Research Article

Research on the Key Technologies of Network Security-Oriented Situation Prediction

Yikun Zhu1 and Zhiling Du2

1School of Mechanical Engineering & Automation, Wuhan Textile University, Wuhan, Hubei 430000, China
2School of Economics and Management, East China JiaoTong University, Jiangxi, Nanchang 330013, China

Correspondence should be addressed to Zhiling Du; 2018048125300096@ecjtu.edu.cn

Received 22 February 2021; Revised 7 April 2021; Accepted 19 April 2021; Published 31 May 2021

Academic Editor: Chenxi Huang

Copyright © 2021 Yikun Zhu and Zhiling Du. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In today’s increasingly severe network security situation, network security situational awareness provides a more comprehensive and feasible new idea for the inadequacy of various single solutions and is currently a research hotspot in the field of network security. At present, there are still gaps or room for improvement in network security situational awareness in terms of model scheme improvement, comprehensive and integrated consideration, algorithm design optimization, etc. A lot of scientific research investments and results are still needed to improve the form of network security in a long and solid way. In this paper, we propose a network security posture assessment model based on time-varying evidence theory for the existing multisource information fusion technology that lacks consideration of the problem of threat occurrence support rate over time and make the threat information reflect the law of time change by introducing a time parameter in the basic probability assignment value. Thus, the existing hierarchical threat posture quantitative assessment technique is improved and a hierarchical multisource network security threat posture assessment model based on time-varying evidence theory is proposed. Finally, the superiority of the proposed model is verified through experiments.

1. Introduction

With the popularity and development of computer and network technology, various network systems have been deeply embedded in the daily production and life of society and individuals [1]. In recent years, network attacks, information leakage, and other ongoing security incidents have exposed the serious problems facing network security [2]. There are many factors that cause the deterioration of the form of network security, both internal and external causes [3]. The first and foremost of the internal causes is the construction level of the network system, which varies with the level of practitioners, the complexity of the system, and whether financial services are involved [4]. For example, in January, the user names and passwords of many network service companies, such as Tianya Community, were made public in clear text, leading to the leakage of a large number of user password habits and e-mail addresses [5–10]. Various security loopholes, such as cross-site attacks, injection, hijacking, and other problems are rife in the network services, and even strong international companies are not immune [11]. In addition to the problems arising from the construction of the network system, deeper problems come from the system platform and some important service programs have been found to have major security vulnerabilities one after another. Use to the use of third-party operating systems or service programs (such as servers and a series of service software), system builders usually cannot and do not have the ability to discover all potential problems and can only rely on software providers or even open source organizations [12–16].

Not to mention that some open source organizations are slow to respond to security and slow to update. Even the system vulnerabilities released by Microsoft are threatened by “zero-day attacks.” Many attackers use the time interval between vulnerability releases and system updates to
successfully implement a large number of attacks. Various sources of threats make various network systems, whether corporate intranet or public network services, full of risks [17]. Globally, the Internet is frequently attacked, network paralysis occurs from time to time, and the security of network systems is constantly under serious threat; in China, the types and numbers of various network attacks continue to grow, especially the proliferation of Trojan horses is the most serious [18]. Network theft, network economic crimes, and large-scale network attacks have posed serious security threats to China’s network infrastructure and important network systems, greatly restricting national economic development and even endangering social stability and national security. Network Security Situation Evaluation (NSSE) is a key technology in network security situational awareness, and the processed security situational elements data will be entered into the network security situational evaluation model for comprehensive evaluation. The evaluation needs to consider comprehensiveness, multiple granularity, and so on [19].

However, due to technical limitations, market expectations, funding, and other issues, most products can solve a single threat or in some cases have better results against certain attacks. But overall there is no unified management and scheduling mechanism and they are unable to cooperate with each other, unable to communicate effectively, and unable to track multiple data sources. This cannot cope with more complex attacks or long-term, potential, and gradual infiltration attacks that cannot be captured. Some interrelated attacks are lost in the tens of thousands of management logs of different products, and a large number of “false positives” have made administrators numb and ignore valuable information. Therefore, the industry has produced a more secure and effective global grasp of the theory of cyber security conditions, and tools are urgently needed. It is hoped that by integrating all aspects of safety information, the current qualitative and safety information can be extracted and calculated. It even quantifies the value of network security status to help administrators take timely remedial and preventive measures. The time decay function is used in the model to solve the dynamic problem of trust, and the stability and scalability of the model are enhanced through the trust prediction mechanism. Finally, the model is applied to the protocol, and the experimental simulation is carried out. The result verifies the safety and effectiveness of the model. The research in this area has also become a hot concern direction, and this paper has done a lot of research work based on this and achieved certain results.

2. Related Work

Here, we present some related work, which combines both external information of monitoring devices and network system environment information to form a situational value that can reflect the network system. It is a comprehensive technology with high requirements for both mathematical method application and network model. At present, the general assessment methods mainly include the following analysis methods: gray evaluation method, fuzzy analysis method, hierarchical analysis method, Delphi expert method, and so on [20]. In another work, based on a large amount of past data information, researchers used the connectivity between them to predict the future security trends in a certain period of time [21]. Just as network attacks follow certain steps and patterns, the same situation exists for network security situations [22]. In addition, scientific methods are used to discover links and laws, accurately predict various network attacks, protect network system security management, achieve a reasonable level of security control before security incidents occur, and conduct targeted preprocessing [23]. Situation prediction techniques mainly include the gray theory prediction method, Bayesian inference-based prediction, autoregressive moving average model prediction, machine learning algorithm prediction, and neural network prediction.

In another case, researchers are mainly to facilitate network administrators to intuitively understand the operating status and development trend of the entire network and to give people a more intuitive feeling [24]. It uses computer graphics and image processing technology to convert static data into dynamic images. The graphics are displayed on the computer screen to realize the interactive connection between the maintenance personnel of the network system and the security data behind. For example, the NGSOC situational awareness platform released by domestic 360 security company and the Cloud Shield situational awareness released by AliCloud provide good examples of network security situational visualization [25].

A network security situational awareness framework is a macro representation of the whole picture of situational awareness. It expresses the functional tasks of each aspect of situational awareness in abstract and general semantics, which helps to show the flow and development of the whole security posture. A good situational awareness framework not only carries the whole process of technology pointing but also shows a clear outline for the next step of development. According to the situational awareness foundation model, a more comprehensive reference model for network security situational awareness currently combines different aspects and types of security systems such as network firewalls, intrusion detection systems, and security audit systems.

2.1. Network Security Posture Framework System. From the collection of information elements, data preprocessing can understand the current network security situation and, at the same time, analyze and predict the future trend of network security changes. The rational analysis of the security situation combines system equipment and resources to achieve effective control, thereby bringing an intuitive and comprehensive response to decision makers. A typical NSSA framework is shown in Figure 1.

In this framework, the NSSA implementation is composed of five levels (stages), starting with security information collection work, understanding events through subsequent processing steps, in which the system provides real-time control feedback, and finally visualizing and
analyzing the security posture based on human-computer interaction. Five of these processing levels are as follows:

Level 0 (data preprocessing): it includes a large amount of unstructured data, optional preprocessing levels for structured data and agile data, and obtains necessary data by obtaining contextual elements; it will become a part of nonuniform data preprocessing operations, such as data desensitization, cleaning, and impurity filtration.

Level 1 (event extraction): after obtaining the relevant element information, the information is extracted to form standardized events, as well as the rules and features of unified events.

Level 2 (situation assessment): correlation and data fusion operations are performed on the collected multisource data, and information events are understood using existing assessment algorithms to form a comprehensive security situational analysis report, which provides supplementary information for subsequent managers.

Level 3 (impact assessment): according to the previous period of the situation, analyze the possible future trends of change, combine the full range of resources and control of the network system, introduce expert experience into the decision, and give an evaluation strategy for the impact of future changes in the situation.

Level 4 (resource management, process control, and optimization): selecting objects for system monitoring, real-time scheduling and allocation of occurring situation events, rational use of system resources, and maximizing efficiency.

2.2. Network Security Posture Indicator Construction Principles. Security posture indicator construction is an indispensable and fundamental part of the NSSA process, which is an indicative sign reflecting the security attributes of the perceived object and provides the basis for measurement and assessment for network security posture understanding and prediction. There are numerous indicators that can have an impact on the network posture, and screening out the posture indicators with typical data forms the data source for subsequent posture sessions and can provide reliable data support for the next step of assessment and prediction. The network security posture indicator system is a collection of indicators that can fully reflect the characteristics of network security, and the indicators are intrinsically linked to each other and play a complementary role, which is the basis for forming standardized objective quantitative analysis conclusions on network security evaluation, and it can reflect the basic appearance, quality, and level of network security of the perceived object. Therefore, the construction of network security posture indicators is of great significance for network security posture perception. The construction of the indicator system needs to refer to certain principles, specifically the construction of the network security posture indicator system from different dimensions.
(1) Hierarchical classification principle: network security posture indicators are hierarchical (some are for the local network and some are for the large-scale network); these indicators have different meanings in different environments, and the processing process varies, so they should be considered in a hierarchical classification.

(2) Similarity principle: in a large macronetwork, there are many influencing factors to be considered, but there is no lack of similarity and cross-measurement data. For example, the distribution of data packets, the distribution size of data packets, and similar indicators should all be taken into consideration.

(3) The principle of the combination of dynamic and static: because the index itself has its own characteristics, such as the distribution of network assets and equipment within a certain period of time, the network topology is not easy to change, while the network traffic information is always required to be processed, filtered, and collected.

Therefore, the indicators of these two categories should be treated differently and combined with the indicators’ own characteristics for the corresponding combination. In a comprehensive consideration of network security, the nature of three aspects is usually used to describe the network security posture, specifically: network base operation, network vulnerability, and network threat level, as shown in Figure 2. When the computing device factor is in the locked state, it is determined that all secure data can be decrypted by any one or more applications located on the computing device. When the computing device is in the locked state, if it is determined in the determining step, there is at least some secure data. If it can be decrypted by at least one or more applications, the first indicator is displayed. These three aspects represent three dimensions, which basically cover all parts of the entity constituting the information network and can reflect the security posture of the network in a more comprehensive way, and many researchers and commercial organizations currently use this approach.

2.3. Network Security Prediction under Fuzzy Logic Theory. There are a large number of fuzzy phenomena in nature, that is, there are things that are not so easy to make distinctions, for example, young and old, fat and thin, tall and short, and long and short; there will be a certain degree of fuzziness among these concepts. For these fuzzy concepts and phenomena, in recent years, with the development of the field of mathematics, gradually formed a modern applied mathematical science to solve fuzzy problems: fuzzy mathematics. This theory was proposed by Professor L. Zadeh of the University of California, a famous American scholar. Fuzzy logic is the key part of fuzzy mathematical theory, which uses the affiliation function instead of the classical Boolean truth-value logic, abandoning the traditional deterministic two-valued truth proposition in the tradition and generalizing this problem to affiliation, which will be more conducive to making innovations in uncertain and fuzzy problems. And fuzzy logic has been widely used in related scientific fields and brings new directions for industrial development. A fuzzy set is defined as follows: for a general set \( U \), any mapping \( \mu_A \) from \( U \) to the interval \([0, 1]\) can determine a fuzzy subset of \( U \), called a fuzzy set \( A \) on \( U \), where the mapping \( \mu_A \) is called the affiliation function of the fuzzy set \( A \), and for an element \( x \) on \( U \), \( \mu_A(x) \) is called the affiliation of \( x \) to the fuzzy set \( A \), which can also be written as \( \tilde{A}(x) \).

\[
\mu_A: U \rightarrow [0, 1] \quad \text{for} \quad x = \frac{1}{\mu_A(x)},
\]

where \( U \) is called the theoretical domain of the fuzzy set \( A \), \( \mu_A \) is the affiliation function of this fuzzy set, any element \( x \) on \( U \) no longer has only two cases of belonging to \( A \) and not belonging to \( A \), and each element \( x \) has an affiliation \( \mu_A \) for \( A \) (x). The degree of affiliation \( \mu_A \) represents the degree, and a higher value of it indicates a higher degree of belonging to \( A \), while the opposite indicates a lower degree of belonging to \( A \). The fuzzy set is transformed into a normal set when the \( \mu_A \) value domain takes the two endpoints of the closed interval \([0, 1]\).

If the theoretical domain \( U = \{x_1, x_2, \ldots, x_n\} \), then the fuzzy set \( \tilde{A} \) on \( U \) can be expressed as

\[
\tilde{A} = \sum_{i=0}^{n} \mu_A(a_i) q_i + p_i
\]

where \( \mu_A(x_i) (i = 1, 2, \ldots, n) \) is the affiliation degree and \( x_i \) is an element in the domain of the argument. When the affiliation degree is 0, the item can be omitted. When the theoretical domain \( U \) is a continuous set, then the fuzzy set \( \tilde{A} \) on \( U \) can be expressed as

\[
\tilde{A} = \bigoplus_{i=0}^{n} \mu_A(x_i).
\]

It should be noted that summation and integration here are not in the original sense and are special representations of fuzzy sets. If the affiliation of all elements on the domain of the argument is given, it can be represented in a similar way to the classical mathematical set, also called here as the sequential pair representation.

\[
\tilde{A} = \sqrt{\sum_{i=0}^{n} X_i}
\]

where each sequential pair consists of an element \( x \) and its corresponding affiliation \( \mu_A(x) \) and the fuzzy set \( \tilde{A} \) contains all combinations thereof.

Since the fuzzy set and its affiliation function form a one-to-one correspondence, the operation of the fuzzy set is also inscribed and represented by the operation of the affiliation function.

Empty set: it is the set whose affiliation function is 0 for all elements \( x \), denoted as \( \emptyset \), i.e.,

\[
\tilde{A}_{\emptyset} = \sum_{i=1}^{n} X_i \iff \mu_A(x) = 0.
\]
Equal sets: consider two fuzzy sets $\tilde{A}$, $\tilde{B}$; if their affiliation functions are equal for all elements $x$, then $\tilde{A}$, $\tilde{B}$ are also equal, i.e.,

$$\tilde{A} = \tilde{B} = \sum_{i=1}^{n} \mu_{\tilde{A}}(x) \Leftrightarrow \mu_{\tilde{A}}(x) = 0. \quad (6)$$

Subsets: in the fuzzy sets $\tilde{A}$, $\tilde{B}$, $\tilde{A}$ being a subset of $\tilde{B}$ or $\tilde{A}$ being contained in $\tilde{B}$ means that for all elements $x$, there is $\mu_{\tilde{A}}(x) \leq \mu_{\tilde{B}}(x)$, denoted as $\tilde{A} \subseteq \tilde{B}$, i.e.,

$$\tilde{A} \subseteq \tilde{B} \Leftrightarrow \mu_{\tilde{A}}(x) > 0. \quad (7)$$

Concatenation: for the concatenation set $C$ of the fuzzy sets $A$, $B$, the affiliation function can be expressed as $\mu_C(x) = \max \{ \mu_{\tilde{A}}(x), \mu_{\tilde{B}}(x) \}$, i.e.,

$$Q = \tilde{A} \cup \tilde{B} \Leftrightarrow \mu_{\tilde{A}}(x) = \max(\tilde{A})(x) > 0. \quad (8)$$

Of course, the basic properties of fuzzy set operations (such as ordinary sets and fuzzy sets) also satisfy the power law, the exchange law, the union law, the absorption law, the distribution law, and the Morgan theorem. Ordinary set relations can only indicate that two factors are either related or unrelated, while fuzzy relations introduce uncertain quantities such as close relations, defined as follows: the direct product space $X \times Y = \{(x, y), x \in X \in Y\}$ of fuzzy relations is a fuzzy set $R$ on $X \times Y$, and the affiliation function $R$ of $R(x, y)$ represents the degree of relationship between element $x$ on $X$ and element $y$ on $Y$. The above fuzzy relation is also the simplest binary fuzzy relation, but of course it can be extended to form an $n$-element fuzzy relation. 50 counters are randomly distributed in an area of 1000 x 1000, of which 10% are malicious binary. The converter uses a mobile model. The router’s communication has a range of 250 m. The data source generator sends 4 cBR streams with a size of 512 B per second, the network bandwidth is 2 Mbps, and the simulation time is 300 s. If $R(x, y)$ takes the value of 0 or 1 special point, the fuzzy relation also degenerates to the ordinary set relation, as shown in Figure 3.

2.4. Neural Networks Predict Cybersecurity. Artificial neurons are the basic information processing units for ANN operation. Figure 4 represents the schematic diagram of the composition of ANN neuron, which has three main components: weighted adder, linear dynamic system, and nonlinear mapping function. $x_i$ denotes the input from other neurons, $u (-)$ denotes the adjustable network connection weight, $\theta$ is the offset signal as the threshold, $y_i$ denotes the output of the neuron, $(-)$ represents the basis function, which is a multiple-input single-output function, and $f (-)$ represents the activation function, which is a nonlinear mapping.
of the output signal $u$ of the basis function and is transformed into the specified range.

Sigmoid function: this function, also called S-shaped function, is most widely used in the ANN field. It is a strictly monotonic increasing function with smoothness and asymptotic characteristics. Its function expression is

$$f_{ij}(x) = \begin{cases} e^{(dQ_j/dt - dQ_i/dt)}, & \frac{dQ_i}{dt} < \frac{dQ_j}{dt} \\ e^{(dQ_i/dt - dQ_j/dt)}, & \frac{dQ_j}{dt} < \frac{dQ_i}{dt}. \end{cases}$$

(9)

Among them, the parameter $\lambda$ is the gain of the sigmoid function, which controls the slope of the function curve; generally, the larger the value of $\lambda$, the steeper the function curve, and the function value domain is $(0, 1)$, which is often applied to the binary classification problem; however, this function also has the disadvantage that it is easy to over-saturate and produce the gradient disappearance phenomenon, which cannot complete the deep network training. Secondly, the mean value of the output of the function is not 0, which affects the operation efficiency of gradient descent.

Bipolar sigmoid function: the tanh function solves the problem of the existence of some unipolar S-shaped functions; it will transform the function value domain from $(0, 1)$ to $(-1, 1)$; compared with the original function, the convergence speed is faster, and the output average value is 0, as shown in Figure 5. Its function expression is

$$y = f(x) = \frac{\exp(\mu_A(x) + \mu_B(x))}{\exp(\mu_A(x) - \mu_B(x))}.$$  

(10)

Neural networks are composed of neurons as the basic unit. If a large number of neurons are connected in a topological structure according to certain rules to form a parallel distributed computing structure, the structure of neural networks as we know it in daily life is formed. In the following, several typical structures of neural networks are introduced according to the neural network connection pattern.

1. Single-layer perceptron: the single-layer perceptron is one of the simplest neural networks proposed by Frank Rosenblatt in 1957 and is mainly a structural model for binary classification problems. The function and mechanism of the single-layer perceptron is very simple and can be used to model simple logic functions with relatively few applications. The input layer as the perception layer in the figure has $n$ neuron nodes, which are only responsible for the collection of external information but have no information processing capabilities. The input layer has $n$ input signals, which constitute the input column vector $X$. The output layer, called the processing layer, is more specific in that each neural unit has information processing capability and the output constitutes the column vector $Y$. The connection weights between the input signals and the processing units are represented by the column vector $W_j$.

2. Feedforward network: feedforward neural network is the most widely used neural network structure model. It has the typical characteristics of the universal neural network structure; this network consists of three layers, which are the input layer, hidden layer, and output layer. In this network, the input signal is transmitted in one direction from the input layer to the output layer, the neurons in each layer are only connected to the neurons in the previous layer, there is no connection between the neurons in the same layer, and the whole network has no feedback, as shown in Figure 6.

3. Feedback-type network: feedback-type neural network establishes another connection between input
and output, that is, the signal of the output layer of the network is re-entered into the input layer through a feedback loop. Compared with the feed-forward neural network, this network has stronger computational ability and associative memory ability. This type of network can be used in real-time signal processing, system control, and other scenarios that require real-time adjustment according to the system state. Feedback-type neural networks can be further divided into full-feedback networks and partial-feedback networks.

The learning of neural networks also refers to the training process of the network structure parameters, through continuous learning to adjust and correct the parameters of the network in time to optimize its own performance and efficiency, so as to achieve the equilibrium conditions to adapt to the changes in the external environment. The learning methods of neural networks can be divided into supervised learning and unsupervised learning. The training of neural networks mainly consists of forward propagation training and backward propagation training. Forward propagation training refers to the entire process from the input layer of the neural network, multiple hidden layers, and then the output layer to the output signal; the backward propagation mainly refers to the process of passing the error signal obtained from the output layer to the input layer in reverse order from back to front. Back-propagation mainly uses the gradient descent and error backpropagation (EBP) algorithms to adjust the weights of the network. In turn, the system error is obtained by comparing the output signal with the desired output signal, and the error of the latter layer is propagated forward layer by layer using chain derivatives to obtain the error signal of each layer, according to which the training network structure is adjusted, and the whole process of continuous cyclic training is the process of neural network learning. The training process can be terminated by artificially setting the
termination conditions, either by setting the maximum number of iterations or by selecting the network convergence to a certain degree. If the number of iterations set is too small, as shown in Figure 7, it may cause the function to not converge well and the neural network to not fit well; if the number of iterations set is too large, it is easy to cause the function to overfit, resulting in insufficient generalization.

3. Analysis of Experimental Results

In order to verify the convergence efficiency of the PSO-LSTM prediction algorithm, the RNN prediction algorithm and LSTM prediction algorithm are combined here to train on the same test set and check their error convergence performance. The difference between the three algorithms is depicted in Figure 8. It can be found that the RNN has a large initial error, a large fluctuation in error convergence, and a long convergence time to the optimal error value during the training process, requiring more than 250 iterations. The LSTM algorithm with more hidden layers has a smaller initial MSE and faster convergence than RNN, requiring 150–200 iterations, but with more parameters, it is easy to fall into the problem of local optimum, and the error performance is only better than that of RNN overall. In contrast, the PSO-LSTM algorithm starts with a smaller error, and the subsequent convergence speed is significantly better than the previous two, with faster convergence time and higher stability. Therefore, it can be judged that introducing the particle swarm optimization algorithm into the LSTM neural network can indeed improve the convergence performance of the network.

In order to verify the prediction accuracy of the PSO-LSTM prediction algorithm, the three prediction methods are also analyzed and compared here, and Figure 9 shows the normalized posture prediction curves of the three for the next 50 days. The physical signal strength of the observation group decreases with time, while the control group is opposite and increases accordingly. Through the comparison, it is found that all three prediction algorithms have better prediction effect on the security posture in the future period, but PSO-LSTM can better track and analyze the security posture trend, overcoming the problem that the original
The actual prediction of the three prediction algorithms is tested in detail here. For the RNN network, the test points on the training set are selected, and the RNN residual distribution is drawn as in Figure 10. After the analysis, it can be found that the first 200 training sample data can show the horizontal band pattern of the residuals well, but the corresponding error’s allowed range is floating between −1 and 1. This is due to the "forgetting" problem of the RNN prediction algorithm over a long period of time, and the overall error is found to be relatively large under RNN training. In terms of NSSE, a network security posture prediction algorithm based on PSO-LSTM neural network is proposed to address the problems of poor applicability and low accuracy of traditional network security posture prediction algorithms. Firstly, the recurrent neural network (RNN) is used to predict the security situation, and the LSTM neural network with "gating" structure is adopted to address the problems of insufficient memory of RNN, easy "forgetting" and gradient disappearance during the training process. The gradient disappearance was solved by reasonably controlling the ratio of input information to current memory information, and the training prediction results were significantly improved. However, it is difficult to select the parameters of the LSTM network during the training process, and it is easy to fall into the local optimum, so the particle swarm optimization algorithm is introduced to achieve the global optimum quickly, reduce the training time, and improve the efficiency. The accuracy and effectiveness of the PSO-LSTM prediction algorithm proposed in this paper are demonstrated through experimental analysis and comparison.

After the training of the PSO-LSTM neural network prediction algorithm, it was tested on the test set individually and the relative error of each sample was obtained. It is found that the accuracy of the proposed prediction algorithm in the test set is slightly lower than that in the training set, but the overall prediction accuracy is still acceptable, and the average relative error is stable at about 5.07% (only 30 samples are listed here). At the same time, the security posture prediction curves on the test set are plotted, and the real values of the posture are compared with the predicted values of the PSO-LSTM algorithm, and the results show that the prediction algorithm proposed in this paper can predict the network security posture in the future period better. In terms of NSSP, a hierarchical situational assessment model based on alert verification and fuzzy inference is proposed to address the problem that the current network security situational assessment model only uses a large amount of IDS alert information without effectively combining the target system configuration information, asset value information, and vulnerability information. And the evaluation system indicators suitable for this model are determined; secondly, the alarm verification process based on multilayer fuzzy mathematical evaluation is implemented to reduce the influence of false alarms, make each alarm message more targeted, and obtain alarm success rate information; then, the fuzzy inference process is applied to achieve a nonlinear mapping of the three alarm elements to synthesize the alarm posture values; then, the alarm posture values are obtained through different levels at the service level; finally, the security posture values are quantitatively calculated at service level, host level, and network system level through different levels, and the threat status at each level is displayed in a hierarchical manner. The assessment model can obtain more comprehensive assessment information and more accurate assessment results than traditional methods.

4. Conclusion

In this paper, we focus on network security situation prediction and propose a PSO-LSTM neural network-based network security situation prediction algorithm. Particle swarm optimization (PSO) is an evolutionary computation technology (evolutionary computation). The basic idea of particle swarm optimization algorithm is to find the optimal solution through collaboration and information sharing between individuals in the group. In order to solve the problem of insufficient memory and the disappearance of the gradient of the recurrent neural network (RNN); the LSTM neural network with gating structure is used to reasonably control the ratio of input information to current...
memory information, and the gradient disappears. LSTM (long short-term memory) is specially designed to solve long-term problems. All RNNs have a chain form of repeating neural network modules. In a standard RNN, this repeated structural module has only a very simple structure, such as a tanh layer. In order to solve the problem of difficult parameter selection of LSTM network and easy to fall into local optimum, particle swarm optimization algorithm is added in the network training to achieve global optimum quickly, reduce the training time, and improve the efficiency. Finally, the three prediction algorithms are compared by experimental analysis, which proves the accuracy and effectiveness of the PSO-LSTM prediction algorithm proposed in this paper, and its application in the field of situational prediction has good results.

Data Availability

No data were used to support this study.

Consent

Informed consent was obtained from all individual participants included in the study references.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References