to power itself and the other antenna is used to send jamming signals to confuse the energy receiver to eavesdrop on legitimate messages.

4. Experimental Design and Conclusion

In the simulation scenario, the number of subcarriers is set to $N = 32$, the path loss index is set to -2, and the noise power spectral density is set to 2 = -60 dBm. The distance from the IT end to the ER end is $d_2 = 2$ m, the distance from the IT end to the IR end is $d_4 = 4$ m, and the distance from the IT to the CJ at the message sending end is denoted by $1d$, and the CJ moves horizontally in a straight line from the IT to the IR ends. The distance from the ER to the IT and IR is in a straight line with a vertical distance of 1 m.

To fully demonstrate that this improved scheme has better system BER simulation performance compared to the original scheme and can effectively increase and improve the BER simulation performance of the system, the following physical layer key generated by 2-bit pure amplitude quantized value amplitude, 1-bit amplitude-phase 1-bit amplitude quantized value generated physical layer key, and 2-bit pure quantized value amplitude generated physical layer key under the improved. The BER of the system is simulated, and the results are compared with the original scheme.

Figure 4 shows the BER ratios of the original scheme and the improved scheme when the physical layer key is generated by 1-bit phase 1-bit amplitude quantization for both the transmitter and the receiver in different SNR environments. It is still obvious from the results of this simulation that as the signal-to-noise ratio of the system continues to steadily increase, the transmission BER of both the original scheme and the improved scheme continues to decrease. It can be seen that both the original scheme and this improved scheme can effectively reduce the transmission BER of the system and improve the data transmission performance of the communication system. From the BER results of this simulation, it is still obvious that the BER performance of the original scheme and the improved scheme is almost the same when the signal-to-noise ratio of the system is 0 dB, and the advantage of the improved scheme becomes more and more obvious as the signal-to-noise ratio of the system increases. The BER of the original scheme is in the order of 10^{-3} when the SNR is 15 dB. The BER of the improved scheme is in the order of 10^{-4}. Compared to the original solution, the improved solution improves the BER performance of the communication system by an order of magnitude. It can be seen that the improved system solution effectively and significantly reduces the probability of the occurrence of signal BER of the whole system during the wireless communication transmission and improves the performance of the communication system.

Figure 5 depicts a plot of the variation of the confidential information rate with the energy harvesting requirement for $d_1 = 1$ m and different power at the IT transmitter. First, the figure shows the performance of the system under the three schemes compared, and what can be seen is that the optimal algorithm proposed in this section performs better than the water injection algorithm and the scheme where all subcarriers are used for sending information and receiving energy in the same case. This is because as the energy harvesting requirement increases, more power in the system is used for energy harvesting and only a small amount of power is used for message sending, and the performance is lower when the more power is sent, the fewer subcarriers in the water injection algorithm can get allocated to power. While all the subcarriers in Algorithm 2 are used for message sending and energy receiving, the eavesdropper eavesdrops more information and the system of Algorithm 2 has a lower rate of information secrecy compared to the algorithm proposed in this section. It can also be seen from the figure that the secrecy rate of the system is zero when the energy harvesting requirement is increased to 0.25 W. This is because the total transmit power of the system can only be used to satisfy the energy harvesting at the ER side and there is no excess power to allocate to the IR side and the CJ side, so the secrecy rate of the system is zero. It can also improve that increasing the transmitting power of the system can improve the performance of the system, which can meet the energy harvesting requirements, and at the same time, the remaining transmitting power can be used for the information receiving end and jammer reception, thus improving the information secrecy rate of the system.

Figure 6 compares the effect of distance on the probability of safe interruption of the system. The simulation parameters are set to $N = 100$, $\Delta f = 10$ kHz, RD = 1 km, $\theta D = \theta E = 20°$, $\alpha = 0.8$, and Cth = 0.1. It can be seen from the figure that the safety interruption probability gradually decreases with increasing distance and the safety performance of the system is improved, but the improvement keeps decreasing. The results of the theoretical analysis asymptotically agree exactly with the results of the analysis at a high signal to dry noise ratio. And then, the simulation results of the phased array security scheme are given in the figure as a comparison. The comparison results show that the dependence

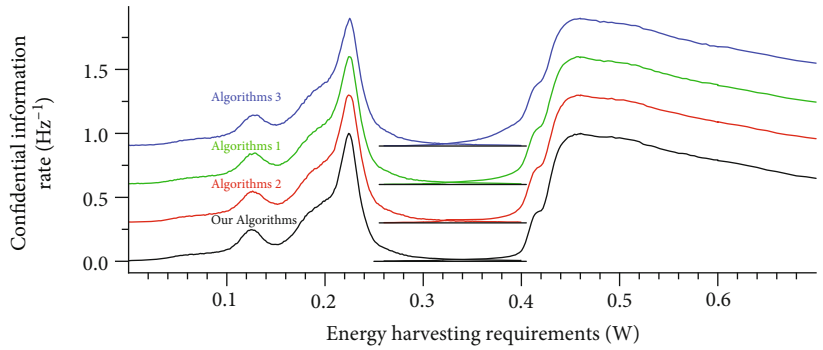

Figure 5: Plot of confidential information rate versus energy harvesting requirements.

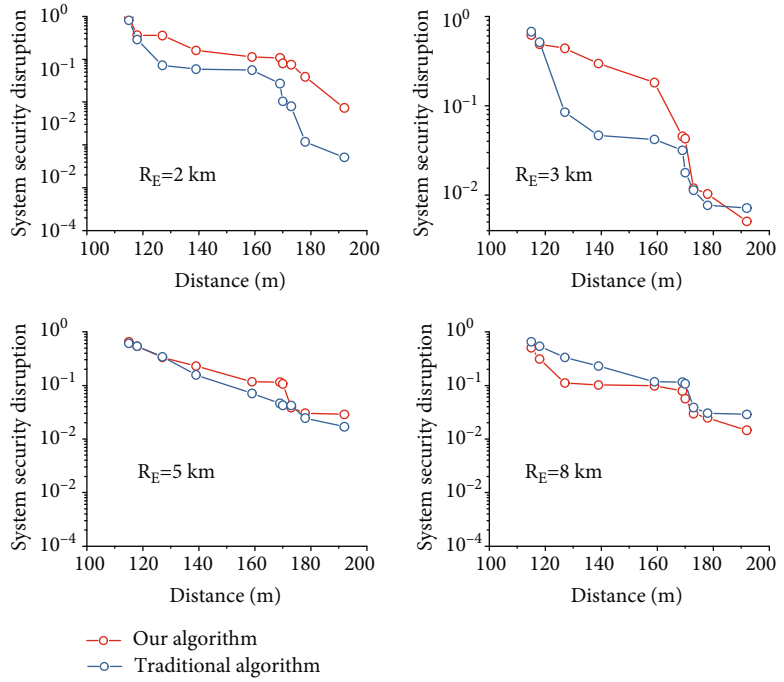

Figure 6: Effects of distance on the probability of system security disruption.

on the distance of the frequency-controlled array makes the frequency-controlled array safety scheme outperform the phased array. Frequency bias occupies an important position in the study related to frequency-controlled arrays. The simulation parameters are set: $N = 100$, $\alpha = 0.8$, and Cth = 0.1, and the locations of the legitimate and eavesdropping users are (10°, 1 km) and (0°, 3 km), respectively. The increase of frequency bias brings the improvement of system security interruption performance. When $\Delta f = 0$, the frequency-controlled array degenerates into a conventional phased array and a large performance gap is observed between the frequency-controlled and phased array security schemes. Once again, it is shown that the frequency-controlled array safety scheme outperforms the phased array scheme.

All channels are assumed to experience Rayleigh flat fading. The target data rate is set to Rth = 0.1 bits/s/Hz and the threshold safe rate is RS = 1 bits/s/Hz. Without loss of generality, the noise power $\sigma 2$ is normalized to unit 1, $\lambda SP = \lambda RP = \lambda P$ and $\lambda kEm = \lambda kE$. For comparison, we also give the results of the conventional relay selection scheme without artificial interference assistance as a benchmark. From all the simulation plots, it can be seen that the Monte Carlo simulation results match perfect with the theoretical analysis curves, thus proving the correctness of our derived results. Figure 7 gives the variation curves of SOP and asymptotic SOP with γ for different γ_p based on three different relay selection schemes, where $\lambda SR = \lambda P = \lambda kD = 1$, $\lambda kE = 5$, $M = 1$, and $N = 6$. First, the SOP of the BRS scheme outperforms the CRS and CRSNJ for γ above 5 dB, proving that the BRS scheme is more effective compared to the other two schemes. This is since the BRS utilizes all known information including the CSI of the primary and interfering channels, while the conventional relay selection schemes (i.e., CRS and CRSNJ) utilize only the CSI of the primary channel, and it is clear that the former has better performance. On the other hand, it can be observed that the CRSNJ scheme saturates the performance at lower signal-to-noise ratios, while the artificial noise-assisted relay

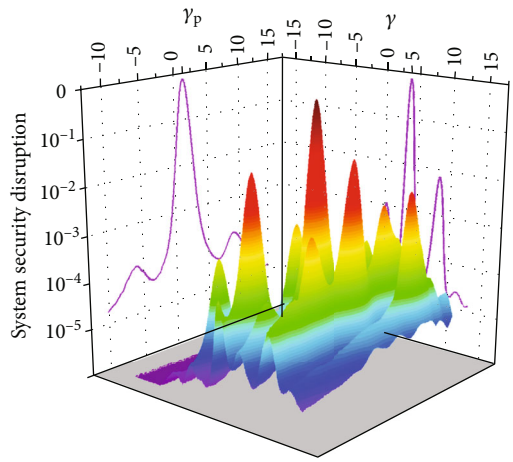

Figure 7: Curves of SOP and asymptotic SOP with γ at different γ_p.

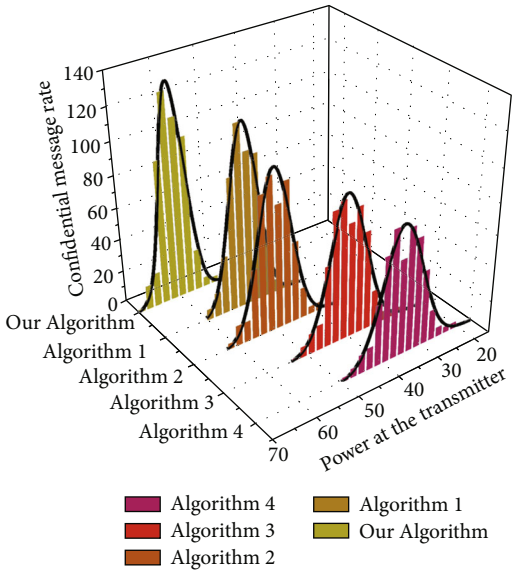

Figure 8: Variation of confidential message rate with power at the transmitter.

selection strategies, i.e., BRS and CRS schemes, achieve better security performance, demonstrating that collaborative interference is a very effective way to improve the security performance of wireless transmissions. It can also be seen that SOP decreases as γ increases since higher γ indicates that higher transmit power is available at ST and collaborative relays. In addition, a floor effect appears in the SOP in the high γ domain. This is because as γ tends to infinity, the transmit power at ST and collaborative relay is limited only by the maximum interference power at PU, making the system a fully cognitive scenario. Thus, in this case, the safety performance of the system does not increase unless γ_p increases. Under the same conditions, the secrecy rate of the system gradually increases as the transmitting power increases.

Figure 8 shows the trend of the secrecy rate of the system with the total transmit power at the IT end for the case of $1d = 1$ m. What can be seen from the figure is that when the acquisition energy requirement is 70 W, the secrecy rate of the system is zero when the sending power at the sending end is lower than 40 W, and under the same condition, the secrecy rate of the system gradually increases as the sending power increases. The optimal solution proposed in this section requires the lowest transmit power when the same secrecy rate is required; in other words, the solution proposed in this section consumes the least amount of energy. In the case of constant transmitting power at the transmitter side, when the energy harvesting requirement increases from 0.05 W to 0.1 W, the secrecy information rate of the system decreases and the transmitting power remains unchanged; the energy harvesting requirement at the ER side needs to be satisfied first, so the remaining power becomes smaller and the power received by the IR side and CJ decreases, so the secrecy information rate shows a decreasing trend.

As a product of the combination of wireless information transmission technology and energy collection technology, the technology effectively improves the utilization of energy, and its emergence has brought great changes and opportunities to the development of wireless communication technology, which can realize the simultaneous transmission of energy and information through some specific technologies and can use radio frequency signals to power some remote areas of the equipment, to extend the life of the equipment. However, with the development of the Internet, every aspect of life involves Internet technology, which also leads to a constant risk of information security for users. From the physical layer security point of view, suitable interference signals can be designed at the eavesdropping end to confuse the eavesdropper and reduce the signal-to-noise ratio of the eavesdropper, which can improve the physical layer security performance of the system to a great extent while ensuring a small impact on the signal-to-noise ratio of legitimate users. OFDM technology is a communication technology with the highest spectrum utilization, which can be used from digital modulation, subcarrier allocation, and other aspects of the system. Power utilization and spectrum utilization can be effectively improved, and it can be said to be one of the main technologies for future mobile communications.

5. Conclusion

This paper focuses on the physical layer security problem in multiantenna wireless communication systems. For the problem of the guided frequency spoofing detection in conventional band MISO communication systems, a random guided frequency sequence-assisted guided frequency spoofing detection algorithm is proposed, which performs guided frequency spoofing detection by examining the difference between the legitimate communication channels estimated in the conventional guided frequency training phase and the random guided frequency training phase. Then, a channel estimation enhancement algorithm that can improve the channel estimation accuracy is proposed for the case of a no-guide-frequency spoofing attack returned by the detector, and a confidential communication algorithm during downlink data transmission is proposed for the case of missed-guide-frequency spoofing detection. Extensive simulation

experiments can prove that the proposed guided frequency spoofing detection algorithm can effectively and accurately detect the attack and outperform other recent guided frequency spoofing detection algorithms. Also, both proposed enhanced algorithms can achieve their respective functions.

For millimeter-wave MIMO communication systems, this paper clearly illustrates the security threats posed by the characteristics of millimeter-wave signals and hybrid beamforming filter structures and proposes codebook-dependent and codebook-independent secrecy hybrid beamforming algorithms according to whether the eavesdropper channel state information is known or not, respectively. In the future, both hardware technology and software development will become stronger, so secure communication should also be better guaranteed. The codebook-independent design is usually more accurate, but the relative complexity is higher, so the proposed algorithm is mainly developed for analog filters implemented with low-resolution phase shifters in practical applications; the codebook-dependent design is usually simpler, but the accuracy is sacrificed, so the proposed algorithm is mainly developed for analog filters implemented with high-resolution phase shifters, which ensures a lower computational complexity of the algorithm while guaranteeing satisfactory secrecy. The proposed algorithm is mainly developed for the analog filter implemented in the high-resolution phase shifter, which ensures a satisfactory secrecy performance while keeping the computational complexity of the algorithm low.

Data Availability

All information is within the paper.

Conflicts of Interest

No competing interests exist concerning this study.

Acknowledgments

This work was supported by the project of design of space-frequency domain joint anti-interception wireless transmission signal based on linear frequency modulation (No. 6142104200202).

References

[1] H. Jung, S. W. Ko, and I. H. Lee, "Secure transmission using linearly distributed virtual antenna array with element position perturbations," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 1, pp. 474–489, 2021.

[2] X. Yuan, Y. J. A. Zhang, Y. Shi, W. Yan, and H. Liu, "Reconfigurable-intelligent-surface empowered wireless communications: challenges and opportunities," *IEEE Wireless Communications*, vol. 28, no. 2, pp. 136–143, 2021.

[3] J. Tang, H. Wen, K. Zeng, R. F. Liao, F. Pan, and L. Hu, "Lightweight physical layer enhanced security schemes for 5G wireless networks," *IEEE Network*, vol. 33, no. 5, pp. 126–133, 2019.

[4] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: challenges and opportunities," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8169–8181, 2019.

[5] J. Li and H. Wu, "Localisation algorithm for security access control in railway communications," *IET Intelligent Transport Systems*, vol. 14, no. 14, pp. 2151–2159, 2020.

[6] Z. Sun, S. Balakrishnan, L. Su, A. Bhuyan, P. Wang, and C. Qiao, "Who is in control? Practical physical layer attack and defense for mmWave-based sensing in autonomous vehicles," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3199–3214, 2021.

[7] W. Zhang, J. Chen, Y. Kuo, and Y. Zhou, "Transmit beamforming for layered physical layer security," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 10, pp. 9747–9760, 2019.

[8] N. Xie, Z. Li, and H. Tan, "A survey of physical-layer authentication in wireless communications," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 282–310, 2021.

[9] B. Li, Z. Fei, C. Zhou, and Y. Zhang, "Physical-layer security in space information networks: a survey," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 33–52, 2020.

[10] S. Xia, X. Tao, N. Li et al., "Multiple correlated attributes based physical layer authentication in wireless networks," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1673–1687, 2021.

[11] S. Yan, X. Zhou, J. Hu, and S. V. Hanly, "Low probability of detection communication: opportunities and challenges," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 19–25, 2019.

[12] C. X. Wang, M. Di Renzo, S. Stanczak, S. Wang, and E. G. Larsson, "Artificial intelligence enabled wireless networking for 5G and beyond: recent advances and future challenges," *IEEE Wireless Communications*, vol. 27, no. 1, pp. 16–23, 2020.

[13] J. Guo, B. Song, Y. Chi et al., "Deep neural network-aided Gaussian message passing detection for ultra- reliable low-latency communications," *Future Generation Computer Systems*, vol. 95, pp. 629–638, 2019.

[14] R. Ma, S. Yang, M. Du, H. Wu, and J. Ou, "Improving physical layer security jointly using full-duplex jamming receiver and multi-antenna jammer in wireless networks," *IET Communications*, vol. 13, no. 10, pp. 1530–1536, 2019.

[15] Z. Kong, S. Yang, D. Wang, and L. Hanzo, "Robust beamforming and jamming for enhancing the physical layer security of full duplex radios," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 12, pp. 3151–3159, 2019.

[16] L. Chettri and R. Bera, "A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 16–32, 2020.

[17] X. Zhang, X. G. Xia, Z. He, and X. Zhang, "Phased-array transmission for secure mmWave wireless communication via polygon construction," *IEEE Transactions on Signal Processing*, vol. 68, pp. 327–342, 2020.

[18] N. Wang, W. Li, A. Alipour-Fanid, L. Jiao, M. Dabaghchian, and K. Zeng, "Pilot contamination attack detection for 5G mmwave grant-free IoT networks," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 658–670, 2021.

[19] M. A. Reşat, M. C. Karakoç, and S. Özyurt, "Improving physical layer security in Alamouti OFDM systems with subcarrier coordinate interleaving," *IET Communications*, vol. 14, no. 16, pp. 2687–2693, 2020.

[20] W. Wen, C. Liu, Y. Fu, T. Q. S. Quek, F. C. Zheng, and S. Jin, "Enhancing physical layer security of random caching in large-

scale multi-antenna heterogeneous wireless networks," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2840–2855, 2020.

[21] M. Ma, S. Tian, Y. Chen et al., "A prototype of co-frequency co-time full duplex networking," *IEEE Wireless Communications*, vol. 27, no. 1, pp. 132–139, 2020.

[22] J. Yang, B. Ai, I. You et al., "Ultra-reliable communications for industrial Internet of things: design considerations and channel modeling," *IEEE Network*, vol. 33, no. 4, pp. 104–111, 2019.