International Journal for Housing Science and Its Applications
Publish August 10, 2025. Volume 46, Issue 4 Pages 192-205

https://doi.org/10.70517/ijhsa46415

Research on Network Security Barrier Construction of Quantum Encryption Technology Enhanced Software Development Security Detection Tool for Power Industry

Hushuang Zeng[1], Songjun Liang[1] and Heng Xia[1,*]
[1] Digital Operation Center, Guangxi Power Grid Co., LTD., Nanning, Guangxi, 530000, China
Corresponding authors: (e-mail: 18767164710@139.com).

Abstract With the growth of power demand, software development in the power industry is becoming increasingly important, but the network security problem is severe. Based on the basic principles of quantum mechanics and quantum key distribution protocol, this paper proposes a quantum key adaptive immune distribution strategy based on SDN, which is comprehensively tested and simulated to verify in the laboratory and current network environment. The experimental results show that under the condition of 15dB line loss, the key formation rate of QKD device reaches 107.014kbps, which is much higher than the standard requirement of 1kbps; in the test of overhead fiber, the cumulative loss of the quantum optical channel after adding the dispersion compensation module is only 12.02dB, which is 23.3% lower than that of the synchronous optical channel of 15.67dB. Simulation analysis shows that under the condition of service intensity of 600k and k=4, the key resource utilization of SDN-based quantum key adaptive immune distribution strategy reaches 0.536, which is about 9% higher than the classical key distribution strategy. The study shows that quantum encryption technology can effectively overcome the limitations of traditional encryption methods, provide unconditional security for software development in the power industry, with strong anti-interference ability, flexible key management and other characteristics, which can significantly improve the network security protection ability of the power system, and provide a new way of thinking for the construction of network security barriers for the security detection tools of software development in the power industry.

Index Terms quantum encryption, power industry, software development, quantum key distribution, software-defined network, security barrier

I. Introduction

With the rapid development of China's national economy, China's demand for electricity has become more and more urgent [1], [2]. Especially in recent years, China's annual power shortage has been expanding year by year, which has seriously restricted the development of various industries and even affected the normal use of electricity by residents [3]-[5]. Power industry software development, which can easily realize the visualization, interactivity and dynamics of the power system, etc., to meet the user's demand for power system software, can solve the above problems [6]-[8]. However, in the process of software development, network security is a very important consideration, so the use of encryption technology to augment the software development is essential [9], [10].

With the development of information technology, there is an increasing need for a reliable and secure communication system to protect information from being stolen or tampered with, and it is in this context that quantum encryption technology has emerged [11]-[13]. The advantages of this encryption method are different from traditional encryption. First of all, traditional encryption methods are based on mathematical puzzles that may be cracked by computers in the future [14]. Whereas quantum encryption relies on the theory of quantum mechanics and it cannot be cracked even with more advanced computers in the future [15], [16]. Secondly, quantum cryptography does not need to trust any intermediary because the intermediary will not know the content of the encryption [17], [18]. As an emerging encryption means, quantum encryption technology has the advantages that traditional encryption technology can not be compared with, and it has obvious advantages in terms of security enhancement of software development in the electric power industry and strong anti-interference ability [19]-[22].

With the rapid development of China's national economy, China's demand for electricity is becoming more and more urgent. Especially in recent years, China's annual power shortfall has been expanding year by year, which has seriously constrained the development of various industries and even affected the normal use of electricity by residents. Software development in the power industry can easily realize the visualization, interactivity and dynamics

of the power system, etc., to meet the needs of users for power system software, which can effectively solve the above problems. However, network security is a very important consideration in the software development process, so the use of encryption technology for software development has become a necessary choice. The development of information technology has led to the need for reliable and secure communication systems to protect information from being stolen or tampered with, and it is in this context that quantum encryption technology has emerged. Traditional encryption methods are based on mathematical puzzles, and there is a risk of being cracked by advanced computers; while quantum encryption technology relies on the theory of quantum mechanics, which is difficult to crack even if more powerful computers appear in the future. Quantum encryption does not require trusting an intermediary, as the intermediary cannot be informed of the encrypted content, a feature that provides an additional safeguard for information confidentiality. As an emerging means of encryption, quantum encryption technology has significant advantages in enhancing the security of software development in the power industry and strengthening the anti-interference ability. Quantum communication technology utilizes the superposition and entanglement of quantum states as the information transmission carrier, compared with traditional bits, quantum bits have higher information capacity, and their information transmission process is non-falsifiable and non-stealable. When applied to electric power information system, quantum communication technology can realize secure key distribution and encrypted communication, ensure the authenticity and integrity of information transmission through quantum authentication technology, effectively deal with electromagnetic interference and other problems, and realize long-distance safe transmission.

Based on the basic principles of quantum mechanics and quantum key distribution protocol, this study explores how quantum cryptography enhances the security of software development in the power industry. Firstly, in-depth analysis of quantum cryptography fundamentals and application scenarios of quantum communication technology in power system is conducted; secondly, quantum SDN structure based on distributed controller and quantum key adaptive immune distribution strategy based on SDN are proposed; then, the performance of QKD devices under various conditions is verified by laboratory and present network environment tests; finally, 14 nodes with actual physical distance and 21 Finally, the NSFNET topology with 14 nodes and 21 QKD links with actual physical distance is simulated to evaluate the service bearing success rate and quantum key resource utilization of the proposed strategy, and compared and analyzed with the classical key distribution strategy. The results of the study will provide theoretical basis and practical guidance for the construction of network security barriers for software development security detection tools in the power industry, which will help promote the innovative application and large-scale deployment of quantum cryptography in the power industry.

II. Quantum encryption-based software security protection strategy proposed

II. A. Fundamentals of Quantum Cryptography

II. A. 1) Fundamentals of Quantum Mechanics

The concept of uncertainty in particles: suppose that there exists a quantum system which has many quanta in a similar state $|\psi\rangle$, and a measurement is made of a mechanical quantity C in one part of this system. Then measurements are made on the mechanical quantity D of another part of this system, and C and D have the following relationship:

$$\Delta C \cdot \Delta D \geq \frac{\left|\langle\psi|[C,D]|\psi\rangle\right|}{2} \tag{1}$$

Here, the standard deviations of the measurements that can be obtained from the above equation are denoted by C and D. The relation between C and D is also $[C,D]=CD-DC$. Assuming that the mean value of the mechanical quantity M is labeled by $\langle M\rangle$, the standard deviation of M is:

$$\Delta M = \sqrt{\langle M^2 - \langle M\rangle^2\rangle} \tag{2}$$

A corollary of the uncertainty formula is that if $[C,D]\neq 0$, then $\Delta C \cdot \Delta D > 0$. For example, if the state of the system is $|0\rangle$, and its mechanical quantities $X(\sigma_x)$ and $Y(\sigma_y)$ are measured, since $[X,Y]=2iZ$, the following relations are available according to the uncertainty principle:

$$\Delta(X)\cdot\Delta Y \geq \langle 0|Z|0\rangle = 1 \tag{3}$$

From the above equation we get that both $\Delta(X)$ and $\Delta(Y)$ are strictly large 0.

The process of not being able to realize a complete copy of any quantum without knowing the quantum state is called the quantum unclonability principle. The proof process uses the principle of superposition of quantum states.

Proof: Suppose that there exists an unknown quantum state $|\psi\rangle$, where a physical process in which a full copy of it can be accomplished can be expressed as $U=(|\psi\rangle|0\rangle)=|\psi\rangle|\psi\rangle$. However this process has no relation to the state of the quantum itself. For any $|\phi\rangle\neq|\psi\rangle$, there is also $U=(|\phi\rangle|0\rangle)=|\phi\rangle|\phi\rangle$. Thus, $|\gamma\rangle=|\psi\rangle+|\phi\rangle$ yields the following relations, e.g.:

$$U(|\gamma\rangle\langle 0|)=U((|\psi\rangle+|\phi\rangle)|0\rangle)=|\psi\rangle|\psi\rangle+|\phi\rangle|\phi\rangle\neq|\gamma\rangle|\gamma\rangle \tag{4}$$

The above formula verifies a different result than the replication of $|\gamma\rangle$, so it can be inferred that this assumption is incorrect.

II. A. 2) Quantum Fourier Transforms

According to the concept of multi-quantum operator algebra, the time-evolving diffusion function required for quantum computation can be dispersed into a sequence of ordered products of primitive diffusion functions. And then each element of the diffusion function can be further decomposed into a single quantum bit rotation operation and a two quantum bit diagonal phase operation gate. These two fundamental quantum operation gates are realized in many two-energy quantum systems.

Next, the quantum Fourier transform algorithm is presented. The quantum Fourier transform theory QFT is defined as follows, for any positive integer x, there is always $0<x<q$, $q=2m$, and the quantum discrete Fourier transform (QDT) of an arbitrary quantum state $|x\rangle$ is:

$$QFT:|x\rangle\rightarrow\frac{1}{\sqrt{2^m}}\sum_{c=0}^{2^m-1}e^{2i\pi cx/m}|c\rangle \tag{5}$$

For example, take $a=1$ and $q=4$ then its quantum discrete Fourier transform is:

$$QFT:|01\rangle=\frac{1}{2}|00\rangle+\frac{1}{2}e^{i\frac{\pi}{2}}|01\rangle+\frac{1}{2}e^{i\pi}|01\rangle+\frac{1}{2}e^{i\frac{3\pi}{2}}|11\rangle \tag{6}$$

This transformation converts the state $|x\rangle$ into a state of equal probability amplitude, where the amplitudes of the phase angles are equal and the phase angles vary according to the law $\frac{2\pi xc}{q}$. However, in a linear iterated state with equal probability amplitudes, each iterated term has the same phase angle. Therefore, based on the construction of linear iterative states with equal probability amplitudes, the quantum discrete Fourier transform should incorporate the proper phase. The fundamental transform of the quantum discrete Fourier transform is actually composed according to two types of quantum transforms. The first type of quantum transform is the single quantum bit rotation transform (W-H transform), which is represented by this matrix as:

$$H=\frac{i}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \tag{7}$$

The change of rotationally controlled phase quantum bit bits is the second transformation of quantum transformations, the two quantum bits j,k of the controlled phase rotational transformation of two quantum bits j,k can be represented by a matrix as:

$$S_{j,k}=\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & e^{i\theta_{k-j}}\end{pmatrix} \tag{8}$$

The marking of the control bit is denoted by k and the marking of the manipulation bit is denoted by j, and the angle of phase change in the middle of the control bit k and the manipulation bit j is controlled by $k>j$, and $\theta_{j-k}=\pi/2^{k-j}$, so that the QFT transformations can be performed by the following links:

$$H_0S_{01}S_{02}\Lambda S_{0(m-1)}H_1S_{12}S_{13}\Lambda S_{1(m-1)}\cdots H_{m-2}S_{(m-1)(m-2)}H_{m-1}H_m|x\rangle \tag{9}$$

II. A. 3) Unconditional Security in Quantum Cryptography

In this section, the security of two quantum key distribution is fully described, and the two essentially independent key distribution protocols are shown to be equivalent after undergoing a series of classical and quantum transformations, a process that completely and clearly verifies the unconditional security of quantum cryptography.

First, some preparations are made for the similarity between the two quantum states which is described by the concept of fidelity.

Definition: assume that the two quantum states are ρ and σ, and the fidelity between ρ and σ is:

$$F(\langle\varphi|,\rho)=tr\sqrt{\rho^{\frac{1}{2}}\sigma\rho^{\frac{1}{2}}} \tag{10}$$

It is clear that when $\rho=\sigma$, $F(\rho,\sigma)=1$ and the closer the two quantum states are, the closer the fidelity is to 1. For example, the fidelity between a pure state $|\phi\rangle$ and an arbitrary state ρ is:

$$F(\langle\varphi|,\rho)=tr\sqrt{\langle\varphi|\rho|\varphi\rangle|\varphi\times\varphi|}=\sqrt{\langle\varphi|\rho|\varphi\rangle} \tag{11}$$

Quantum entanglement purification, a most basic quantum key distribution protocol. The quantum secrecy enhancement is shown in Figure 1. Where $U_A=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & i\\ -i & 1\end{bmatrix}$ and $U_B=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & i\\ i & 1\end{bmatrix}$.

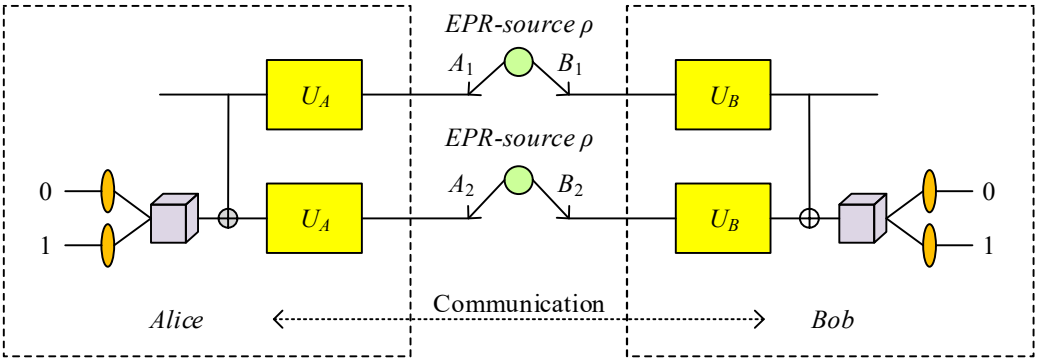

Figure 1: Quantum secrecy enhancement

From the above figure, it can be obtained that two EPR resources are assumed to produce the same $|\Phi^+\rangle=(|00\rangle+|11\rangle)/\sqrt{2}$ entangled state of the quantum, i.e., $A_1B_1=A_2B_2=|\Phi^+\rangle$, however, since the quantum state transmitted through the channel is affected by noise effects changed, so the fidelity of ρ vs. $|\Phi^+\rangle$ is:

$$F\left(\left|\Phi^+\right\rangle,\rho\right)=\sqrt{\left\langle\Phi^+\left|\rho\right|\Phi^+\right\rangle}\le 1 \tag{12}$$

The channel requirement here is to satisfy $F(|\Phi^+\rangle,\rho)>0.5$. The sender and receiver are trying to send through their respective quantum bits A_1,A_2 and local operations B_1,B_2 in order to obtain a state with fidelity 1 with $\left|\Phi^+\right\rangle$. Quantum security enhancement can accomplish such a task. As can be seen from Fig. 1, the sender first performs the U_A transformation of A_1,A_2, and the receiver then does the inverse of the B_1,B_2 change U_B for B_1,B_2. And then A_1,A_2 and A_1,A_2 are fed into the quantum heterodyne gate:

$$U_{C-NOT}=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix} \tag{13}$$

Then measure $|0\rangle,|1\rangle$ of the outputs A_2 and B_2 and get the final measurement. Assuming the results are the same, the sender and receiver will leave A_1 and B_1 and ignore A_2 and B_2. And then, the same operation will be done on ρ as the same input.

II. B.Quantum communication technology and its role in power systems

Quantum communication technology is a means of information transmission based on the principle of quantum mechanics, which has unique advantages [23], [24].

Firstly, quantum communication technology uses the superposition and entanglement of quantum states as the transmission carrier of information, and compared with the traditional classical bits, quantum bits have higher information capacity. Secondly, the information transmission process of quantum communication technology is unforgeable, and once stolen, it will be destroyed immediately. Finally, the information transmission process of quantum communication technology is not stealable. Because the transmitted information is delivered through measurement, the original information cannot be recovered once it is stolen. In the electric power information system, quantum communication technology can be applied to both confidential transmission and authentication. For confidential transmission, quantum communication technology can realize secure key distribution and encrypted communication. Through technologies such as quantum random number generator and quantum error correction code, safe and reliable keys can be distributed, and through technologies such as quantum invisible state transmission and quantum remote sensing, safe information transmission can be realized. For authentication, quantum communication technology can ensure the authenticity and integrity of information transmission through quantum authentication technology.

Quantum communication technology can provide a higher level of confidential transmission to ensure that power information is not stolen or eavesdropped during transmission. Due to the nature of the quantum state, eavesdropping by any third party during transmission will result in interference of the quantum state, which can be detected by both sides of the communication. Quantum communication technology can be combined with quantum authentication methods to ensure the integrity of the identity and data of the communicating parties in the power information system. By utilizing the special properties of quantum states and the interfering nature of quantum measurements, quantum authentication can prevent potential attacks and data tampering. Power information systems usually face various sources of interference, such as electromagnetic interference and signal attenuation. Quantum communication technology, with its strong anti-interference capability, can better cope with these interference sources and ensure the reliable transmission of power information. Power information system usually involves a wide range of transmission, and traditional communication methods may be limited by signal attenuation. Quantum communication technology can realize secure transmission over long distances and overcome the limitations of traditional communication methods.

II. C.Quantum Secure Communication Network Fundamentals

Quantum mechanics lays the foundation for mankind's understanding and transformation of nature, and its development and breakthroughs are the triggers and catalysts for waves of quantum technological revolutions. The first wave led to technologies such as semiconductors, lasers and atomic energy. The second wave brought about cutting-edge technologies such as quantum communication, quantum computing and quantum measurement. The essence of quantum secure communication technology is to accomplish quantum key distribution for data services, and its key distribution principle is shown in Figure 2. Among them, quantum key distribution mainly includes quantum channel, classical channel and business channel. The quantum channel is the channel for transmitting single photons between Alice and Bob, following the BB84 protocol, and each single photon is encoded according to certain rules. The classical channel, on the other hand, is the channel where Alice and Bob transmit quantum key negotiation information, generate quantum keys, and provide encryption services for the business system. The business channel is the channel for the business system to transmit business data, which is mainly realized by the quantum VPN gateway to establish IPsec tunnels to protect all kinds of power business data and prevent information theft.

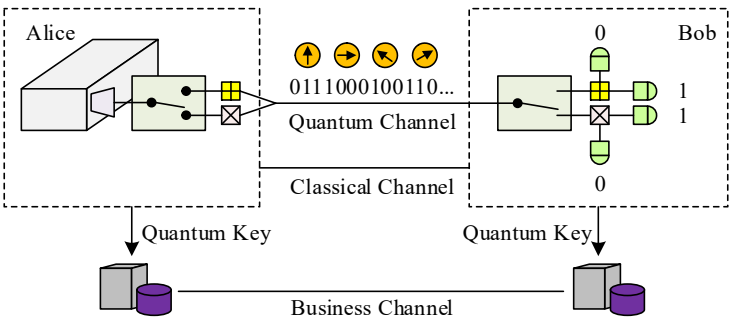

Figure 2: Quantum key distribution principle

II. D.Quantum Authentication and Key Distribution Strategies

II. D. 1) Software Defined Networking Foundation

Software Defined Networking (SDN) is not a specific form of network, but a different design idea from traditional networks [25], [26]. The main idea is to collect all the control functions of the forwarding devices in the network and manage them in a unified way by a single controller module.

SDN network architecture has four main features:

Digital and control separation: network forwarding devices nowadays only have data forwarding functions, and the control plane functions are transferred to the SDN controller for unified management in the form of issuing flow table entries.

Centralized control: The SDN controller can directly obtain information about the network as a whole through the interface with the equipment and plan accordingly.

Open interfaces: When new services are launched, it is no longer necessary to fully upgrade physical network equipment, but only need to be realized in the programming interfaces reserved for external applications at the application layer.

Programmable network: Network functions can be programmed by external applications.

Each of the three layers of the SDN architecture is responsible for the realization of different network functions, which are described in detail below:

(1) Forwarding plane

The forwarding plane is mainly composed of general-purpose network equipment, which only has basic data forwarding functions, so that networks deployed by different operators can use unified equipment, which facilitates the maintenance and update of network equipment. The control plane functions are transferred to the control plane uniformly through softwareization for centralized control and management. Currently, OpenFlow switches are widely used in SDN networks.

(2) Control plane

The control plane mainly includes the SDN controller and the management functions of the controller, responsible for the management and control tasks within the SDN architecture. This includes the acquisition and analysis of network configuration information, management and allocation of network resources, scheduling and processing of network traffic, as well as routing and rerouting planning during communication processes. The control plane transmits control information by issuing flow table entries, which require support for the OpenFlow protocol from the underlying devices. Since the control plane has many functions and undertakes critical tasks, it generally needs to run on a well-performing processor, which can be arranged centrally or shared by multiple processors. The control plane is also a bridge connecting the data forwarding plane and the application plane. The north direction obtains the application programming information, and the south direction sends out the management and control parameters through the flow table entries, thus controlling the overall operation of the network.

(3) Application Layer Plane

The application plane is mainly to provide interfaces for external applications, which allows users to program and implement the featured applications and interact with the control plane to realize the applications. Typical applications include OSS, Openstack, and so on.

II. D. 2) Quantum Software-Defined Networking Models

IPsec protocol-based extensions to the OpenFlow protocol to enforce a southbound secure channel for SDN networks. In this paper, we propose a software-defined network model based on quantum key distribution protocol, hereafter referred to as QSDN.

II. D. 3) Distributed Controller Based Quantum SDN Architecture

The QSDN structure is assumed to be divided into two layers. The first layer is m controllers, each of which shares N EPR pairs with each other respectively, and each of which governs $n(n \geq m)$ network nodes, and each of which shares N EPR pairs with each of the nodes it governs respectively. Each node in the network owns shared information S between them, and S contains several strings of shared information, only one of which is used in each key distribution process, and which string of shared information is used is negotiated and sent down through the controllers, which divide each S into two segments, S_1 and S_2, equally in advance before sending it down.

II. D. 4) SDN-based quantum key adaptive immune distribution strategy

(1) Adaptive immunization eavesdropping strategy

The eavesdropping immunization phase requires the use of shared information between nodes S. The controller segments the negotiated shared information and sends it down to B_{11} and B_{ii} respectively. B_{11} and B_{ii} perform the same processing on S_1, S_2 respectively with the pre-agreed method as follows.

Step1: Extend S_1, S_2 with a one-shot function F to obtain a sufficiently long S_1', S_2', denoting the different parameters of the non-orthogonal state particles to be interspersed, respectively.

Step2: Group S_1', S_2' as $S_{1'} = (S_{11}, S_{12}, \cdots, S_{1p}, B, V)$, where $S_{11}, S_{12}, \cdots, S_{1p}$ are of length K, and their values denote the interpolation Position. The length of B and V is p (i.e., the number of non-orthogonal state particles is p), which denote the measured bases and values of non-orthogonal state particles, respectively. The size of p is adaptively adjusted by the SDN controller according to the strength of the eavesdropping attack, so as to realize adaptive immunity to eavesdropping attacks, and different attack strengths correspond to different sizes of p values.

Step3: Node B_{11} generates a string of non-orthogonal state particles similar to the BB84 protocol, with B as the base and V as the value. 0 in B denotes the $\{|0\rangle, |1\rangle\}$ base and 1 denotes the $\{|+\rangle, |-\rangle\}$ base. In $\{|0\rangle, |1\rangle\}$ base, 0 means $|0\rangle$-state and 1 means $|1\rangle$-state. 0 in $\{|+\rangle, |-\rangle\}$ base means $|+\rangle$ state, 1 means $|-\rangle$ state.

Step4: B_{11} sends L_2 to B_{ii} (ignoring the quantum loss incurred during transmission).

Step5: B_{ii} measures the received L_2, based on the S_2' obtained from its own processing with the corresponding basis for the corresponding interspersed bits (non-orthogonal particles) in L_2. If the error rate is below a certain threshold, the next step is continued, otherwise eavesdropping is considered to exist. The setting of the threshold has an important impact on the eavesdropping detection results; if the threshold is too high, it leads to an increase in the leakage rate, which reduces the security of the network. If the threshold is too low, the false alarm rate of the system will increase, which will greatly reduce the success rate of communication. Therefore it is very important to set the threshold value reasonably. Let the bit error rate of quantum channel be ℓ_{QBER}, when the system adopts L EPR states for eavesdropping detection, the eavesdropping detection threshold N of the system should be satisfied:

$$N \le L(2\ell_{QBER} - \ell_{QBER}^2) \tag{14}$$

(2) Security and key distribution efficiency analysis of adaptive immune eavesdropping

Assume that the attacker Eve entangles the additional particle into the EPR pair used by B_{11} and B_{ii}, and obtains the measurement information about B_{ii} by measuring the additional particle. Assuming that the EPR pair that is exchanged by B_{11} and B_{ii} doing entanglement is $|\phi_{ab}^{+}\rangle$, particle a and particle b belong to B_{11} and B_{ii}, respectively.Due to Eve's intervention, the EPR pair in the channel is entangled with Eve's additional particles, and $|\phi_{ab}^{+}\rangle$ into a composite state $|\varphi_{abe}\rangle$. According to the principle of maximal information accessible in quantum information theory i.e. the Holevo sector:

$$S(\rho) - \sum_i P_i S(\rho_i) = \chi(\rho) \tag{15}$$

From Eq. $S(\rho)$ is the upper bound of $\chi(\rho)$. Therefore, the amount of mutual information that B_{ii} can extract from $|\varphi_{abe}\rangle$ is limited by $\chi(\varphi_{abe})$. Obviously, the amount of information Eve can obtain about B_{ii} must satisfy less than or equal to B_{ii}, and denoting the amount of information Eve can obtain by I_{Eve}, there is:

$$I_{Eve} \le \chi(\varphi_{abe}) \tag{16}$$

Since entropy decreases with increasing fidelity, assume that the fidelity of $|\varphi_{ab}\rangle$ with $|\varphi_{abe}\rangle$ is:

$$F(|\varphi_{ab}\rangle, \varphi_{abe}) = Tr\sqrt{\langle\varphi_{ab}|\varphi_{abe}|\varphi_{ab}\rangle} \tag{17}$$

For equation (17) squared there is:

$$F(|\varphi_{ab}\rangle, \varphi_{abe})^2 = \langle\varphi_{ab}|\varphi_{abe}|\varphi_{ab}\rangle = 1 - \gamma \tag{18}$$

where $0 \le \gamma \le 1$. Therefore $S(\varphi_{abe})$ has an upper bound, and $\varphi_{abe}^{\max}$ that satisfies the upper bound is a diagonal density matrix, and its diagonal elements are $1-\gamma$, $\gamma/3$, $\gamma/3$, $\gamma/3$. Therefore, the entropy of φ_{abe} is:

$$S(\varphi_{abe}^{\max}) = -(1-\gamma)lb(1-\gamma) - 3\times\frac{1}{3}\gamma lb\frac{1}{3}\gamma \tag{19}$$

Substituting Eq. (19) into Eq. (18), we have:

$$I_{Eve} \le -(1-\gamma)lb(1-\gamma) - \gamma lb\frac{1}{3}\gamma \tag{20}$$

Since $|\phi_{ab}^{+}\rangle$ is the only correct measurement, let d be the probability that Eve introduces an error, and because of equation (18), we have $d = \gamma$. Substituting this equation into Eq. (20), we have:

$$I_{Eve} \le -(1-d)lb(1-d) - dlb\frac{1}{3}d \tag{21}$$

Efficiency is one of the most important metrics to verify that quantum key distribution protocols can be applied to large-scale networks. Quantum bit efficiency is defined as:

$$\eta_{qbit} = \frac{n_{ulti}}{n_{sum}} \tag{22}$$

where n_{ulti} is the number of quantum bits that can be used to get the key, and n_{sum} is the total number of quantum bits actually transmitted in the quantum channel. According to Eqs. (18), (21), and Eq. (22), the following model can be obtained:

$$\begin{cases} I_{Eve} \le (1-Q)^{1/\alpha\eta n_{sum}} lb(1-Q)^{1/\alpha\eta n_{sum}} \\ -[1-(1-Q)^{1/\alpha\eta n_{sum}}]lb\left[\frac{1}{3}-\frac{1}{3}(1-Q)^{1/\alpha\eta n_{sum}}\right] \\ \eta = \frac{1}{(\alpha+1)} \\ p = \alpha\eta n_{sum} \end{cases} \tag{23}$$

where p is the number of non-orthogonal state particles, Q is the probability that Eve is detected by the system, η is the key distribution efficiency, and α is the ratio of non-orthogonal state particles to the number of entangled particles.

III. Practical application of quantum key distribution strategies

III. A. Environmental Adaptability Analysis and Testing of Quantum Secure Communication for Electricity

The QKD equipment in this test of grid-specific quantum confidential communication equipment adopts phase modulation coding and adds dispersion compensation module in the transmission line to ensure stable and efficient quantum key distribution in long-distance optical fiber. The device can realize on-demand, real-time and secure distribution of keys and provide key reading interface for upper-layer applications, and is the core equipment of wide-area quantum confidential communication backbone network.

III. A. 1) Laboratory Long Range QKD System Testing

The test object of this project is to verify the hourly average key generation rate of the QKD equipment system at a given attenuation for a long-distance coiled fiber situation in the laboratory. The equipment required to realize the QKD system network management or host computer control software. The test results QKD key code rate read through the network management or host computer control software.

Test steps:

(1) Configure the tested point-to-point QKD equipment for normal operation and record the loss value of the actual quantum fiber channel.

(2) Use 50km standard single-mode fiber (corresponding to 10dB), plus 6dB adjustable optical attenuator, giving the required 15dB channel attenuation conditions.

(3) Test the SPD photon detection count value, QBER, and hourly average key code rate of the QKD device under this attenuation condition.

QKD system coding rate and transmission capability test environment:

A standard single-mode fiber (G652) is used to simulate the actual channel loss for QKD system hourly code rate testing, and the fiber tray configurations for the 2 nominal channels are shown in Table 1.

Channel 1 test: 50km fiber is connected to a grating fiber-type dispersion compensation module, which has a nominal insertion loss of 0.4dB.

Channel 2 test: 100km fiber is connected to a dispersion compensated fiber type dispersion compensation module. This dispersion compensated fiber has a length of 15km and a span loss of 6dB, as measured by OTDR.

Table 1: Two types of fiber optic disc configuration parameters for the channel

Channel number	Fiber disc configuration (km)	Nominal channel loss (dB)
Channel 1	50	10
Channel 2	100	20

For the channel with the maximum transmission loss (channel 3) corresponding to the QKD device's committed code rate (>1kbit/s), the channel loss is determined using the longest channel fiber plus an adjustable attenuator. For other channel loss points, the available fiber optic discs are used in combination with adjustable attenuators in 1dB increments.

QKD equipment key code rate read through the network management and host computer control software. The minimum time interval for key code rate statistics is 6 seconds, and the code rate statistics are calculated by dividing the code volume of all test times by the average statistics of the test times, and updated every 6 seconds.

The channel test results are shown in Table 2, and channel 3 is the 1kbps code-forming rate limit.

(1) When the actual link is 50kmSMF+DCM, the channel loss including dispersion compensation module is: (10+0.4dB)=10.4dB.

(2) When the actual link is 100kmSMF+DCM, the channel loss including dispersion compensation module is: (20+6dB)=26dB.

When the channel loss is ≤3dB, there is a phenomenon that cannot be coded. When the channel loss is 0dB, the QKD software interface shows that the coding rate is 0. This is because when the channel loss is ≤3dB, the optical power arriving at the detector at the receiving end is too large, which is close to the critical saturation count range of the detector, and the detected output is abnormal, which leads to the coding of no security key.

Finally, it is concluded that the key encoding rate is 107.014kbps under the condition of 15dB line loss (50km+6dB adjustable attenuation), 4.112kbps under the condition of 24dB line loss (100km+2dB adjustable attenuation), and no key encoding under the condition of ≤13dB line loss. The QKD equipment can meet the requirement of hourly average code rate ≥1kbps under the condition of total link attenuation ≤13dB.

Table 2: Channel test results

Channel 1 (10dB)	Code rate (kbps)	QBER (%)
Maximum value	385.214	1.423
Minimum value	264.339	0.892
Mean value	270.176	1.135
Channel 2 (20dB)	Code rate (kbps)	QBER (%)
Maximum value	13.524	4.523
Minimum value	11.336	1.208
Mean value	12.029	2.549
Channel 3 (25dB)	Code rate (kbps)	QBER (%)
Maximum value	3.859	4.669
Minimum value	2.714	1.124
Mean value	3.046	2.983

III. A. 2) Testing of long-distance QKD systems on existing networks

The test object of this project is for the overhead fiber optic line, and the main purpose is to verify whether the attenuation of the fiber optic line is reduced after adding dispersion compensation module in the long distance transmission line. The equipment required for the experiment is OTDR tester, portable light source and optical power meter. This OTDR test should be conducted without the access of QKD equipment.

Test steps:

(1) Remove the QKD equipment connection from the fiber line under test.

(2) Test the fiber line length and line loss using the OTDR.

(3) Using a portable light source and optical power meter, measure end-to-end loss.

Test Results:

The test overhead fiber is a 1000kv extra high voltage fiber optic line. Use OTDR to test fiber length, light source and optical power meter to test end-to-end loss. The overhead fiber length and loss test results are shown in Table 3.

In comparison, the cumulative loss of the quantum optical channel is smaller. It can be seen that its line loss can be reduced by adding dispersion compensation module in the fiber.

Table 3: Overhead fiber length and loss test results

	Overhead fiber length (km)	Overhead optical fiber loss (dB)
Quantum optical channel	65.23	12.02
Synchronous optical channel	67.50	15.67

The quantum optical channel OTDR test results are shown in Figure 3. No. 19, location 65km, loss is -0.124dB and cumulative loss is 11.25dB.

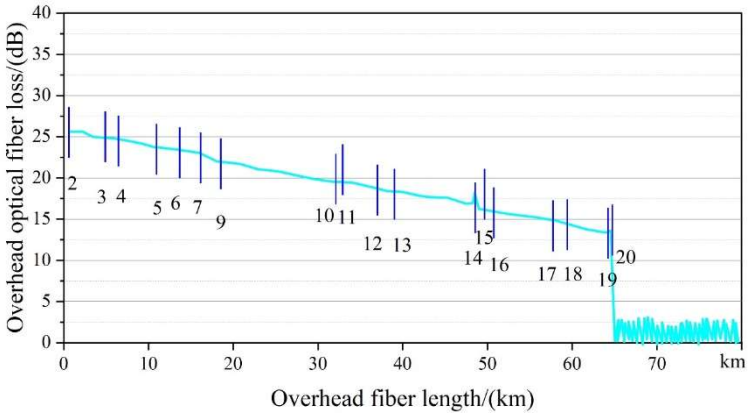

Figure 3: Quantum optical channel OTDR test results

The synchronous optical channel OTDR test results are shown in Figure 4. No. 14, the position is at 50km, the loss is 0.294dB and the cumulative loss is 12.08dB. No. 15, the position is at 67.5km, the cumulative loss is 15.67dB.

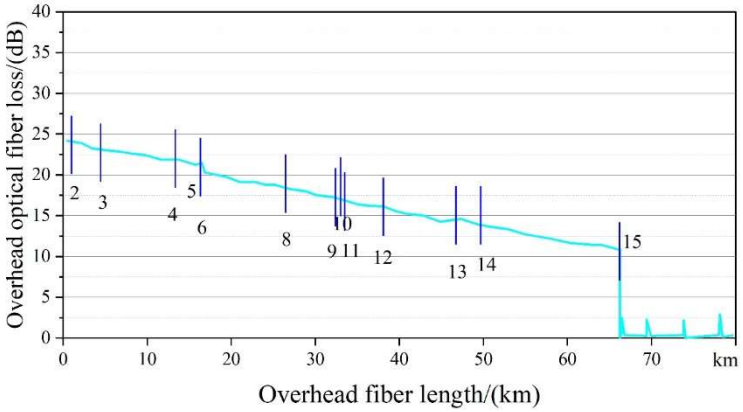

Figure 4: Synchronous optical channel OTDR test results

III. B. Quantum Key Distribution Strategy Simulation and Result Analysis

In order to evaluate the performance of the SDN-based quantum key adaptive immune distribution strategy proposed in this paper, the NSFNET topology with 14 nodes and 21 QKD links with actual physical distances is used for simulation in this chapter.

III. B. 1) Analysis of the success rate of service bearers

The service bearing success rate is shown in Fig. 5. The figure reflects the service bearing performance of the SDN-based quantum key adaptive immune distribution strategy in the face of encrypted service requests with the same service strength.

The independent variables in the figure are the number of optional quantum key distribution paths $K = 2/3/4$ and the encryption service strength, which starts from 300 κ and increases by 50 κ until 600 κ.

The dependent variable is the different quantum encryption service bearing success rate SP exhibited by the quantum key adaptive immunity distribution strategy under different conditions when facing the same encryption service. The results of which classical key distribution strategy can be used as a control group for the SDN-based quantum key adaptive immune distribution strategy proposed in this paper.

The figure reflects the trend of constructing different service bearing success rates of two quantum key distribution strategies in the quantum key distribution network when $T_{\kappa} = 100u$ (which means that the security requirements of quantum encryption services are more general in this scenario) when facing encrypted service requests of the same service strength.

When setting $T_{\kappa} = 100u$ (which means that in this scenario, the security requirements of quantum encryption services are higher and the available time threshold of quantum keys is smaller) to observe the service bearing success rate, keeping K constant, the service bearing success rate of the SDN-based quantum key adaptive immune distribution strategy slowly decreases with the increase of the service intensity.

Meanwhile keeping the service intensity constant, the SP of SDN-based quantum key adaptive immune distribution strategy will increase significantly with the increase of K, and both perform better than the results of classical key distribution. It is clear that increasing the number of optional key resource distribution paths can lead to a significant improvement in the performance of all quantum key strategies.

Even when $K = 4$ and $T_{\kappa} = 600\kappa$, the improvement of SDN-based quantum key adaptive immune distribution strategy over the original one is about 9%.

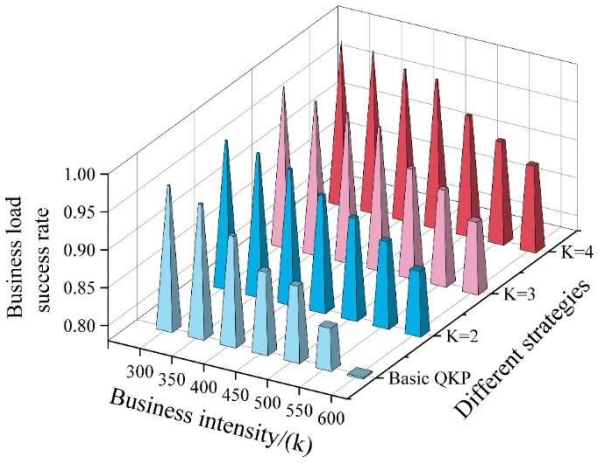

Figure 5: Business load success rate

III. B. 2) Quantum Key Resource Utilization Analysis

The key resource utilization is shown in Fig. 6. The results of which classical key distribution strategy can be used as a control group for the SDN-based quantum key adaptive immune distribution strategy proposed in this paper.

The trend of the different key resource utilization of the two virtual quantum key distribution strategies in the quantum key distribution network is constructed when $T_{\kappa} = 50u$ in the face of encrypted service requests with the same service strength.

The SDN-based quantum key adaptive immune distribution strategy has a key resource utilization rate of 0.536 when k=4 and the service intensity is 600k.

Setting $T_{\kappa} = 50u$ for observing KRU and keeping K constant, the SDN-based quantum key adaptive immune distribution strategy maintains a stable key resource utilization rate after a steady rise as the intensity of the service increases. Meanwhile, keeping the service intensity unchanged, the KRU of SDN-based quantum key adaptive immune distribution strategy will increase with the increase of K, which indicates that by increasing the number of

optional quantum key distribution paths, the KRU of SDN-based quantum key adaptive immune distribution strategy will be significantly improved.

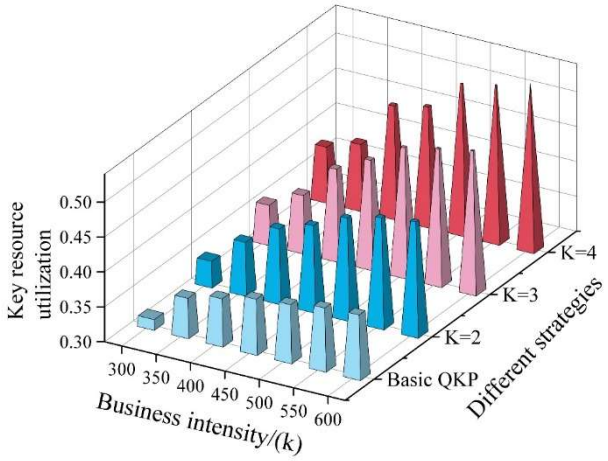

Figure 6: Key resource utilization

When $T_{\kappa} = 30u$, the quantum key resource utilization is shown in Fig. 7.

When observing the success rate of service bearing in the figure, it is not difficult to find that, keeping K unchanged, the KRU of SDN-based quantum key adaptive immune distribution strategy first rises slightly and then drops rapidly and substantially, much earlier and larger than the drop when $T_{\kappa} = 50u$.

The difference is that at this time the quantum key security requirements are extremely high, and thus the downward trend of KRU is more obvious and rapid.

As can be seen from the figure, when the service intensity is not very high, keeping the service intensity unchanged, the KRU of SDN-based quantum key adaptive immune distribution strategy will increase with the increase of K, which obviously increases the number of optional quantum key distribution paths, and has a good effect on the improvement of the KRU of SDN-based quantum key adaptive immune distribution strategy.

In summary, the simulation results show that regardless of the available time threshold of quantum key resources, the SDN-based quantum key adaptive immune distribution strategy is slightly better than the KRU of the classical key distribution strategy, and the advantage becomes more obvious with the increase of the value of K and the increase of the intensity of the service.

When the quantum key availability time threshold is narrowed (i.e., increasing the security requirements for the quantum key), all the above mentioned advantages are further amplified. Therefore, this paper proposes that the SDN-based quantum key adaptive immune distribution strategy can indeed not only better utilize the service bearing performance of quantum key distribution network, but also maintain a better utilization of key resources compared with the classical key pool.

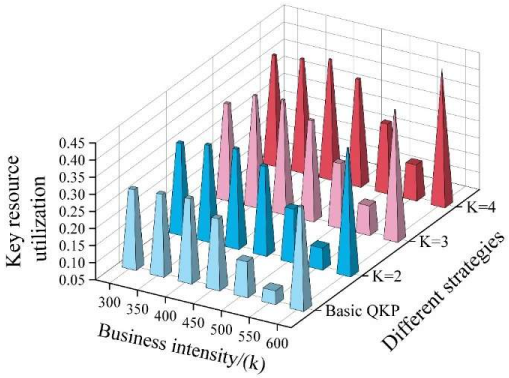

Figure 7: When $T_{\kappa} = 30u$, quantum key resource utilization

IV. Conclusion

This paper discusses the application of quantum cryptography in software development security detection tools in the power industry, and constructs a quantum key adaptive immune distribution strategy based on SDN. The study comprehensively evaluates the performance and practicality of the strategy through theoretical analysis, experimental testing and simulation verification. Laboratory tests show that in a 50km fiber-optic plus DCM link (channel loss of 10.4dB), the average key formation rate reaches 270.176kbps, and the QBER value is kept at a low level of 1.135%. In the present network test, on a 65.23km long overhead fiber-optic line, the cumulative loss of the quantum optical channel is only 12.02dB, which is lower than that of the synchronous optical channel by 3.65 dB. Simulation results show that when the number of optional paths for quantum key distribution is k=4 and τ=1, the SDN-based quantum key adaptive immune distribution strategy improves the service bearing success rate by about 9% compared with the classical strategy; when τ=0.5, the gap between the two strategies in terms of the success rate of the service bearing expands from 5% to 13% as the service intensity increases from 300 to 600.

This study proves that quantum cryptography can effectively overcome the limitations of traditional encryption and provide a higher level of security for software development in the electric power industry, featuring unconditional security, strong anti-jamming ability, and flexible key management. Future research will further optimize the quantum key distribution protocol, explore the application in more complex network environments, and study the integration with blockchain and other technologies to provide all-round protection for information security in the power industry.

References

[1] He, Y., Wang, M., Guang, F., & Zhao, W. (2020). Research on the method of electricity demand analysis and forecasting: The case of China. Electric Power Systems Research, 187, 106408.

[2] Lin, B., & Zhu, J. (2020). Chinese electricity demand and electricity consumption efficiency: Do the structural changes matter?. Applied Energy, 262, 114505.

[3] Lin, J., Zhu, K., Liu, Z., Lieu, J., & Tan, X. (2019). Study on a simple model to forecast the electricity demand under China's new normal situation. Energies, 12(11), 2220.

[4] Fan, J. L., Hu, J. W., & Zhang, X. (2019). Impacts of climate change on electricity demand in China: An empirical estimation based on panel data. Energy, 170, 880-888.

[5] Baoguo, S., Xiangdong, S., Jiangtao, L., Xiang, W. A. N. G., & Ding, M. A. (2017). Analysis on the China's electricity demand growth under the new economic norm. Electric Power, 50(1), 19.

[6] Bakulina, A., Kondrateva, O., & Loktionov, O. (2020, April). Software Package Development to Improve Occupational Safety at Electric Power Industry Enterprises. In 2020 V International Conference on Information Technologies in Engineering Education (Inforino) (pp. 1-4). IEEE.

[7] Lin, L., Wang, Y., Yang, H., Shi, C., & Lu, W. (2021, October). Research and Practice of Software Development Technique for Electric Power Application. In 2021 IEEE 5th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC) (Vol. 5, pp. 1602-1607). IEEE.

[8] Georgiou, S., Rizou, S., & Spinellis, D. (2019). Software development lifecycle for energy efficiency: techniques and tools. ACM Computing Surveys (CSUR), 52(4), 1-33.

[9] McCoy, E. (2025). CYBERSECURITY REAL-WORLD APPLICATIONS FOR THE SOFTWARE DEVELOPMENT LIFE CYCLE. Land Forces Academy Review, 30(1), 148-161.

[10] Jain, S. (2024). Integrating Privacy by Design Enhancing Cyber Security Practices in Software Development. Journal Of Multidisciplinary, 4(11), 1-11.

[11] Wang, Y., & Song, X. (2020). Quantum science and quantum technology. Statistical Science, 35(1), 51-74.

[12] Harinath, D., Bandi, M., Patil, A., Murthy, M. R., & Raju, A. V. S. (2024). Enhanced Data Security and Privacy in IoT devices using Blockchain Technology and Quantum Cryptography. Journal of Systems Engineering and Electronics (ISSN NO: 1671-1793), 34(6).

[13] Ajala, O. A., Arinze, C. A., Ofodile, O. C., Okoye, C. C., & Daraojimba, A. I. (2024). Exploring and reviewing the potential of quantum computing in enhancing cybersecurity encryption methods. Magna Sci. Adv. Res. Rev, 10(1), 321-329.

[14] Kandula, S. R. (2025). BREAKING TRADITIONAL ENCRYPTION: QUANTUM COMPUTING RISKS TO WEB AND MOBILE APPLICATIONS. International Journal of Advanced Research in Engineering and Technology (IJARET) Volume, 16, 329-342.

[15] Lee, Y., Nam, T., & Yune, S. (2024). Encryption and Decryption Technology for Quantum Computing. International Journal of Business Studies and Innovation, 4(3), 8-13.

[16] Zornetta, A. (2024). Quantum-safe global encryption policy. International Journal of Law and Information Technology, 32(1), eaae020.

[17] Bruno, L., & Spano, I. (2021). Post-quantum encryption and privacy regulation: Can the law keep pace with technology?. Eur. J. Privacy L. & Tech., 72.

[18] Kuang, R., & Chan, A. (2023). Quantum encryption in phase space with displacement operators. EPJ Quantum Technology, 10(1), 26.

[19] Li, Y., Zhang, P., & Huang, R. (2019). Lightweight quantum encryption for secure transmission of power data in smart grid. IEEE Access, 7, 36285-36293.

[20] Broadbent, A., & Islam, R. (2020). Quantum encryption with certified deletion. In Theory of Cryptography: 18th International Conference, TCC 2020, Durham, NC, USA, November 16–19, 2020, Proceedings, Part III 18 (pp. 92-122). Springer International Publishing.

[21] Kaltenbaek, R., Acin, A., Bacsardi, L., Bianco, P., Bouyer, P., Diamanti, E., ... & Bassi, A. (2021). Quantum technologies in space. Experimental Astronomy, 51(3), 1677-1694.

[22] Khalil, M., Chan, A., Plant, D. V., Chen, L. R., & Kuang, R. (2024). Experimental demonstration of quantum encryption in phase space with displacement operator in coherent optical communications. EPJ Quantum Technology, 11(1), 49.

[23] Xuandiyang Lu. (2021). Research on the Development and Problems of Quantum Communication Technology. Advances in Computer, Signals and Systems,5(1).

[24] AmairiPyka Sana. (2021). Industrialization of quantum communication technologies:The landscape of the photonics industry for the future of secure communication and quantum key distribution solutions. PhotonicsViews,18(6),28-31.
[25] Sukhveer Kaur,Krishan Kumar & Naveen Aggarwal. (2025). Enhancing DDoS defense in SDN using hierarchical machine learning models. Journal of Network and Computer Applications,239,104168-104168.
[26] Qing Hu,Jiabing Liu,Zhengfei Wang,Haoyu Si,Sinian Jin,Ying Zhang & Jinhai Li. (2025). Research on intelligent ship resilient network architecture based on SDN. Computer Communications,236,108151-108151.