A key distribution protocol based on quantum entanglement swapping for unmanned surface vehicle

Lingyu Qin¹,²,*, Ying Li¹,² and Shibo Wang¹,²

¹ Navigation College, Dalian Maritime University, Dalian 116026, China
² Environment Information Institute, Dalian Maritime University, Dalian 116026, China

*Corresponding author. Email: qinlingyu3@163.com

Abstract. Aiming at the problem of Unmanned Surface Vehicle's (USV) secure communication, this paper proposes a key distribution protocol based on quantum entanglement swapping for USV. Compared with the current techniques, this paper uses the principle of quantum unclonability and quantum entanglement in quantum mechanics to realize the secure communication of USV. Meanwhile, in view of the low visibility at sea and the influence of weather such as wind and waves, this study adopts a key distribution architecture of quantum relay to realize the establishment of quantum channel between any two ships and obtain the absolutely secure key eventually. Therefore, the proposed method can provide long-distance, secure and reliable communication for USVs in the civil and military fields.

1. Introduction

With the development and application of unmanned vehicles and unmanned aerial vehicles, as well as the continuous innovation of artificial intelligence and other technologies, facing with the low speed of ships, difficulty of maritime rescue, imperfect protection system of marine environment pollution, military detection with high performance requirements and other tasks, USV have become a development direction of ship intelligence with their small size and flexible operation. As the scope of offshore operations and demand for multiple tasks increase, the collaborative operation of multiple USVs has become a research hotspot in future ship development [1].

At present, many countries have launched relevant research and experiments on unmanned ships. The University of Michigan developed the "BathyBoat" unmanned boat for lake water depth and environmental measurement [2]. The “Springer” USV is designed by the Marine and Industrial Dynamic Analysis (MIDAS) Research Group at Plymouth University for marine environmental monitoring [3]. The relay USV "SCOUT" developed by the Massachusetts Institute of Technology has completed a number of communication experiments between USV and AUV (Autonomous Unmanned Vehicle) [4]. Aiming at the problem of under-driven USV navigation control, Yi et al. designed a USV navigation tracking control algorithm with dynamic tracking ability [5]. Qiu et al. proposed a robust path tracking controller based on TLC technology, neural network and auxiliary design system, which perfected the USV path tracking control strategy [6]. Cui et al. proposed a multiple USV network topology optimization control algorithm based on improved particle swarm optimization, which considered the connection benefits and costs comprehensively, and constructed a reliable topology structure for multiple USV network [7]. In maritime communication, due to the vast sea area and the great influence of wind and waves and other weather, how to ensure the long-distance, secure and
reliable communication is the top priority for the application of USV. Quantum communication can provide a secure communication system that is theoretically absolutely secure [8]. Therefore, how to combine the principle of quantum unclonability and quantum entanglement in quantum mechanics to realize long-distance secure communication is the main research content of this paper.

2. Principle of quantum entanglement swapping
Quantum communication includes Quantum Key Distribution (QKD), Quantum Teleportation (QT), Quantum entanglement, Quantum Secure Direct Communication (QSDC), etc. QKD is a core technology of quantum communication [9]. Based on the idea of relay swap, this paper proposes a QKD architecture using quantum entanglement swapping for USV. The architecture sets up a quantum entanglement swapping module that realizes the establishment of a long-distance quantum channel to ensure that any two ships in the system can share the key safely.

2.1. Quantum state
Qubit is the basic unit of quantum information [10], and its quantum state can be expressed by (1). $|\phi\rangle$ represents a qubit; $|0\rangle$ and $|1\rangle$ represent two states of the qubit; $\alpha$ and $\beta$ are complex numbers, and $\alpha^{*}\beta + \beta^{*}\alpha = 1$. When we observe the state of qubit, it is in state $|0\rangle$ with probability $|\alpha|^{2}$ and in state $|1\rangle$ with probability $|\beta|^{2}$.

$$|\phi\rangle = \alpha |0\rangle + \beta |1\rangle$$

2.2. Quantum entanglement swapping
Quantum entanglement is the essence of quantum mechanics [11]. A typical quantum system in entangled states can be represented by Bell states. There are 4 types of Bell states, as follows:

$$|\phi^{+}\rangle_{12} = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$$

$$|\phi^{-}\rangle_{12} = \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle)$$

$$|\psi^{+}\rangle_{12} = \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle)$$

$$|\psi^{-}\rangle_{12} = \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle)$$

The two qubits before measurement are in uncertain states. If one of them is measured, the state of the other will collapse to a certain state. Therefore, if the initial states of the two pairs qubits in Bell states are $|\psi^{+}\rangle_{10} = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$ and $|\psi^{-}\rangle_{14} = \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle)$, Bell basis measurement can be performed on qubits 2 and 3 to complete entanglement swapping. Then qubits 1 and 4 become a pair of entangled qubits as (6).
\[
\left|\varphi^+\right\rangle_{12} \otimes \left|\varphi^-\right\rangle_{34} = \frac{1}{\sqrt{2}} \left( \left|00\right\rangle_{12} + \left|11\right\rangle_{12} \right) \otimes \frac{1}{\sqrt{2}} \left( \left|01\right\rangle_{34} + \left|10\right\rangle_{34} \right)
\]
\[
= \frac{1}{2} \left( \left|00\right\rangle_{13} \left|01\right\rangle_{24} + \left|00\right\rangle_{13} \left|10\right\rangle_{24} + \left|11\right\rangle_{13} \left|01\right\rangle_{24} + \left|11\right\rangle_{13} \left|10\right\rangle_{24} \right)
\]
\[
= \frac{1}{2} \left( \left|00\right\rangle_{13} \left|00\right\rangle_{24} + \left|00\right\rangle_{13} \left|10\right\rangle_{24} \right)
\]
\[
= \frac{1}{2} \left( \left|00\right\rangle_{13} \left|00\right\rangle_{24} + \left|00\right\rangle_{13} \left|10\right\rangle_{24} + \left|11\right\rangle_{13} \left|01\right\rangle_{24} + \left|11\right\rangle_{13} \left|10\right\rangle_{24} \right)
\]
\[
- \frac{1}{2} \left( \left|00\right\rangle_{13} \left|00\right\rangle_{24} + \left|00\right\rangle_{13} \left|10\right\rangle_{24} + \left|11\rangle_{13} \left|01\rangle_{24} + \left|11\rangle_{13} \left|10\rangle_{24} \right) \right)
\]

If the selected Bell basis measurement result is \( \left|\varphi^-\right\rangle_{34} \), the remaining qubits are in an entangled state of \( \left|\varphi^-\right\rangle_{34} \), as shown in Table 1.

**Table 1.** Swapping results for each initial entangled states.

| Initial entangled state | Bell basis measurement | Swapping results |
|-------------------------|------------------------|-----------------|
| \( \left|\varphi_0\right\rangle \otimes \left|\varphi_1\right\rangle \) | \( \left|\varphi_0\right\rangle \) | \( \left|\varphi_0\right\rangle \) |
| \( \left|\varphi_1\right\rangle \otimes \left|\varphi_0\right\rangle \) | \( \left|\varphi_0\right\rangle \) | \( \left|\varphi_0\right\rangle \) |
| \( \left|\varphi_0\right\rangle \otimes \left|\varphi_1\right\rangle \) | \( \left|\varphi_0\right\rangle \) | \( \left|\varphi_0\right\rangle \) |
| \( \left|\varphi_1\right\rangle \otimes \left|\varphi_0\right\rangle \) | \( \left|\varphi_0\right\rangle \) | \( \left|\varphi_0\right\rangle \) |

3. **Key distribution protocol**

3.1. *The quantum entanglement swapping module*

In order to realize the quantum entanglement swapping of USVs, this paper designs a quantum entanglement swapping module, which is mainly composed of quantum access unit, quantum storage unit, quantum entanglement pair manufacture unit, single-photon measurement unit, Bell basis measurement selection unit, Bell basis measurement units, and auxiliary information unit. As illustrated in Fig. 1, quantum access unit is responsible for receiving the distributed photon in entangled state, and quantum storage unit is for storing the received photons for single-photon measurement or Bell basis measurement. Quantum entanglement pair manufacture unit can generate quantum pairs in entangled states, and can distribute the quantum pairs. Single-photon measurement unit includes right-angle basis measurement and diagonal basis measurement, and is used with auxiliary information unit to verify the safety of quantum channel. Bell basis measurement selection unit is responsible for the selection of Bell basis measurement units, and Bell basis measurement units can complete the entanglement swapping to establish quantum channels.
Quantum access unit

Quantum storage unit

Quantum entanglement pair manufacture unit

Figure 1. Component units of quantum entanglement swapping module.

3.2. The overall process of protocol

The procedure is illustrated in Fig. 2 and Fig. 3. Fig. 2 shows the quantum entanglement swapping and Fig. 3 shows the process of key distribution.

Step 1: USV A and remote USV B (or command and control center) negotiate an unmanned ship C (between A and B) as the relay USV, and inform C to establish the quantum channel. If C has free Bell basis measurement units, it will inform A and B that they can start to establish the quantum channel.

Step 2: The quantum entanglement pair manufacture units of A and B prepare a random sequence of entangled pairs with length L, which is larger than the length of the required key. These randomly generated states are initial states of A and B, and the results are saved to their auxiliary information units, respectively;

Step 3: A and B distribute one qubit from each entangled pair in their sequences to form new qubit sequences, respectively. And then send them to C keeping the original order. A and B store the remaining qubit sequences in their quantum storage units, which are denoted as $L_A$ sequences and $L_B$ sequences, respectively;

Step 4: C stores the received qubit sequences into quantum storage unit, and marks them as sequences $C_A$ and $C_B$, respectively. A series of Bell measurements are carried out on the corresponding quantum pairs in $C_A$ and $C_B$ sequences by Bell basis measurement selection unit, and the results are saved to the auxiliary information unit and sent to A. After the measurement, the $L_A$ and $L_B$ sequences stored in A and B will form entangled pair sequences, and the quantum channel between A and B will be established by entanglement swapping;

Step 5: After the establishment of quantum channel, the security detection is carried out. B selects $T$ positions ($T > L - T$ > key length) from the $L_B$ sequence randomly and sends them to the single-photon measurement units for measurement. The units select right-angle basis or diagonal basis randomly, and save the position information and measurement basis information of the selected T qubits to auxiliary information unit. Then sends the information of positions, measurement basis, measurement results and initial entanglement pair sequence to A;
Step 6: A saves the received information to auxiliary information unit, and performs the corresponding basis measurements for the qubits at corresponding positions in L^A sequence. According to the measurement results sent by relay unmanned ship C and the initial sequence status of A and B, A can infer the measurement results of B combined with its own measurement results. If the initial states of A and B are $|\psi\rangle_a \otimes |\phi\rangle_b$, and the measurement result of C is $|\phi\rangle$, then the residual qubits of A and B are in the shared entangled state of $|\psi\rangle$. If the measurement result of A is 0, the measurement result of B is inferred to be 1, and vice versa. Then, A compares its inference results with the results sent by B, and can determine whether the quantum channel between A and B is secure according to the bit error rate.

Step 7: After the security of the quantum channel between A and B is determined, the qubits at the P position need to be deleted from the entangled pairs sequence, and the record of the auxiliary information unit is updated. The key is generated by the remaining (L-T) entangled pairs between them. Because only A has enough information (initial sequence information of A and B, and measurement result information of C), the entangled pair information shared by A and B can be known according to Table 1. B measures the remaining L^B -P sequence with right-angle basis or diagonal basis randomly, and sends the measurement basis information to A. Then A also measures the remaining L^A -P sequence on the corresponding measurement basis. According to the information of the entangled states, A can infer the results of B. And the results form the key.
Begin
Does C have remaining Bell basis measurement units?
Y
A and B prepare a random sequence of entangled pairs with length L
Distribute the qubits and to C in order
Perform Bell basis measurement on C^- and C^+ to realize quantum channel establishment
Generate the key
End

Security detection?
N
Y

Figure 3. Princess of the key generation.

4. Conclusion
This study realizes the long-distance safe and reliable communication of USV on the sea. The proposed method reduces the possibility of eavesdropping in communication by introducing the quantum key distribution protocol. In addition, a quantum entanglement swapping module is designed to realize the key distribution architecture of quantum relay, which can better solve the problems of short distance communication caused by factors such as poor natural environment and low visibility. Therefore, the proposed method can guarantee the long-distance safe communication of USVs in military combat missions and maritime supervision ultimately, and provides new ideas and methods for the research and development in the field of USVs’ communication.

References
[1] S. Zhang, Z. Liu, X. Zhang et al.: “Development and Prospect of Unmanned Vessel [J]”, World Shipping, Vol.38, No.9, pp.29-36 (2015)
[2] Brown H, Jenkins L, Meadows G, et al.: “BathyBoat: An autonomous surface vessel for stand-alone survey and underwater vehicle network supervision”, Marine Technology Society Journal, Vol.44, No.4, pp.20-29 (2010)
[3] R. Song, Y. Liu, and R. Bucknall: “Smoothed A* algorithm for practical unmanned surface vehicle path planning”, Applied Ocean Research, Vol.83, pp.9-20 (2019)
[4] J. Curcio, J. Leonard and A. Patrikalakis: “SCOUT - a low cost autonomous surface platform for research in cooperative autonomy”, Proceedings of OCEANS 2005 MTS/IEEE, Washington, DC, Vol.1, pp.725-729 (2005)
[5] G. Yi, Z. Liu, J. Zhang and J. Dong: “Research on Underactuated USV Path Following Algorithm”, 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chongqing, China, pp.2141-2145 (2020)
[6] Qiu, B., Wang, G., Fan, Y., Mu, D. and Sun, X: “Robust path-following control based on trajectory linearization control for unmanned surface vehicle with uncertainty of model and
actuator saturation”, IEEJ Trans Elec Electron Eng, Vol.14, No.11, pp.1681-1690 (2019)
[7] Cui et al.: “Network topology optimization control algorithm for multiple unmanned surface vehicle”, Control Theory & Applications, Vol.33, No.12, pp.1639-1649 (2016)
[8] S. Wengerowsky, S. K. Joshi, F. Steinlechner, H. Hübel and R. Ursin: “An Entanglement-Based Wavelength Multiplexed Quantum Communication Network”, 2019 Conference on Lasers and Electro-Optics Europe & European Quantum Electronics Conference (CLEO/Europe-EQEC), Munich, Germany, pp.1-1 (2019)
[9] Webster, J.G., Martin, V., Martinez-Mateo, J. and Peev, M.: “Introduction to Quantum Key Distribution.”, in Wiley Encyclopedia of Electrical and Electronics Engineering, doi:10.1002/047134608X.W8354 (2017)
[10] F. Xu, M. Curty, B. Qi and H. Lo: “Measurement-Device-Independent Quantum Cryptography”, IEEE Journal of Selected Topics in Quantum Electronics, Vol.21, No.3, pp.148-158 (2015)
[11] H. Hubel, A. Poppe, M. Hentschel and A. Zeilinger: “A portable QKD system based on entanglement”, 2008 Conference on Lasers and Electro-Optics and 2008 Conference on Quantum Electronics and Laser Science, San Jose,CA, pp.1-2 (2008)