Security and Safety, Vol. 1, 2022006 (2022)
https://doi.org/10.1051/sands/2022006
sands.edpsciences.org

Research Article OPEN ACCESS

Information Network

Secure transmission technology based on direct modulation with random channel characteristics

Rong Yang[1] and Aiqun Hu[2,*]

[1] *School of Cyberspace Security, Southeast University, Nanjing 211189, China*
[2] *State Key Laboratory of Mobile Communications, Southeast University, Nanjing 210096, China*

Received: 25 January 2022 / Revised: 6 March 2022 / Accepted: 26 March 2022 / Published online: 22 June 2022

Abstract Aiming at the problem of insufficient security in the existing wireless data transmission, a security transmission technology based on direct modulation with random channel characteristics is proposed. The method first estimates channel characteristics using the preamble in the communication frame, and then embeds channel characteristics into the I/Q modulator. After that, the modulated constellation diagram undergoes random hopping of the constellation position compared with the original constellation diagram, thus achieving the effect of secure transmission. Due to the reciprocity of the uplink and downlink channels, channel characteristics estimated by the downlink receiver are almost the same as those estimated by the uplink receiver, and the correct plaintext data can be recovered by performing corresponding demodulation with them. Compared with the existing scheme of quantizing channel characteristics and then encrypting data, the method reduces the performance loss caused by quantization. In addition, its bit error rate is lower than that of the quantization method. In general, it has higher security and convenience.

Keywords Channel reciprocity, Channel state information (CSI), Physical layer security, Channel characteristics, Constellation diagram

Citation Yang R and Hu A. Secure transmission technology based on direct modulation with random channel characteristics. Security and Safety 2022; **1**: 2022006. https://doi.org/10.1051/sands/2022006

1 Introduction

In recent years, secure transmission technology based on the physical layer has received extensive attention. The wireless transmission channel has the characteristics of spatial uniqueness, short-term reciprocity, and time variability [1], which is the basis of physical layer security. Theoretically speaking, using the channel state information to modulate data can achieve the security transmission effect close to 'one-time pad' [2]. The 'one-time pad' here means that over time, channel state information (CSI) and the key generated according to the CSI will change accordingly.

At present, many types of research on secure transmission methods based on physical layer channel characteristics have been carried out internationally. For example, the constellation of the signal can be designed by various methods such as phase rotation, constellation ambiguity, amplitude adjustment and symbol order adjustment [3]. These methods effectively protect the data, so that eavesdroppers cannot demodulate the correct information from the constellation diagram. Xi *et al.* [4] proposed a physical layer security encryption scheme based on constellation fuzzy design, which uses channel coefficients as keys to

* Corresponding author (email: aqhu@seu.edu.cn)

solve the problem of non-secrecy of key pre-sharing. A three-dimensional constellation rotation method was proposed [5], which can obtain higher spectral efficiency and energy efficiency, and the encryption transformation is more flexible. Li *et al.* [6] proposed a technology for secure transmission of the wireless communication physical layer based on polarization state modulation, which introduces the polarization domain. In this method, a random and fast-changing channel precoding matrix is designed, and the high-dimensional constellation diagram is further disturbed, which makes the information highly concealed. Li *et al.* [7] introduced an efficient random physical layer key extraction scheme based on vector quantization, which uses vector quantization to convert channel information into 0 and 1 bit streams, and performs error correction and randomness enhancement processing through a fuzzy extractor. As a result, the key generation rate is improved and the bit error rate (BER) is reduced.

Many of the above technologies use algorithms that quantify channel characteristics and then encrypt data. It is well known that quantizing data will lead to performance loss. Quantization method has the disadvantage that once an error occurs, it cannot be restored. What is more, the security transmission technology based on three-dimensional constellation rotation and vector quantization has relatively high algorithm complexity and consumes a lot of resources. Therefore, if there is an algorithm that does not have quantification loss and can be easily calculated to realize the secure transmission of data, the efficiency and security of communication will be greatly improved.

Based on this consideration, this paper proposes a secure transmission technique CSI-quadrature phase-shift keying (QPSK) based on direct modulation with random channel characteristics. The characteristic of this technique is that CSI information is embedded in the I/Q modulator. The specific method is that the sender first obtains CSI through channel estimation, and inputs the CSI into the modulator while sending data. The modulation method inside the modulator is to multiply the real part of the CSI by the I channel and the imaginary part by the Q channel. Compared with ordinary I/Q modulation, the amplitude and phase of the points in the constellation diagram are changed. Moreover, even if the eavesdropper can eavesdrop on the corresponding constellation diagram, he cannot judge whether the constellation diagram has been processed and in what manner, which ensures security to a certain extent. In theory, due to the reciprocity of the uplink and downlink channels, the CSI estimated by the receiver within the coherence time range is almost the same as the CSI estimated by the sender. Using this CSI for corresponding demodulation, the correct plaintext can be recovered.

In this paper, Section 1 introduces the state-of-the-art research on secure transmission using physical layer channel characteristics and proposes the method of this paper. Section 2 introduces the basic principles of the secure transmission technology of directly modulating data with random channel characteristics, including the transmission and reception models, the extraction of channel state information and modulation methods. Section 3 realizes this security transmission technology through experiments and analyzes its performance indicators, mainly the comparison of BER. Section 4 summarizes the full text and introduces the advantages and disadvantages of this scheme as well as its application prospects.

2 Principle

2.1 Transmission and reception models

The theoretical model of this paper is a three-node transmission and reception model, including legitimate communication parties Alice, Bob, and an eavesdropper Eve [8].

As shown in Figure 1, legitimate communication parties Alice and Bob perform channel estimation from the preamble of the communication frame firstly to obtain channel characteristic parameters h_{AB} and h_{BA} (such as signal amplitude, envelope, and phase). Because the channel has the characteristics of spatial uniqueness, short-term reciprocity, and time-variability [9], the channel is relatively stable, and channel characteristics remain almost unchanged in the same time slot or in the coherent time period [10]. According to the multipath characteristics of the channel and the 1/2 wavelength theory, channel observations h_{AC} and h_{BC} obtained by the eavesdropper Eve located outside the coherent distance around Alice and Bob are independent of channel observations h_{AB} and h_{BA} between the legitimate communication parties. Therefore, the spatial location of the eavesdropper Eve determines that he cannot obtain channel characteristics between the legitimate communication parties. Under ideal conditions, channel characteristics h_{AB} and h_{BA} estimated by Alice and Bob are consistent. This method can avoid the process of

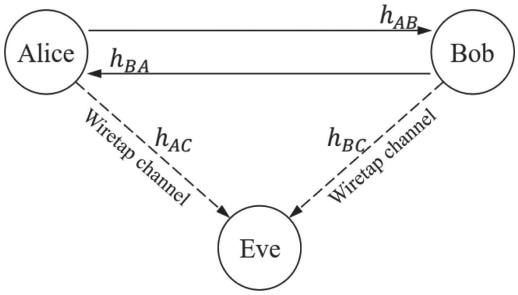


Figure 1. Three-node transmission and reception model

sharing the key, that is, avoid the possibility of being eavesdropped during the key transmission process. Therefore, security is further guaranteed.

2.2 Extraction of channel state information

The channel characteristic parameter used in this paper is the channel state information (CSI). CSI usually refers to the channel frequency response of the wireless multipath channel [11]. When the transmission frequency is f, CSI can be expressed as:

$$H(f) = \sum_{n=1}^{N} a_n e^{-j2\pi f \tau_n}. \tag{1}$$

In the above formula, a_n represents the amplitude, N represents the total number of samples, and τ_n is the sampling time. CSI reflects the overall amplitude attenuation and phase offset of the wireless channel. In actual wireless communication, when the wireless signal arrives at the receiver along different paths, the signals of different amplitudes and phases are superimposed to form the final received signal [12]. CSI reflects the amplitude attenuation and phase offset after the superposition of multiple propagation paths.

In the system of time division duplex (TDD) communication, this paper takes the preamble structure of IEEE 802.11g as an example to illustrate how to extract the CSI. As shown in Figure 2, the preamble field of the physical layer frame structure contains 10 repeated short training symbols and 2 repeated long training symbols. t1 to t10 represent short training symbols, and T1 and T2 are long training symbols. Their main functions are to perform channel estimation and signal synchronization. Short training symbols can estimate large frequency offset and long training symbols are used for symbol fine synchronization and channel estimation [13]. After CSI has been estimated from the long training symbols of the previously received message, it is applied to the modulation of the data segment portion of the message to be sent this time.

As shown in Figure 3, Alice and Bob take turns sending packets. In the same time slot or coherence time, since the uplink and downlink signals have experienced similar environments in the channel, which is called short-term reciprocity, channel coefficients h_{AB} and h_{BA} obtained by Alice and Bob through channel estimation are almost the same. However, in the actual system, h_{AB} and h_{BA} cannot be completely consistent due to the half-duplex mode of the system, the fingerprint of the transceiver, the channel noise [14], *etc.* Signals received at legitimate communication parties can be expressed as:

$$y_{R1} = h_{AB} * x_A + n_{R1}, \tag{2}$$
$$y_{R2} = h_{BA} * x_B + n_{R2}, \tag{3}$$

where x_A and x_B are the signals sent by Alice and Bob, respectively, h_{AB} and h_{BA} are channel coefficients detected by Alice and Bob, and n_{R1} and n_{R2} are the noise at the receiving antenna.

The above formulae (2) and (3) can be transformed into the frequency domain:

$$Y_{R1} = H_{AB} X_A + N_{R1}, \tag{4}$$
$$Y_{R2} = H_{BA} X_B + N_{R2}. \tag{5}$$

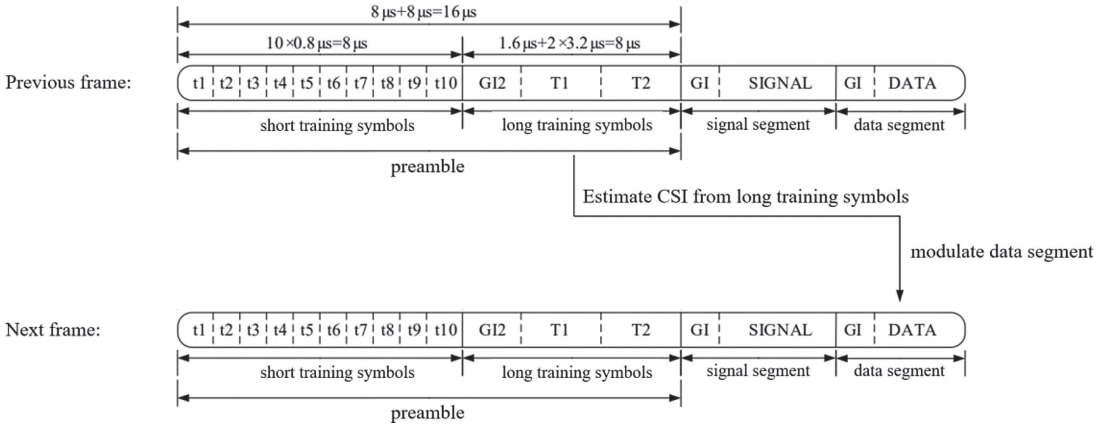


Figure 2. Schematic diagram of preamble CSI extraction (previous frame) and modulation area (next frame) of physical layer frame structure

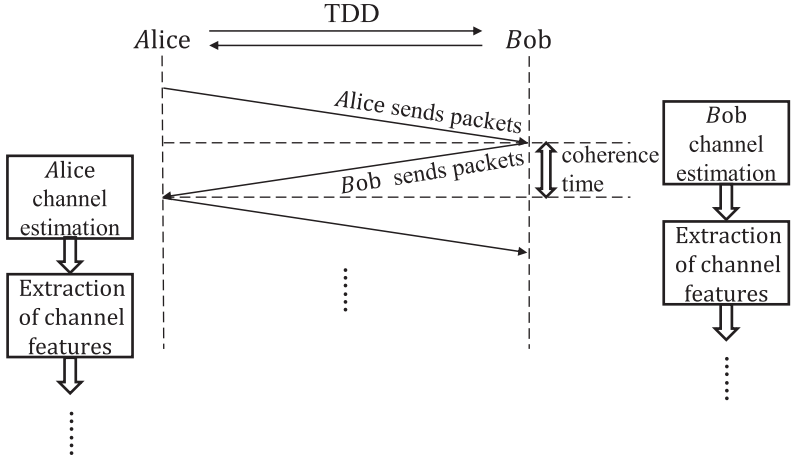


Figure 3. Extraction process of channel features

Frequency responses H_{AB} and H_{BA} of the wireless channel in the above formula are defined as the channel state information (CSI), which is the frequency domain representation of channel multipath characteristics. When ignoring noises N_{R1} and N_{R2}, channel frequency responses H_{AB} and H_{BA} can be estimated as:

$$H_{AB} = Y_{R1} X_A^{-1}, \tag{6}$$

$$H_{BA} = Y_{R2} X_B^{-1}. \tag{7}$$

Channel frequency responses H_{AB} and H_{BA} are composed of amplitude and phase, which are expressed as follows:

$$H_{AB} = |H_{AB}| \, e^{j\theta_{AB}}, \tag{8}$$

$$H_{BA} = |H_{BA}| \, e^{j\theta_{BA}}, \tag{9}$$

where $|H_{AB}|$ and $|H_{BA}|$ are magnitudes of H_{AB} and H_{BA}; θ_{AB} and θ_{BA} are the phases of H_{AB} and H_{BA}.

2.3 Modulation method

The CSI-based direct modulation and demodulation method proposed in this paper is based on the traditional I/Q modulation method, and the CSI is embedded in the traditional modulator. The specific

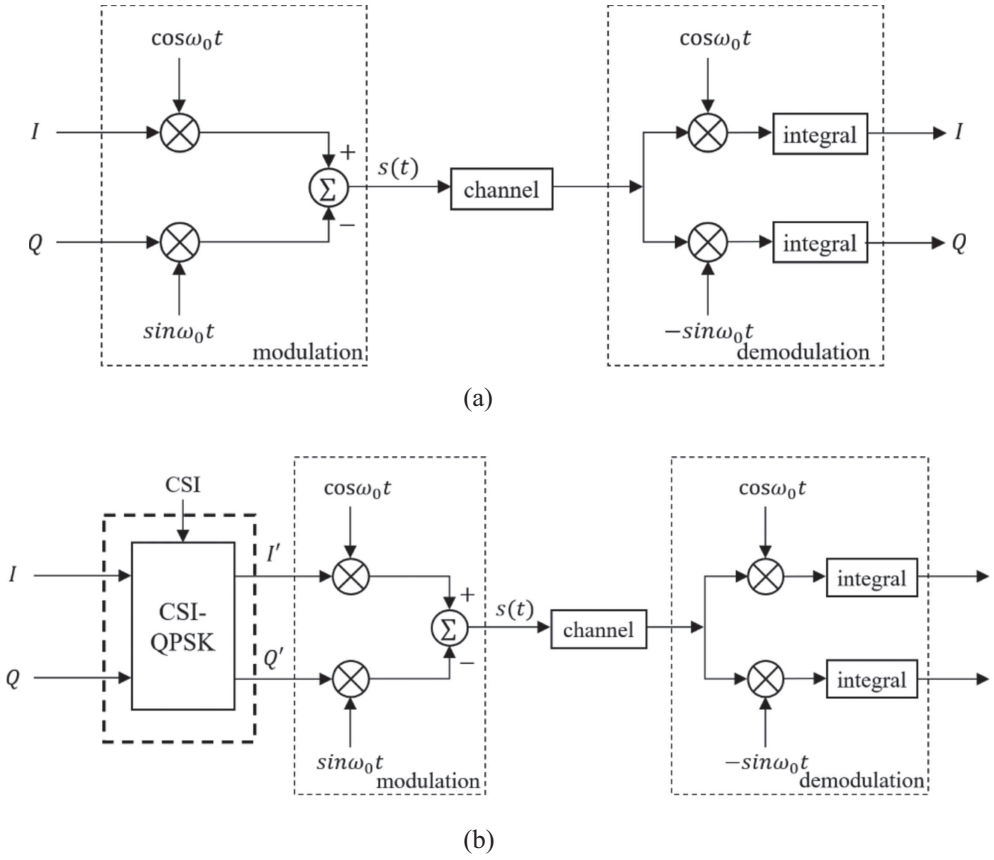


Figure 4. Schematic diagram of traditional QPSK and CSI-QPSK: (a) Schematic diagram of traditional QPSK modulation and demodulation; (b) Schematic diagram of CSI-QPSK method

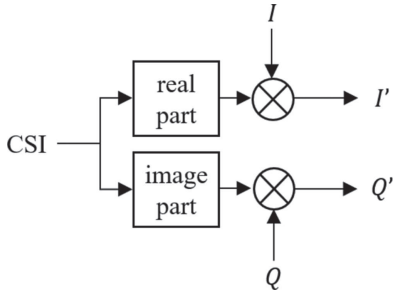


Figure 5. Schematic diagram of the internal structure of CSI-QPSK

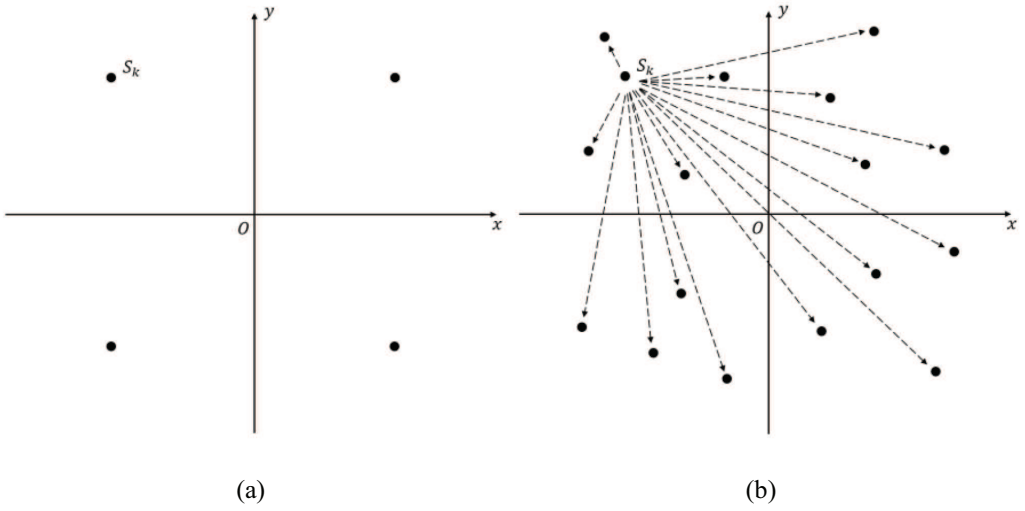
method is to multiply the real part of the CSI by the channel I and the imaginary part by the channel Q, which directly changes the modulated input signals of channel I and channel Q. The modulation process is shown in Figure 4b.

As shown in Figure 5, the internal structure of CSI-QPSK is to multiply the real part and imaginary part of each subcarrier of CSI to channels I and Q of the modulator, respectively. Suppose that the complex values of the 52 CSI are $H_k = a_k + b_k \times i, k = 0, 1 \ldots\ldots 51$. Data of channel I and channel Q are: $I = \{I_1, I_2, \ldots\ldots I_N\}, Q = \{Q_1, Q_2, \ldots\ldots Q_N\}$. The data output by CSI-QPSK is shown in formula (10):

$$\begin{cases} I_n^{'} = a_k \times I_n,\ k = \mathrm{mod}\,(n, 52), \quad n = 1, 2, \ldots\ldots N; \\ Q_n^{'} = b_k \times Q_n,\ k = \mathrm{mod}\,(n, 52), \quad n = 1, 2, \ldots\ldots N. \end{cases} \tag{10}$$

Table 1. Relationship between input signal, I/Q signal, and output signal phase after adding CSI

Input signal s1s0	Original I/Q signal	I/Q signal after adding CSI	Output signal phase
00	+1, +1	$(+1)*a_k$, $(+1)*b_k$	$\arctan(b_k/a_k)$
01	−1, +1	$(-1)*a_k$, $(+1)*b_k$	$\arctan(-b_k/a_k)$
11	−1, −1	$(-1)*a_k$, $(-1)*b_k$	$\arctan(b_k/a_k)$
10	+1, −1	$(+1)*a_k$, $(-1)*b_k$	$\arctan(-b_k/a_k)$



(a) (b)

Figure 6. I/Q modulation and CSI-QPSK modulation constellation: (a) I/Q modulation constellation diagram; (b) CSI-QPSK modulation constellation

The above formula expresses that 52-bit CSI is used to encrypt data repeatedly. Although the CSI is reused, since there is no process of directly transmitting the CSI and the points modulated with the CSI are indeed kept random under the influence of noise, the security of encryption can be guaranteed. However, when the SNR is too high and the noise is reduced, the modulated points will show a certain pattern and regularity. Moreover, using the limited-bit CSI repeated encryption will indeed increase the probability of eavesdroppers stealing information. Of course, if the data expansion method can be used to expand the 52-bit CSI into more bits under the condition of ensuring the CSI correlation, security will be further improved.

The corresponding relationship among the input signal, I/Q signal, and output signal phase after the CSI is embedded in the modulator is shown in Table 1.

After adding the CSI, the output signal amplitude becomes $\sqrt{a_k^2 + b_k^2}$. The phase also jumps from the original phase to any other quadrant according to the CSI. Taking the point in the first quadrant as an example, the schematic diagram is shown in Figure 6b, and the other three quadrants are similar.

During demodulation, the information output from the I/Q channel is divided by the value of the real and imaginary parts of the CSI estimated from the preamble of the received data so that the plaintext information can be recovered. The presence of channel noise can interfere with the constellation diagram. Particularly, for constellation points close to the axis, channel noise may cause them to cross quadrants. Therefore, even if the CSI estimated by the sender and receiver are completely consistent, bit errors will occur.

3 Experiment and analysis

The CSI data extraction device used in this experiment is the ESP32 chip module. The software is esp-idfv4.2, python3.7.0, Cmake3.5. The communication interface is socket, and the communication protocol is UDP. MATLAB is the simulation software used for CSI data processing, modulation and demodulation.

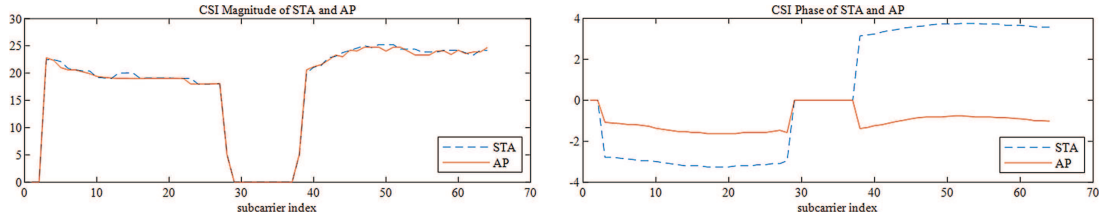


Figure 7. Raw CSI magnitude and phase maps: (a) Raw CSI magnitude map; (b) Raw CSI phase map

In the ESP32 chip module, the CSI consists of the frequency channel response of the subcarrier, which is recorded by a two-byte signature character. The first byte is the imaginary part and the second byte is the real part, which can be obtained directly by the software. The channel state information in this paper is the traditional long training field LLTF in the channel frequency response.

As shown in Figure 7, in the actual signal transmission process, H_{AB} and H_{BA} will have poor consistency under the influence of noise, time delay, device fingerprint and other factors [15]. Therefore, the CSI needs to be processed before executing the CSI-QPSK algorithm. The specific steps are as follows:

(1) Discarding unwanted frequencies, normalizing the energy and correcting the phase.
   (a) Each OFDM symbol has 64 subcarriers, of which only 52 are used. Firstly, according to the frame structure of 802.11g, the remaining meaningless zeros should be discarded to retain meaningful information.
   (b) Since the energy when data are sent and received is different, the CSI amplitude needs to be normalized, which can preliminarily improve the consistency of the CSI amplitude. The normalization formula used in this experiment is as follows:

$$x_{\text{normalization}} = \frac{x - x_{\min}}{x_{\max} - x_{\min}}. \tag{11}$$

   (c) Due to the lack of strict synchronization requirements when using long preamble symbols for channel estimation, resulting in inconsistent phases, there may be a sudden phase change. By correcting the phase and compensating for the phase beyond the range, the consistency of the phase can be greatly improved.

(2) Using filtering and polynomial fitting can further improve the consistency of CSI.
In order to reduce the glitches and sudden changes in the CSI curve, filtering and polynomial fitting methods can be used to smooth the curve, remove some of the effects of noise and device fingerprints, and better reflect the original channel information.

(3) Regularizing the range of channel coefficients can facilitate subsequent modulation.
In order to limit the points of the modulated constellation map to a reasonable range, the amplitude of the channel coefficient needs to be adjusted to the range of $0-2$, and the phase needs to be adjusted to the range of $-\pi-\pi$.

(4) Disordering the CSI to remove correlation.
Due to the great correlation between adjacent frequency points of the CSI, the randomness of the modulation coefficient is insufficient. In order to prevent attackers from cracking, it is necessary to decorrelate the measured values first. Disordering channel coefficients is the simplest way to decorrelate.

After data preprocessing, the consistency of CSI between the sender and receiver is greatly improved. The comparison before and after CSI processing is shown in Figure 7. Figure 7 is the original magnitude map and phase map of CSI, and Figure 8 is the CSI amplitude map and phase map after discarding unnecessary frequency points, normalization, phase correction, filtering, and regularization.

The CSI data after the above processing are subjected to out-of-order operations known to both sides, and then input to the I/Q modulator for modulation.

After simulation, the experiment transmits data in Additive White Gaussian Noise (AWGN) channel with 10 dB noise. The constellation diagram obtained by the QPSK modulation method and CSI-QPSK

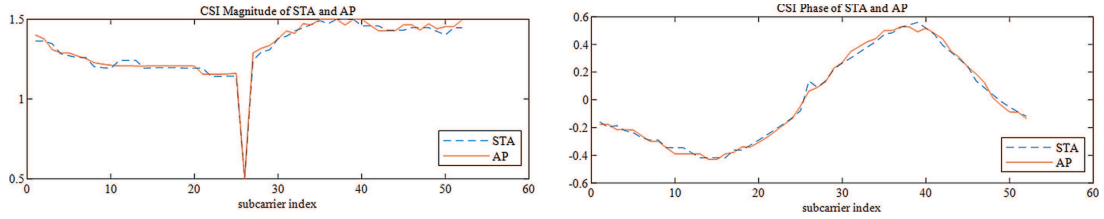


Figure 8. CSI magnitude and phase maps after preprocessing: (a) CSI magnitude map after preprocessing; (b) CSI phase map after preprocessing

modulation and demodulation is shown in Figure 9. In order to easily see the process of QPSK and CSI-QPSK modulation and demodulation, the points in the first, second, third, and fourth quadrants are marked in red, green, blue, and yellow, respectively, in the following figure.

It can be seen from Figure 9b that after CSI-QPSK modulation, the points originally fixed in the four quadrants have jumped, and the points in each quadrant are randomly jumped to any one of the four quadrants. According to Figure 9c, the set of constellation points in the four quadrants is mostly recovered after demodulation. A small number of constellation points that are not correctly demodulated generally only jump to the adjacent quadrant of the correct quadrant, because the probability of one bit error in the demodulation process is much greater than the probability of two errors. Since the CSI of the sender and receiver is not completely consistent, points in Figure 9c after CSI-QPSK demodulation are more scattered than those in Figure 9a.

As shown in Figure 10, the theoretical BER of QPSK, the BER of CSI-QPSK and the quantization method are compared. In the experiment of this paper, a fourth-order quantization method suitable for CSI data is adopted [16], and then the quantized data are used as a key for encryption, and finally QPSK modulation and demodulation are performed. We can see that the BER of the CSI-QPSK method is generally lower than that of the quantization method, because the quantization method introduces more quantization errors.

After calculation, the average value of the CSI correlation between Alice and Bob reaches about 0.96. The reason why the BER is still high in the case of high correlation is that the modulation and demodulation method in this paper is based on quadrant hopping, and as long as the symbols of the CSI of the two communication parties are different, even if the SNR is high, the correct plaintext cannot be demodulated.

The BER curve of the adjusted CSI-QPSK method is shown in Figure 11. When the signal-to-noise ratio reaches between 25 and 30 dB, the BER can reach the order of 10^{-3}. After analysis, even if the CSI consistency between the two parties is high, bit errors will still occur. The reason is that under the influence of noise, constellation points close to the coordinate axis may cross the coordinate axis during transmission, which will result in the inability to demodulate the correct plaintext. The improvement method is to perturb and adjust the constellation points close to the coordinate axis to keep a certain distance from the coordinate axis. For specific data, move the point within 0.05 distance from the coordinate axis to a position 0.05 away from the coordinate axis to further reduce the BER, as shown in Figure 12.

In Figure 12, when SNR reaches 20–25 dB, the BER after processing the points away from the coordinate axis can reach 10^{-3}. Under the same conditions of 10^{-3} BER, the SNR is about 10 dB lower than when the point is not processed away from the coordinate axis. If the distance between the point and the coordinate axis continues to increase, the BER will be further reduced, but it must be controlled within a certain range to prevent the modulated constellation from deviating from the normal shape.

4 Conclusion and future work

In this paper, a secure transmission technology CSI-QPSK based on direct modulation with random channel characteristics is proposed, and the feasibility of the method is verified by taking the frame structure of the IEEE 802.11g protocol as an example. This method has many advantages. First, compared

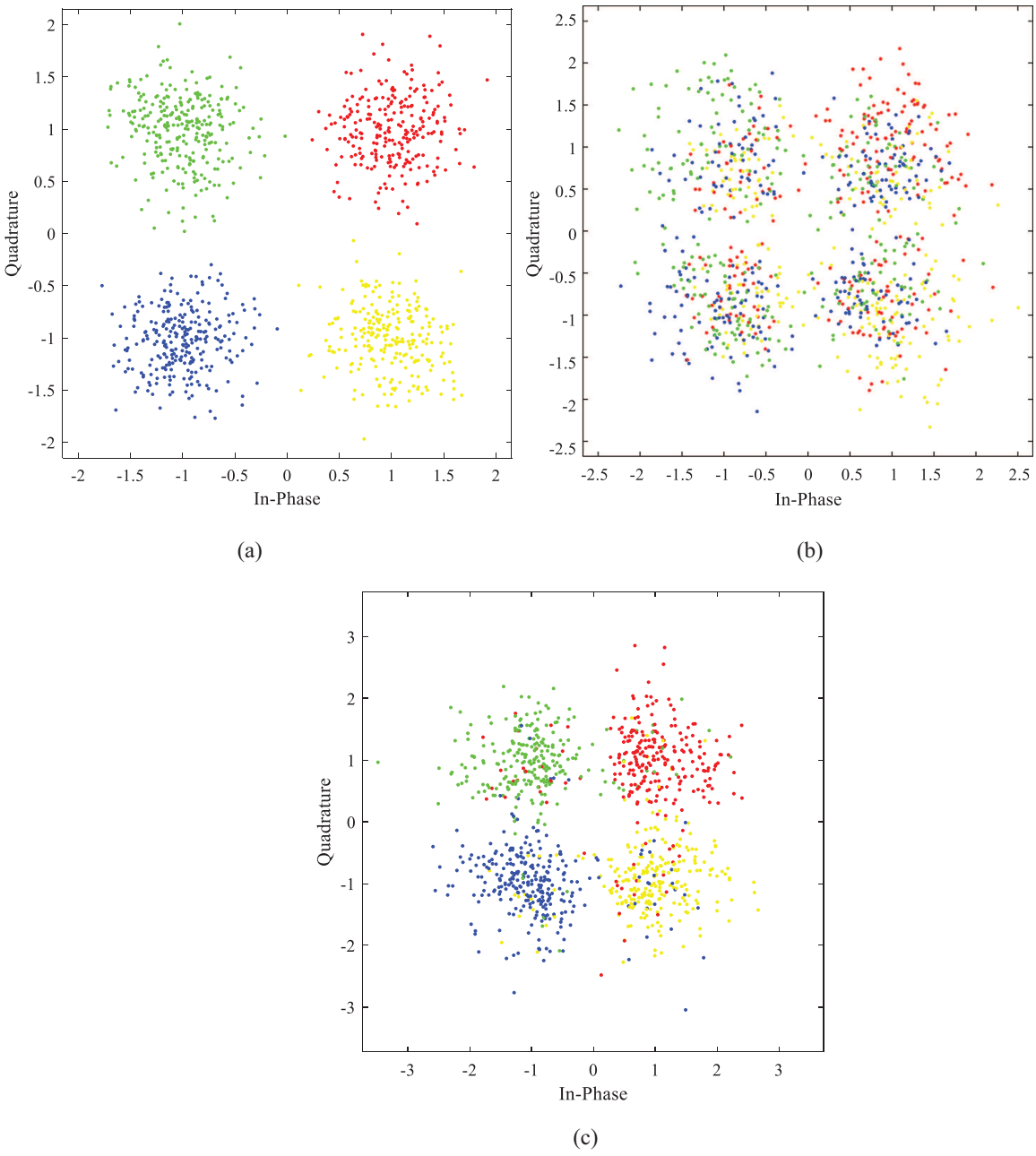


Figure 9. Comparison of constellation diagrams generated by QPSK modulation, CSI-QPSK modulation and demodulation: (a) Constellation diagram of QPSK modulation; (b) Constellation diagram of CSI-QPSK modulation; (c) Constellation diagram demodulated by CSI-QPSK

with the traditional key generation scheme based on channel characteristics, there is no quantization step, that is, the performance loss caused by quantization is avoided, and BER is reduced to a certain extent. Second, in terms of algorithm complexity, this paper preprocesses the CSI and then embeds it directly into the modulator. The steps are simple and effective. Third, this method uses random channel characteristics for modulation, which can be updated in a short time. Moreover, the direct modulation process is only completed at the physical layer, and the whole process has nothing to do with the upper layer data, which guarantees security to a certain extent.

However, due to the inconsistency of the CSI between the sender and the receiver, as SNR increases, the BER will have a fixed lower limit.

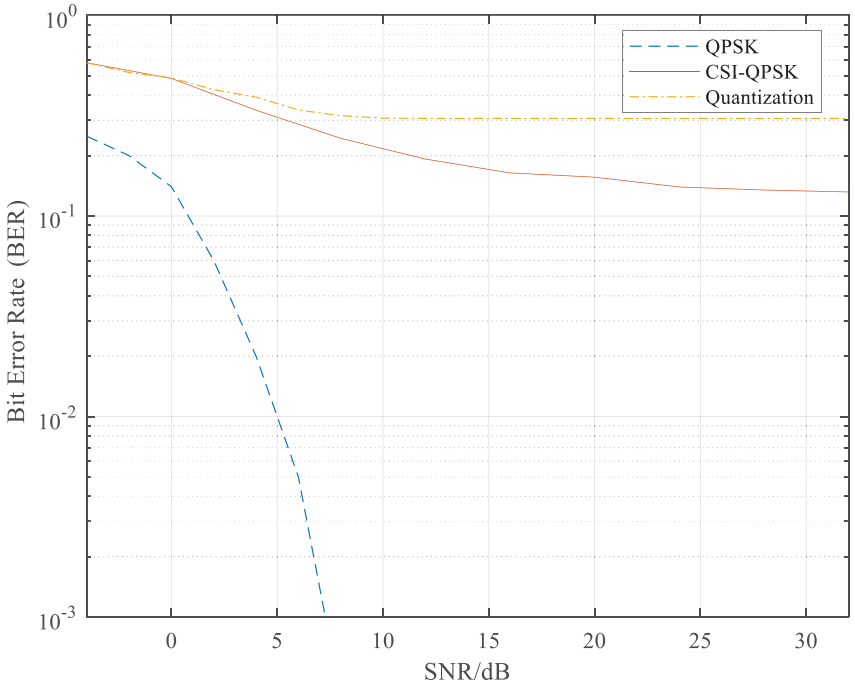


Figure 10. BER curves of QPSK, CSI-QPSK, and Quantization methods

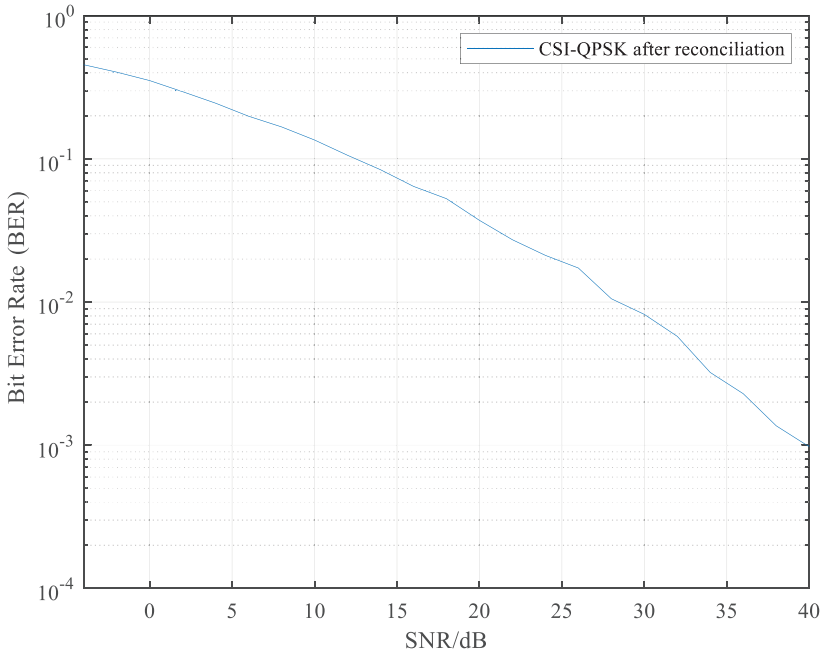


Figure 11. BER after information reconciliation

The security transmission technology CSI-QPSK based on direct modulation with random channel characteristics proposed in this paper can enhance the link of physical layer modulation and demodulation in wireless communication, thereby protecting the security of data in channel transmission.

In the future work, we can further study how to expand the 52-bit CSI into more bits of correlated and random data to avoid repeated use of CSI for encryption, so as to enhance the security of data transmission. What is more, it is necessary to continue to study how to further improve the CSI consistency between the transmitter and the receiver. However, blindly pursuing the improvement of consistency

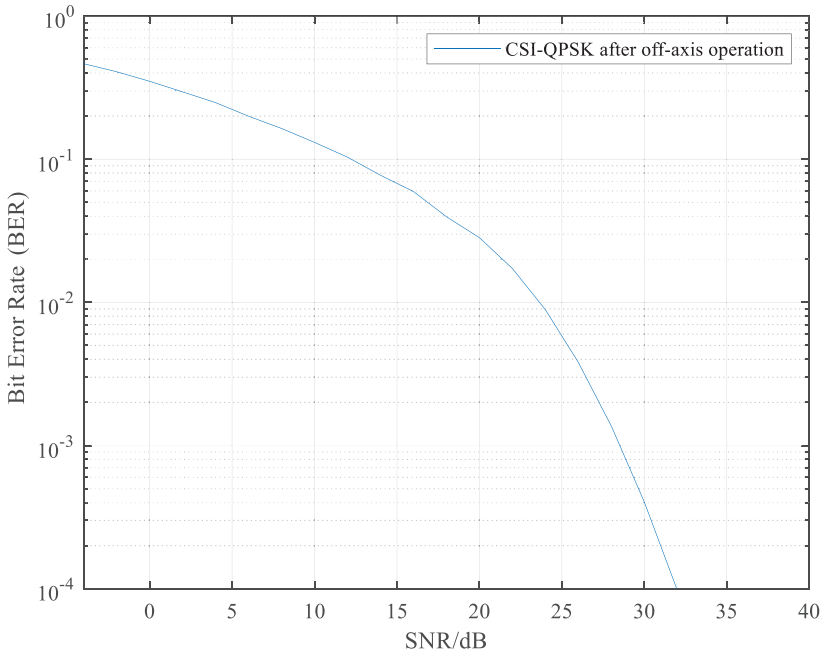


Figure 12. BER after off-axis operation

often leads to the reduction in randomness, that is, security will be reduced. Therefore, how to choose a compromise between randomness and consistency of CSI is also a problem that needs further research.

Conflict of Interest

The authors declare that they have no conflict of interest.

Data Availability

No data are associated with this article.

Authors' Contributions

Aiqun Hu proposed the secure transmission technique CSI-QPSK based on direct modulation with random channel characteristics and guided the overall work of this paper. Rong Yang studied the CSI-QPSK method, practiced it, and then wrote this paper.

Acknowledgements

We thank the anonymous reviewers for their helpful comments.

Funding

This work was supported by Jiangsu Province Key R&D Program (Grant No. BE2019109).

References

[1] Patwari N, Croft J and Jana S et al. High-rate uncorrelated bit extraction for shared secret key generation from channel measurements. IEEE Trans Mob Comput 2010; **9**: 17–30.
[2] Zhang J, Woods R and Duong TQ et al. Experimental study on channel reciprocity in wireless key generation. In: The 17th IEEE International Workshop on Signal Processing Advances in Wireless Communications-Edinburgh, United Kingdom, 2016.
[3] Xi CJ, Gao YY and Sha N. Influence of channel estimation error on physical layer security encryption scheme. Comput Eng 2020; **46**: 122–9.
[4] Xi CJ, Gao YY and Sha N. Performance research of fuzzy design method for physical layer security constellation. Comput Sci 2020; **47**: 304–11.
[5] Li XQ, Li W and Lei J et al. Physical layer security encryption algorithm based on 3D constellation rotation in OFDM system. Electron J 2017; **45**: 2873–80.
[6] Li M, Liang LL and Wei D. Wireless communication physical layer security transmission technology based on polarization state modulation. J Inf Secur 2018; **3**: 105–17.

[7] Li X, Li XH and Yang D et al. An efficient random physical layer key extraction scheme based on vector quantization. Electron J 2016; **44**: 275–81.
[8] Hu AQ and Li GY. A survey of wireless communication physical layer security methods. Data Collect Process 2014; **29**: 341–50.
[9] Li GY, Yu JB and Hu AQ. Physical layer security method based on device and channel characteristics. J Cryptogr 2020; **7**: 224–48.
[10] Xi C, Gao Y and Nan S et al. Constellation symbol obfuscation design approach for physical layer security. In: 2018 10th International Conference on Communication Software and Networks (ICCSN)-Chengdu, 2018, 264-9.
[11] Yubo S, Bing C and Tianyu Z et al. Identification method of wireless device based on hybrid feature fingerprint. Comput Res Develop 2021; **58**: 2374–99.
[12] Yubo S, Bing C and Tianqi W et al. Enhancing packet-level Wi-Fi device authentication protocol leveraging channel state information. Wirel Commun Mob Comput 2021; **2021**: 2993019.
[13] Zhang J. Research and Application of IEEE 802.11g Physical Layer Transmission. China: Xidian University, 2015.
[14] Ren K, Su H and Wang Q. Secret key generation exploiting channel characteristics in wireless communications. IEEE Wireless Commun 2011; **18**: 6–12.
[15] Li GY, Hu AQ and Shi L. Key generation method for wireless channel. J Cryptogr 2014; **1**: 211–24.
[16] Han QQ. Research on Quantization Method of Physical Layer Key Generation. China: Xidian University, 2019.

Rong Yang received her B.S. degree in information science and technology from Southeast University, Nanjing, China, in 2020. She is currently pursuing her Master's degree at Southeast University. Her main research interest is physical layer security.

Aiqun Hu received his B.Sc. (Eng.), M.Eng.Sc., and Ph.D. degrees from Southeast University in 1987, 1990, and 1993, respectively. His research interests include data transmission and secure communication technology.