Digital Twins Based on Quantum Networking

Zhihan Lv, Chen Cheng, and Houbing Song

Abstract

This work aims to improve the communication security of the industrial Internet of Things (IIoT) based on digital twins (DTs). The related technologies of quantum communication are introduced to improve network communication. Firstly, the key DTs technologies in the construction of IIoT are expounded. Also, the characteristics of quantum communication are analyzed. Secondly, a channel encryption scheme based on quantum communication is proposed to ensure the communication security of IIoT. The scheme uses the five-particle entanglement state and two-particle bell state as entanglement channels to realize two-particle quantum teleportation. Finally, an Adaptive Key Residue algorithm is proposed based on the quantum key distribution mechanism. The algorithm verification suggests that the success rate of service distribution decreases with the increase in network load. When the service load reaches 1000, the Adaptive Key Residue algorithm can maintain a success rate of service distribution in the network higher than 0.6. Besides, the success rate of service distribution increases with the growth of the total key generation rate V and the key pool capacity C. The research results reported here are of great significance for realizing the secure communication of IIoT systems based on digital twins to ensure the effective operation of network communication and the secure transmission of data.

Introduction

The industrial Internet of Things (IIoT) platform builds a service system based on the collection, aggregation, and analysis of massive data oriented to the digital, networked, and intelligent needs of the manufacturing industry. It can ensure the comprehensive connection, on-demand supply, and intelligent scheduling of production resources and realize the technological accumulation and application innovation of the industrial production process [1, 2]. With the advancement of the IIoT applications, the digital twins (DTs) technology has been given new vitality. The IIoT has extended the value chain and life cycle of DTs and highlighted the advantages and capabilities of DTs based on models, data, and services [3]. Specifically, IIoT is essential for the collection and exchange of various data of physical entities. The IIoT platform utilizes its advantages of resource aggregation, dynamic configuration, and supply and demand docking to integrate and use various resources to empower DTs. It can collect the energy consumption data of equipment, production lines, and workshops in real-time through the sensors and other information systems installed in each energy link of the factory and construct the DTs of production, products, and performance to analyze and evaluate the actual production. IoT puts forward higher requirements for the collection and intelligent processing of data information. Based on the advantages of large scale, standardization, and high security, Cloud Computing can meet the development needs of IoT [4].

With the increasing demand for information technology in the communication link of the IIoT, it is imperative to integrate new information technology to improve communication efficiency and increase communication security. Quantum mechanics was born in the early 20th century, showed the vast microscopic world in front of people, and changed the way humans look at the world; it also gave birth to modern technologies such as Lasers, Transistors, Integrated Circuits, and Nuclear Magnetic Resonance Imaging, which completely changed human life [5]. With the rapid development of interdisciplinary sciences such as Quantum Informatics, the Second Quantum Revolution has quietly arrived in recent decades. Emerging Quantum technologies enable unconditionally secure communications, exponential leaps in computing power, and precision measurements beyond classical limits. The vigorous development of emerging technologies such as quantum communication, quantum sensing, and quantum computing will significantly impact the world. Quantum communication includes quantum teleportation and quantum key distribution (QKD). Quantum teleportation is crucial to improving information transmission efficiency [6]. Encrypting data can effectively solve the security problems in the process of industrial Internet data transmission. However, the traditional algorithm based on the public-private key system is increasingly likely to be attacked and cracked during the critical exchange process. Quantum communication technology based on the principles of quantum mechanics can effectively solve the security problems of industrial Internet data in the transmission and storage process.

Quantum teleportation is still in the theoretical research stage, but exploring QKD technology is of immeasurable value. This work expounds

Digital Object Identifier:
10.1109/MNET.001.2200131

Zhihan Lv is with Uppsala University, Sweden; Chen Cheng is with The Second Monitoring and Application Center, CEA, China; Houbing Song is with Embry-Riddle Aeronautical University, USA.

on the critical technologies for constructing IIoT based on DTs. Next, communication links in the DTs IoT are studied. The core content of quantum communication is innovatively introduced, combined with the characteristics of quantum communication. This work effectively solves a series of security authentication problems of IIoT systems based on DTs and ensures the effective operation of network communication.

DTS Network Communication Based on Quantum Communication

IIoT Architecture via DTs

The Industrial DTs technique is the fusion and innovative application of multiple digital technologies to build accurate physical object models in digital space based on modeling tools [7]. It can also use real-time Internet of Things (IoT) data to drive model operation and build comprehensive decision-making capabilities through data and model integration to promote closed-loop optimization of the entire industrial business process. The mapping relationship between the physical entity and the DTs can be established according to the specific steps in Fig. 1. First, a simulation analysis model is established; meanwhile, the digital transformation model is constructed between each thread for the remote operation and maintenance control process. Secondly, intelligent manufacturing, digital inspection, and cyber-physical systems are integrated into a complete whole-link system. Next, the model of the whole life cycle of the remote operation and maintenance is constituted through digital threads. This model is synchronized with the embedded cyber-physical system to realize real-time observation of all conditions of actual physical equipment through the big data platform. Finally, seamless integration is carried out from all aspects of product design, production, operation, and maintenance to form the final DTs image of the intelligent manufacturing factory system and realize feedback on system operation and maintenance design. A digital thread is a communication bridge between several DTs corresponding to a particular physical entity or a specific type of physical entity. These DTs reflect the model views of different sides of the physical entity. The mechanism or engine capable of realizing multi-view model data fusion is the core of digital thread technology.

The accurate two-way mapping and real-time interaction between the physical workshop and the virtual workshop can combine all elements, processes, and business data of the physical workshop, virtual workshop, and workshop service system [8]. The workshop twin data facilitate the iterative operation of workshop production factor management, production activity planning, and production process control among physical workshops, virtual workshops, and workshop service systems. In this way, a new workshop operation model can be built under the premise of meeting specific goals and constraints to optimize workshop production and management. Based on the basic state of the physical entity, the DTs make a highly realistic analysis of the model and data in a dynamic and real-time manner for monitoring, predicting, and optimizing the physical entity.

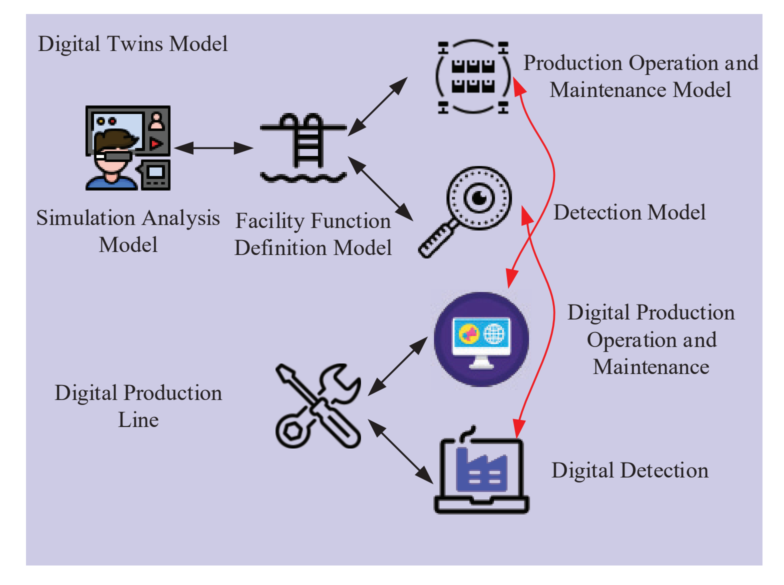
Digital Twins Model
Production Operation and Maintenance Model
Simulation Analysis Model
Facility Function Definition Model
Detection Model
Digital Production Operation and Maintenance
Digital Production Line
Digital Detection

FIGURE 1. IIoT architecture based on DTs.

Encryption Scheme Based on the IoT Communication Channel

The application of the IoT in the future network era will become even more extensive. However, IoT faces an increasingly complex environment with the proliferation of connected devices. Moreover, it is easy for network attackers to eavesdrop and attack the network by taking advantage of IoT devices' limited computing, storage capabilities, and security vulnerabilities, which will cause heavy losses to users [9, 10].

Concerns that upcoming quantum computers could shake or invalidate today's encryption methods are driving much work forward. In the era of quantum computing, it is challenging to process long enough to provide well-secure encryption keys and digital signatures for devices with limited memory, energy, and communication resources. Quantum Computing can communicate securely and protect keys. In other words, each device has a unique key that is hard to crack. In quantum communication, QKD technology supports sharing secure keys between two remote entities (Alice and Bob) to prevent eavesdroppers on encoded Photons [11]. Based on this, this study proposes a two-particle quantum teleportation scheme using the five-particle entanglement state and two-particle bell state as entanglement channels. Suppose that the sender Alice, the receiver Bob, and the controller Charlie are the three parties of the communication. If Alice wants to send information to Bob for measurement, she first needs to encode the original text. A third-party Charlie provides critical assistance in this process. Figure 2 displays the teleportation transmission process of the quantum channel.

During the transmission of quantum information (Fig. 2a), Alice measures the Bell States of two particles (A, 5) and (B, 7) and transmits the results to the receiver Bob and the controller Charlie, respectively. Next, Charlie measures the maximally Greenberger Horne Zeilinger (GHZ)

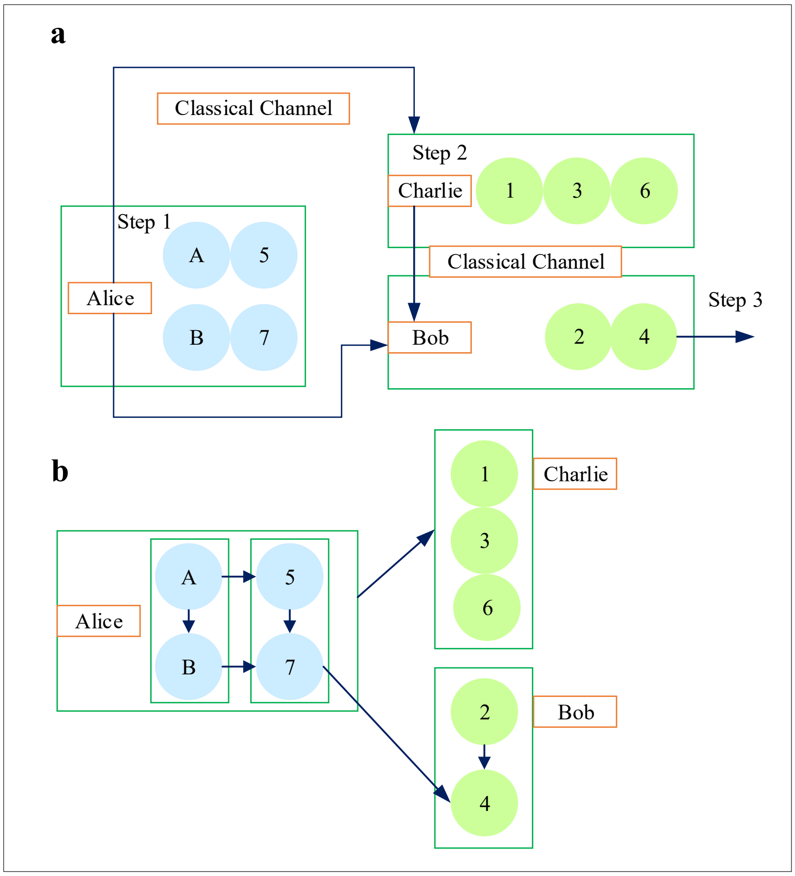

FIGURE 2. Teleportation process of the Quantum channel.

entanglement state of the particle he owns and sends the result to Bob through the classical channel. If and only if Bob and Charlie cooperate with each other, they can get the original information sent by Alice. Finally, Bob performs an appropriate unitary transformation on the result to complete the reconstruction of the original data. Figure 2b shows the transmission of Quantum states held by the three communicating parties. Alice holds particles 5, 7, A, and B, Bob has particles 2 and 4, and Charlie holds particles 1, 3, and 6. Ultimately, in the Quantum Teleportation scheme, particles 1, 2, 3, 5, and 6 constitute five GHZ States, and particles 4 and 7 form the Bell States.

Alice mainly adopts decoy photon technology to detect eavesdropping in the security evaluation of this scheme. Assuming that Charlie is the eavesdropper, he will cooperate with the eavesdropper Eve to intercept the measurement results sent by Alice to Bob. Charlie sends a prepared entanglement state to Bob. At this time, the particles owned by Bob and Alice are no longer an entangled pair, and the information obtained by Bob when reconstructing the original information is wrong. Suppose the three communicating parties do not detect the eavesdropping attack in advance. When Alice completes the Bell State measurement of the two particles she owns, the quantum state system composed of the particles owned by Bob, Charlie, and the attacker Eve will collapse into a five-particle GHZ entanglement state, and the quantum state of Eve will collapse, and Eve's quantum state will not change at all. If Eve eavesdrops on the channel, limited by Heisenberg's Uncertainty Principle, Eve cannot use the two schemes A and B to measure the same quantum bit simultaneously, so Eve cannot copy the information measured by Bob.

Adaptive Key Balance Algorithm Based on the QKD Mechanism

Cryptographers have proposed asymmetric encryption algorithms to solve the problem of key transmission by using some properties of mathematical functions [12]. For example, it is easy to calculate function values according to parameters, but it is not easy to inverse parameters according to function values. These algorithms employ public key encryption and private key decryption. In these algorithms, only the public key is transmitted in communication, ensuring the safety of communication information.

Quantum computers have mighty computing power, posing a significant security threat to the traditional IoT based on computationally complex cryptographic security systems. The QKD technology can guarantee the security of IoT based on the basic principles of quantum mechanics and enable both parties to share an unconditionally secure Quantum key. Quantum encrypted communication is mainly divided into two steps: QKD through Quantum channels and ciphertext transmission through traditional channels [13]. The two communicating parties obtain a pair of quantum keys that are entirely random and known only to the communicating parties through QKD. In this step, only the keys are generated and distributed. During ciphertext transmission, the sender uses the obtained Quantum key to encrypt the information into ciphertext, and the receiver decrypts the received ciphertext to complete the communication secrecy.

Wireless encryption is the primary way to transmit quantum keys to IoT devices on the edge side of quantum IoT (from edge gateways to QKD devices). Therefore, different key distribution schemes can be selected according to different locations and characteristics in the network. Commonly used key distribution schemes are divided into three categories: key distribution of backbone networks and metropolitan area networks, key distribution of access networks, and key distribution of the edge side, as shown in Fig. 3. Some key distribution schemes of metropolitan area networks and backbone networks adopt an underground communication network. In this way, the QKD equipment is distributed on the network nodes, and the shared quantum key is generated based on the QKD protocol to ensure communication security between nodes.

In quantum IoT, request/response service is an essential service model requiring Quantum key resources. Usually, end-to-end communication relies on elliptic encryption, but the mathematical theory of this algorithm is complicated. Besides, in the era of continuous development of quantum computers, the encryption scheme is easy to be cracked. The core principle of the adaptive key distribution scheme discussed is to secure the communication between two devices through the generated key. The premise of this scheme is that a corresponding key pool needs to be constructed for these two arbitrary IoT devices to provide encryption keys for information transmission between them. Since the key generation in the network needs to be completed by the quantum transmitter and the quantum receiver, the key resources are precious. Therefore, it is necessary to improve the utilization of key resources.

When constructing the key pool, firstly, a key pool is built between the edge gateway and the optical line terminal. The key transmitter in the edge gateway and the key receiver in the optical line terminal jointly generate the key and store it in the key pool. Secondly, a key pool is constructed between different edge gateways in the same optical line terminal, which requires one relay generation. The quantum keys generated between the optical line and two different edge gateways are K1 and K2, respectively. K1 is encrypted by K2 at the optical line terminal. Then, K1 is transmitted to the next edge gateway, which can decrypt K1 through K2. Thirdly, a key pool is constituted between two edge gateways in different optical line terminals, similar to the second step, which needs to go through multiple relay generations. Finally, the key is generated through the edge gateway according to the key generation mechanism, and the encrypted quantum key is transmitted to the IoT device.

Next, this study proposes an adaptive quantum key balance scheme to achieve high utilization of the keys generated in the network. The core idea of this scheme is that the generation rate of quantum keys that can be possessed in the next stage principally depends on the balance of the previous key pool. Algorithm 1 lists the specific content of the Adaptive Quantum Key Balance algorithm proposed here. First, this algorithm calculates the key utilization rate of each key pool in the network when a business arrives in the Quantum IoT. Then, it calculates the sum of the key utilization rates of the optical line terminal internals-quantum key pool (OLTs-QKP) of each optical line terminal are calculated and the sum of key utilization of all cross optical line terminal internals-quantum key pool (COLT-QKP). After that, the time interval between the two tasks is calculated according to the time when the previous task arrived to solve the balance of each key pool. If the key pool balance required by the business is greater than the business key demand, the required key pool balance is updated, and the key utilization rate of the current key pool is calculated; otherwise, no additional operation will be performed. It is essential to ensure the same key generation rate of OLTs-QKP under the two optical line terminals and take the minimum value of the calculated key utilization rate of OLTs-QKP. The related key utilization rate of OLTs-QKP and OLT-QKP utilization are corrected, and the key generation rate is updated for each optical line termination.

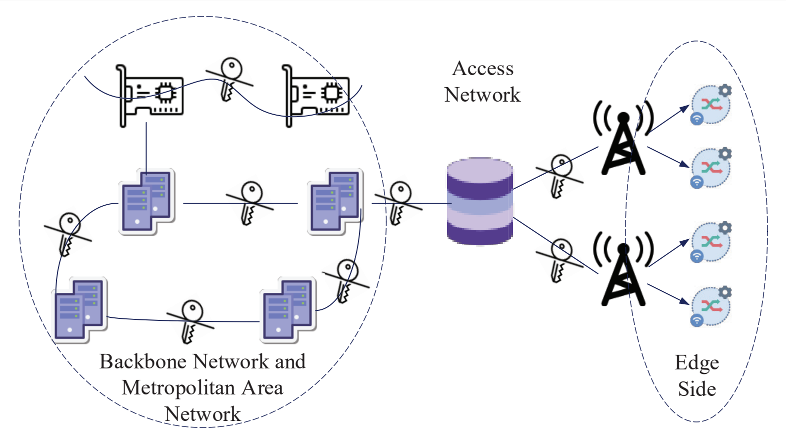

FIGURE 3. Key distribution scheme.

```
Input: task request $R(s, d)$, key demand $K_{sd}$, initial time $t_0$
Output: key generation rate $v_{ij}^{xy}$ for each key pool
For all key pools $P_{ij}^{xy}$ do
Calculate the key utilization ratio $r_{ij}^{xy}$;
End for
For all OLTs do
Calculate the sum of the utilization of OLTs-QKP $R_{out}^{x}$
 Calculate the sum of the utilization of COLT-QKP;
End for
For task request $R(s, d)$ do
    Record the current time $t$;
        For all $P_{ij}^{xy}$ do
    Calculate the key pool balance $M_{sd}^{xy}$ of each key pool;
        If $M_{sd}^{xy}$ is greater than $C_{sd}^{xy}$, then $M_{sd}^{xy}$ is equal to $C_{sd}^{xy}$;
        End If
        Calculate $r_{ij}^{xy}$;
        End For
If $M_{sd}^{xy}$ is greater than $K_{sd}$
Update the calculation method of $M_{sd}^{xy}$;
End if
Calculate OLTs minus QKP
Solve the minimum value $v_{ij}^{xy}$
Update $v_{in}^{x}$ and $v_{out}^{x}$
Calculate $v_{ij}^{xy}$ for each QKP;
End for
End
Return $v_{ij}^{xy}$
```

ALGORITHM 1. Specific contents of the adaptive key residue algorithm of quantum.

Java platform is used to simulate the adaptive key residue algorithm of quantum to verify the specific application performance. The grid designed here covers three metropolitan area network nodes, and all are connected to an optical line terminal. The terminals of each optical line are connected to two edge gateways, where quantum transmitters and Quantum receivers are placed for them to generate quantum keys. Assume that the total rate that each optical line terminal can provide is *V*, and the key capability of each quantum key pool is *C*. In the quantum IoT, all services obey Poisson distribution, and the number of keys required by each service is *X*. The two dimensions of the key generation rate *V* and the key pool capacity *C* will be used to verify their impact on the business success rate.

Quantum Secure Communication Scheme in IIoT

Encrypting data can effectively solve the security problems in the data transmission process of the IIoT. Quantum communication technology based on the principles of Quantum mechanics avoids the vulnerability of traditional algorithms based on public and private key systems. It improves the data transmission and storage security in IIoT [14, 15]. The innovation of quantum encryption technology lies in the key distribution technology, which solves the complex problem of key generation in each encryption algorithm. Based on this, this article proposes two secure quantum communication schemes in IIoT.

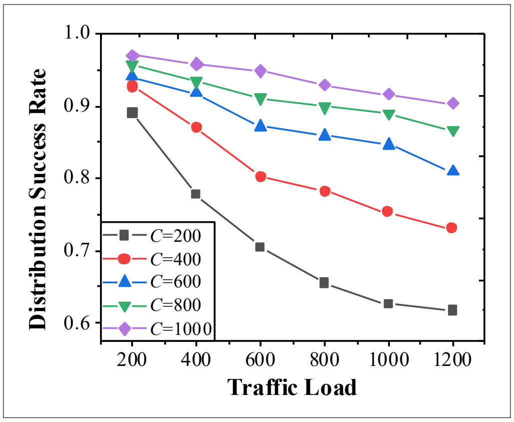

FIGURE 4. Influence of key pool capacity on the success rate of business distribution.

In the fixed encryption scheme, the data collected by each IoT device is aggregated at the router end. Besides, the QKD network encrypts the aggregated data to ensure the security of data transmission in the public network. Finally, the decryption operation is completed at the data aggregation layer using the symmetric key in the QKD network. In the second mobile encryption scheme, the QKD network provides different Quantum keys to separate encryption of the data collected by each IoT device. After that, the router completes the data aggregation and transmits it to the aggregation layer through the public network. Finally, like the fixed encryption scheme, the symmetric key in the QKD network is used to complete the decryption operation at the data aggregation layer.

Regarding the data properties of quantum channels, QKD transmits the secret key, while teleportation transmits the collapsed quantum state. As far as key readout is concerned, QKD uses single-photon measurements. This scheme amplifies a single photoelectron signal excited by a single photon, identifies and extracts extremely weak photoelectron signals through techniques such as pulse discrimination and digital counting, and achieves the ultra-sensitive limit of photodetection. Dissimilarly, teleportation communication takes Belkey measurements. Two quantum bits are measured based on four Bell States. First, the two quantum bits are converted into the Bell State. Then, the measurements are made on a 0 and 1 basis. In terms of the way of information transmission and the amount of data carried, both Quantum key and teleportation communication require additional classical communication and transmit 1-bit information via 1-bit data.

Results and Discussion

Performance Evaluation of Adaptive Key Residue Algorithm for the Quantum DTs Network

In this experiment, the value of the total key generation rate V provided by the optical line terminal is set to 2, and the number of keys required by each service is set to 10. The value of C ranges from 200 to 1,000 and increases by 200 each time. Figure 4 illustrates the effect of the key pool capacity on the business success rate. It can be seen that as the network load increases, the success rate of service distribution decreases. When the service load reaches 1,000, the algorithm can still ensure that the success rate of service distribution in the network is higher than 0.6. Under the same load, the success rate of service distribution grows with the increase in the key pool capacity *C*. But when the capacity increases over 800, the rise of the success rate of service distribution begins to decrease. This trend indicates that the capacity of the key pool in the quantum IoT should be reasonably increased by comprehensively considering various factors, such as the business volume in the network, to improve the business success rate.

Furthermore, the capacity C of each key pool is uniformly set to 200, and the number of keys required by each service is set to 10. The value of *V* is set to be 1 ~ 6 and incremented by one each time to explore the success rate of service distribution under different key generation rates. Figure 5 shows the effect of the key generation rate on the service success rate. The results suggest that the success rate of service distribution decreases as the network load increases. However, in the case of the same load, the success rate of service distribution increases with the growth of the total key generation rate *V* of the optical line terminal. It can be seen that the success rate of services in the network can be effectively improved by increasing the total key generation rate of the optical line terminal. However, since the number of QKD devices affects the total key generation rate to a certain extent, the cost factor should be taken into account when improving the total key generation rate.

Security Analysis of the Quantum Communication Technology

In the process of analyzing the security of quantum communication technology, if the quantum channel is secure, the generated key is considered secure. Suppose that the eavesdropper is Eve, and Eve can only access two sequences, which are the Electron Paramagnetic Resonance particle pair sequences held by Alice and Bob, respectively. During the eavesdropping process, Eve can pretend to be Bob or Charlie to receive the particle sequence sent by Alice. Moreover, Eve can also disguise himself as Alice and send the pseudo-particle sequence prepared by himself to Bob and Charlie. During this process, the three communication parties cannot immediately detect Eve's eavesdropping behavior.

Before Bob receives the S_1 sent out by Alice, Alice will hide the position of the detected particles. Therefore, in the process of eavesdropping, eavesdropper Eve cannot obtain the shared key and its hash function, so he cannot obtain the verification codes of Alice and Bob. Eve can only eavesdrop by intercepting S_1. Firstly, Z-base measurement is carried out on S_1, and then the corresponding pseudo sequence S_1' is prepared according to the measurement results.

Assume that the result obtained by Eve after measuring S_1 is 1. Since S_2 exists on Alice's side, even if S_1 is intercepted by Eve, Eve still has 50 percent of the particle states indistinguishable. After Eve transmits the prepared pseudo-particles to Bob, Bob uses h{K} to measure the h{K} pseudo-particle sequence. If the h{K} corresponding to a particle is 1, Bob will measure the pseudo particle with the Z-base sequence; if the h{K} corresponding to the particle is 0, Bob will use the X-base to measure the pseudo-sequence of the particle, and the result is inconsistent with Alice. Therefore, if the eavesdropper Eve takes this kind of attack, the success rate is 25 percent. Let the total number of detected sample particles be S, then the probability of Eve being found is 1 – (25 %)^{S}.

The security analysis of the quantum communication scheme reported here primarily evaluates the probability of being eavesdropped on but not found. In this scheme, Alice transmits 1 bit, and the average probability that Bob receives it correctly is 75 percent. Similarly, if Alice transmits an N bit of data to Bob, the probability that Bob receives it is 0.75N, showing that the scheme's security is reliable.

Conclusion

This study discusses the security issues of IIoT communication based on DTs. Considering that quantum secure communication covers the key content of QKD, this study innovatively introduces the content of quantum communication to solve security problems of network communication. Firstly, a two-particle quantum teleportation scheme is constructed using the five-particle entanglement states and the two-particle Bell states as entanglement channels. If Alice sends an N bit of data to Bob, the probability that Bob receives it is 0.75N, indicating that the scheme is safe and reliable. Besides, a quantum adaptive key residual scheme is proposed. The key utilization rate of each key pool in the network is calculated when a business arrives in the quantum IoT. Then, the sum of the key utilization of each OLTs-QKP and COLT-QKP is calculated. The experiments in this article confirm that the Adaptive Key Residue algorithm balances the key utilization of all key pools in the network. The research content reported here is of great significance for maintaining secure communication in the IIoT. However, since this study does not consider the influence of the computing power of the IoT device on the success rate of business distribution, there are still some limitations. Follow-up research will optimize this problem.

References

[1] C. Urrea and D. Benítez, "Software-Defined Networking Solutions, Architecture and Controllers for the Industrial Internet of Things: A Review," *Sensors*, 2021, vol. 21, no. 19, p. 6,585.

[2] M. Browne, "Artificial Intelligence Data-Driven Internet of Things Systems, Real-Time Process Monitoring, and Sustainable Industrial Value Creation in Smart Networked Factories," *J. Self-Governance and Management Economics*, 2021, vol. 9, no. 2, pp. 21–31.

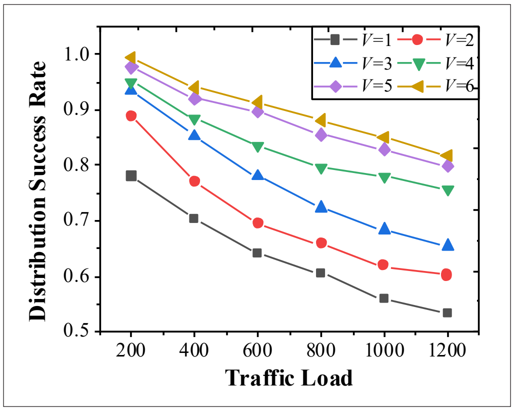

FIGURE 5. Influence of key generation rate on the service distribution success rate.

[3] Z. Zhou *et al.*, "Secure and Latency-Aware Digital Twin Assisted Resource Scheduling for 5G Edge Computing-Empowered Distribution Grids," *IEEE Trans. Industrial Informatics*, 2021, vol. 18, no. 7, pp. 4933–43.

[4] C. Stergiou *et al.*, "Secure Integration of IoT and Cloud Computing," *Future Generation Computer Systems*, 2018, vol. 78, pp. 964–75.

[5] R. Ranjith, S. Piramasubramanian, and M. G. Madhan, "Effect of Number of Quantum Wells on Modulation and Distortion Characteristics of Transistor Laser," *Optics & Laser Technology*, 2022, vol. 147, p. 107,655.

[6] Z. H. Yan *et al.*, "Generation of Non-Classical States of Light and Their Application in Deterministic Quantum Teleportation," *Fundamental Research*, 2021, vol. 1, no. 1, pp. 43–49.

[7] Z. H. Lv *et al.*, "Secure Deep Learning in Defense in Deep-Learning-As-a-Service Computing Systems in Digital Twins," *IEEE Trans. Computers*, 2021, vol. 17, no. 5, p. 1,714.

[8] T. Y. Pang *et al.*, "Developing a Digital Twin and Digital Thread Framework for an 'Industry 4.0' Shipyard," *Applied Sciences*, 2021, vol. 11, no. 3, p. 1,097.

[9] C. Stergiou *et al.*, "Security, Privacy & Efficiency of Sustainable Cloud Computing for Big Data & IoT," *Sustainable Computing: Informatics and Systems*, 2018, vol. 19, pp. 174–84.

[10] C. L. Stergiou, K. E. Psannis, and B. B. Gupta, "IoT-Based Big Data Secure Management in the Fog Over a 6G Wireless Network," *IEEE Internet of Things J.*, 2020, vol. 8, no. 7, pp. 5164–71.

[11] C. Liu *et al.*, "Multicarrier Multiplexing Continuous-Variable Quantum Key Distribution at Terahertz Bands Under Indoor Environment and in Inter-Satellite Links Communication," *IEEE Photonics J.*, 2021, vol. 13, no. 4, pp. 1–13.

[12] J. Ahn *et al.*, "Toward Quantum Secured Distributed Energy Resources: Adoption of Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD)," *Energies*, 2022, vol. 15, no. 3, p. 714.

[13] M. H. Adnan, Z. Ahmad Zukarnain, and N. Z. Harun, "Quantum Key Distribution for 5G Networks: A Review, State of Art and Future Directions," *Future Internet*, 2022, vol. 14, no. 3, p. 73.

[14] H. Weng *et al.*, "A Quantum Chaotic Image Cryptosystem and Its Application in IoT Secure Communication," *IEEE Access*, 2021, vol. 9, pp. 20481–92.

[15] H. Yi. "A post-Quantum Secure Communication System for Cloud Manufacturing Safety," *J. Intelligent Manufacturing*, 2021, vol. 32, no. 3, pp. 679–88.

Biographies

Author biographies were not available at press time.