Analysis of Network Security Countermeasures From the Perspective of Improved FS Algorithm and ICT Convergence

Zhihong Zhang

Anhui Technical College of Water Resources and Hydroelectric Power, HeFei 231603, China
E-mail: zzh@ahsdxy.edu.cn

Received 22 November 2022; Accepted 28 December 2022;
Publication 03 March 2023

Abstract

In this paper, the forward selection (FS) algorithm is introduced on the basis of information and communication technology, and the design of intrusion detection method for communication network is carried out. By studying the classification and detection pattern matching of communication network intrusion behavior, extracting the intrusion behavior features of communication network based on FS algorithm, and optimizing the intrusion detection and learning effect based on the limit learning machine, the intrusion behavior attributes of communication network are clarified, and a new detection method is proposed to solve the problems of low detection accuracy and low recall in the current intrusion behavior detection of complex communication network environments. Compared with the intrusion detection method based on GA-SVM algorithm, the accuracy of the detection results reaches 94.23%, and the recall rate exceeds 97%, which is obviously better than the 85% accuracy and 75% recall rate of the traditional detection method, which can

Journal of Cyber Security and Mobility, Vol. 12_1, 1–24.
doi: 10.13052/jcsm2245-1439.1211

ensure the security of the communication network environment. In addition, this paper proposes the APDR dynamic comprehensive information security assurance system model, which has considerable flexibility and can respond to current network security requirements.

Keywords: FS algorithm, extreme learning machine, network intrusion, communications technology.

1 Introduction

As mankind enters the era of knowledge economy, informatization is transforming from a technological revolution to an industrial revolution, and has become an irreversible trend of economic and social development [1, 2]. At present, informatization has become an important driving force for promoting China's urban development, bringing the required information resources to urban economic development, and injecting new vitality into the development of urban economy. Information infrastructure is the foundation of information development and the neural network of cities [3]. The information security guarantee system is the guarantee of information development and an important part of urban security, which is of great significance to the information construction of cities [4–6].

Information is an important strategic resource for today's social development. Information technology and the information industry are changing traditional production, management and lifestyle, and becoming new economic growth points [7–9]. Science and technology with information technology as the core have been widely used in important national infrastructure fields such as finance, communications, energy, transportation, education, scientific research, social security and social security [10, 11]. As an important information infrastructure, the information and communication industry is one of the main components of the information industry and the pillar of the information industry [12, 13]. Under the macro background of China's reform, opening up and economic construction, which has achieved a series of remarkable results, in order to better develop the national economy, promote social progress, adapt to the global development trend of informatization, and strive to improve the country's comprehensive competitive strength, the Chinese government actively draws on the development experience of developed countries and regions in the world, judges the hour and sizes up the situation, seizes development opportunities, and clearly puts forward the development strategy of "promoting industrialization with informatization" in the

"Tenth Five-Year" Plan for National Economic and Social Development, and the communication industry is implemented as China. The important infrastructure of the development strategy of "promoting industrialization with informatization" has played a role in multiplying benefits, and the development of the information industry has brought about a greater increase in social benefits. As the carrier of network media information, the security of the Internet affects the secure transmission of information on network media [14]. Moreover, as a medium, China's network media also shoulders the important task of safeguarding the overall interests and image of the country as a link between the government and the public to transmit information and guide the correct direction of public opinion [15]. Therefore, at present, an urgent problem to be solved in front of China's network media builders is: what kind of information security guarantee system can be established to escort the development of network media informatization? It is precisely under such tasks and requirements that this paper attempts to give an information security guarantee system model through the study and research of information security guarantee theory, and on the basis of this model, a more complete and effective information security guarantee system is designed and planned for network media [16].

HTP model, as an important theoretical basis for network security management, applies network security related management system standards as a comparison in this paper, which has certain theoretical significance: on the one hand, compared with the relevant network security theoretical models used in previous studies, the HTP model fully integrates both technology and management, making up for most of the model focusing on technical problems, and pays more attention to the role of "people" in the influencing factors of network security compared with other network security research models. It can comprehensively improve the reliability of information systems [17, 18]. On the other hand, ISO27000 information security management system as a national network security management system standard, according to the standard system to divide the threat factors, and then establish the HTP model for empirical verification, can accurately reflect the network security problems existing in the grassroots government information system, help enrich the application mode and scope of HTP theory.

Therefore, researchers in related fields have carried out in-depth research on this problem, and realized the design and research of a variety of intrusion detection methods and technologies [19]. Due to the late start of this research, most of the current detection methods or technologies only stay

at the theoretical level, and some of the detection methods applied to the actual can not achieve dynamic and preventive safety monitoring of communication networks during application. At the same time, due to the complex communication network environment, if the traditional detection method is introduced in the detection process, it is impossible to accurately identify the intrusion behavior, so the utilization value of the monitoring results is also low. FS algorithm is a feature selection algorithm based on machine learning, which can realize the effective extraction of data, information and other features, thereby providing more favorable conditions for subsequent recognition. In practical applications, the extreme learning machine can be regarded as a typical single hidden layer forward neural network, and the effective training of the algorithm can be realized by using this structure, so as to further improve the application performance of the algorithm. Therefore, based on the application advantages of FS algorithm, in order to further improve the security of communication network and ensure that users' privacy is not leaked during communication transmission, the design and research of intrusion detection methods are carried out on the basis of the introduction of FS algorithm and extreme learning machine technology.

With the rapid development of the current communication network environment, there are also serious network security threats. Through this study, a new intrusion detection method is proposed, which can play a more important role in ensuring the security of communication networks. In this paper, FS algorithm and extreme learning machine are applied to the detection field in the research process, which can realize the discovery of hidden laws in the communication network data set and effective identification of intrusion behavior. However, due to the limited research time and capacity, the complexity of various calculations in detection was not taken into account in the research process, so there is still much room for improvement of detection efficiency in practical applications.

2 Theoretical Background

2.1 Background of Network Security Theory

Network security, known as the security of the Internet, more precisely, can maintain the normal and secure operation of the relevant components of the network, with integrity, availability, confidentiality, controllability and reviewability. Network security is a key issue involving national security, and with the advent of the information age, it plays a pivotal role in the future

development of the country. Network security is a comprehensive discipline involving computer science, network technology, and other disciplines. Network security is divided into two levels: network security and information security. Network security means that the network can effectively ensure the continuity and efficiency of services. System security can ensure the safe use of information processing and transmission systems. The network security referred to in this article mainly refers to four aspects, the first aspect is hardware security, including the security of network hardware and storage media. The second aspect is software security, which ensures that the network can be safely operated and prevents illegal operations. The third aspect is the security of operation services, which can ensure the normal exchange of information on the network. The fourth aspect is data security, that is, the security of data stored and circulated in the network.

Network management refers to monitoring, controlling, coordinating and reporting failures of various network resources. Network security management usually refers to the management actions to ensure the security of network management objects, and is the network management related to security. With the increasing importance of network security and the increasingly complex and close relationship and influence on network information systems, network security management has gradually developed into an important branch of network management. Network security management involves many industries and departments in society. This paper focuses on government network security management, which means that government information in the public sector is guaranteed in the life cycle of information generation, dissemination, processing and distribution, archiving, etc. It is the basis for maintaining social order. The protection of government information and the handling of emergencies are the information level of national security protection, and government network security is also a kind of national security.

2.2 Network Security Standards and Models

ISO/IEC 27000 is widely recognized in the international field as the most emblematic standard. ISO 27001 is one of the most critical standards, so ISO 27001 is often used as the authoritative safety management standard.

The network security protection model is in the process of continuous development, gradually changing from static to dynamic. Because the network security problem is in a constant process of change, the static model cannot solve the corresponding problem, and the dynamic model perfectly

solves the problem, so the dynamic model gradually replaces the static model. At present, the main dynamic network security models include PDR, PPDR, PDRR, P2OTPDR2, etc.

(1) PDCA cycle method

The PDCA cycle was first proposed by Dr. Hughhart, an American quality management expert. The PDCA cycle is divided into four phases: planning, execution, inspection, and adjustment. These stages are repeated. The ISO27000 standard follows the above iterative process to continuously identify problems and improve the ISMS system to achieve the goal of network security. The PDCA round-robin method is one of the more basic models in the network security model.

(2) PPDR model

The PPDR model developed by the American Internet Security System Corporation is an early dynamic model of information security [20]. At the heart of this model is the security policy, a circular system of protection, detection, and response that work together to ensure network security. The model adopts certain protection technology, with the help of corresponding detection tools, combined with a series of measures to deal with the threats to the system promptly to ensure that the system maintenance is in a safe state. It can be seen from the circulating system diagram that in the PPDR model, the security policy is in the center of the diagram, so the formulation of security policy is relatively important, so the formulation of security policy plays a very important role in network security protection.

(3) PDRR model

The PDRR dynamic model is based on the PPDR model (see Figure 1) to add recovery functions, which is still based on security policies, but its advantage is that when encountering problems and failures, it can carry out timely and effective recovery, and maintain its security through four parts: protection, monitoring, response, and recovery. The model secures the object of protection, tracks, and monitors at any time, and if there is a threat, takes action until a secure state can be reached.

(4) P2OTPDR2 model

The P2OTPDR2 model includes policy, people, operations, technology, protection, detection, response, and recovery. The model contains three parts, the outermost part of the model is composed of four links of protection, detection, response, and recovery of the PDRR model, and the intermediate level penetrates the peripheral links, as shown in Figure 3. The intermediate

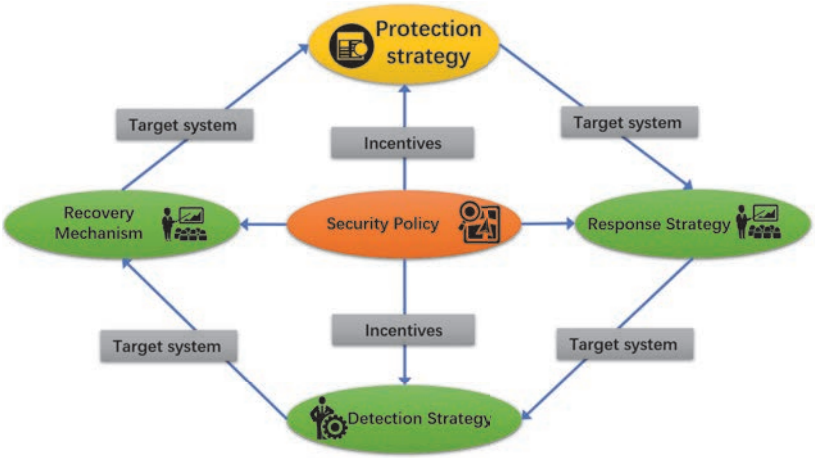

Figure 1 PDRR model.

level is composed of three basic elements: people, operations, and technology. Because people are conscious and can exercise certain controls, they are in the most important position among the three basic elements. The security policy is located in the center, in the key position in the construction of the security system, the middle layer is to manage and control network security, and the four parts of the periphery can carry out certain security protection for the whole process, to prevent problems and failures. It can be seen from the above that the model effectively guarantees the protection of security.

(5) HTP model

Domestic network security experts Chen Wei and Sun Qiang first proposed an HTP model with certain research values, as shown in Figure 4, which draws on the idea of the "barrel principle" in management, which is also applicable to the field of network security. The three components that make up the model are personnel management, technical means and safety products, activity processes, and overall framework. In the HTP theoretical model, personnel management is a relatively important factor in network security protection, and personnel organization management plays a key role in the construction of security defense lines.

This model shows that people management is at the heart of the cybersecurity system. This extends to the government, where workers are most likely to threaten the network security system, and if the initiative of employees can be fully exerted, it can improve network security protection capabilities to a certain extent.

Figure 2 P2OTPDR2 model.

Figure 3 HTP model.

As China is at a relatively backward level in network security protection, China has learned from and referred to foreign advanced experience in network security protection. According to literature review, many enterprises have chosen PPDR and PDRR models as models of network security management. If the network security management system is built on the PPDR and PDRR models, only the impact of technology on network security

needs to be considered, that is, virus prevention can ensure the security of information. Therefore, enterprise managers actively build and install firewalls, anti-virus software and anti-intrusion detection systems, and take them as the core of security management. However, this approach is too one-sided. It only ensures that one aspect of network security is protected. There are still many other factors threatening the enterprise network security. In order to achieve the enterprise network security goal, enterprises must consider all factors comprehensively and build a perfect management system.

3 Design of Dynamic Comprehensive Information Security Assurance System Model

3.1 Model Design

At present, the demand of network media in information security is multi-faceted, and multi-level, and single technology or product will be difficult to meet the security demand of network media information systems. Therefore, we need to stand based on the existing security system theory and model and design a more complete information security assurance system to meet the current security needs of network media. In the process of establishing the model, we mainly followed the following ideas:

(1) Emphasize relevant laws, regulations, and policy basis

As far as the security guarantee system of network media is concerned, we must use these existing laws, regulations, and policies as the fundamental means of security guarantee as reasonably and effectively as possible, and we must never leave this foundation alone to talk about technology.

(2) Follow the design idea of system engineering to consider the planning and construction of the system

When planning and building the information security guarantee system of network media, we should consider it as a whole, not only focusing on the technical system, but also the people-centered organization system and media website management system. We should organically combine these three security elements, and plan and build according to the idea of system engineering.

(3) Hierarchical consideration of security units

The process of data transmission is decomposed into some basic elements, and the network functions related to specific applications are identified and

classified to form some independent functional layers. This is the famous 150-RM seven-layer model.

(4) Emphasize the dynamics of the safety process

The information security guarantee system of network media must have the dynamic nature of following the changes in information environment, which is mainly reflected in the security process.

In the multi-channel ship wireless mobile communication network, the average value of all data abnormal node characteristics in the undetected data set B with mixed intrusion data is recorded as $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_m)^T$, where, $m = 1, 2, \ldots$ is the total average value of data abnormal node characteristics and T is the transpose matrix. According to to $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_m)^T$, constituting the data characteristic matrix $T_\alpha = F[\alpha\alpha^T]$, where F is the correlation degree of matrix elements. In this case, use $\bar{\alpha} = F[\alpha]$ as the element in the matrix. According to the above data characteristics, compare the characteristics of normal data and mixed intrusion data, and the corresponding relationship is:

$$\varsigma = G^T\alpha \tag{1}$$

where G^T is the characteristic matrix of normal data. According to the calculation results, the differences in extracting the characteristics of abnormal nodes are as follows:

$$E_\alpha = F[(\alpha - \bar{\alpha})(\alpha - \bar{\alpha})^T] \tag{2}$$

Comprehensive (1) and (2), the characteristics of mixed intrusion data are:

$$\gamma = \sum_{k=1}^{m} F[\alpha_k - \hat{\alpha}_k] \tag{3}$$

where k is the matrix element at any position in the data characteristic matrix, $\hat{\alpha}_k = \sum_{k=1}^{m} \alpha_k w_k - \beta_k w_k$ is the weighted value of the data abnormal node feature, w_k is the feature quantity corresponding to the element in the matrix, β_k is the element in the characteristic matrix of normal data. The characteristic value of mixed intrusion data can be obtained from Equation (3), and based on this, mixed intrusion data existing in the network can be mined.

3.2 APDR Dynamic Comprehensive Information Security Assurance Architecture Model

A good information security guarantee plan must have a good structural model for overall guidance. Based on the above requirements analysis and

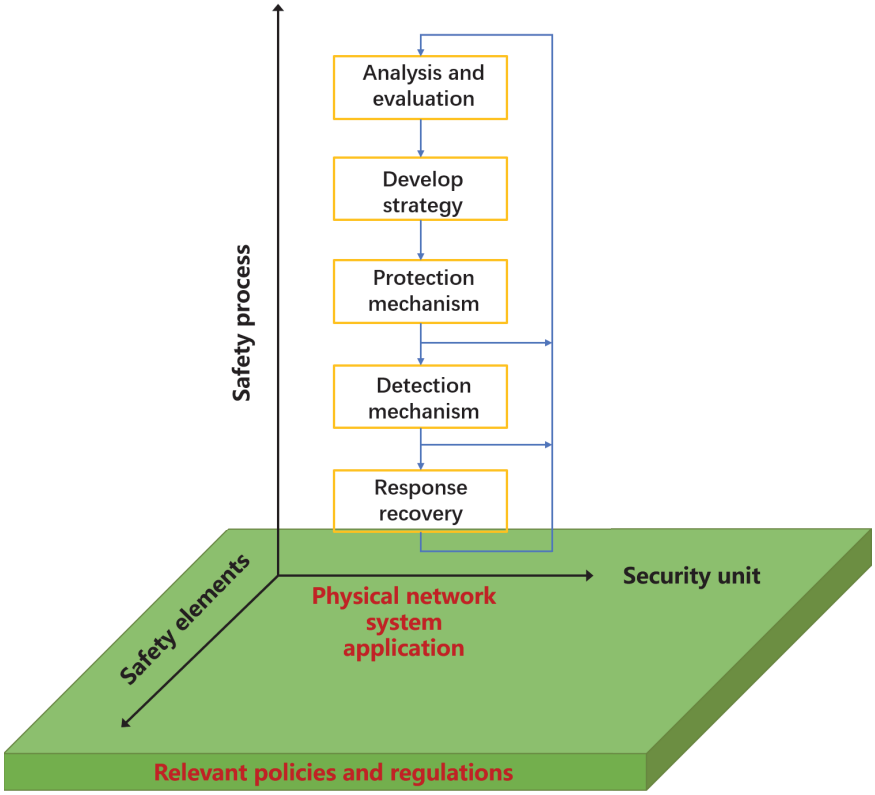

Figure 4 APDR dynamic comprehensive information security assurance architecture model.

system engineering life cycle theory, this paper designs an APDR dynamic comprehensive information security assurance architecture model, as shown in Figure 4.

Dynamic and comprehensive information security assurance architecture is a multi-level, multi-faceted, and three-dimensional security architecture divided into several levels. The model is briefly described below.

(1) Legal Foundation

Information criminal activities are inseparable from the imperfection of the legal system in information security and the ineffective punishment of criminals; it is precisely for this reason that China's relevant departments have formulated some regulations, policies, and standards in light of the current specific conditions, such as the State Secrets Bureau's "Interim Regulations on the Management of Computer Information System Confidentiality," the

"Regulations on the Management of International Internet Confidentiality of Computer Information Systems," and the "Notice on Strengthening the Management of Government Internet Information Confidentiality." Although its completeness needs to be further discussed, after all, it is the crystallization formed based on certain lessons learned at present, so it has become the guiding principle for the formulation of information security policies by various enterprises and institutions in China and the legal basis for the construction of information security projects. In the process of building their information security guarantee system, online media must also follow these relevant laws, regulations, and policy standards to ensure their legality, so that there are laws and regulations to follow.

(2) Secure element

The security unit here is considered according to the layered thinking of 051-RM. According to the actual situation of network media, this paper abstracts the security unit into four parts from bottom to top: physical security, network security, system security, and application security, forming a hierarchical "defense in depth" system, as shown in Figure 6 below:

In the Figure 5 above, physical security is to protect media computer network equipment, facilities, etc. from environmental accidents, human operation errors or errors, and various computer crimes caused by physical channel damage, physical channel eavesdropping, attack (interference) on physical channels, etc.

Network security needs to ensure that the network only allows authorized customers to use authorized services, ensure that the network routing is correct, and avoid interception or snooping. The system platform security requires to ensure the access control of the operating system and be able to audit the applications on the operating system. The system application security shall ensure the safe operation of network media application software services built on the corresponding operating system, such as database server, e-mail server, main Web server, etc., and provide users with safe and effective services.

(3) Security elements

In the process of information security construction, people often pay more attention to technology and products. However, at present, with the increase in the complexity of software and hardware, various vulnerabilities are also emerging; Coupled with the increasing complexity and diversification of hacking technology, if security issues are considered from a single technology and product level, even if every aspect is done, it is still fragmented and

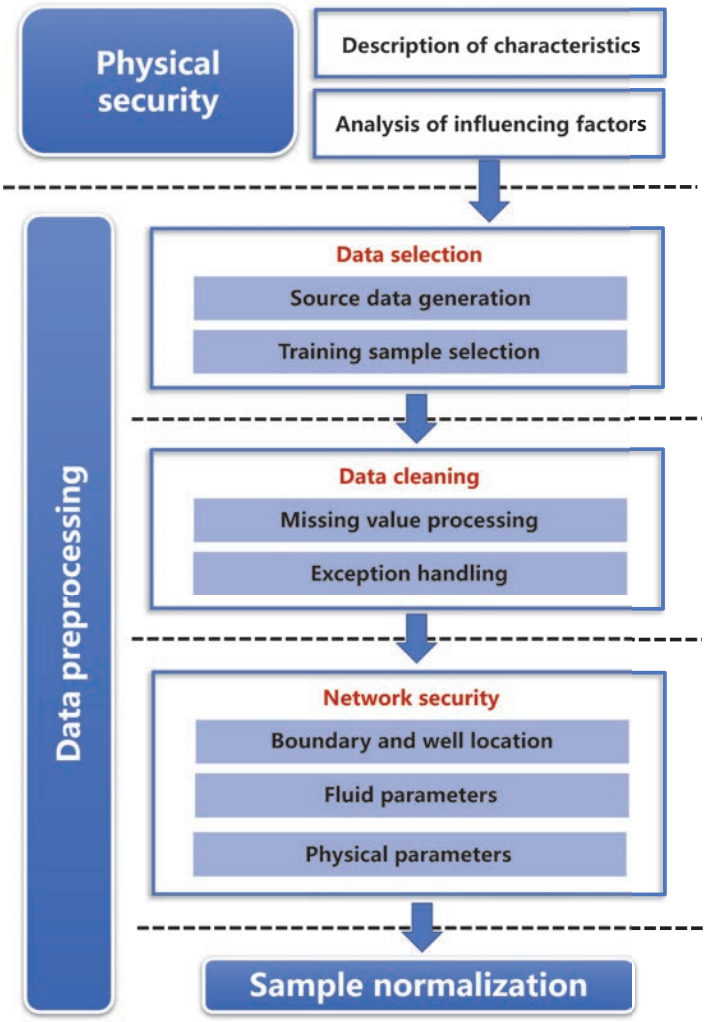

Figure 5 Hierarchical security elements.

fragmented, and the information system cannot be reliably guaranteed. The "barrel principle" also applies to information security: the weakest point of security is like the shortest block of wood on the wall of a barrel, and it is also the first choice for hackers to attack the system. Therefore, the intensity of protection measures in all aspects of information security should be relatively balanced. Therefore, in the process of planning and building the information security system of online media, we must not only pay attention to technology

and products but also pay enough attention to the two elements of people and management.

Management is a security element that requires special attention. Although "three points of technology, seven points of management" is not a universal experience, it emphasizes one point: only by implementing effective security management from beginning to end to all aspects of security construction, the long-term stability of information security can be guaranteed.

Foreign sources indicate that most of the attacks were carried out by insiders. Therefore, the most important thing about security is to attach great importance to it ideologically. Fully paying attention to the subjective initiative of employees and doing a good job in the ideological and political work of personnel can greatly improve the security of the system. In addition, any safety management or technical means are inseparable from the implementation and organization of personnel, so when considering the combination of technology and management, we must also pay attention to its feasibility for the internal personnel of the media.

4 Communication Network Intrusion Behavior Feature Extraction Based on FS Algorithm

4.1 Communication Network Intrusion Behavior Feature Extraction Based on FS Algorithm

After clarifying the categories of intrusion behavior of the communication network, to extract the characteristics of intrusion behavior, the FS algorithm is introduced, and the traffic audit record of the communication network is taken as the extraction object to extract the characteristics of the intrusion behavior, to find abnormal intrusion. Figure 7 shows a schematic diagram of the feature extraction process based on the FS algorithm.

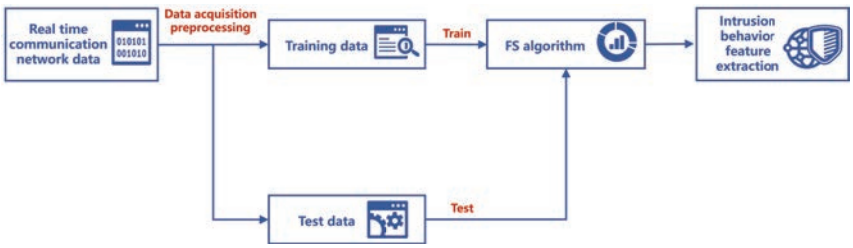

Figure 6 Schematic diagram of feature extraction process based on FS algorithm.

Combined with the content in Figure 7, after obtaining the original data of the communication data, to facilitate subsequent operations, it is first necessary to preprocess it, divide the data under each attribute into the data, and record its connections to each other. Then the FS algorithm is used to extract the intrusion behavior features, and an infinitely differentiable activation function is selected, to avoid the adjustment of each parameter in the FS algorithm, randomly select two sets of parameters, and ensure that these two sets of parameters remain unchanged during the training process, and obtain the extraction results through the smallest and undertaker way, which can be expressed by the following formula:

$$\overset{\min}{\beta} = \|H\beta - T\| \tag{4}$$

In Equation (4), the least squares solution is dedicated; H represents the matrix input in the hidden layer; T represents the constant term. Based on the relationship in Equation (4), the relationship between the generalized inverse of the hidden layer output matrix and the connection weights is further obtained:

$$\hat{\beta} = H^{+}T \tag{5}$$

4.2 Intrusion Behavior Detection and Learning Effect Optimization Based on Extreme Learning Machine

After extracting the characteristics of intrusion behavior in the communication network according to the above content, the intrusion behavior of an unknown communication network is detected. At the same time, to further improve the application effect of the FS algorithm, it is selected to use an extreme learning machine to train it.

Functions that take activation define the function as:

$$f(x) = \frac{1}{1 + e^{-x}} \tag{6}$$

Based on the above formula (6), a function with infinite differentiability of any interval is selected, which is used as an improved function of the FS algorithm, and a correction parameter is introduced to improve the accuracy of the FS algorithm in the extraction of features of communication network intrusion. At the same time, this calculation process is much simpler, so the additional amount of calculation is directly negligible. After the introduction of the extreme learning machine, the training of the FS algorithm can be achieved by a very small number of additional parameters, and the number of

additional parameters is the same as the total number of signals during data transmission in the communication network. At this time, the total number of weights can also be ignored during the calculation process, to ensure that the FS algorithm will not cause overfitting and cause additional risks in the actual application process, to further optimize the learning effect of the FS algorithm. After clarifying the above discussion, when training the FS algorithm, the FS algorithm is introduced into the input layer of the extreme learning machine but the hidden layer forward neural network structure, and given k hidden layer neurons and the above activation function in the structure, through continuous iterative training, the FS algorithm can approximate any different samples in the communication network traffic audit record data with zero error. At the same time, to avoid falling into the local optimal solution during the detection process, the selection of the initial cluster center should be realized by setting a distance threshold, and for the initial cluster center, the distance between each data point and the adjacent data point should be compared to determine whether there is a problem of falling into the local optimal solution. In the structure of the extreme learning machine, the cluster analysis can be completed by optimizing the FS algorithm for connections and similar attack behaviors that do not have communication network intrusion behavior in the training set. The cluster center data under multiple different attributes are mined, and the data set composed of these data is used as a high-quality training set and reintroduced into the input to complete the learning, to fully improve the accuracy of intrusion detection through continuous iteration.

4.3 Test Environment

According to the characteristics of mixed intrusion data extracted in this study, the LOF algorithm is used to design the mixed intrusion data mining process as follows:

(1) Input mixed intrusion data feature set O.
(2) Determine the characteristic data object p of the mixed intrusion data.
(3) Calculate the distance of each mixed intrusion data feature data object. The calculation steps are as follows: calculate the distance from all data to the object in the data feature set; Select different minimum distances among all distances; In the different minimum distances, select a maximum distance as the distance of the mixed intrusion data feature data object.
(4) Calculate the neighborhood distance of the mixed intrusion data feature data object. Suppose there are nearest neighbors, record all data with a

distance less than or equal to as a set, including data objects, and select the shutdown data set, which contains 50,000 pieces of data, of which only 17,278 are normal, and other data are intrusion data.

Three methods are used to mine the mixed intrusion data in the shuttle dataset. Under 9 different mixed intrusion attack modes, the amount of mixed intrusion data mining generated is shown in Table 3. It can be seen from Table 3 that the more types of mixed attacks are, the less mixed intrusion data is mined. Among them, comparison method 1 mines the amount of mixed intrusion data, which is less than 30000, and the amount of mixed intrusion data mined is the least; The amount of mixed intrusion data mined by comparison method 2 is lower than 32000. Although it is better than comparison method 1, the amount of mixed intrusion data mined by comparison method 2 is also less. The method in this paper is more efficient than the comparison method in mining mixed intrusion data. Through the above contents, the problem of data redundancy in the data set during the intrusion detection process of the location communication network can be effectively avoided, so as to avoid the problem of frequent connection data in the process of training and classification, and reduce its impact on the accuracy of the final detection results.

4.4 Comparative Experiments

To further verify the effect of the proposed method in practical application, the traditional intrusion detection method based on the GA-SVM algorithm is taken as the control condition, and the feasibility and application advantages of the proposed intrusion detection method are verified by comparing the detection results of the two detection methods. In the experiment, the two detection methods are applied to the same experimental environment, and the basic parameters of the experimental environment include: 2.20 GHz Intel Corei5 CPU, four 4 GBRAM computers, and one for simulating the sending end user in the communication network; One for simulating the receiving end user in the communication network; One for the application of the intrusion detection method proposed herein; The other is used to apply traditional intrusion detection methods based on GASVM algorithms. Four computers form a complete communication network environment, in which the application of two detection methods is realized. To ensure the objectivity of the evaluation results, the accuracy and recall of the test results were selected as the evaluation index, and the application performance of the two test methods was measured from two aspects. After determining

the evaluation index, the data from the NSL-KDD dataset is selected as the research object, applied to the sending end-user computer and the receiving end-user computer, and 10,000 pieces of data are randomly selected as the test set during the communication process to detect whether there is network intrusion behavior. To improve the universality of the experiment, the data types in the test set include data types that are common in various communication networks, such as Normal data, DOS data, U2R data, etc. Before ingesting data, it is also necessary to standardize it according to the following Equation (7):

$$x_1 = \frac{x - \bar{x}}{\sigma} \tag{7}$$

In Equation (7), x_1 represents the normalized communication network data; x represents the characteristic value of the original communication network data; x represents the average of the characteristic values of all raw communication network data; Represents the standard deviation of the original communication network data feature values. According to the above formula, the standardized processing of the data in all test sets is completed, to complete the entire experimental preparation. Combined with the above experimental preparation, the accuracy of the test results of the two detection methods is first tested, and the accuracy can be calculated by the following formula:

$$P = TP/(TP + FP) \tag{8}$$

In Equation (8), P represents the accuracy of the test result; TP indicates the number of network connections in the network environment that the intrusion attack is correctly judged as the intrusion attack during the communication process; FP represents the number of network connections for which a non-intrusion attack was judged to be an intrusion attack. Combined with the above formula (8), the accuracy of the detection results of the two detection methods is calculated, and the results are plotted as a comparison chart as shown in Figures 7 and 8:

Figures 7 and 8 Comparison of the accuracy of the experimental results of the two detection methods from the experimental results obtained in Figure 2, it can be seen that the detection method based on the FS algorithm and limit learning machine detects the intrusion behavior in the communication network under the above experimental conditions, and the accuracy of the detection results is significantly higher than that of the traditional intrusion detection method based on GA-SVM algorithm. The lowest accuracy of the detection method in this paper is 94.23%, while the traditional detection method does not reach 85%. Therefore, further analysis of the above results

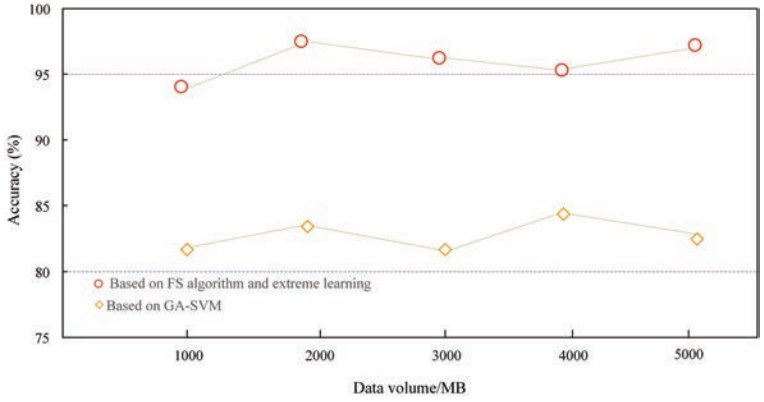

Figure 7 Comparison chart of the accuracy of experimental results of the two detection methods.

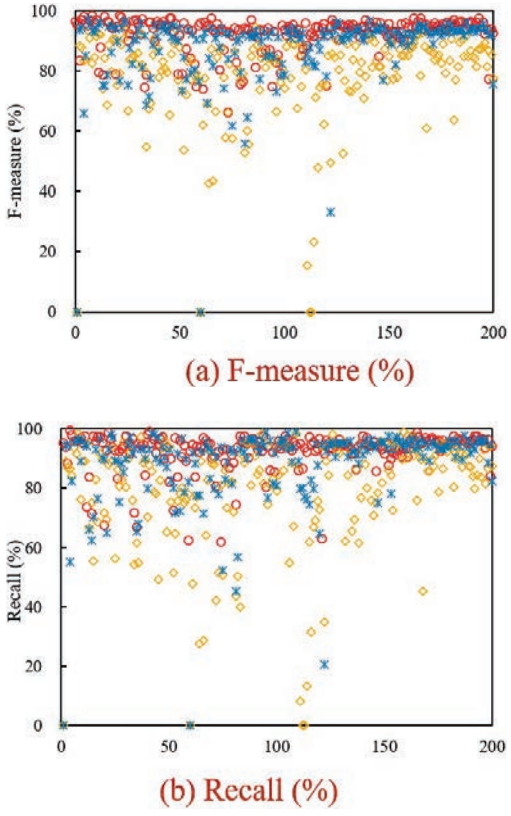

Figure 8 Continued

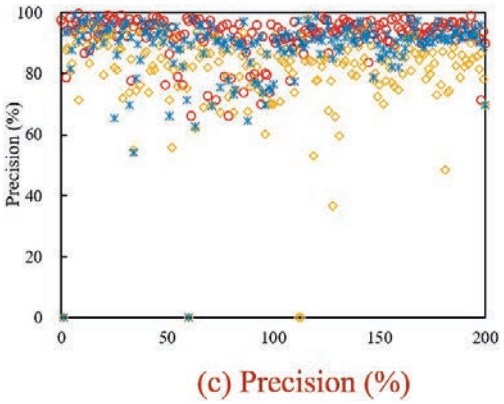

Figure 8 Comparison of various parameters of the algorithm.

preliminarily proves that the detection method proposed in this paper can effectively improve the accuracy of detection results and realize the accurate detection of communication network intrusion behavior in practical applications.

5 Results and Discussion

Through comparative analysis, we can see that the recall rate of detection results of detection methods based on the FS algorithm and extreme learning machine in this paper is in the range of 97.00%∼98.50%, while the recall rate of detection results based on the GA-SVM algorithm exceeds 75.00% in the first detection. Later, with the continuous increase of the number of detection samples, the recall rate of detection results also shows a downward trend. But the detection method based on the FS algorithm and limit learning machine proposed in this paper does not have this problem. Therefore, through the above experiments and the experimental results obtained, it is further proved that the detection methods proposed in this paper can effectively improve the recall rate of detection results, improve the application value of detection results, and improve the completeness of detection methods in this paper. Based on the above two evaluation results, the detection method proposed in this paper based on the FS algorithm and extreme learning machine is applied to the real communication network environment, which can achieve accurate detection of intrusion behavior and improve the communication security of the communication network to a certain extent.

6 Conclusion

With the rapid development of the current communication network environment, there are also serious network security threats. Through this study, a new intrusion detection method is proposed, which can play a more important role in ensuring the security of communication networks. The main conclusions of this study are as follows:

(1) In this paper, we use the characteristics of mixed intrusion data to mine mixed intrusion data, and use experiments to verify the feasibility of this method, which provides a reference for future research.
(2) In this paper, the FS algorithm and extreme learning machine are applied to the detection field in the research process, which can realize the discovery of hidden laws in the communication network data set and effective identification of intrusion behavior.
(3) The lowest accuracy of this method is 94.23%, while the lowest accuracy of the traditional method is less than 85%. Therefore, further analysis of the above results preliminarily proves that the detection method proposed in this paper can effectively improve the accuracy of detection results in practical applications, and achieve accurate detection of communication network intrusion.
(4) In this paper, the recall rate of detection results of detection methods based on the FS algorithm and extreme learning machine is in the range of 97.00%∼98.50%, while the recall rate of detection results of detection methods based on the GA-SVM algorithm exceeds 75.00% in the first detection. Later, with the continuous increase of the number of detection samples, the recall rate of detection results also shows a trend of continuous decline, But the detection method based on the FS algorithm and limit learning machine proposed in this paper does not have this problem.

Data Availability

The experimental data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declared that they have no conflicts of interest regarding this work.

Funding Statement

There is no specific funding to support this research.

List of Notations and Abbreviations

FS	Forward Selection
GA-SVM	Support vector machine optimization based on genetic algorithm
ICT	Information and Communications Technology
HTP	Human and management
	Technology and products
	Process and framework
PDR	Protection
	Detection
	Response
PPDR	Policy
	Protection
	Detection
	Response
PDRR	Protect
	Detect
	React
	Restore
P2OTPDR2	Policy
	Protection
	Operation
	Technology
	People
	Detection
	Response
	Restore

References

[1] Azeez, N. A., S. O. Idiakose, C. J. Onyema, and Van Der Vyver, C. 2021. Cyberbullying Detection in Social Networks: Artificial Intelligence Approach. *Journal of Cyber Security and Mobility*, 745–774.

[2] Alqarni, A. A. 2022. Majority Vote-Based Ensemble Approach for Distributed Denial of Service Attack Detection in Cloud Computing. *Journal of Cyber Security and Mobility*. 265–278.

[3] Fujs, D., Mihelic, A., and S. Vrhovec. 2019. Social Network Self-Protection Model: What Motivates Users to Self-Protect? *Journal of Cyber Security and Mobility.* 467–492.

[4] Li, X., H. Li, B. Sun, and F. Wang. 2018. Assessing information security risk for an evolving smart city based on fuzzy and grey FMEA. *Journal of Intelligent and Fuzzy Systems.* 34(4): 2491–2501.

[5] Yan, N. 2022. Legal Guarantee of Smart City Pilot and Green and Low-Carbon Development. *Journal of Environmental and Public Health*. doi: 10.1155/2022/4280441

[6] Zhang, C. 2020. Design and application of fog computing and Internet of Things service platform for a smart city. *Future Generation Computer Systems*. 112: 630–640.

[7] Garetti, M., and M. Taisch. 2012. Sustainable manufacturing: trends and research challenges. *Production planning and control.* 23(2–3): 83–104.

[8] De Reuver, M., C. Sørensen, and R. C. Basole. 2018. The digital platform: a research agenda. *Journal of information technology.* 33(2): 124–135.

[9] Senge, P. M., G. Carstedt, and P. L. Porter. 2001. Next industrial revolution. *MIT Sloan management review*, 42(2): 24–38.

[10] Ijaz, S., M. A. Shah, A. Khan, and M. Ahmed. 2016. Smart cities: A survey on security concerns. *International Journal of Advanced Computer Science and Applications*, 7(2).

[11] Yampolskiy, R. V. 2022. On the Controllability of Artificial Intelligence: An Analysis of Limitations. *Journal of Cyber Security and Mobility*. 321–404.

[12] Zhang, L., X. Hu, W. Rasheed, T. Huang, and C. Zhao. 2019. An enhanced steganographic code and its application in voice-over-IP steganography. *IEEE Access*, *7*, 97187–97195.

[13] Aceto, G., V. Persico, and A. Pescapé. 2019. A survey on information and communication technologies for industry 4.0: State-of-the-art, taxonomies, perspectives, and challenges. *IEEE Communications Surveys and Tutorials.* 21(4): 3467–3501.

[14] Bodapati, J. D., and N. Veeranjaneyulu. 2019. Feature extraction and classification using deep convolutional neural networks. *Journal of Cyber Security and Mobility*. 261–276.

[15] Lin, L. W. 2010. Corporate social responsibility in China: Window dressing or structural change. *Berkeley J. Int'l L.* 28, 64.
[16] Wang, W., and Z. Lu. 2013. Cyber security in the smart grid: Survey and challenges. *Computer networks.* 57(5), 1344–1371.
[17] Siponen, M. T. 2000. A conceptual foundation for organizational information security awareness. *Information management and computer security.*
[18] Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, 523–548.
[19] Kabiri, P., and A. A. Ghorbani. 2005. Research on intrusion detection and response: A survey. Int. *J. Netw. Secur.* 1(2): 84–102.
[20] Yamaguchi, Y., A. Ogawa, A. Takeda, and S. Iwata. 2015. Cyber security analysis of power networks by hypergraph cut algorithms. *IEEE Transactions on Smart Grid*. 6(5): 2189–2199.

Biography

Zhihong Zhang is a mathematics student of Anhui University since1994. He graduated from Anhui University with a bachelor's degree in Applied Mathematics in 1998, and then obtained a master's degree in Computer Science and Technology from Anhui University in 2004. He is mainly engaged in the research of neural network algorithm. Since his graduation, he has been working in the Anhui Technical College Of Water Resources And Hydroelectric Power, engaged in teaching and scientific research, and his research field is the neural network security in the direction of the Internet of Things.