ingegneria sismica
International Journal of Earthquake Engineering
Anno XLIII - Num. 1 - 2026

Research on the Optimization Algorithm of Artificial Intelligence Network Security Management Based on All-IP Internet of Things Convergence Technology

Ke'er Yang[1,*]

[1] Jiangsu Tobacco Company Huai'an City Company, 223001, Jiangsu, China

SUMMARY: *This paper briefly describes the concept of all-IP IoT convergence-related technologies with the main line of research on the optimization of AI network security management. 6LoWPAN technology is also introduced to realize the seamless integration of low-power mesh network and core IP backbone, so as to realize the optimization of AI network security management technology. Aiming at the 6LoWPAN hierarchical routing algorithm's problems such as control message redundancy and unreasonable parent node selection, a load-balancing-based hierarchical routing algorithm (LB-HiLow) is proposed and optimized by two improvement mechanisms, namely, optimal parent node selection and path repair. Finally, the effect of the AI network security management optimization algorithm under the all-IP IoT convergence technology is analyzed through the assessment of network security posture and the control of network security risk. The results show that the 6LoWPAN technology introduced in this paper can meet most of the application requirements for AI network security management. In addition, the effect of using the method of this paper on network security risk control reaches a good level, and the total score of the overall risk control evaluation reaches 85.86.The experiment verifies that the posture prediction performs well in both real-time and prediction accuracy, and is applicable to the posture prediction evaluation of AI network security management under the all-IP IoT convergence technology.*

KEYWORDS: *All-IP, 6LoWPAN, LB-HiLow, IoT convergence technology, network security*

1 Introduction

With the rapid development of the Internet, network management and optimization has become an important topic. Traditional network management methods can no longer meet the needs of high efficiency and intelligence, so artificial intelligence technology has been introduced into network management to achieve network management and optimization through intelligent algorithms and automated processing [1, 2].

The key technologies of artificial intelligence in network management mainly include data analysis and model construction, intelligent algorithms and decision-making. The first task of AI network management is to collect and analyze network data and construct a model suitable for network optimization [3]. The key to data analysis lies in the statistics and mining of a large amount of network data to discover the problems and bottlenecks in the network [4, 5]. Model construction, on the other hand, is based on the results of data analysis to build mathematical models that can accurately predict network behaviors and problems [6]. On this basis, AI network management requires the automatic adjustment and optimization of the network

*18852330601@163.com
https://doi.org/10.65102/is2026024
Published: 30 April, 2026

through intelligent algorithms. Intelligent algorithms include techniques such as machine learning and deep learning, which can be used in network management to automatically make decisions and optimize the allocation of network resources, and the use of intelligent algorithms can greatly improve the efficiency and accuracy of network management [7-9].

The application of artificial intelligence in network management and optimization is reflected in resource optimization and scheduling, fault detection and automatic repair and security management and risk warning. Network management based on artificial intelligence can achieve intelligent optimization and scheduling of network resources, including bandwidth allocation, server load balancing, etc [10, 11]. Through intelligent algorithms and data analysis, the network management system can dynamically adjust the allocation of resources according to the current network load and business requirements to ensure efficient network operation and high-quality services [12-14]. Meanwhile, with the help of AI technology, the network management system can monitor the status of network equipment and services in real time and discover potential failures in time [15-17]. By analyzing historical failure data and network behavior patterns, network management systems can quickly determine the cause of the failure and automatically take measures to repair it [18, 19]. Network security, on the other hand, is an important aspect of network management, and artificial intelligence can provide stronger support for network security [20, 21]. By using intelligent algorithms to analyze and monitor network data, network management systems can detect network attacks and intrusions in real time and take timely countermeasures [22-24].

The application of artificial intelligence in the optimization of cybersecurity management is an important way to ensure the security of network information, but at the same time, the ethical and privacy issues brought by artificial intelligence should not be ignored. Literature [25] analyzes AI-based meta-universe cybersecurity techniques, discusses academic and industrial perspectives, specifies the challenges faced by AI in meta-universe cybersecurity, and proposes future research directions aiming to enhance the security and privacy of the meta-universe. Literature [26] is based on a systematic literature study aimed at identifying academic results of AI-driven cyber attacks and analyzing them in order to derive cybersecurity measures to provide defenses against potential future threats. Literature [27] discusses the threats in the new era of cyberspace and systematically analyzes the rapid growth of cyber threats and proposes to promote cyber security optimization through the implementation of artificial intelligence methods. Literature [28] points out the shortcomings of traditional cybersecurity solutions and analyzes existing cybersecurity research using AI techniques, revealing that AI techniques improve anomalous intrusion detection in the fight against cybercrime. Literature [29] investigated the potential of AI as an emerging tool in enhancing cybersecurity by providing a case study demonstrating the application of AI in a cybersecurity environment. Literature [30] proposed a deep learning based cyber intrusion detection system in supervisory control and data acquisition aimed at protecting industrial control systems from cyber attacks and verified the effectiveness of the system. Literature [31] systematically reviewed the literature on the application of AI in user access authentication, network situational awareness, and hazardous behavior monitoring, pointed out the many limitations faced by AI in network security management, and proposed a conceptual intelligent network security model. Literature [32] systematically investigates the ethical and privacy issues in the deployment of AI in cybersecurity, emphasizing the importance of responsible decision-making, privacy protection, and transparency. Literature [33] emphasized the important role of AI in protecting cybersecurity, specifying that AI is more portable and effective in large-scale anomaly detection and malware classification. Literature [34] explored the ways in which AI technology can be applied in cybersecurity, based on a comprehensive literature review to understand the multiple

ways in which AI technology can be applied in enhancing cybersecurity measures and analyzed the effectiveness and challenges of AI in cybersecurity management.

The article first introduces the concepts of all-IP IoT, all-IP network structure and the construction of all-IP IoT. To enhance the security of the network and the mobility of the terminals, IPv6 technology is introduced in this paper. In order to realize the seamless integration of low-power mesh network and core IP backbone, an IPv6-based 6LoWPAN technology is also introduced as a way to realize the optimized management of AI network security under the all-IP IoT convergence technology. After that, a load-balancing-based hierarchical routing algorithm LB-HiLow is proposed to maintain the load balance of the network and reduce the average end-to-end delay through the optimal parent node selection mechanism. The performance of LB-HiLow technique in network security management is tested through simulation analysis. Finally, a network security posture assessment model and a network security management evaluation index system are established to evaluate the network security posture and network security risk management based on LB-HiLow.

2 6LoWPAN based network security management optimization algorithm

2.1 All-IP for the Internet of Things

2.1.1 Full IP

All-IP is an IP-based network that includes the basic capabilities of network control, transport within and between access systems, and mobility management, all provided by IP technology [35]. That is, the process of structure IP, protocol IP to service IP. The all-IP network includes the IPization of the transport network, bearer network, core network, access network, etc., i.e., IP as the bearer and transmission technology is extended from the core network to the wireless access network, wireless interface and even mobile terminals. The unified IP transmission mechanism in the core network will also evolve into a fully distributed network structure.

2.1.2 Unified all-IP network architecture

Converged IP network helps to provide a more flexible and faster network environment, creating an adaptive network with high availability and supporting a variety of different service characteristics. All-IP network structure to IP technology as the core, Everying over IP, to provide real-time, non-real-time data, different service quality level requirements of multimedia services; IP over everying, that is, IP running on the link layer technology of the hybrid network structure, the IP technology and other service quality assurance mechanism effective combination. In the all-IP network structure, the connection between the user and the network is no longer a best-effort access located in the access network, but a converged service provided through the coordination of different layers of the network. The all-IP network reflects the development trend of heterogeneous network convergence and the business demand for flexible deployment of services, which requires that the services and applications are based on IP technology and that IP-based connections can be realized through a variety of different access methods.

2.1.3 Construction of an All-IP Internet of Things

All-IP IoT is constructed based on an all-IP core network. In IoT, the all-IP network is able to support various transmission modes, including the modes of object-object, object-human,

client-server, human-group, and ubiquitous transmission. In addition, the all-IP network is capable of handling various real-time and non-real-time services. Even for the large amount of data sent from a large number of terminals with high frequency and low load, the all-IP is able to handle it well. The all-IP network guarantees the mobility of users, terminals and sessions through a high-performance and highly reliable mobility management mechanism, allowing users to freely choose terminal devices and move freely without being restricted by the access system. Both within and between access systems, the all-IP network provides seamless terminal mobility to ensure that users have an uninterrupted service experience. At the same time, in order to achieve mobility between different types of access systems and optimize mobility performance, the all-IP network provides common open interfaces to control terminal mobility between access systems, and also provides corresponding open interfaces for the functions it supports to solve the problem of terminal mobility across access systems.

2.2 Optimization techniques for network security management based on 6LoWPAN technology

2.2.1 6LoWPAN network architecture

The Internet TCP/IP protocol cluster is precisely a unified Internet communication protocol standard. As the next generation of IP protocols, the introduction of IPv6 will make it easier for a large number of diverse terminals to access the IP network and greatly enhance network security and terminal mobility. 6LoWPAN [36] is a protocol for wireless personal area networks based on IPv6. 6LoWPAN is essentially the end network, which consists of several low-power WLANs.6LoWPAN structure is shown in Fig. 1. In the figure, R denotes routing nodes and H denotes host nodes, which share an IPv6 address prefix. In this structure diagram, we have selected several typical LoWPAN networks to form the 6LoWPAN network, which are Simple LoWPAN, Extended LoWPAN, and LoWPAN with multi-hop Ad-hoc structure.From the figure, we can see that Simple LoWPAN is connected to the network through the LoWPAN Edge Router, and the Backhaul is of the point-to-point form; while the extended LoWPAN is connected to the network through a backbone line, which is connected to a number of edge routers to realize the communication. Ethernet is a typical example, while Ad-hoc networks are standalone. Regardless of the structure, which consists of a number of 6LoWPAN nodes.

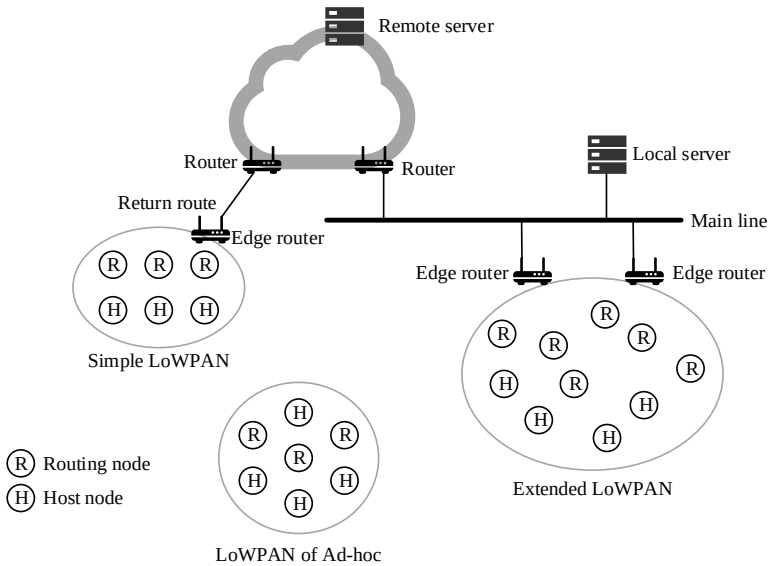

Figure 1: Structure diagram of 6LoWPAN

There are several hosts and routing nodes, and at least one edge router within a wireless personal area network (LoWPAN), where the nodes can be present in only one network or in multiple LoWPANs at the same time, and can move freely. In this case, the edge router plays an important role in the process of connecting LoWPAN to the IP network, and it has multiple roles of routing, 6LoWPAN header compression, and neighbor discovery in the whole network. Routing nodes and edge routers work together to assign IPv6 prefixes to the nodes in the network, and the neighbor discovery function of the edge router also has to complete the work of node registration and fault tolerance processing.

2.2.2 6LoWPAN Protocol Stack

In comparison with the IP protocol, in simple terms, the 6LoWPAN protocol stack is a PAN combination of IPv6 and IEEEE 802.15.4 through an adaptation layer. It differs from the IP protocol in the following ways:

(1) 6LoWPAN only supports IPv6 protocol;

(2) 6LoWPAN basically does not use the TCP protocol, but instead uses the UDP protocol which is simple, efficient and less complex and is compressed by the 6LoWPAN format;

(3) ICMPv6 is used to control message forwarding;

(4) Application layer protocols all exist in binary format and are application-specific.

2.2.3 6LoWPAN Addressing

The 6LoWPAN addressing method is similar to the addressing method in Ethernet and other IPv6 networks, where IPv6 addresses are automatically generated from the LoWPAN prefix and link address. The difference is that since this is a low-power network, a link-layer addressing method is used for compression techniques by direct mapping of link-layer addresses to IPv6 addresses. This method supports both unique long addresses and configured short addresses.

IPv6 consists of a 64-bit prefix and a 64-bit IID, totaling 128 bits in length.The IID for IPv6 can be generated by SAA based on the MAC address of the wireless interface. To facilitate simplified compression, in 6LoWPAN the link address and IID are considered to be one-to-one correspondences, thus eliminating the need for address resolution. As mentioned earlier, IPv6 prefixes can be obtained through neighbor-discovered route announcement messages, which then together with the known link address form the IPv6 address of the 6LoWPAN, thus ensuring a high header compression ratio.

2.2.4 6LoWPAN header format

At the heart of 6LoWPAN is the adaptation layer, which serves to compress IPv6 and the UDP headers that follow it. In addition, segmentation of long messages and addressing of mesh networks are also functions performed by the adaptation layer. Since much of the information is shared by nodes in the same LoWPAN, some of the IPv6 address space can be omitted.

The 6LoWPAN header type is sent through the Send Type field, followed by the IPv6 compressed header. If IPv6 is followed by a UDP or IPv6 extension header, it is compressed according to the next header compression method.

2.3 Fundamentals of the LB-HiLow algorithm

The LB-HiLow algorithm is mainly divided into two mechanisms: optimal parent node selection mechanism and path repair mechanism. The two mechanisms are described in detail below.

2.3.1 Optimal parent selection mechanism

The optimal parent node selection mechanism divides the process of selecting a parent node for an entry requesting node into the following three steps:

Step 1: When a new node wants to join a 6LoWPAN network, it first detects whether there is already a 6LoWPAN network within its communication range through the scanning program: if more than one valid node is detected, it sets the J,R,M bit to 1, 0, 1, respectively, and broadcasts the "network request" to all nodes to make the association. Execute step 2.

Step 2: When the coordinating node i receives the "request for network access" message, it first determines the number of its children nodes:

If the number of child nodes is equal to MC, it indicates that the number of child nodes of node i has reached the upper limit, and it will not accept other nodes as its child nodes, so it will not process the request message, otherwise, it will execute ②;

② If the number of child nodes is less than MC, it indicates that the number of child nodes of node i has not reached the upper limit, so it continues to judge the M flag bit, if the M flag bit is 0, it indicates that there is no other candidate parent node, so it calculates the 16-bit short address of the requesting node based on the address assignment equation and associates it with it successfully; if the M flag bit is 1, it indicates that there are more than one candidate parent node, node i will detect its remaining energy P_i, the number of child nodes m_i and the depth value D_i, if $P_i/(m_i+2)$ is less than the threshold LPE, it will no longer process the request message, otherwise it performs ③; namely:

$$FC = MC^{*}AP + N, 0 < N \le MC \tag{1}$$

where MC is the maximum number of children of the parent node, AP is the address of the parent node, and the newly joined node is the N th child of the parent node, then the calculated FC is the address of the newly joined child node:

$$W_i = \frac{P_i}{(m_i+2)*(MC^{D_i})} \tag{2}$$

③ Calculate the weight value W_i of node i according to the above equation, and set J,R,A to 1, 0, 1 respectively, and send the "access confirmation" message with its weight value to the requesting node, and then perform step 3.

Step 3: Assuming that the requesting node receives "admission confirmation" messages from n selected parent nodes, it records the order in which it receives i from each of the selected parent nodes, labels it as O_i, extracts its weight W_i, and selects the node with the largest weight value as its optimal parent node $N_{\max}$:

$$N_{\max} \Leftarrow \max\{W_1, W_2, \cdots, W_n\} \tag{3}$$

If the number of selected parent nodes that satisfy the above equation is two or more, the order of their arrivals is compared, and the node with the smaller order value is selected as its optimal parent node $N_{\max}$, which ensures that the selected parent node has a smaller transmission delay while satisfying the load balancing requirement.

2.3.2 Path repair mechanisms

The path repair mechanism specifically divides the path repair process into the following 3 steps:

Step 1: In the process of data transmission, when node j finds that the next hop node fails, it will first determine the relationship between the failed node and itself, so as to determine whether it is upstream path repair or downstream path repair.

Step 2: When the coordination node i receives the “repair request” message, it judges the relationship between the failed node and itself, and selects the corresponding execution step according to the different relationships.

Step 3: Suppose the repairing node receives “repair confirmation” messages from n candidate stepfather nodes. Record the order in which messages from each candidate stepfather node i are received, marked as O_i, and extract its weight W_i. The successfully repaired node will sequentially update the 16-bit short addresses of its descendant nodes. Assuming the parent node's original address is AP_{old} and the new address is AP_{new}, with the maximum number of child nodes being MC, the update formula for the new address AC_{new} of the corresponding descendant node relative to the child node's original address AC_{old} is as follows:

$$AC_{new} = (AP_{new} - AP_{okl}) * MC + AC_{okl} \tag{4}$$

The specific process of the path repair mechanism is shown in Figure 2.

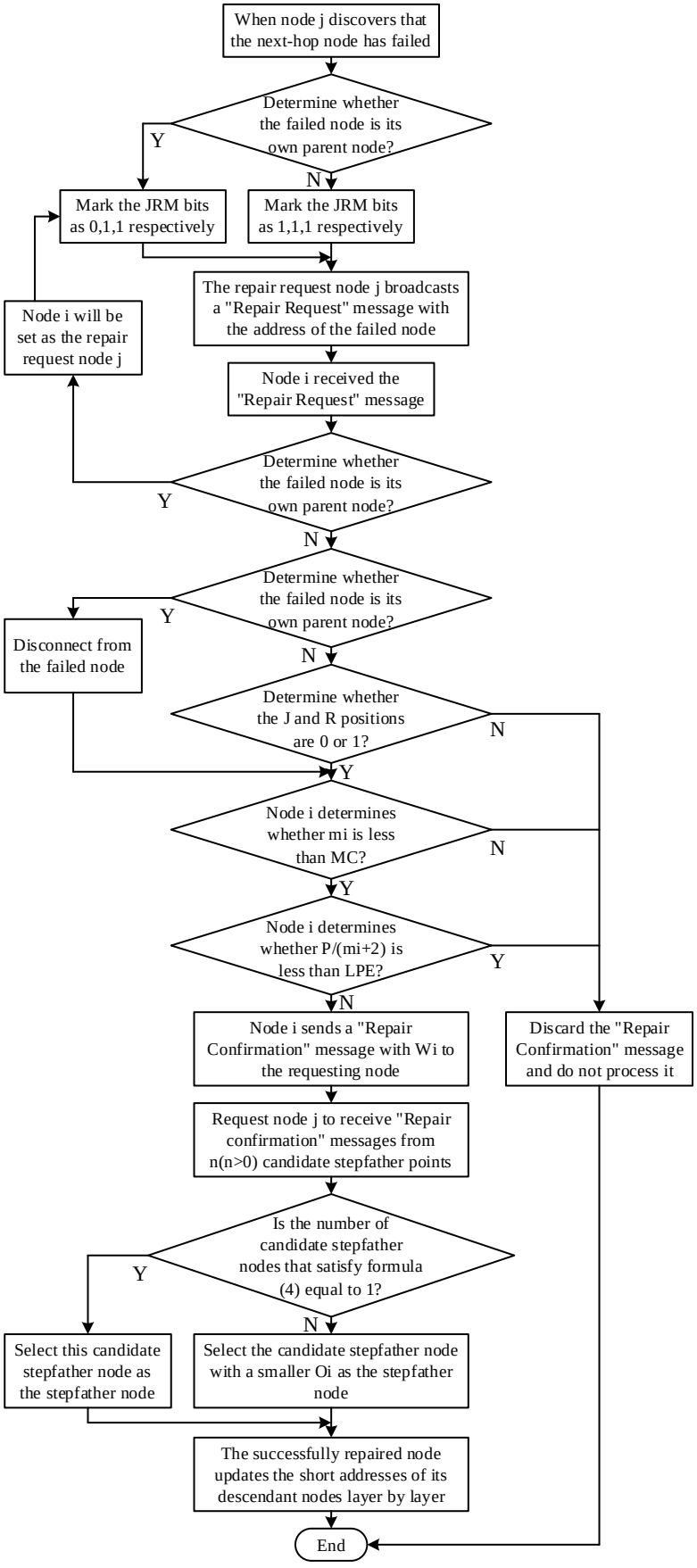

Figure 2: Flowchart of path repair

2.4 Performance Testing of LB-HiLow Technology in Network Security Management

2.4.1 Test Methods

Test Environment: The network configuration selected for this experiment consists of a linear topology comprising one source node, one destination node, and six relay nodes. All data transmission in the tests utilizes UDP. Table 1 compares the test environments of this experiment and the XX experiment.

Table 1: The test environment of this paper experiment and XX experiment

Comparative item	Silicon Labs experimental environment	Experimental environment of this paper
Hardware platform	EFR32 Mighty Gecko:	LB-HiLow sensor Board (STM32F103):
	32-bit Cortex-M4 core	32-bit Cortex-M3 core
	Main frequency 40MHz	75MHz main frequency
	32KB RAM, 256KB Flash	64KB RAM, 512KB Flash
	2. 4GHz radio transmission power 16. 5dBm	2.4GHz radio transmission power +0dBm
Protocol stack	Silicon Labs Thread Stack	Google Nest Open LB-HiLow
	Bluetooth Mesh	

(1) Unicast Latency

The testing principle for unicast latency is illustrated in Figure 3. This paper employs Round-Trip Time (RTT) to evaluate the unicast latency performance of the LB-HiLow network. The source node runs the Requester program, waiting for a user key press. Upon key activation, it sends a packet of specified payload length to the Responser and starts timing. Timing stops upon receiving the response from the Responser. The destination node runs the Responser program (UDP Server), waiting to receive the packet and then sending an identical packet back to the source.

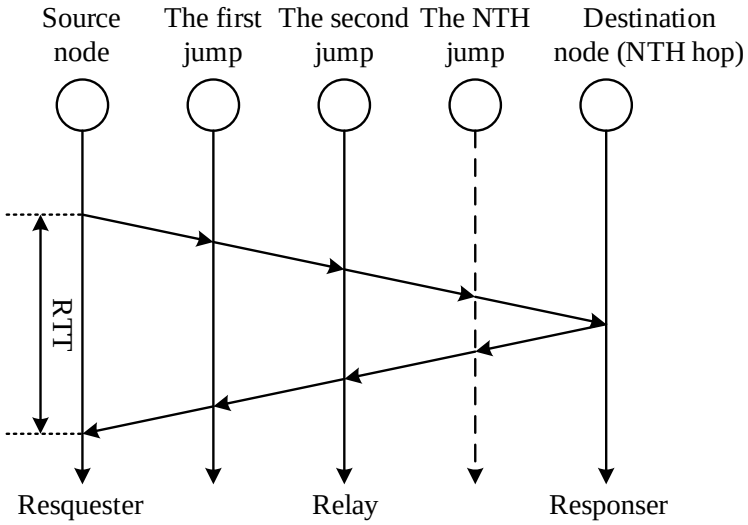

Figure 3: Principle of unicast Delay Testing

(2) Throughput

The throughput testing principle is illustrated in Figure 4. A specified number of data packets are sent to the destination node. The destination node runs the Receiver program to record the number of packets correctly received. If the final count of packets sent by the Sender matches the count received by the Receiver, the Sender's transmission rate is increased, and the experiment is repeated. The maximum transmission rate at which no packet loss or errors occur at either end is determined. The total amount of data transferred per unit time is then calculated as the throughput.

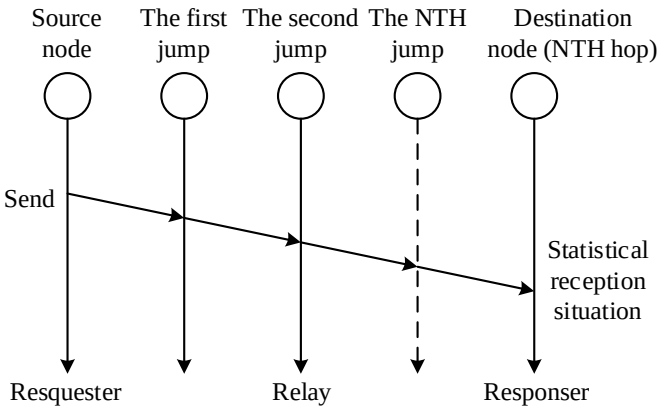

Figure 4: Throughput Testing Principle

(3) Simulation Parameters

The experiment randomly places 36 nodes within a 120×120 grid to simulate a DODAG-generated tree-like network topology. In the LB-HiLow network, the gateway load threshold $L_{diredoll} = 30$, $T = 5$. Node load follows a Poisson distribution with $\lambda = 5$, while link quality and remaining energy composite factors follow an exponential distribution with $\lambda = 5$.

Under these simulation parameters, the generated LB-HiLow network is shown in Figure 5, where node 7 is identified as the root gateway.

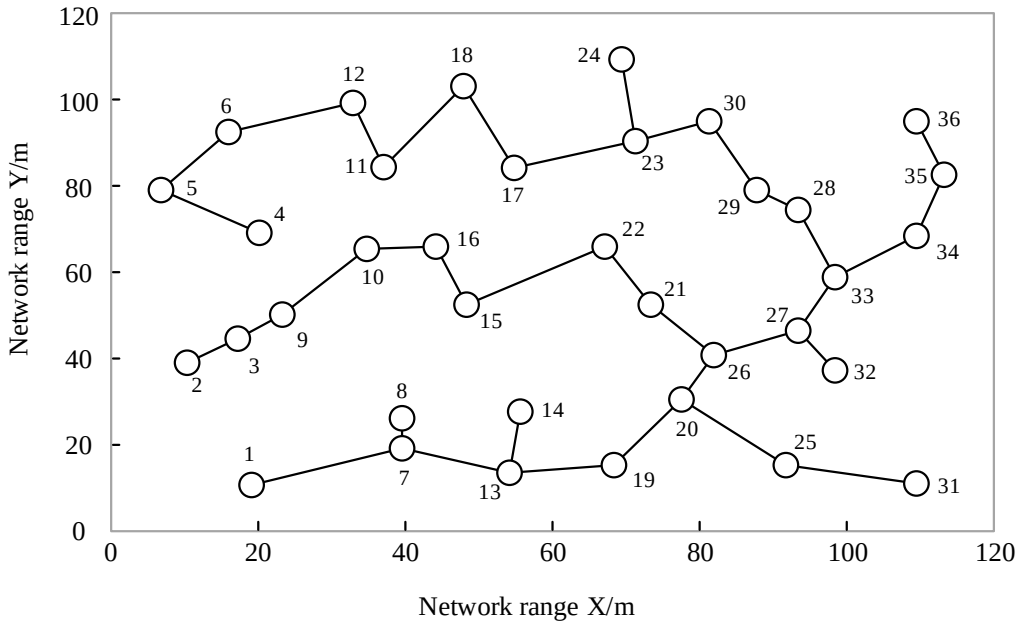

Figure 5: Simulation network topology diagram

2.4.2 Test Results and Analysis

(1) Unicast Delay and Hop Count

With a payload length set to 50 bytes, the number of relays was incrementally increased from 1 to 6. The relationship between unicast communication delay and hop count in the LB-HiLow network system is shown in Figure 6. As depicted, the network's unicast communication delay increases with the hop count. Under small payload conditions, LB-HiLow and ZigBee exhibit favorable delay performance, while Bluetooth Mesh demonstrates relatively higher delay—though none exceed 180ms. For cybersecurity management scenarios under full IP IoT convergence technology, delays within 180ms can meet the application requirements of most AI-based cybersecurity management systems.

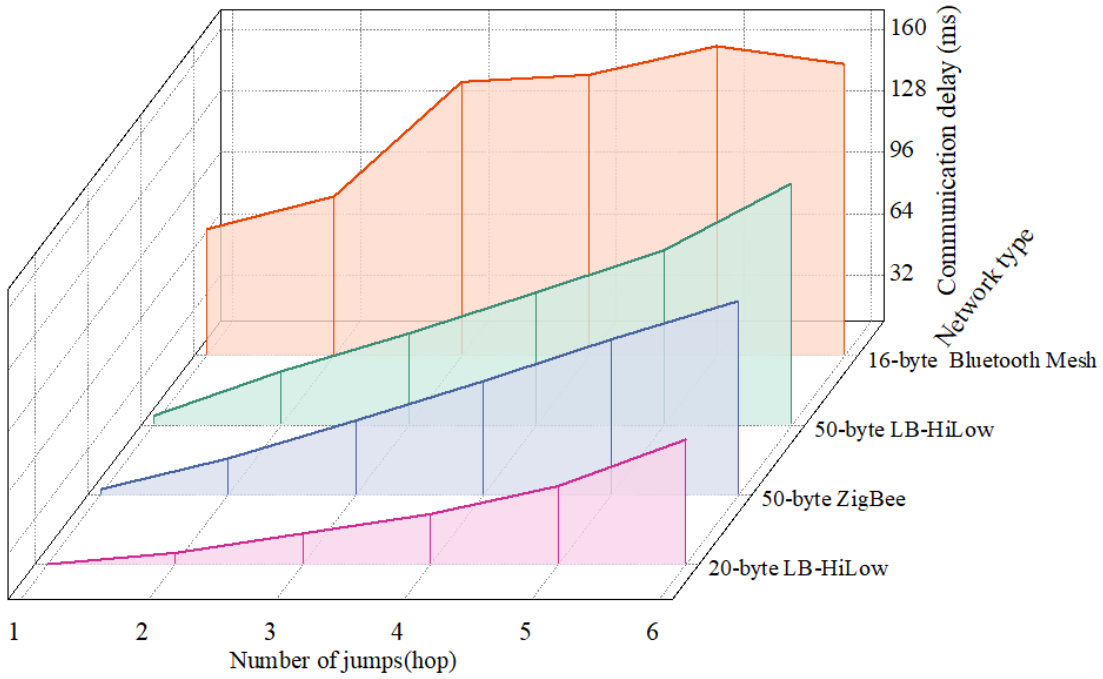

Figure 6: The relationship between delay and frequency jump

(2) Unicast Delay and Payload Length

With a hop count of 5, the relationship between unicast delay and payload length is shown in Figure 7. It can be observed that as the effective payload length increases, the communication delay in the LB-HiLow network gradually increases. A noticeable jump in communication delay occurs between payload lengths of 68 and 78 bytes, caused by packet fragmentation due to individual physical frames being unable to accommodate the entire user payload. Furthermore, a positive correlation exists between the two metrics overall.

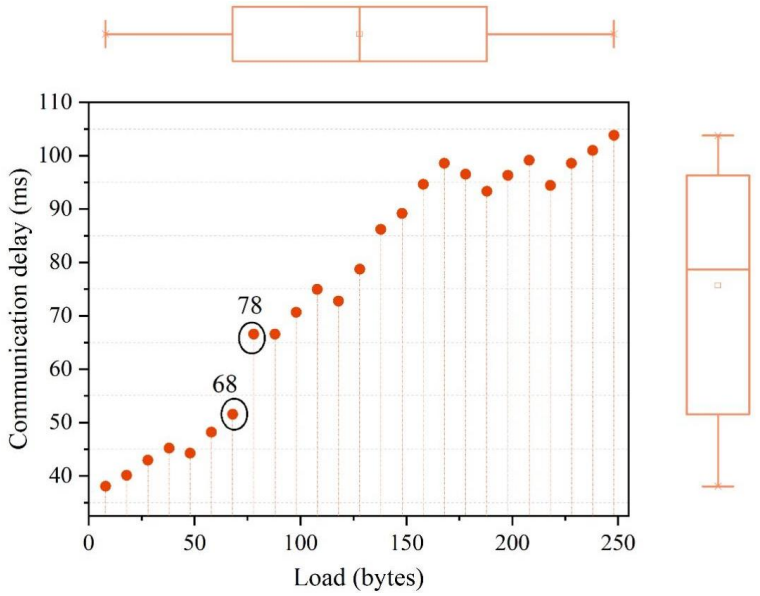

Figure 7: Relationship between delay and load length

The relationship between network latency and payload length is illustrated in Figure 8. It can be observed that as the effective payload length increases, communication latency across all networks also increases. Under heavy payload conditions, Bluetooth Mesh's communication latency struggles to meet the requirements for optimizing artificial intelligence-based cybersecurity management within an all-IP IoT convergence framework. In contrast, LB-HiLow and ZigBee maintain relatively low communication latency, exhibiting a more gradual increase in latency as the effective payload length grows.

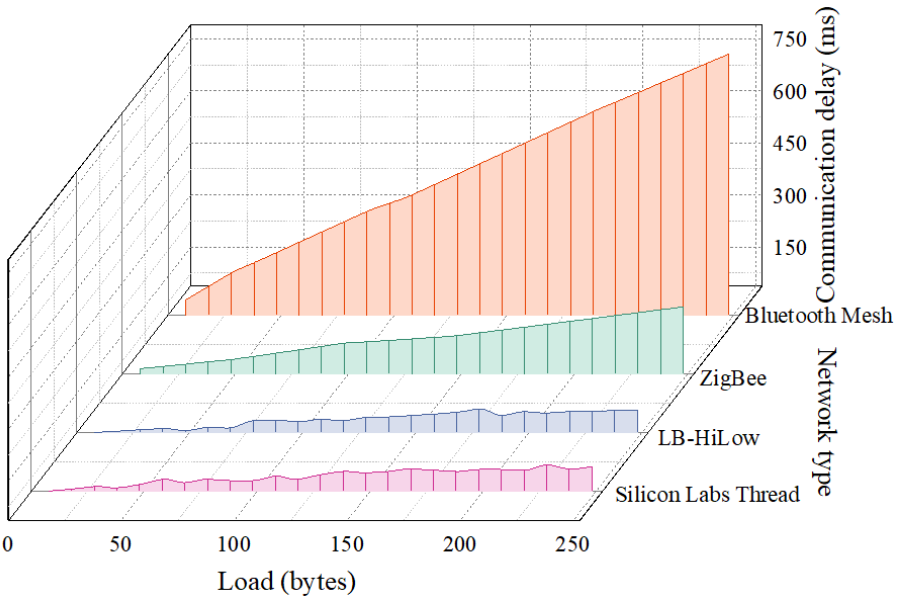

Figure 8: Relationship between different network delays and load length

(3) Throughput

Throughput testing employed a fixed-length payload, with the LB-HiLow UDP payload length set to 100 bytes. The relationship between throughput and hopping frequency is illustrated in Figure 9. As the number of hops increases, the throughput of the LB-HiLow network declines rapidly. Under identical conditions, LB-HiLow demonstrates a significant

advantage in throughput compared to ZigBee and Bluetooth, while Bluetooth Mesh exhibits the lowest network throughput. This indicates that the LB-HiLow network system constructed in this paper possesses excellent network performance, with unicast latency falling below the 180ms response time typically required for human-machine interaction.

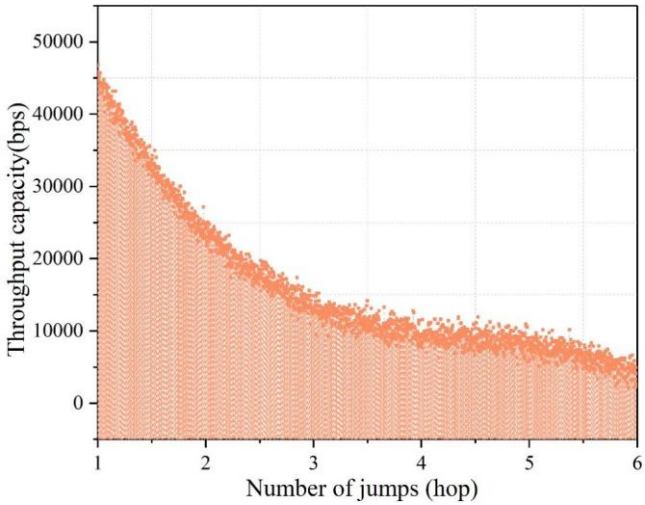

Figure 9: The relationship between throughput and frequency hopping

(4) Comparison of Gateway Deployment Schemes

Within the same network, gateway deployment was implemented using both the LB-HiLow algorithm and the NP algorithm. The experimental results for gateway deployment under the LB-HiLow and NP algorithms are shown in Figures 10 and 11. Both algorithms partitioned the network into multiple branches. Analysis reveals that the LB-HiLow algorithm ultimately identifies 6 gateways, with node numbers: 7, 11, 15, 20, 29, 33. The NP algorithm also identifies 6 gateways, with node numbers: 7, 15, 18, 20, 27, 28. The results demonstrate that both algorithms can achieve multi-gateway deployment in the LB-HiLow network.

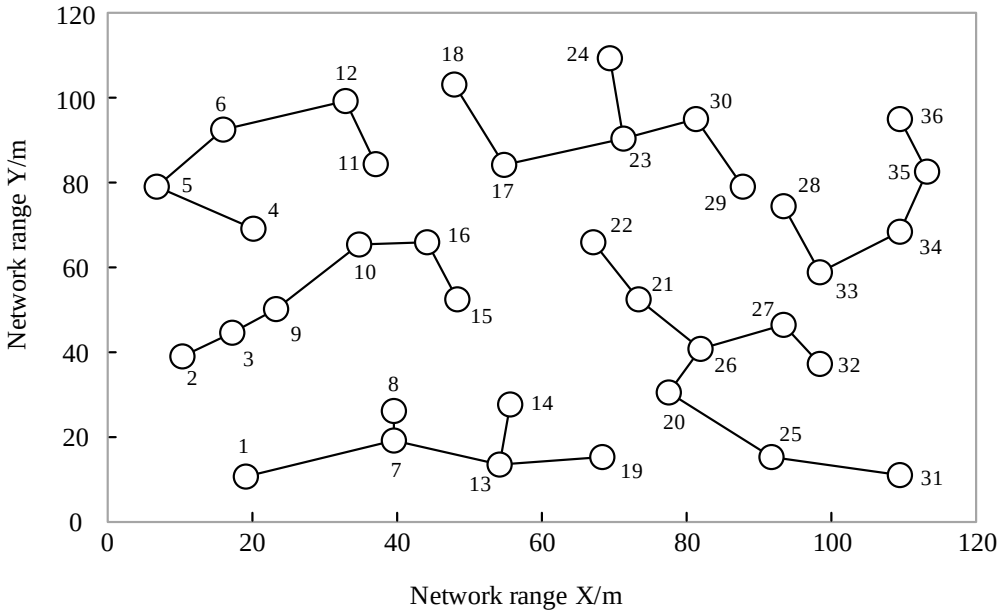

Figure 10: Experimental results of LB-HiLow algorithm

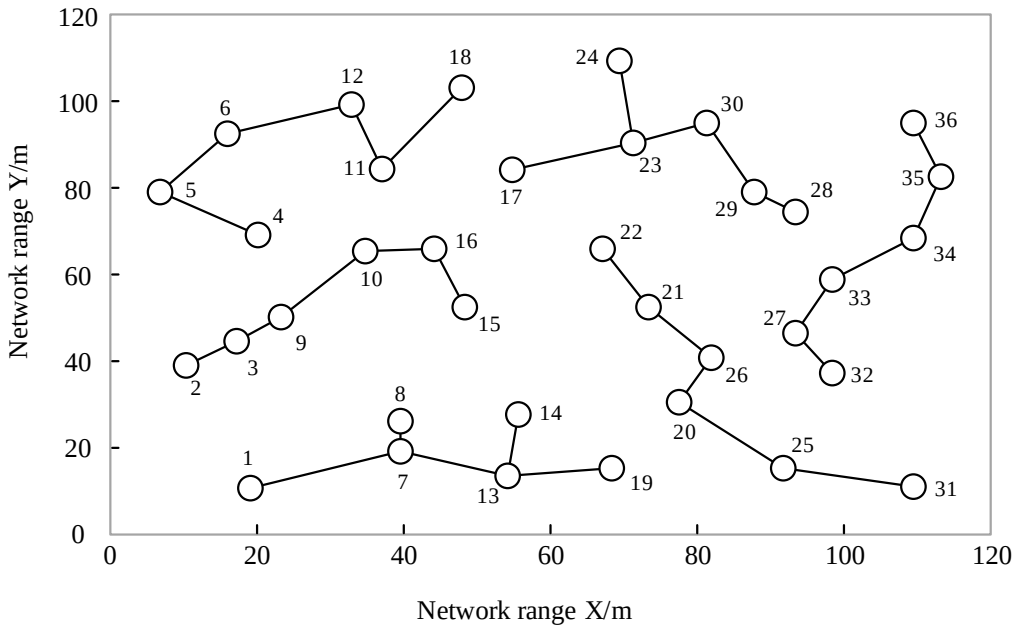

Figure 11: Experimental results of NP algorithm

3 Analysis of Cybersecurity Management Optimization Outcomes

3.1 Establishing a Cybersecurity Posture Assessment Model

3.1.1 Establishing a Security Posture Assessment Indicator System

This paper proposes a novel security posture assessment method based on convolutional neural network algorithms. The approach subdivides cybersecurity posture into three sub-postures: Basic Operation, Vulnerability, and Threat, establishing corresponding evaluation metrics for each to comprehensively, objectively, and accurately assess network security status. Specifically: The Vulnerability sub-state monitors network vulnerabilities and security infrastructure, involving metrics such as total security devices, open ports, and vulnerability severity. The Threat sub-state tracks attack exposure, encompassing indicators like alert counts, Transmission Control Protocol (TCP) packet analysis, and attack severity.

3.1.2 Data Acquisition and Preprocessing

First, obtaining comprehensive and accurate cybersecurity-related data from cybersecurity monitoring systems, public data sources, or third-party data providers is crucial. This primarily includes security logs, attack incident records, vulnerability information, and other data that form the foundation for model training and evaluation. Second, based on the specific requirements of cybersecurity posture assessment, it is necessary to select relevant and representative features from the raw data. These features should cover the effectiveness of security measures, the frequency and types of attacks, and the exploitation of vulnerabilities.

3.1.3 Extracting Cybersecurity Posture Features

In practice, before establishing an evaluation model, it is necessary to first extract representative cybersecurity posture features. To accurately capture the dynamic characteristics of the security

posture, posture element data from multiple time steps is used as input to form a multi-time-step, multi-channel data set Xi, expressed as follows:

$$X_i = [\, ft_1,\, ft_2, L,\, ft_r \,] \tag{5}$$

In the equation, f_{t_i} denotes the data at the i th time step for each channel, where i ranges from 1 to T, and L represents the number of time steps in X_i.

3.1.4 Multi-Channel Feature Fusion

After extracting security posture features, multi-channel fusion is required. Feature vectors from each channel are concatenated in dimension to form a comprehensive feature matrix (FM), expressed as follows:

$$FM = [cf_1, cf_2, cf_3, cf_4] \tag{6}$$

In the formula, c_{f_i} represents the output feature vector for each channel. Although the dimensionality of the original input data may vary across different channels, after feature extraction and uniform processing, the feature vectors can be directly concatenated to form a complete feature matrix. Multi-channel fusion aims to effectively reduce or eliminate noise by rationally concatenating feature vectors from multiple channels, while ensuring the accuracy and integrity of the original feature data.

3.1.5 Evaluation Model Development and Situation Assessment

This paper employs convolutional neural network algorithms and multi-channel feature fusion techniques to construct a practical and efficient cybersecurity assessment model. The model's development primarily involves three stages: sample generation, dynamic analysis, and evaluation result output. When building the evaluator, the Inception module is introduced, utilizing a cascaded design of 1×3 convolution kernels to replace traditional 1×5 kernels, thereby optimizing computational efficiency. To further enhance feature extraction, a differential operator is applied to sharpen the input data. The specific formula is as follows:

$$g^{l}(x) = \begin{cases} Af(x) & + f_s^{l}(x) s_c > 0 \\ Af(x) & + f_s^{l}(x) s_c < 0 \end{cases} \tag{7}$$

In the equation, $f_s^i(x)$ denotes the functional form of filter l performing filtering operations on specific input features; $g^{'}(x)$ represents all feature indicators output after processing by this filter; while $f(x)$ encompasses all original input features fed into the filter. A serves as a universal sharpening tool to enhance key features; s_e functions as the core parameter of the sharpening operation, whose value determines the intensity of sharpening.

3.2 Cybersecurity Posture Assessment Based on LB-HiLow

To validate the effectiveness of cybersecurity management, it is necessary to subject it to certain attacks. Under the framework of full IP IoT convergence technology, this paper evaluates the optimization effects of AI-based network management by using three attack methods—“node risk level measurement,” “cybersecurity posture fusion,” and “cybersecurity posture

prediction"—as testing subjects.

The main configuration is as follows: Three subnets composed of ordinary nodes, each equipped with a threat severity measurement module; Three attackers executing simulated UDP Flood, TCP SYN Flood, and DOSnuke attacks respectively; A server subnet containing three servers, each equipped with a node criticality measurement module, a situation fusion module, and a situation prediction module.

Three attackers continuously launched attacks on the network, configuring ordinary nodes with parameters such as /ow=4 and sec=8, while servers were set to /ow=8. To validate the effectiveness of network security posture assessment and prediction under varying attack intensities, four attack intensity levels were set: 0.1-1Kpackets/s, 1.1-2Kpackets/s, 2.1-3Kpackets/s, and 3.1-4Kpackets/s. Experiments were conducted at each of these four levels and at an unpredictable level, with each experimental run lasting 800 seconds.

3.2.1 Node Hazard Level Metric

Ordinary nodes possess a hazard level measurement function, capable of providing measurement results for the node itself. The assessment center delivers security posture evaluations for the entire network, while the prediction center provides posture forecasts for the entire network. Taking an attack intensity level of 2.1-3K packets/s as an example, the node hazard level measurement is illustrated in Figure 12. The results reveal that across four attack intensity levels and the indeterminate level, ordinary nodes exhibit highly similar trends in attack intensity and risk severity. This indicates that when ordinary nodes are subjected to supply chain attacks, the integrated full-IP IoT technology faces heightened security management risks within artificial intelligence networks. Consequently, utilizing the proposed cybersecurity posture assessment model to measure network node risk severity enables faster identification of optimized cybersecurity management outcomes.

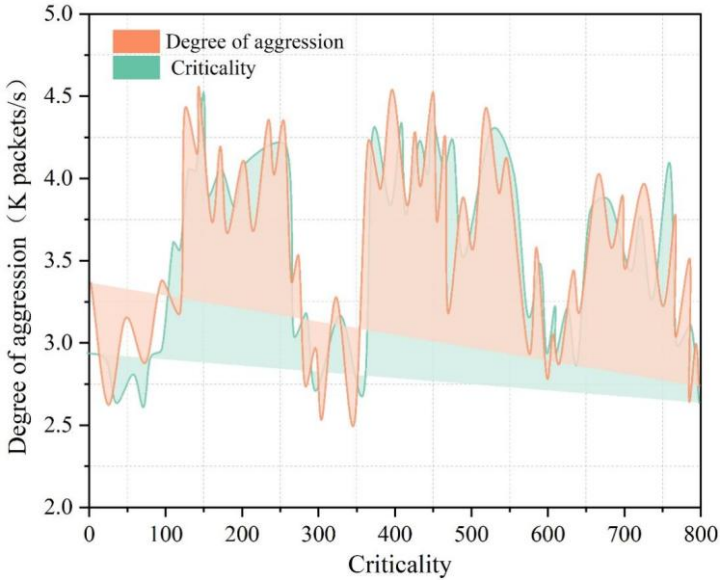

Figure 12: Node risk degree measurement

3.2.2 Cybersecurity Situation Integration

Cybersecurity posture integration serves as one of the metrics for evaluating cybersecurity management. Therefore, this paper assesses cybersecurity management based on the results of the cybersecurity posture assessment model, utilizing the outcomes of cybersecurity posture integration. The results of cybersecurity posture integration are presented in Figure 13. The

findings indicate that under cybersecurity posture integration based on the cybersecurity posture assessment model, the attack severity and threat severity in network management are closely correlated to a certain extent. We can evaluate the effectiveness of cybersecurity management in artificial intelligence networks by analyzing the results of cybersecurity posture integration.

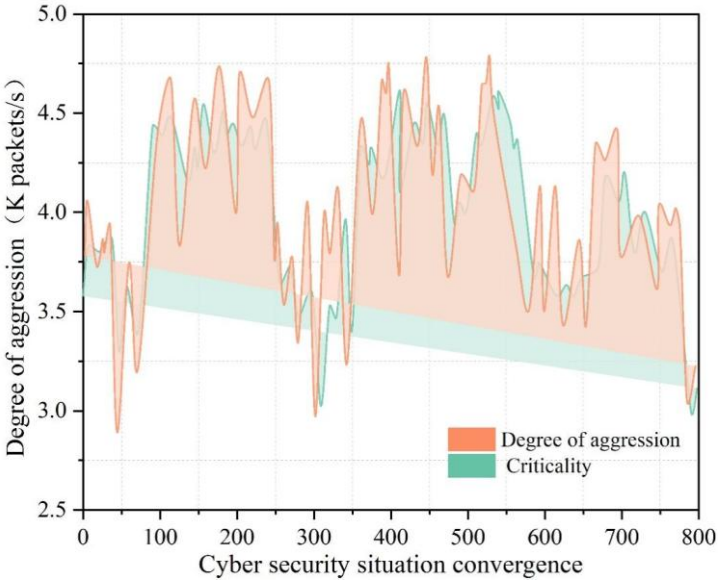

Figure 13: Cyber security situation convergence

3.2.3 Cybersecurity Landscape Forecast

The cybersecurity situation forecast is shown in Figure 14. Results from predicting the network security situation using the cybersecurity situation assessment model developed in this paper indicate that regardless of the severity of attacks, the risk level of cybersecurity management is accurately forecasted and consistently remains lower than the attack severity. This demonstrates that the management techniques based on this cybersecurity situation assessment model can accurately predict network security. The combined experimental results validate that the situation forecast performs well in both real-time capability and prediction accuracy, making it suitable for forecasting cybersecurity situations in large-scale networks.

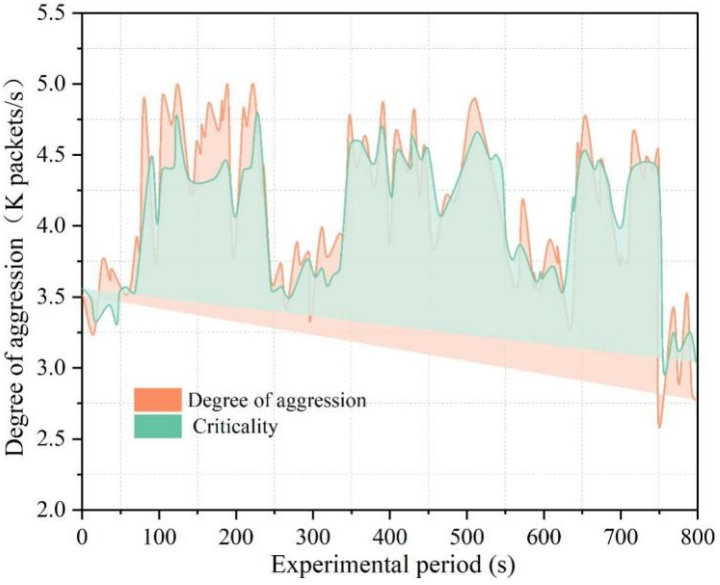

Figure 14: Network security situation prediction

3.3 Evaluation of Cybersecurity Risk Management Effectiveness

To preemptively implement cybersecurity posture assessment and predictive modeling, one must first develop functional modules for security posture evaluation and forecasting. Subsequently, utilizing foundational models on the simulation platform, establish cybersecurity posture assessment and prediction models guided by principles of system design, cybersecurity, and network communication. Next, to ensure controllable attacks, establish network attack simulation models. Finally, run cybersecurity posture assessment and prediction simulations and analyze the simulation results.

This paper treats each device in the network as a node, meaning each node should possess a threat level measurement function to quantitatively assess its own security status in real time. One device should also serve as an assessment fusion center, performing dual functions of node importance measurement and posture assessment. Additionally, another device should act as a prediction management center, utilizing historical assessment data from the assessment fusion center to forecast cybersecurity posture.

Drawing upon the successful simulation of the Chinese Air Force LAN by XXX University Laboratory, this paper establishes its simulation model. The model comprises four subnets: three primarily composed of host devices and one primarily composed of server devices. Within each subnet, all devices are connected via a Cisco 2900 series secondary switch, while subnets interconnect via a Cisco 6500 series primary switch. All links utilize 100BaseT Ethernet twisted-pair cables. The number of nodes and corresponding functions for each subnet are detailed in Table 2.

Table 2: The number of nodes in each subnet and their functions

Network name	Number of nodes	Function
Subnet 1	55	Node risk degree measurement
Subnet 2	46	Node risk degree measurement
Subnet 3	50	Node risk degree measurement
Subnet 4	6	Node risk degree measurement, evidence weight allocation, security situation assessment, security situation prediction

3.3.1 Development of an Evaluation Indicator System for Risk Control Effectiveness

This paper categorizes the effectiveness of risk control in artificial intelligence network and information security risk management into four levels, with corresponding evaluations of “Excellent,” “Good,” “Average,” and “Poor.” An “Excellent” level indicates high risk control capability in AI network and information security risk management, where all risk factors are effectively addressed during operations with highly visible results. Good risk control effectiveness indicates a relatively high level of risk management capability within AI network and information security risk management. Most risks encountered during operations can be effectively controlled through risk mitigation measures, yielding favorable outcomes. However, some risks remain inadequately controlled despite implemented measures, resulting in limited effectiveness. A moderate level of risk control effectiveness indicates average risk control capabilities in AI network and information security risk management. Control measures prove relatively ineffective for most risks arising during operations. A poor level of risk control effectiveness indicates virtually non-existent risk control capabilities in AI network and information security risk management, meaning current risk control measures have little to no

impact on emerging risks. The cybersecurity management evaluation indicator system is shown in Table 3.

Table 3: Network security management evaluation index system

Primary indicator	Secondary indicators	The abbreviated form of a name	Third-level indicators	The abbreviated form of a name
Network and information security risk management control	Network security	A	Set security domain classification and network policy setting for the computer	A1
			Computer operating system hardening	A2
			Server unified permission management	A3
	Information safety	B	Records of use of artificial intelligence networks	B1
			Security level classification of artificial intelligence networks	B2
			The standardization of the use of artificial intelligence networks	B3
	Business continuity	C	Data disaster classification record	C1
			Implementation record of data disaster protection measures	C2
			Data disaster recovery status records	C3

3.3.2 Application of Safety Risk Management Effectiveness Evaluation

Following the summary of management operations for various host devices, the Information Center mandates that administrators promptly archive all records generated during the management process. On the 30th of each month, the Information Center convenes a summary meeting to review the execution of host device management tasks from the preceding month. By analyzing records from the host device management process, deficiencies in work are promptly identified, and corrective measures are proposed. Dedicated IT personnel oversee the implementation of these measures, establishing a closed-loop management system for artificial intelligence cybersecurity under the fully IP-based IoT convergence technology.

The Information Center employs a combined approach of the Analytic Hierarchy Process (AHP) and Fuzzy Comprehensive Evaluation Method to assess the effectiveness of risk control measures across various host management processes, comprehensively reflecting the efficacy of risk control strategies.

(1) Determination of Indicator System Weights

The weighting of indicators for AI cybersecurity management risk control effectiveness is shown in Table 4.

Table 4: Weight of risk control effect index in network security management

Third-level indicators	The abbreviated form of a name	Weight
Set security domain classification and network policy setting for the computer	A1	0.4021
Computer operating system hardening	A2	0.3444
Server unified permission management	A3	0.2535
Records of use of artificial intelligence networks	B1	0.4848
Security level classification of artificial intelligence networks	B2	0.2746
The standardization of the use of artificial intelligence networks	B3	0.2406
Data disaster classification record	C1	0.3711
Implementation record of data disaster protection measures	C2	0.3535
Data disaster recovery status records	C3	0.2754

(2) Fuzzy Comprehensive Evaluation

Based on the risk control effectiveness evaluation index system for various host equipment management operations at the Information Center and the weight values assigned to each indicator, a set of evaluation criteria was further established. The evaluation criteria set V = {$V1$, $V2$, $V3$, $V4$} = {Excellent, Good, Average, Poor}. A sample of 1,000 respondents was selected to rate the three-level indicators for security risk control effectiveness in various host equipment management operations at the Information Center. The membership degrees of experts' evaluations for each indicator were calculated, yielding a fuzzy relationship matrix. The fuzzy comprehensive evaluation results for the security management risk control effectiveness of various host equipment management operations are shown in Table 5. The comment set was scored on a percentage basis with R = {100, 80, 60, 50}. Cybersecurity risk control evaluation: S1 = W*R = 85.39; Information security risk control evaluation: S2 = W*R = 82.17 Business continuity risk control evaluation: S3 = W*R = 88.94; Overall Risk Control Evaluation: S = W * R = 85.86.

Based on the risk effectiveness evaluation results, the Information Center demonstrates good overall security risk control effectiveness in managing various host devices. Business continuity risk control is relatively strong, achieving 88.94 points, while cybersecurity risk control is also relatively strong, achieving 85.39 points. Both areas have attained a “good” evaluation for risk control effectiveness.

Table 5: Fuzzy comprehensive evaluation result of safety management effect

Metric	Fuzzy relational matrix			
	Outstanding	Good	Secondary	Bad
A1	0.7119	0.2649	0.0232	0.0000
A2	0.7004	0.2996	0.0000	0.0000
A3	0.5682	0.3367	0.0951	0.0000
B1	0.6029	0.3028	0.0452	0.0491
B2	0.7847	0.2036	0.0117	0.0000
B3	0.6601	0.3291	0.0108	0.0000
C1	0.7168	0.2755	0.0077	0.0000
C2	0.7254	0.2085	0.0249	0.0412
C3	0.6955	0.2504	0.0452	0.0089

Based on the Level 1 fuzzy comprehensive evaluation results from the Information Center regarding the risk control effectiveness of various host equipment management operations, the overall risk control effectiveness for security management tasks across all host equipment categories has reached a satisfactory level. This indicates that the risk control measures implemented for this work have been relatively effective. However, the Level 2 fuzzy comprehensive evaluation results reveal that enhanced control measures are still required in the information security risk management phase for all host equipment management operations. This will better mitigate security risks throughout the management processes of various host equipment.

For information security risk management, it is necessary to conduct risk assessments once again based on three aspects: usage records of AI networks, security level scores, and compliance with usage standards. If new information security risk-related assessment items were identified during the previous execution process, they should also be incorporated into the new round of network and information security risk assessments. Subsequently, implement and inspect the control and effectiveness evaluation of quantified security risk factors. This approach establishes a closed-loop management framework for the information center's network and information security, enhancing governance capabilities for AI network security and information security management within an all-IP IoT convergence environment.

4 Conclusion

This paper analyzes the effectiveness of artificial intelligence-based cybersecurity management under IoT convergence technologies using 6LoWPAN technology and evaluates the security posture. Results indicate that the constructed 6LoWPAN network demonstrates excellent performance in unicast communication latency and network throughput. By implementing and inspecting workflows for controlling and evaluating the effectiveness of quantified security risk factors, a closed-loop system for information center network and information security management has been achieved. This enhances control capabilities for AI cybersecurity and information security management within an all-IP IoT convergence environment. The cybersecurity posture assessment yields reasonable and effective results, with predictive outcomes demonstrating real-time accuracy.

About the Author

Keer Yang born in 1995 in Hechuan District, Chongqing. She obtained a master's degree from Hohai University. She is currently a data administrator at the Jiangsu Tobacco Company Huai'an City Company, mainly responsible for data management and information security.
18852330601 @163.com

References

[1] Alowaidi, M., Sharma, S. K., AlEnizi, A., & Bhardwaj, S. (2023). Integrating artificial intelligence in cyber security for cyber-physical systems. Electronic Research Archive, 31(4).

[2] Aloqaily, M., Kanhere, S., Bellavista, P., & Nogueira, M. (2022). Special issue on cybersecurity management in the era of AI. Journal of Network and Systems Management, 30(3), 39.

[3] Farooq, M., & Khan, M. H. (2023). Artificial intelligence-based approach on cybersecurity challenges and opportunities in the Internet of Things & edge computing devices. International Journal of Engineering and Computer Science, 12(7), 25763-25768.

[4] Al-Rubaye, R. H. K., & Türkben, A. K. (2024). Using artificial intelligence to evaluating detection of cybersecurity threats in ad hoc networks. Babylonian Journal of Networking, 2024, 45-56.

[5] Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. Ieee Access, 8, 23817-23837.

[6] Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology & Electronic Engineering, 19(12), 1462-1474.

[7] Cao, G., Lu, Z., Wen, X., Lei, T., & Hu, Z. (2017). AIF: An artificial intelligence framework for smart wireless network management. IEEE Communications Letters, 22(2), 400-403.

[8] Jiang, W., Strufe, M., & Schotten, H. D. (2017, June). Intelligent network management for 5G systems: The SELFNET approach. In 2017 European conference on networks and communications (EuCNC) (pp. 1-5). IEEE.

[9] OLANIYI, R., OLUGBILE, H., & OKWUOBI, O. (2025). THE ROLE OF ARTIFICIAL INTELLIGENCE IN NETWORKING-A REVIEW. GEN-MULTIDISCIPLINARY JOURNAL OF SUSTAINABLE DEVELOPMENT, 3(1), 15-45.

[10] Khilar, R., Mariyappan, K., Christo, M. S., Amutharaj, J., Anitha, T., Rajendran, T., & Batu, A. (2022). Artificial Intelligence-Based Security Protocols to Resist Attacks in Internet of Things. Wireless Communications and Mobile Computing, 2022(1), 1440538.

[11] Lysenko, S., Bobro, N., Korsunova, K., Vasylchyshyn, O., & Tatarchenko, Y. (2024). The role of artificial intelligence in cybersecurity: Automation of protection and detection of threats. Economic Affairs, 69, 43-51.

[12] Nweke, C. C., Eze, P. C., Ezenugu, I. A., & Okorogu, V. N. (2024). Methods, Potentials and Challenges of Machine Learning Based Artificial Intelligence Systems in Cyber Security. Methods, 20(3), 91-107.

[13] Shandilya, S. K., Choi, B. J., Kumar, A., & Upadhyay, S. (2023). Modified firefly optimization algorithm-based IDS for nature-inspired cybersecurity. Processes, 11(3), 715.

[14] Xia, F., & Zhou, Z. (2024, June). Methods for Computer Network Security Management Assisted by Artificial Intelligence Models. In 2024 2nd International Conference on Mechatronics, IoT and Industrial Informatics (ICMIII) (pp. 682-685). IEEE.

[15] Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022). Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. Electronics, 11(2), 198.

[16] Jimmy, F. (2021). Emerging threats: The latest cybersecurity risks and the role of artificial

intelligence in enhancing cybersecurity defenses. Valley International Journal Digital Library, 1, 564-74.

[17] Dalal, A. (2018). Cybersecurity And Artificial Intelligence: How AI Is Being Used in Cybersecurity To Improve Detection And Response To Cyber Threats. Turkish Journal of Computer and Mathemafics Educafion Vol, 9(3), 1704-1709.

[18] Mishra, S. (2023). Exploring the impact of AI-based cyber security financial sector management. Applied Sciences, 13(10), 5875.

[19] Yue, D., & Han, Q. L. (2019). Guest editorial special issue on new trends in energy internet: Artificial intelligence-based control, network security, and management. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49(8), 1551-1553.

[20] Devi, V. K., Asha, S., Umamaheswari, E., & Bacanin, N. (2023, April). A Comprehensive Review on Various Artificial Intelligence Based Techniques and Approaches for Cyber Security. In International Conference on Information and Communication Technology for Intelligent Systems (pp. 303-314). Singapore: Springer Nature Singapore.

[21] Jana, S., Biswas, R., Banerjee, C., Patra, T., Pal, M., & Pal, K. (2024). Leveraging Artificial Intelligence for Enhancing Cybersecurity: A Comprehensive Review and Analysis. Int. J. Adv. Res. Sci. Commun. Technol, 173-183.

[22] Tao, F., Akhtar, M. S., & Jiayuan, Z. (2021). The future of artificial intelligence in cybersecurity: A comprehensive survey. EAI Endorsed Transactions on Creative Technologies, 8(28).

[23] Farea, A. H., Alhazmi, O. H., & Kucuk, K. (2024). Advanced Optimized Anomaly Detection System for IoT Cyberattacks Using Artificial Intelligence. Computers, Materials & Continua, 78(2).

[24] Zhang, Z. (2025, February). Research on the Design of an Artificial Intelligence-Based Cybersecurity Automatic Early Warning System. In 2025 5th International Conference on Consumer Electronics and Computer Engineering (ICCECE) (pp. 652-657). IEEE.

[25] Awadallah, A., Eledlebi, K., Zemerly, M. J., Puthal, D., Damiani, E., Taha, K., ... & Yeun, C. Y. (2024). Artificial intelligence-based cybersecurity for the metaverse: Research challenges and opportunities. IEEE Communications Surveys & Tutorials, 27(2), 1008-1052.

[26] De Azambuja, A. J. G., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial intelligence-based cyber security in the context of industry 4.0—a survey. Electronics, 12(8), 1920.

[27] Nawaf, L., & Bentotahewa, V. (2025). Optimization of cyber security through the implementation of AI technologies. Journal of Intelligent Systems, 34(1), 20240226.

[28] Dapel, M. E., Asante, M., Uba, C. D., & Agyeman, M. O. (2023, January). Artificial intelligence techniques in cybersecurity management. In Cybersecurity in the Age of Smart Societies: Proceedings of the 14th International Conference on Global Security, Safety and Sustainability, London, September 2022 (pp. 241-255). Cham: Springer

International Publishing.

[29] Okdem, S., & Okdem, S. (2024). Artificial intelligence in cybersecurity: A review and a case study. Applied Sciences, 14(22), 10487.

[30] Alzahrani, A., & Aldhyani, T. H. (2023). Design of efficient based artificial intelligence approaches for sustainable of cyber security in smart industrial control system. Sustainability, 15(10), 8076.

[31] Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., ... & Choo, K. K. R. (2022). Artificial intelligence in cyber security: research advances, challenges, and opportunities. Artificial Intelligence Review, 55(2), 1029-1053.

[32] Sontan, A. D., & Samuel, S. V. (2024). The intersection of Artificial Intelligence and cybersecurity: Challenges and opportunities. World Journal of Advanced Research and Reviews, 21(2), 1720-1736.

[33] Merlano, C. (2024). Enhancing cyber security through artificial intelligence and machine learning: a literature review. Journal of Cybersecurity, 6, 89.

[34] Ofusori, L., Bokaba, T., & Mhlongo, S. (2024). Artificial intelligence in cybersecurity: a comprehensive review and future direction. Applied Artificial Intelligence, 38(1), 2439609.

[35] Haiping Si, Changxia Sun, Baogang Chen, Lei Shi & Hongbo Qiao. (2019). Analysis of Socket Communication Technology Based on Machine Learning Algorithms Under TCP/IP Protocol in Network Virtual Laboratory System. IEEE Access,7,80453-80464.

[36] Fatma Foad Ashrif, Elankovan A. Sundararajan, Mohammad Kamrul Hasan & Rami Ahmad. (2025). A Secure and Lightweight Group Mobility Authentication Scheme for 6LoWPAN Networks. Sensors,25(5),1458-1458.