Research on quantum communication network based on random matrix theory

Jin Xi, Xue Su and Yiping Li*
Wuhan Railway Vocational College of Technology, Wuhan, Hubei 430205, China
*Yiping Li is Corresponding author (yipingemail@sohu.com)

Abstract. The application of quantum communication network structure has attracted much attention. In this paper, stochastic matrix method is used to analyze quantum communication network structure. Firstly, the point-to-point quantum communication technology is studied, and then the quantum communication network structure between multi-point users is analyzed. Combined with the classical wireless network communication technology, the quantum teleportation and quantum entanglement state between quantum dots are analyzed by random matrix theory, then the analysis extends to quantum communication network system. The simulation results show that the stochastic matrix theory can accurately analyze the channel characteristics of quantum communication networks.

1. Introduction
Network communication has become an integral part of our life, which also poses unprecedented challenges to the issues on information security. Quantum secure communication technology based on the principles of quantum mechanics, provides the only method to guarantee absolute information security. There are three main directions in the study of quantum communication, which are quantum key distribution (QKD), quantum secure direct communication (QSDC) and quantum secret sharing (QSS). Among these three directions, the quantum key distribution is the core of quantum communication. From the practical point of view, quantum key distribution will inevitably develop from end to end into quantum key distribution network [1]. Nowadays, the United States, the European Union, China, Japan and other countries and regions are conducting field research on quantum key distribution networks and trying to popularize its application [2].

2. Point-to-point Quantum Communication
Quantum communication refers to a new type of communication method that uses quantum effects for information transmission. It mainly includes methods like quantum key distribution (QKD), quantum secure direct communication (QSDC), and quantum secret sharing (QSS) [3].

The core of quantum communication is the quantum key distribution: Quantum key distribution refers to the method of establishing a shared key by using quantum states as information carriers and using quantum mechanical principles to transmit through quantum channels. The quantum key distribution protocol model is shown in Figure 1. The sending end prepares the quantum state, and then transmits it to the receiving end through the quantum channel for detection, and then both parties perform data processing through the classical channel. The data processing includes operations such as the comparison of measurement basis, data negotiation, and compactness amplification, and at last the
final key is obtained to complete the process of quantum key distribution. For the entangled state quantum key distribution protocol, the sending end must complete the preparation of the entangled pair and measure the retained entangled particles, while the receiving end measures the entangled particles transmitted through the quantum channel, and then the two parties process data through classical channels. Experiments prove that through quantum key distribution, an absolutely secure key can be obtained through the negotiation between two distant communication parties, and theoretically the secure communication is achieved since the classical information can be encrypted by using this key.

3. Multi-user Quantum Communication Network
In order to expand the application, it is urgent to network the point-to-point communication method to meet the needs of multi-user communication. Therefore, the point-to-point quantum communication must transition to the multi-user quantum communication network.

3.1. Principle of Quantum Communication Network
The classical cryptographic communication currently used in quantum communication network can be divided into two categories, symmetric cryptosystems and asymmetric cryptosystems. The symmetric cryptosystem is also known as the private key cryptosystem, with the working principle that the communicating parties share a private key that only they know. The sender uses this key to encrypt the information to be transmitted to the receiver, and when the receiver obtains the ciphertext it would decrypt the information. The asymmetric cryptosystem is also known as the public key cryptosystem. Its working principle is that the receiver first selects a set of private keys that only it knows, calculates the corresponding public key according to the private key, and publishes the public key to all objects that are ready to transmit information to it. The sender encrypts the information by using the public key and passed the information to the recipient. It is difficult to reveal the original information from the ciphertext only with the public key. Both the public key and the private key are required to restore the ciphertext to the original text. The security of such cryptosystems depends on the computational complexity, and the widely used RSA cryptosystem is based on this principle.

3.1.1. The basic Principle
According to the basic principle of the E91 protocol in RSA cryptography, the two-bit quantum system can be in the two-particle coherent superposition state and the quantum entangled state. The two-particle coherent superposition state refers to the direct product that cannot be decomposed into a single coherent superposition state, and thus will display more quantum mechanical properties than single bits. If two quantum states are respectively represented by $|0\rangle$ and $|1\rangle$, the quantum entangled state can be expressed as:

$$|\varphi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$  (1)

The state of any one of the EPR entangled pairs is uncertain before measurement. Once one particle measurement has a definitive result, the state of the other particle is determined describes a
two-particle system in a spin state which represents the spin-up state of the particle and represents the spin-down state of the particle. Measuring the spin of the first particle, the upward spin and the downward spin can be obtained with a 50% probability; but when the first particle is found to spin down, the entire wave function collapses to state. At this time, when the second particle is measured again, and the spin-up result is obtained as a consequence. Even if the two particles are separated far apart, this association still exists. It is this property that makes quantum entanglement pairs widely used in quantum key distribution systems.

3.1.2. The Protocol Process

![Protocol flow chart](image2.png)

The principle of quantum key distribution using EPR entanglement is shown in Figure 2. Assume that Alice has prepared an EPR entangled state.

\[ |\psi^+\rangle_{AB} = \frac{1}{\sqrt{2}} (|00\rangle_{AB} + |11\rangle_{AB}) \]  

(2)

Alice passes particle B to Bob and owns particle A. There may be an eavesdropper Eve on quantum channels 1 and 2. Alice and Bob randomly select the measurement base Z or the measurement base X to measure the respective particles to determine whether the channel is safe. If the channel is secure, Alice and Bob can discard the result of the inconsistent measurement basis through the classic channel to generate a post-screen key. The final key is further negotiated by error correction and compactness amplification.

The specific processes are as follows:

1. A set of entangled pairs of spins of 1/2 are generated by the EPR entanglement source and sent to Alice and Bob, respectively.

2. Alice and Bob respectively use a random measurement basis to detect the spin state of the arriving particles. The measurement direction used by Alice is \{0°, 45°, 90°\}, and Bob’s is randomly selected within \{45°, 90°, 135°\}. The measurement directions are represented by vectors \(a_i\) and \(b_j\), respectively. In the measurement result, the up-spin state is recorded as +1, and the down-spin state is recorded as -1.

3. Alice and Bob publish the directions used by their measurements through the classical channel, but do not publish the measurement results. If the two parties or either party have no measured results, they would turn to divide the remaining results into two categories. One is the result obtained when the same measurement direction is used, and the other is the result obtained when different measurement directions are used.

4. Then the two parties publish the second category of measurement results, so that the value of the entangled bit correlation coefficient \(S\) is obtained by the following two equations.

\[ E(a_i, b_j) = P_+ (a_i, b_j) - P_- (a_i, b_j) \]  

(3)

\[ S = E(a_i, b_i) + E(a_i, b_j) + E(a_i, b_3) + E(b_i, b_j) + E(b_i, b_3) + E(b_j, b_3) \]  

(4)

Then, it is compared with the theoretical value of the entangled bit correlation coefficient to determine whether or not there is interference from Eve.

5. If it is judged that the communication process is not interfered, the first type of measurement
result obtained in the third step is used to generate a key.

3.1.3. Security analysis
If Alice and Bob choose the same measurement basis, they will get consistent measurement results; if the selected measurement vectors are inconsistent, there will be no correlation between the results. Alice and Bob use the Bell inequality to detect eavesdropping during particle transmission. If Alice and Bob's measurements follow Bell's inequality, then it shows that there exists eavesdropping; if their measurements violate Bell's inequality, then the quantum channel is safe.

3.2. Wireless Quantum Communication
In quantum network communication, whether direct transmission or quantum teleportation is used to transmit quantum signals, only distances of several tens of kilometers to hundreds of kilometers can be reached. In order to realize quantum secure communication in wireless communication systems, it is necessary to deal with the problem of limited transmission distance of quantum signals in free space.

In a quantum relay routing scheme, each intermediate node shares an EPR pair with its upstream and downstream nodes. It can be found that each intermediate node can function as an EPR pair generator, and this node can establish an entangled quantum channel with both upstream and downstream nodes. This observation facilitates the development of quantum switching routing solutions. Quantum teleportation and quantum entanglement swapping techniques are used in the proposed quantum-switched routing scheme. The schematic diagram is shown in Figure 3. The scheme can complete the entanglement swapping by performing the Bell state measurement at the intermediate node to realize the direct establishment of the entangled quantum channel between the upstream and downstream nodes. Until the entangled quantum channel is established between the source node and the destination node, and then the quantum teleportation is used to complete the wireless remote transmission of the quantum state.

The quantum circuit schematic of the quantum-switched routing scheme is shown in Figure 4. It can be verified as follows: In the scheme, the entanglement swapping can establish an EPR pair between the source node and the destination node through an intermediate node. The quantum circuit diagram is shown in Figure 4 (a) shown. We share the EPR of the source node (ie Alice) and the intermediate node (ie Candy).

After the entangled quantum channel is established between the source node and the destination node, the source node can perform quantum teleportation and transmit the quantum state y to the destination node. The quantum circuit diagram of quantum teleportation is shown in Figure 4(b). Figure 4 is a quantum circuit diagram of a quantum switched routing scheme that is an extension of quantum teleportation. Initially, the intermediate node is responsible for establishing an EPR pair between the source node and the destination node. Then, with the help of the entanglement-assisted quantum channel, the source node can trigger the quantum teleportation, thereby completing the remote transmission of the qubit. This means that even if the EPR pair is not shared between the two sites, the scheme can still transmit the qubits to the remote quantum site through the intermediate nodes.
4. Research on Random Matrix Theory and Quantum Communication

First of all, we focus on how to use quantum matrix theory to describe quantum communication through the field of classical wireless communication, while combining with random matrix analysis in the field of quantum communication wireless.

4.1. Using a Random Matrix to Describe the Channel of Quantum Wireless Communication

Current wireless channels have features such as fading, wideband, multi-user, and multiple antennas. Many papers on information theory have studied the channel capacity of such linear memoryless channels. This type of channel can be expressed as

$$ y = Hx + n $$

In the formula, $x$ is the K-dimensional input vector, $y$ is the N-dimensional output vector, and $n$ is the N-dimensional additive cyclic symmetric Gaussian noise, and both can be replicated variables. In addition to the limitations of the transmitting and receiving ends, the characteristics of the channel can be described by this N × K dimensional complex-valued random channel matrix $H$.

4.2. Analysis of Quantum Wireless Communication Channel Based on Random Matrix

As we all know, channel capacity is an important performance indicator of wireless communication systems. The following is an example of channel capacity analysis[5]. Assuming that the channel matrix $H$ is fully known at the receiving end, we will prove that when there is input power control, the channel capacity of channel equation (5) is determined by the distribution of the singular values of the channel random matrix $H$.

The empirical cumulative distribution function $(c, d, f)$ of an $N \times N$-dimensional Hermitian matrix $A$, namely the empirical spectral distribution function (ESD), can be defined as:

$$ F^N_X (x) = \frac{1}{N} \sum_{i=1}^{N} \{ \lambda_i (A) \leq x \} $$

In the formula $\lambda_i (A)$ is the eigenvalue of the random matrix $A$, and $l\{x\}$ is the indication function. $F^N_X (x)$ converges when $N \to \infty$ and the corresponding limit (asymptotic ESD) is denoted as $F_A (x)$.

Assuming that the input signal $x$ in equation (5) is an independent and identically distributed $(i, j, d)$ Gaussian random variable, the mutual information subject to $H$ can be given by

$$ J_{SNR} = \frac{1}{N} I(x, y | H) = \frac{1}{N} \log_{\text{det}} (I + \text{SNR} H H^+) = \frac{1}{N} \sum_{i=1}^{N} \log (I + \text{SNR} \lambda_i (H H^+)) $$
\[
\int_0^\infty \log(1+\text{SNR}_x) dF_{\text{SNR}}(x)
\]  

(7)

Wherein, \(\lambda_i(HH)\) is equivalent to the square of the i-th singular value of the random matrix H.

The mathematical expectation of equation (7) is the channel capacity if the receiver is fully aware of the channel state and the channel variation is stable and the states are experienced. More generally, the distribution of the random variable formula (7) determines the interrupt capacity.

Another important performance metric in classical wireless communications is the linear minimum mean square error (MMSE), which determines the maximum output signal to interference ratio. For independent and identically distributed input signals, the arithmetic mean of MMSE can be given by

\[
\text{MMSE}_{\text{SNR}} = \frac{1}{K} \min_{y} \{ \frac{1}{K} \text{Tr}\{ (1+\text{SNR}_x)HH^{-1} \} \} = \frac{1}{K} \sum_{i=1}^{K} \frac{1}{1+\text{SNR}_x} \lambda_i(HH)
\]

(8)

It can be seen from the two excellent results of equations (7) and (8) that the two most basic performance indicators (channel capacity, MMSE) can be obtained by the empirical spectral distribution function of the singular value (square) of the channel random matrix. Therefore, it is important to properly represent this empirical spectral distribution function. However, it can be seen from equations (7) and (8) that \(F_{\text{SNR}}(x)\) is closely related to the specific channel random matrix H, and if \(F_{\text{SNR}}(x)\) can be independent of the specific channel H, it will be used for engineering applications. It has extremely significant significance\(^6\). In order to achieve this, you need to complete the following 2 steps:

1. The average state is obtained by studying the expectation of performance indicators under channel H, which requires specifying a probability structure.
2. Determine a feasible solution so that equations (7) and (8) do not depend on specific signal selection.

Asymptotic analysis (in the case of large dimensions, ie \(K \rightarrow \infty, N \rightarrow \infty, \beta = K/N\)) is an effective solution to satisfy the above two points. First, when the dimension tends to infinity, the calculation of the average performance index is simplified. The homogeneous, asymptotic analysis method makes the equations (7) and (8) not depend on the specific channel random matrix H\(^7\). Specifically, in most cases, the asymptotic RMT guarantees that under the condition of \(K \rightarrow \infty, N \rightarrow \infty, \beta = K/N\), its empirical singular value distribution has the following excellent characteristics suitable for wireless communication:

(a) Insensitivity: the asymptotic feature distribution is insensitive to the probability density function of the random matrix element;
(b) ergodicity: the spectrum of any random matrix almost converges to the asymptotic feature distribution;
(c) Fast convergence: the empirical singular value distribution can quickly converge to its asymptotic limit distribution;

All of these features are attractive both in terms of the analysis of wireless communication systems and the design of wireless communication systems. Therefore, we can use RMT to deal well with related issues in wireless communications.

4.3. Quantum wireless communication simulation based on random matrix theory

The specific theory of the random matrix is used to analyze the theoretical performance of the de-correlation (DEC) receiver, and the accuracy of the theoretical analysis is illustrated by comparing with the simulation results.
Now consider a Gaussian white noise synchronous DS-CDMA channel for M users. The discrete time signal model at the receiving end of the system is:

\[ r = S A b + n \]  

Here \( n \sim N(0, \sigma^2) \). The DEC receiver is multiplied at the receiving end to represent the Moore-Penrose generalized inverse. The singular value decomposition can be obtained:

\[ S^{++} = V \sum U^*, S = (S^*)^+ S^* \]  

Here \((S^*)^+ = V \Lambda^+ V^*\), is a \( N \times M \) diagonal matrix with \( \sigma_i > 0, i=1,2,\ldots,r \) and other diagonal arrays of zero. \( \Lambda \) is a \( M \times M \) diagonal matrix with the element of \( \lambda_i = \sigma_i^2 \).

The DEC receiver output vector is:

\[ x = P_v A b + S' n \]  

Here \( P_v = S^+ S = V \tilde{V}^* \), \( \tilde{V} \) is a \( M \times M \) diagonal matrix in which the first \( r \) diagonal elements are 1, and the other elements are 0. Thus, the SIR of the DEC receiver is obtained using RMT. In Figure 5, a comparison of theoretical analysis and simulation results is given. The simulation uses QPSK modulation, AWGN channel, and spreading factor \( N=128 \). The theoretical value of the BER formula based on the above formula is substituted into this condition:

\[ P_e = Q(\sqrt{1/m}) \]  

Here:

\[ Q(y) = \frac{1}{\sqrt{2\pi}} \int_y^\infty e^{-t^2/2} dt \]  

Figure 5 illustrates that at \( N = 128 \), the performance of the decorrelated receiver in the DS-CDMA system can quickly converge to the theoretical limit performance in the simulated environment. At the same time, the simulation results clearly reflect the influence of the ratio \( \beta \) between the user number and the spreading factor on the system error performance. When the number of users is the same as the spreading factor (\( \beta=1 \) in the figure), the system obtains the best error performance.

5. Conclusions and recommendations
Random matrix theory, which is quietly rising in recent years, has been a focus of attention among many foreign scholars. This paper first introduces the mathematical background of random matrix theory which is closely related to wireless communication, and then expounds the connection between the theory and quantum wireless communication system, and answers the question of why to use random matrix theory in wireless communication systems. In the end, the specific examples are used to intuitively show the power of random matrix theory in dealing with wireless communications. With the development and improvement of this theory, its application in the field of wireless communication will be increasingly deep and extensive.

References
[1] ASSCHE G V.2006. Quantum Cryptography and Secret- Key Distillation [M]. New York: Cambridge S University Press
[2] Zhang Yang. 2012. *Optical fiber quantum cryptography experiment and practical research* [D]. Hefei: University of Science and Technology of China

[3] Xue Su and Guoxin Song. 2016. A Cloud Data Access Control Optimization Technology Based on Security Policy[J]. *Journal of East China University of Science and Technology(Natural Science)*, 42(6): 858-862

[4] Ma Ruilin. 2006. *Quantum Cryptography Communication* [M]. Beijing: Science Press

[5] ZARIFIK, GERSHMAN A B. 2008. Asymptotic performance analysis of blind minimum output Energy receivers for large DS-CDMA systems [J]. IEEE trans on signal processing 56(2):650

[6] ZHANG, JCHONG E, TSE D N C. 2001. *Out put MAI distributions of linear MMSE multiuser receivers in DS-CDMA systems* [J]. IEEE trans on information theory, 47(3): 1028-1144

[7] LIL, TULINO A M, VERDU S. 2004. *Design of reduced-rank MMSE multiuser detectors using random matrix methods* [J]. IEEE Trans on information theory, 50(6): 986-1008