Optimization of Network Security Intelligent Early Warning System Based on Image Matching Technology of Partial Differential Equation

Huan Wang[1] and Xin Li[2,*]

[1]*Modern Education Technology Center, Hebei University of Engineering, Handan, Hebei 056038, China*
[2]*Academic Journal Editorial Office, Hebei University of Engineering, Handan, Hebei 056038, China*
E-mail: Li_2726@163.com
[*]*Corresponding Author*

Received 16 November 2023; Accepted 16 December 2023;
Publication 09 April 2024

Abstract

In order to effectively avoid network information leakage and computer network paralysis, and improve the ability of computer network security early warning, it is necessary to design a computer network security intelligent early warning system based on network behavior. Security warning is considered as the second defense mechanism behind the firewall. It can monitor and warn the network without affecting the network performance, so as to provide real-time protection for external attacks, internal attacks and misoperations, and improve the network security. This paper designs an intelligent early warning system for network security based on partial differential equation image matching technology. The system adopts B/S development mode, and the server and browser are located in the campus network. Data fusion technology is used to assess network security, predict

Journal of Cyber Security and Mobility, Vol. 13_3, 461–488.
doi: 10.13052/jcsm2245-1439.1336

potential threats, and add new intrusion features to the feature database for subsequent use. In this paper, a target matching algorithm based on partial differential equation is proposed by using partial differential equation. The algorithm calculates the phase difference through the algebraic combination of orthogonal filter outputs. For scenes with continuous disparity changes, the error matching rate of this algorithm is lower than that of Michael Bleyer algorithm and vertical constraint algorithm. In general, the disparity map generated by this algorithm has high matching accuracy. The results show that the distribution of alarm information is reasonable and in line with the actual situation.

Keywords: Partial differential equation, image matching, network security, intelligent early warning system.

1 Introduction

With the rapid development of information technology, the application of web network is gradually becoming a new direction of the development of science, technology and economy in the new era, and the convenient performance of Web network can be used to give early warning to emergency events in various industries. It is not enough for a country to keep its vigilance and effectively defend against sudden attacks in cyberspace, just relying on traditional security protection technologies such as cryptography, trusted computing foundation, firewall, intrusion detection technology, etc. After the registered users are granted specific access rights and operation rights with the consent of the administrator, the workload of authorization management can be greatly reduced. In a specific organizational structure, roles are formed to meet specific tasks [1]. In order to effectively avoid the problems of network information leakage and computer network paralysis, and improve the computer network security early warning ability, it is necessary to design the computer network security intelligent early warning system based on network behavior. According to the current network security situation, users hope to predict future network attacks, identify the attacker's final attack intention, and give an early warning to the upcoming attacks. Monitor security-related activities by checking specific attack patterns, independent events, existing defects and other possible vulnerabilities [2]. Give an early warning to possible attack events, prevent intrusion, and stop intruders from controlling or destroying the network or host.

The wireless network optimization analysis system based on early warning and intelligence plays a huge role in daily optimization and special optimization. It is reflected in the active discovery and resolution of unknown problems. Second, it is reflected in the troubleshooting and solving of existing network problems. Network optimization personnel use the functional advantages of the optimization guide of the wireless network optimization analysis system based on early warning and intelligence. Through multi-dimensional correlation analysis of equipment alarm, performance indicators, parameters, adjacent cells, GIS, and MR data. Locate the causes of network problems, output solutions, and implement solutions. The verification and continuous adjustment shall be carried out repeatedly according to the implementation effect to ensure the implementation effect of the scheme. The wireless network optimization analysis system based on early warning and intelligence is accurate and complete in data query. The advantages in data analysis diversity and intelligent analysis are gradually recognized and recognized by front-line optimization personnel [3]. The platform is used more and more frequently in the optimization work in various cities. In the past, optimization data were collected and analyzed manually. The time period for analyzing the data of the whole network reaches 180 minutes, and through the data query and analysis function of the network optimization platform, the ability to optimize the collection and analysis of data has been greatly improved.

Traditional network security warning methods mostly use feature filtering technology, which identifies and alerts abnormal traffic by setting specific network traffic characteristics. However, this method often finds it difficult to deal with increasingly complex network attack methods, such as zero day attacks, advanced persistent threats (APT), and so on. Traditional filtering methods can to some extent eliminate noise, but their effectiveness in preserving image feature information is not ideal. The image denoising method based on partial differential equations can effectively balance the contradiction between denoising and preserving image structural information. The denoised image can achieve good visual effects. This article mainly studies the application of partial differential equations in image denoising. Therefore, this article proposes a network security intelligent warning system based on partial differential equation image matching technology, aiming to optimize the existing network security warning system. The innovative improvements of the method in this article are as follows:

1. This article starts from data and conducts in-depth analysis of network traffic data to discover the characteristics and patterns of network

attacks. Compared to traditional rule-based feature filtering methods, this data-driven approach can better adapt to increasingly complex network attack methods.

2. In this article, I introduced partial differential equation image matching technology, which treats network traffic data as images. By comparing the image features of normal traffic and abnormal traffic, accurate identification of abnormal traffic is achieved. This method can effectively deal with new attack methods such as traceless attacks and zero day attacks.
3. Through machine learning and deep learning algorithms, our system can automatically learn and optimize warning models, improving the accuracy and timeliness of warnings. In addition, we can dynamically adjust the warning model based on real-time changes in network traffic to adapt to changes in the network environment.

Section 1 describes the development background of web network information security. The wireless network optimization analysis system based on early warning and intelligence plays a huge role in daily optimization and special optimization. Section 2 cites relevant references to the conceptual framework of the network security early warning structure. Section 3 analyzes and designs the overall development of the intelligent network security early warning system. In the process of cluster fusion analysis, the mathematical verification of the theoretical basis of partial differential equation is carried out. Section 4 collects data from a company's internal network using network monitoring tools. The image matching algorithm combining the integrated feature consistency model and phase correlation is used to match target images with different sizes, numbers and rotation angles, which shows that the algorithm has good versatility. The parallax image obtained by this algorithm has clear boundary, accurate positioning, and the parallax in low texture areas has been recovered well. Section 5 summarizes the full text, and the results show that the network security intelligent early warning system designed in this paper based on partial differential equation image matching technology is reasonable and in line with the actual situation.

2 Related Work

At present, the research on network information security early-warning system in China is still in its infancy, which transforms the passive prevention of network security into active defense. Therefore, it is necessary to research and develop the early warning system. The network security early warning structure includes user network behavior collection module, server security center module, system administrator module, etc., aiming at the usage behavior, the characteristic values that can represent and measure the usage behavior are obtained through research, and the usage behavior is described quantitatively. In order to maintain national information security, carry out research on resisting information attacks and tracking and counterattacking information attacks, and establish a perfect intelligent early warning system for network security is an effective way to ensure the normal operation of the national network system itself [4–6]. Yu et al. put forward the concepts of threat assessment, indication and alarm of information warfare attacks, and the conceptual framework of an open information source decision support system [7]. Zhao et al. predicted the attack by constructing the attack outline, which included the historical activities of the attack, attack tools, operation steps, targets, motives and so on. However, it costs a lot to construct the attack profile network [8]. Wu designed and studied the network security situation awareness system, which is a new technology to realize network security detection and early warning [9]. With the rapid development of computer stereo vision in recent years, stereo vision matching algorithm is a very important and difficult problem [10, 11]. At present, binocular vision is a hot research topic in the field of computer vision. This research is to apply the binocular vision system of human eyes to computer vision, so that it can achieve and surpass the effect of human eyes. Wang et al. put forward an improved Moravee operator, and the experiment shows that this operator is stable when the image is rotated, illuminated and perspective deformed [12]. Tang et al. put forward a hierarchical image matching algorithm based on wavelet transform, which extracts points of interest from each decomposed image to match, and further improves the speed by using parallel strategy [13]. HongbinWANG et al. summarized the progress of stereo matching in 1980s, including a large number of new matching methods, the introduction of hierarchical processing concept, and the use of trinocular constraints to reduce the ambiguity of stereo matching [14]. Yang et al. summarized and discussed the problems of dynamic stereo and active stereo, early occlusion and no texture, and the realization of real-time stereo vision [15]. Yan et al. summarized the corresponding point matching algorithm from the angle of geometric calculation, focused on the matching solution of occlusion problem, and discussed the actual platform of real-time stereo vision in typical applications [16].

Security early warning is a kind of proactive security protection technology, which provides a useful supplement to firewall and other protection mechanisms, such as providing real-time protection against external attacks, internal attacks and misoperation. Security warning is considered as the second layer of defense mechanism after firewall, which can monitor and warn the network without affecting the performance of the network, thus providing real-time protection against external attacks, internal attacks and misoperation, and improving the security of the network. Early warning plays an increasingly important role in this link. Early warning is mainly to predict potential or possible network threats according to the signs of network threats such as abnormal network traffic, abnormal network operation, virus threats, etc., and issue an early warning or issue a global warning through an early warning mechanism according to the local network threats that have occurred. Relatively speaking, the foreign computer network system appeared early, and the network system institutions were relatively perfect, and a large-scale network security intelligent early warning system market has been formed [17, 18]. However, the development of intelligent early warning system of network security by foreign enterprises is only aimed at the network security of our company. Early warning technology should be used to monitor and identify intrusion attempts and behaviors on large-scale protected networks, and corresponding defense measures should be taken in advance to strengthen network security before the intrusion occurs or causes serious consequences. According to the fixed pattern, the network intelligent early warning system can find the correlation between the network alarm information and the inherent law of the machine, make an accurate judgment on the attack intention of the final attacker, and realize timely and effective alarm. Network security intelligent early warning system has the characteristics of real-time dynamic and active intrusion prevention, so it can make up for the shortcomings of other static network security tools.

3 Research Method

3.1 System Requirement Analysis

With the help of network computers, computers scattered in different places can establish corresponding communication and network resource sharing. Through the scanning of vulnerabilities and viruses in the computer system, the system data is tested, audited and evaluated, so as to analyze and identify the user's own use behavior. Then, when there are abnormal behaviors in the use of the computer network, by tracking the records and behavior analysis in the use process, the attack characteristics can be added to the computer security system, which is convenient for later query, analysis and statistics. At the same time, based on the users' network usage habits, effective analysis and prediction are carried out. Finally, combined with the analysis results, information is sent to the early warning system, so as to ensure the security of the computer network. According to the needs of its operation, annotation and data simulation are put forward. The concept of workflow is closely related to computer, and its definition needs the help of computer technology. At the same time, the operation, management and information transmission of workflow all need the support of computer technology.

The overall development purpose of the intelligent network security early warning system is to establish an all-round and all-weather network security detection and prevention system that can include monitoring systems and early warning centers in all network areas. As a network security system that can be handed over to each other, it has a multi-level security early warning mode. As the third-level early warning mode of network security protection. Networks at all levels can cooperate with each other, and establish unified protective measures with the superior network early warning center, taking into account the occurrence of special circumstances. In a well-divided network area, such as security devices, hosts, routers, etc. in the area, the network warning center needs to observe the working status of these devices in real time and scan the potential threats of these devices. It is the distributed network security intelligent early warning system that needs to have the ability to prevent hackers from invading. At the same time, when being attacked by hackers, it can take corresponding measures to make up for the losses caused by network attacks in time. At the same time, it can back up the corresponding attack information in the network database, which can cause faster response ability in the next attack.

The network intelligent early warning system takes the original network packet as the data source to monitor and analyze all communication services through the network in real time. Analyze the online alarm information, adopt the method of data fusion, and combine with the safety information database to reduce the number of false positives, false positives and alarms. Discover whether there are signs of violating security policies and being attacked in the network or system. At the same time, we can find potential threats and predict possible virus invasion and network attack. Assess the threat degree of network attack. The system administrator can effectively monitor and evaluate the network system. It can capture and detect network packets in real time. The distributed security early warning system is composed of multiple regional early warning centers distributed in the network. Each regional early

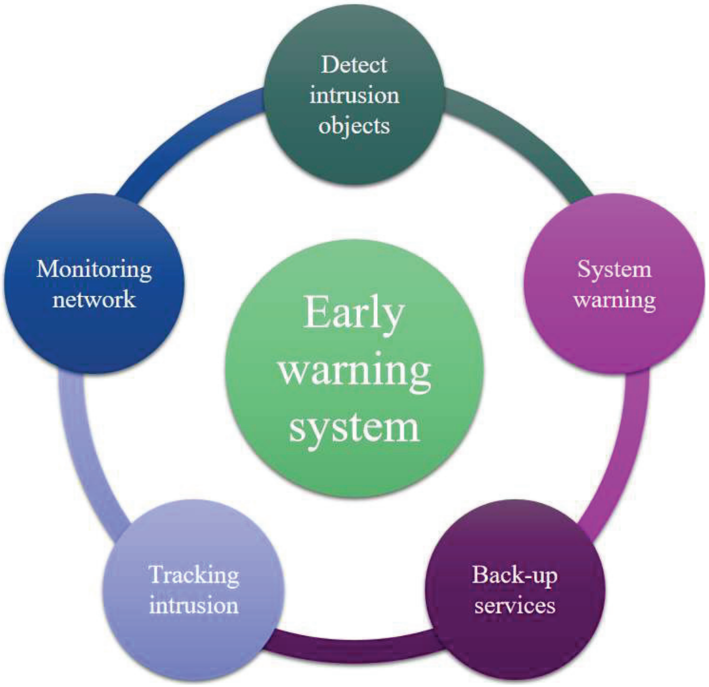

Figure 1 Overall function analysis of the system.

warning center integrates alarm information and can work independently and cooperate with each other.

Network demand distribution means that the network security intelligent early warning system can monitor all kinds of data information flowing into the network area at any time, control the data flow in and out of the network system according to the current network situation, and make normal access to the system. The overall function analysis of the system is shown in Figure 1.

Establish an early warning mechanism, that is, by monitoring the network data stream in real time, identifying and recording intrusion and destructive access and operation, and by analyzing and processing the data, making an alarm level, providing various alarm modes, classifying threat events, and making statistics and analysis of threats. Establish a tracking mechanism, that is, judge the trail of the attacker and the intruder, locate the location of the attack source, and infer the route of the attacker in the network, so as to provide valuable information for the system's event handling and response, and provide sufficient evidence for forensic work afterwards.

The wireless network optimization analysis system based on early warning and intelligence plays a huge role in daily optimization and special optimization. It is reflected in the active discovery and resolution of unknown problems, and the second is reflected in the investigation and resolution of existing network problems. Network optimization personnel make use of the functional advantages of the optimization wizard of the wireless network optimization analysis system based on early warning and intelligence. Through multi-dimensional correlation analysis of equipment alarm, performance indicators, parameters, adjacent cells, GIS, and MR data. The cause of network problems shall be located, the scheme output and the scheme implementation shall be carried out, and the verification and continuous adjustment shall be carried out according to the implementation effect to ensure the implementation effect of the scheme.

Through the analysis of users' network usage behavior, not only can network managers have a better understanding of users' usage behavior research, but also the necessary information warning for the prediction of users' behavior, so as to ensure that the formulated strategies have sufficient basis for reference. The systematic behavior prediction can effectively predict the future behavior of users by systematically learning the changes of users' network usage behavior and combining the corresponding laws.

3.2 Overall Design of Network Intelligent Early Warning System

Network security intelligent early warning system is to monitor the intrusion detection devices in the network, monitor the threat entities in a large range, analyze the collected information effectively, discover the intrusion tendency and potential threats of the attackers in time, evaluate the threat level, and provide effective tools to respond to emergencies in time. The intelligent early warning system of network security designed in this paper detects the intrusion behavior in the network through the monitoring center module, evaluates the network security situation based on the detected intrusion attacks, and predicts the influence range of possible future attacks [19]. To realize network security early warning, it is necessary to capture messages, compress alarm data, analyze the causality of alarms, extract potential threats by using data fusion and other technologies, and make early warning and inference to the global network according to these local threat information, and cooperate with the response system to make early warning to all threats. In this paper, the command of the monitoring center is used to send an early warning to each detection domain, and the response module is used

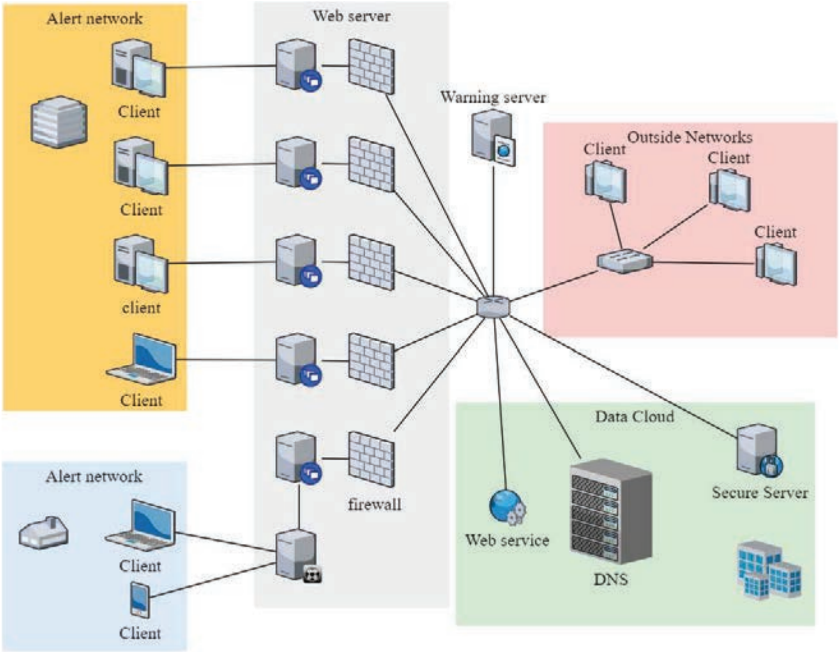

Figure 2 Flow chart of network security intelligent early warning system.

to implement the response program to crack the possible future attacks and conduct threat assessment. B/S development mode is adopted, and the server and browser are located in the campus network. The server Linux is used as the development platform, responsible for network data capture, filtering, intrusion detection analysis and early warning. The browser is responsible for displaying the running results of the functional modules to the user with an intuitive interface.

Figure 2 shows the analysis of the workflow of the network security intelligent early warning system.

The workflow of the system is described as follows: the monitoring center collects data, judges the attack, sends the alarm information to the regional early warning center, uploads the determined intrusion information to the early warning center after reduction and other processing, and the early warning center performs relevant processing to remove redundancy and repeated alarms. The data fusion technology is adopted to evaluate the network security, predict the potential threats, and add the new intrusion features to the feature database for subsequent use. The whole system contains many regional early warning centers, which can receive the information from the detection system and deal with it accordingly. These regional early warning centers can work independently and cooperate with each other at the same time.

Data sources can be divided into host data and network data. These two data sources have their own characteristics and are complementary in their respective application fields. Here, we mainly use network data as the data source of network security intelligent early warning system. In Ethernet, all communication is broadcast, which means that all network interfaces in the same network segment can access the data transmitted on the physical media. Each network interface in the network has a unique hardware address, which is the MAC address of the network card. In a practical system, the network card sends and receives data, and the system judges whether to accept it or not according to the acceptance mode set by the network card driver.

In this paper, this kind of linkage system between repeated and concurrent events is called redundant relationship. Therefore, according to the repeated and concurrent merging granularity, the events belonging to redundant relationship can be filtered and merged layer by layer according to the attribute characteristics corresponding to each granularity, thus effectively reducing the number of original alarm events.

First of all, before the cluster fusion analysis, the alarm information should be verified and merged. After merging, the output alarm event set x is obtained. There are:

$$x = f(x_1, x_2, \ldots, x_n) \tag{1}$$

$(x_1, x_2, \ldots, x_n)$ is the alarm information satisfying a certain redundancy relationship in the network, and f is the process of merging redundant information, and it is the merged output alarm information. This process is called redundant merging process.

Each piece of alarm information can be expressed as a vector:

$$D_i = (T_{i1}, T_{i2}, \ldots, T_{ij}) \tag{2}$$

i, j is the subscript of the ith vector and the jth attribute, the parameter n is the vector length, and T_{ij} is the value of each component.

$$SIM(D_1, D_2) = \frac{\sum_{j=1}^{n} E_j SIM(T_{1j}, T_{2j})}{\sum_{j=1}^{n} E_j} \tag{3}$$

D_1, D_2 is the alarm vector to be matched, T_{1j}, T_{2j} is the characteristic component of the alarm vector, and E_j is the matching weight of each characteristic component, which depends on the influence degree of the characteristic component in the overall matching.

Among these rules, there are many rules with strong correlation, and the frequency of these rules is very high. Traditional data association algorithms have very important advantages in mining these rules. This paper introduces the concept of interest degree to explain the meaning of this aspect:

Interest degree: the support degree of association rule analysis $X \Rightarrow Y$ of set D:

$$S = Support(X, Y) \tag{4}$$

Given the confidence level as:

$$C = \frac{Support(X \cup Y)}{Support(X)} \tag{5}$$

Related expressions of interest:

$$I_R = \frac{Support(XY)}{Support(X)Support(Y)} \tag{6}$$

Due to the detection of known attack types, misuse detection has a high detection rate, but the effect of misuse detection for unknown and new attacks is not ideal. Therefore, misuse detection is performed first, and then anomaly detection is performed. Here, we adopt the detection method of combining misuse detection with anomaly detection. The specific implementation process is shown in Figure 3.

The anomaly detection module uses the association rule algorithm to mine the frequent patterns in the connection record database. For these frequent patterns, add attachment features, such as host statistical features, time statistical features, etc., for connecting a record. If the similarity is greater than the specified threshold, it is determined that the current behavior is normal, and the normal pattern library is updated.

If the similarity is less than the specified threshold, it is considered as an attack intrusion or an attack, and an alarm response is made. The tracking module adopts information tracking technology, and its goal is to judge the trail of attackers and intruders, locate the location of the attack source, and deduce the route of attackers in the network. Thereby providing valuable information for the event processing and response of the system.

In general network management system, event correlation focuses on detecting the alarm information caused by network failure, and the format of these alarm information is relatively fixed. In the network security intelligent

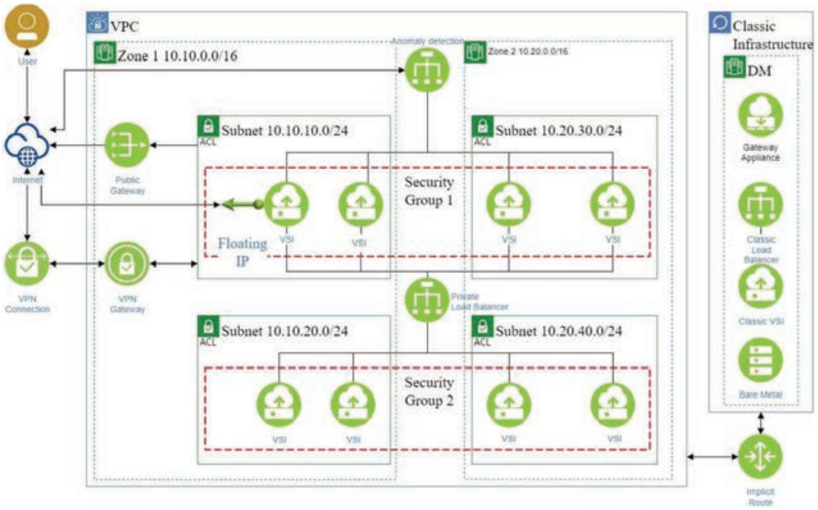

Figure 3 Intrusion analysis model based on data mining.

early warning system, the attacker's attack strategy is more complicated and unpredictable, so it is more complicated to realize alarm correlation in the early warning system. The evaluation of any one of them includes two parts: one is to calculate the corresponding attack energy, and the other is to divide the network into different security levels according to the calculated attack energy value. In this system:

$$e = f(\theta_h, \lambda, c, \delta_t) = (\ln 15)^c \theta_h \cdot \delta_t \cdot (\ln 10)^\lambda \tag{7}$$

Among them, c is the level of attack type. According to the definition of snort rule set, it can be divided into three levels: high, medium and low. θ_h is the importance level of monitoring the attack target host in the network. λ indicates whether the target host is an attack springboard or not. δ_t is the importance weight of the attack time period.

The method of evaluating the attack energy E_{att} of the object is as follows:

$$E_{\mathrm{att}} = \sum_{j}^{N} e_j \tag{8}$$

Monitor the attack energy generated by a certain type of attack in the network in ΔT time. Where N is the number of such attacks in ΔT, and e_j is the attack energy of each attack.

3.3 Key Technology Realization

In the network topology of the early warning system based on network security incidents, a network contains many kinds of nodes, such as subnets, routers, switches and various servers. In a subnet, it can also contain subnets, routers, switches, etc. In this way, the whole network topology can be represented by a "whole-part" hierarchical structure, so the design method of combination mode can be adopted. When the application program needs to call this algorithm, it will make the application program extremely large and difficult to maintain, occupying system resources and affecting the running effect of the system. In addition, different situations require different algorithms, and if all algorithms are hard coded into classes, the program will become bloated, which is difficult to understand and maintain. We often only need an object instance of database connection pool to realize the connection with the database. Therefore, in the implementation of database connection, we adopt the single-piece pattern to design the data connection class.

Once there is peak data or abrupt data, the data will be compared and judged according to the environmental attributes of the monitored side to determine whether it is abnormal data. The early warning system based on web network can set the permission of different users according to the level of users, and only the authorized personnel can access the database, query and modify the data. A new detection model is generated by learning, and once a new detection model is generated, the new model is sent to the anomaly evaluation module. Therefore, when the data collection is stopped, the records of data collection can be viewed through the database administrator page. This indicates that the structure of the test meets the expectation, and that the early warning system can realize the function of early warning of computer network security.

In the process of machine recognition, it is often necessary to register all or part of known images with unfamiliar images in space. According to an image with a known pattern, the process of finding a sub-image corresponding to this pattern in an unfamiliar image is called image matching. Image matching is a multi-step process. Generally, the image should be pre-processed, mainly noise filtering. As a new method in spatial domain filtering, image filtering based on partial differential equation can adapt to smooth filtering according to different structure information of image. Under the premise of effective noise filtering, the edge structure information of the image can be well preserved. Such methods have been widely used in image denoising, image restoration, etc. This paper mainly studies the theoretical basis and methods based on partial differential equations. At the same time, some progress has been made in applying nonlocal filtering methods to this kind of methods. It has promoted the development of other image processing technologies and some mathematical theories. Then, according to the selected matching method, the features of the template and the image are extracted, and the high-dimensional data of the image and the template will be reduced to low-dimensional feature vectors. Then, according to the search strategy, the feature set of the image and the template is matched, and finally the matching result is obtained [20].

Generally, the following relationship exists between the template T that requires image matching and the potential matching object P:

$$\begin{pmatrix} \hat{x} \\ \hat{y} \end{pmatrix} \approx \begin{pmatrix} \beta_{11} & \beta_{12} \\ \beta_{21} & \beta_{22} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} \tag{9}$$

Where $(x, y) \in T$, $(\hat{x}, \hat{y}) \in P$, $\alpha_i, \beta_{i,j}$ are constants, "$\approx$" the difference between the two sides can be approximated by a higher-order polynomial related to (x, y) and its neighborhood.

When the assumption that the local structure of the image exists is not valid, the phase matching algorithm loses its effectiveness because the amplitude of the band-pass output signal is too low, that is, the problem of phase singularity. When the output of the filter is zero, the phase cannot be determined, that is, the phase output is singular. To solve this problem, the improved method usually detects and eliminates phase singularities through certain threshold conditions.

For phase-based stereo matching, the parallax can only be determined when the effective maximum parallax does not exceed the half wavelength of the filter. In the coarse-fine pyramid matching framework, for the l-layer, the effective parallax maximum is 2^{l-1} times of the half wavelength of the filter of this layer, that is:

$$d_{\max} = 2^{l-1} \cdot \frac{\pi}{w_c^l} \tag{10}$$

It is noted that the cosine value of phase deviation at the point of phase consistency is very large, while the absolute value of phase deviation sine is very small, and the gradient of sine is the largest at the origin. Therefore, the sine value of the phase deviation can increase the sensitivity of the phase consistency. Change the phase deviation function for calculating phase consistency to:

$$\Delta\Phi(x) = \cos(\Phi(x) - \bar{\Phi}(x)) - |\sin(\Phi_n(x) - \bar{\Phi}(x))| \tag{11}$$

$\Phi(x)$ is the energy proportional to the phase angle, and $\bar{\Phi}(x)$ is the average phase angle.

The selection of matching algorithm has great influence on image matching results, and practical matching algorithm not only requires less computation, but also has good anti-noise ability and anti-geometric deformation ability. Therefore, this paper proposes an object matching algorithm based on phase correlation by combining frequency domain matching algorithm with image feature extraction method by using partial differential equation. In this algorithm, the phase difference is calculated by algebraic combination of the outputs of orthogonal filters, and the main part of the phase difference is directly obtained. There is no need to explicitly calculate the local phase of the left and right images, which greatly reduces the amount of calculation and has a high computing speed. The flow chart is shown in Figure 4.

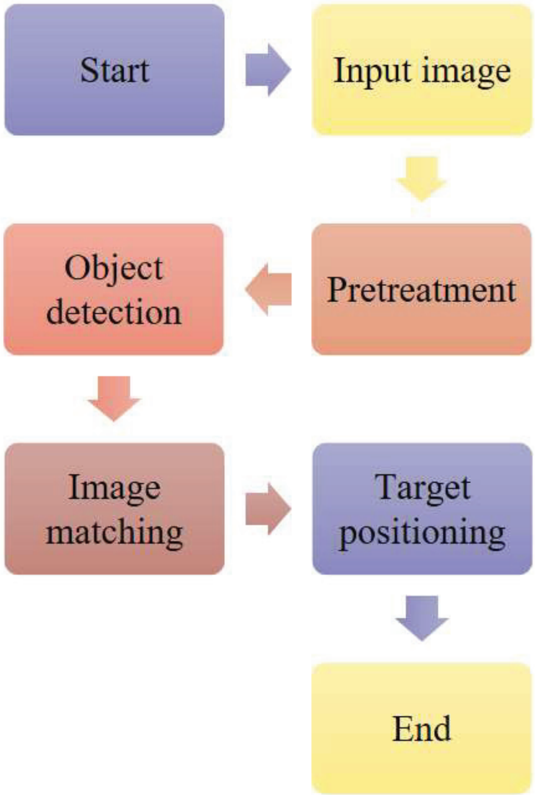

Figure 4 Flow chart of target matching algorithm.

Geometric operations can change the spatial relationship of objects in an image, which can be regarded as moving objects in the image. The general definition of image operation is:

$$g(x, y) = f(u, v) = f(p(x, y), q(x, y)) \tag{12}$$

Where, $u = p(x, y), v = q(x, y)$ uniquely describes the spatial transformation, that is, the input image $f(u, v)$ is transformed from (u, v) coordinate system to the output image $g(x, y)$ in (x, y) coordinate system.

According to the translation invariance, the objective function is constructed, and the local motion of the image is finally estimated by the optimized strategy. It is assumed that the following relationship is satisfied between two corresponding blocks of two quadlet wavelet transform image pairs:

$$O_t(x, y) = O_r(x + r_1(x, y), y + r_2(x, y)) \tag{13}$$

Where $r_1(x, y), r_2(x, y)$ is the translation amount of each pixel point corresponding to the direction respectively.

In addition, to avoid explicit phase calculation, the local frequency Φ_l', Φ_r' can be calculated as follows according to the method in reference:

$$\Phi_l'(x) = \frac{R_{G,c} dR_{G,s}|dx - R_{G,s} dR_{G,c}|dx}{R_{G,c}^2 + R_{G,s}^2} \tag{14}$$

$$\Phi_r'(x) = \frac{L_{G,c} dL_{G,s}|dx - L_{G,s} dL_{G,c}|dx}{L_{G,c}^2 + L_{G,s}^2} \tag{15}$$

For each area obtained by color segmentation, the accurate parallax plane is estimated according to the initial parallax map obtained after parallax left-right consistency detection. Each parallax plane has three parameters, $\theta_1, \theta_2, \theta_3$, to characterize the relationship between parallax $disp$ and pixel coordinates (x, y) in the reference image, as shown in formula (16):

$$disp(x, y) = \theta_1 x + \theta_2 y + \theta_3 \tag{16}$$

Where $disp(x, y)$ is the parallax at the pixel (x, y), and $\theta_1, \theta_2, \theta_3$ is the plane parameter of the parallax plane to which the pixel (x, y) belongs.

This is a symmetric object with size t at the origin. The convolution result of scale n at the origin is:

$$I_n(0) = \left(\int_{-t}^{t} g_n(x) dx \right) + 0i \tag{17}$$

4 Analysis and Discussion of Results

This article uses various tools and software for network monitoring and data collection. Based on specific network architecture and monitoring requirements, the network monitoring tools used include Zabbix and Nagios. These tools can provide real-time monitoring and data collection of network traffic, device status, security events, and more. For the experimental simulation of the target matching algorithm, programming languages and tools such as Matlab or Python were used to achieve it. These tools have powerful numerical calculation and signal processing capabilities, making it easy to implement complex algorithm logic and conduct simulation experiments. This article uses network monitoring tools to collect data from the company's internal network. These tools can monitor network traffic and collect data related to target matching algorithms. We monitored the network traffic between two detection points in the company and collected data related to phase difference calculation. There may be log files in the company's network system that record network activities and events. These log files can provide data information about target matching algorithm experiments, such as detecting satellite settings, events and anomalies during the experiment process, etc. This test simulates setting up two important detection points in a company's internal network, and setting up corresponding detection satellites in the corresponding workstations, so as to simulate the experimental process. This test needs to make detailed statistics on the original data of the monitoring center, the alarm data generated by the regional early warning center, and the alarm levels and the number of alarms generated in each time period, with one hour as the statistical time period.

According to the process of regional early warning center's alarm fusion, count the number of original alarms in monitoring center, pre-processed alarms in regional early warning center and alarms at various levels after situation assessment in one hour, and count them once a day. The corresponding data are stored in Table 1. Figure 5 shows the comparison data of alarm numbers in each stage of early warning.

It can be seen that the alarm fluctuates greatly, and the number of alarms rises sharply in a certain period of time, up to 3,348 alarms at most. After pretreatment, the number of alarms decreases greatly, and tends to be stable, with few great fluctuations, which shows that the distribution of generated alarm information is reasonable and accords with the actual situation.

This paper illustrates the effectiveness of this algorithm from several aspects: the image matching algorithm combining comprehensive feature consistency model and phase correlation is used to match images with

Table 1 Alarm quantity in each stage of early warning

Time	Original Alarm	Pre-processed Alarm Situation	Notification
2:12	2732	38	2137
3:12	371	5	2133
4:12	1070	35	1629
5:12	2431	28	411
6:12	1685	2	254
7:12	1115	13	1687
8:12	2431	12	1530
9:12	125	21	119
10:12	374	13	942
11:12	1855	3	3244
12:12	2050	9	683
13:12	2266	34	2761
14:12	1281	30	3196
15:12	1487	37	338
16:12	1922	37	631
17:12	754	6	1457
18:12	3304	42	105
19:12	207	15	1897
20:12	212	38	2868
21:12	504	6	1206
22:12	3197	20	1190
23:12	2641	41	452
0:12	3348	5	1761

different sizes, numbers and rotation angles of targets, which shows that this algorithm has good universality; The matching of images with different brightness and contrast shows that the algorithm is invariant to the brightness and contrast of images. The calculation depends on the image filtering results after each iteration of de-noising. After iterative operation, the error between the similarity measure between two image slices and the similarity measure between the two in the original noiseless image becomes smaller and smaller. The smaller the error is, the more accurately it represents the similarity in the image. Iterative nonlocal filtering makes use of image similarity in the process of denoising. This method has a good effect on protecting the texture and edge structure of the image.

In order to get the rotation of the image, this paper combines Fourier-Mellin transform to make an experiment. Image matching results are shown in Table 2 and Figure 6.

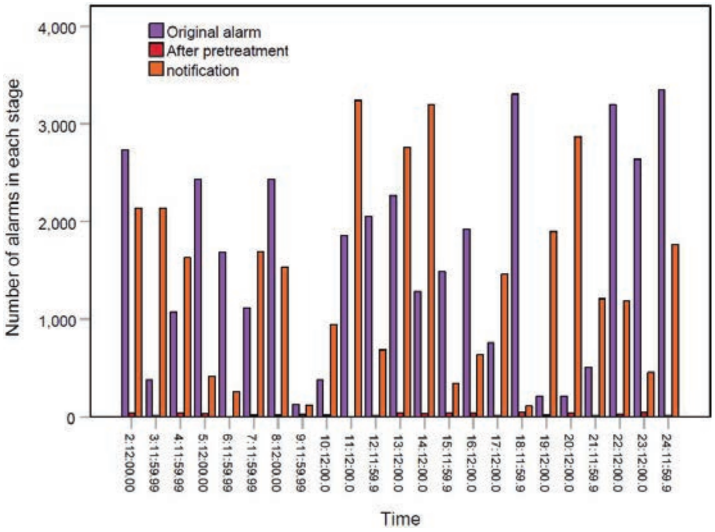

Figure 5 Comparison data chart of alarm number in each stage of early warning.

Table 2 Transform experimental results

Serial Number	Rotation Preset Value	Rotation Calculated Value	Scale Transformation
1	34.409	23.131	0.999
2	−18.066	−38.884	0.982
3	36.882	−14.78	1.178
4	25.274	13.584	0.965
5	24.217	10.541	1.012
6	−6.154	−33.359	1.17
7	10.156	−27.817	1.195
8	−21.308	−26.567	0.93
9	−5.771	6.014	0.962
10	14.252	−9.253	0.949
11	5.949	24.968	1.204
12	23.21	5.651	1.011
13	37.999	5.577	1.146
14	32.341	17.929	1.098
15	48.421	−34.197	0.965
16	32.767	−22.56	0.988
17	4.483	−31.109	1.05
18	−9.283	14.454	1.178
19	3.686	−14.445	1.06
20	23.835	−33.978	1.136

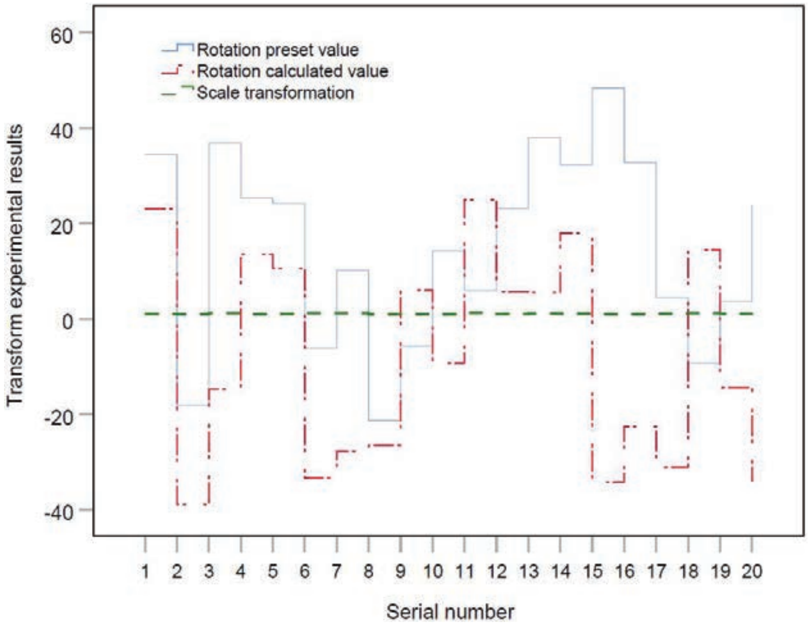

Figure 6 Transform the curve of experimental results.

The experimental results show that combining Fourier-Mellin transform, the image matching effect is better in accuracy and time. It is suitable for the registration between two images with rotation transformation. It should be noted that the image should be within the allowable range of scale transformation of 0.9∼1.15. If it exceeds the range, the matching effect will be poor.

Matching Hough spectrum has the characteristics of translation, rotation, scaling and periodicity, which makes it suitable for image registration. In order to verify its performance, a lot of experiments have been done on the shapes provided by SIID shape set. Figure 7 is the Hough spectrum representation of the corresponding shape. The experimental results show that the registration method based on Hough spectrum has good registration effect and accuracy for any complex shape.

In order to further verify the influence of noise on the registration accuracy, different levels of zero-mean Gaussian white noise are added to the image of the shape to be registered. The actual translation, scaling and rotation parameters are (−12, −8) pixels, 1.5., 11 degrees, which are respectively registered with the template shape. The results are shown in Table 3.

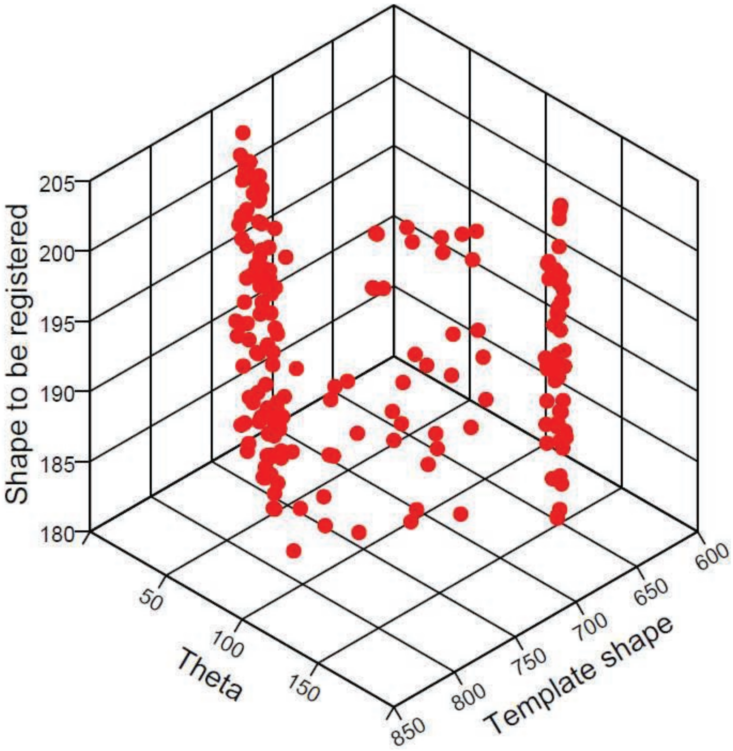

Figure 7 Hough spectrum representation of shape.

Table 3 Registration results in different noise levels

Group	Noise Variance	Translation (Pixels)	Zoom	Rotation Parameter(°)
1	0.226	(−12, −8)	1.218	10
2	0.436	(−12, −8)	1.255	12
3	0.569	(−12, −8)	1.366	10
4	0.736	(−18, −8)	1.471	11

When a moderate zero-mean white Gaussian noise is added to the shape to be registered, it has no significant influence on the translation and rotation parameters of the registration, and has little influence on the scaling parameters. When the noise is large and the noise variance is 0.736, the noise has a great influence on the registration result. Generally speaking, the registration method based on Hough spectrum has strong anti-noise ability.

In order to test the effectiveness of the algorithm, this paper uses standard test pictures for experiments and compares them with several typical

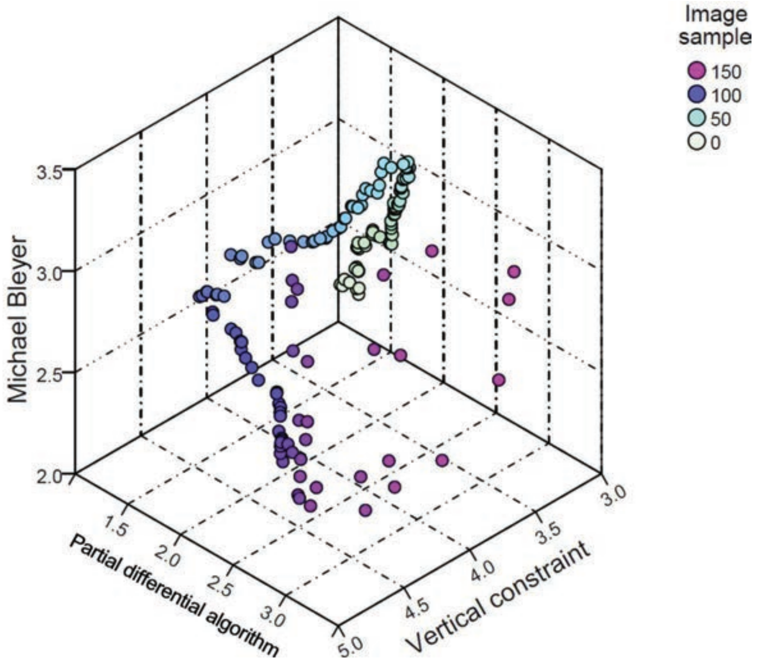

Figure 8 Comparison of mismatch rates in non-occluded areas.

algorithms. Accuracy comparison of target matching algorithm is shown in Figures 8 and 9.

It can be seen from the figure that the disparity map obtained by this algorithm has clear boundary and accurate positioning, and the disparity in the low texture area has been well restored. For scenes with continuous disparity changes, the error matching rate of this algorithm is lower than that of Michael Bleyer algorithm and vertical constraint algorithm. Generally speaking, the disparity map generated by this algorithm has high matching accuracy. Although the accuracy is high, the execution time of the algorithm is long, which is mainly related to the segmentation time of the mean shift algorithm.

In the field of network security, this image matching technology based on partial differential equations can be used to identify and match abnormal patterns in network traffic. For example, it can be used to detect complex network attacks such as zero day attacks and advanced persistent threats (APT). By collecting traffic data in the network and using this image matching technology for analysis, abnormal traffic patterns can be effectively identified, so

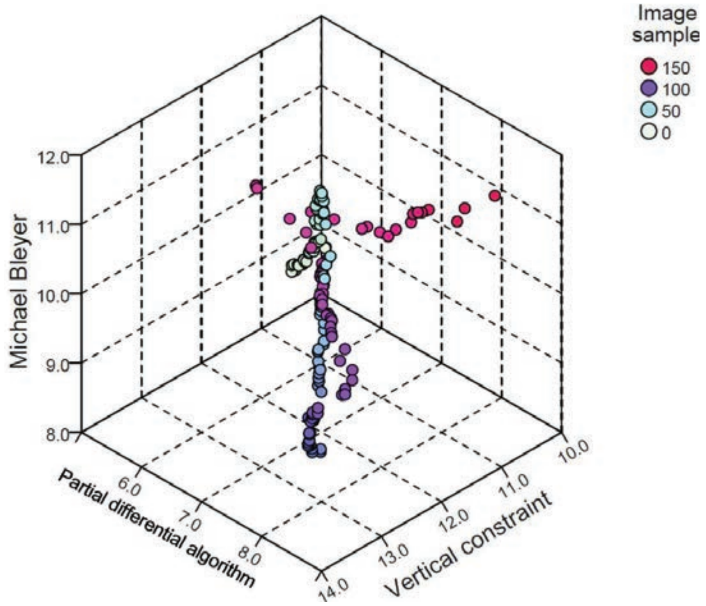

Figure 9 Comparison of parallax boundary mismatch rate.

that early warnings can be triggered in time to help network security experts take corresponding defensive measures.

In addition, this technology can also be integrated with other network security technologies to form a comprehensive network security protection system. For example, it can be integrated with intrusion detection system (IDS), firewall and other security devices or systems to form a multi-layer defense system. In this case, the image matching technology based on partial differential equation can provide in-depth analysis and recognition of network traffic, while other security devices can provide more extensive and preliminary protection to jointly achieve effective protection of network security.

5 Conclusion

At present, the research on network information security early-warning system in China is still in its infancy, which transforms the passive prevention of network security into active defense. Therefore, it is necessary to research and develop the early warning system. In this paper, an intelligent early warning system of network security based on partial differential equation image matching technology is designed. This system adopts B/S development mode, and the server and browser are located in the campus network. The server Linux is used as the development platform, which is responsible for network data capture, filtering, intrusion detection analysis and early warning. The whole system contains many regional early warning centers, which can receive the information from the detection system and deal with it accordingly. These regional early warning centers can work independently and cooperate with each other at the same time. After pre-processing, the number of alarms is greatly reduced, and tends to be stable, with few great fluctuations, which shows that the distribution of generated alarm information is reasonable and accords with the actual situation. For scenes with continuous disparity changes, the error matching rate of this algorithm is lower than that of Michael Bleyer algorithm and vertical constraint algorithm.. Generally speaking, the disparity map generated by this algorithm has high matching accuracy. However, in terms of algorithm robustness and scalability, image matching methods based on partial differential equations may face challenges when dealing with complex network traffic data. Although some improvement measures such as data-driven and intelligent warning are mentioned in the article, the efficiency and accuracy of algorithms may be affected when facing large-scale and high complexity network traffic data. Future research can further explore how to improve the robustness and scalability of algorithms to adapt to larger and more complex network environments.

Acknowledgement

This research is based on the 2022 Industry-University Cooperative Education Project of the Ministry of Education, “Development and Application of Online Distance Education Platform Based on Green Campus Construction”, (No. 220902251235901).

This research was granted by Journal of Colleges and Universities of Hebei Province, “Research on the Influence of WeChat Public Platform from the Perspective of Planning Behavior Theory”, (No. HBXB2022ZD007).

References

[1] Yi M, Xu X, Xu L. An intelligent communication warning vulnerability detection algorithm based on iot technology. IEEE Access, 2019, 7(99), 164803–164814.

[2] Behi M, Ghasemigol M, Vahdat N H. A new approach to quantify network security by ranking of security metrics and considering their relationships. International Journal of Network Security, 2018, 20(1), 141–148.

[3] Vajjha H, Sushma, P. Techniques and limitations in securing the log files to enhance network security and monitoring. Solid State Technology, 2021, 64(2), 1–8.

[4] Einy S Oz C, Navaei Y D. The anomaly- and signature-based ids for network security using hybrid inference systems. Mathematical Problems in Engineering, 2021, 2021(9), 1–10.

[5] Lin P, Chen Y. Network security situation assessment based on text simhash in big data environment. International Journal of Network Security, 2019, 21(4), 699–708.

[6] Li Y, Hua N, Li J, Zhong Z, Zheng X. Optical spectrum feature analysis and recognition for optical network security with machine learning. Optics Express, 2019, 27(17), 24808.

[7] Yu J, Hu M, Wang P, Sundhararajan M, Gao X. Z, Nejad H. V. Evaluation and reliability analysis of network security risk factors based on d-s evidence theory. Journal of Intelligent & Fuzzy Systems, 2018, 34(2), 861–869.

[8] Zhao D, Song H, Li H. Fuzzy integrated rough set theory situation feature extraction of network security. Journal of Intelligent and Fuzzy Systems, 2021, 40(1), 1–12.

[9] Wu D. A network security posture assessment model based on binary semantic analysis. Soft Computing, 2022, 26(20), 10599-10606.

[10] Jiang C. Network security and ideological security based on wireless communication and big data analysis. Wireless Communications and Mobile Computing, 2022, 2022(3), 1–6.

[11] Kou G, Wang S, Tang G. Research on key technologies of network security situational awareness for attack tracking prediction. Chinese Journal of Electronics, 2019, 28(01), 166–175.

[12] Wang Z, Fang B. Correction to: application of combined kernel function artificial intelligence algorithm in mobile communication network security authentication mechanism. The Journal of Supercomputing, 2019, 75(9), 5965–5965.

[13] Tang D, Jing W, Ma J, Zhou B, Qian L J. Design of high average power opcpa based on simultaneous temperature and wavelength insensitive phase-matching. IEEE Photonics Journal, 2018, 2018(99), 1–1.

[14] Hong B W, Zhi L Z, Hua F L. Image-text cross-modal matching method based on stacked cross attention. Journal of Signal Processing, 2022, 38(2), 285–299.

[15] Yang J, Wen C K, Ji S, Gao F. Beamspace channel estimation in mmwave systems via cosparse image reconstruction technique. Communications, IEEE Transactions on, 2018, 66(10), 4767–4782.

[16] Yan, J H, Wang, J C, Zhang Y. Remore sensing image quality assessment based on the ratio of spatial feature weighted mutual information. Journal of Imaging Science and Technology, 2018, 62(2), 20505.1–20505.12.

[17] El H H M, El R W. A, El S W, El R E, Mahmoud K R, El S F A. Optimal multi-scale geometric fusion based on non-subsampled contourlet transform and modified central force optimization. International journal of imaging systems and technology, 2019, 29(1), 4–18.

[18] Liu F, Yang J, Liu Y, Li H. Digital image correlation with topology-based matching algorithm on dots pattern and its application in large deformation measurement of nitrile–butadiene rubber. Measurement Science and Technology, 2021, 32(10), 105026.

[19] Jan J B, Ahmadi V, Fathi D. Low-voltage electrically-induced second harmonic generation in a silicon waveguide based on modal phase matching. Journal of Lightwave Technology, 2020, 38(22), 6272–6279.

[20] Zhang B, Long H, Jiang F. Optical image encryption algorithm based on coherent superposition and equal modulus vector decomposition. Dianzi Yu Xinxi Xuebao/Journal of Electronics and Information Technology, 2018, 40(2), 438–446.

Biographies

Huan Wang was born in HanDan, China, in 1975. From 2000 to 2003, she studied in Beijing Information Science and Technology University and received her bachelor's degree in 2003. From 2007 to 2011, she studied in Hebei University and received her master's degree in 2011. From 2019 to 2022, she studied in Woosuk University in South Korea and received her Doctor's degree in 2022. Currently, she works in Hebei University of Engineering. She has published ten papers, three of which have been indexed by EI. Her research interests are included the research, development, design and operation of distance education system.

Xin Li studied in Shandong Normal University and received her bachelor's degree in 2005. From 2006 to 2008, she studied in Beijing Jiaotong University and received her master's degree in 2008. From 2019 to 2022, she studied in University of the Cordilleras and received her Doctor's degree in 2022. Currently, she works in Hebei University of Engineering. She has published five papers, one of which have been indexed by EI. Her research interests are digital education, education management.