Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 1777560, 9 pages
https://doi.org/10.1155/2022/1777560

Research Article

Security Evaluation of Situational Awareness in Cyberspace Based on Artificial Neural Network-Back Propagation

Weihong Han, Hafiz Muhammad Jamsheed Nazir, and Shudong Li

Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou 510006, China

Correspondence should be addressed to Weihong Han; hanweihong@gzhu.edu.cn
and Hafiz Muhammad Jamsheed Nazir; hmj.nazir@yahoo.com

Received 26 September 2021; Revised 11 August 2022; Accepted 1 September 2022; Published 13 October 2022

Academic Editor: Pierre-Martin Tardif

Computer network security has become increasingly controversial among many businesses as a result of the rise in cyber threats. Artificial neural network (ANN) is mature research in this field, whereas the traditional algorithm is slower, in feedback error, and has the disadvantage of easy convergence to local extreme value. To guide against these threats, in this paper, ANN-back propagation (BP) algorithm is used to establish the relationship between the level of cyber security situational awareness (CSA) and the perceptual parameters and quantitatively evaluate the situational awareness. This study established the ANN-back propagation (BP) to make the relationship between the level of cyber security situational awareness (CSA) and the perceptual parameters, which evaluates situational awareness. The ANN-BP with variable step size learning strategy and simulated annealing method is used for optimization to build a virtual network environment. The proposed model offers better precision, improved sensitivity, and higher (0.987%) accuracy.

1. Introduction

Computing resources, cyber security, software programs, and data are protected from attack using a combination of policies, techniques, technologies, and procedures [1]. Cyber security is comprised of several rules, technologies, and processes that work in concert [2]. Application, network, host, and data-level cyber security mechanisms exist. Several tools, such as firewalls, antivirus software, intrusion detection systems (IDSs), and intrusion protection systems, are used to prevent and detect security breaches and assaults (IPSs) [3, 4]. However, many opponents still possess an advantage because all they need to do is to take advantage of a vulnerability in the systems that need to be protected is find one. A wider attack surface is created as a result of the growing number of internet-connected systems. As the attackers become smarter, they build zero-day exploits and malware that evade security safeguards, allowing them to remain undetected for extended periods [5]. They are attacks which have never been seen before but are generally variations on a previously known one. Exploitation strategies are being commoditized, which exacerbates the situation by allowing for quick distribution without organizations that abuse their permitted access [6]. Compromise indications are present throughout an attack's lifecycle; there may even be substantial indicators of an oncoming attack. Finding these markers, which may be dispersed across the environment, is a problem. Figure 1 depicts the cyber security situation awareness cycle.

Applications, servers, smart devices, and other cyber-enabled resources create massive amounts of data from machine-to-machine and human-to-machine interactions. Data generated by cyber security technologies, such as the security information event management (SIEM) system, might overwhelm security analysts [7]. The military program's security posture can be improved by utilizing data science in cyber security. Data analytic-based cyber protection technologies are starting to appear. System signatures are

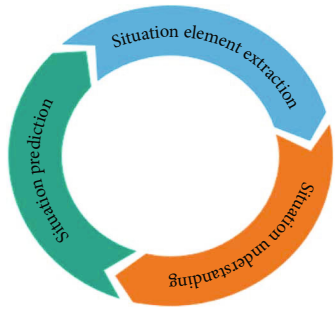

Figure 1: Cyber security situation awareness cycle.

being replaced by network intrusion detection systems (NIDS), which analyze packet transmission [8]. Figure 2 depicts the cyber security situation awareness attributes.

A robust intrusion detection system (IDS) is required to protect against all of these threats. ANN, decision tree (DT), support vector machine (SVM), naive Bayes, and other machine learning (ML) algorithms have been used to detect threats [9]. With the rise of cyber threats, computer network security has become a major issue for many businesses. A robust intrusion detection system (IDS) is required to protect against all of these threats. ANN, decision tree (DT), support vector machine (SVM), naive Bayes, and other machine learning (ML) algorithms have been used to detect threats. Considering the various threats, it is necessary to employ a combination of strategies to effectively improve intrusion detection in computer networks. This is because invaders are getting a foothold in the cyber world, and the consequences for businesses are difficult to quantify. The ANN is the most advanced research in this field; however, the traditional BP approach is slow in terms of feedback error and has the drawback of being quickly convergent to local extreme values.

This study develops a better model for detecting threats on a computer network. To accurately forecast threats, a comparison of ANN-BP and DT is studied. With this study, a network administrator can be rest assured based on these predictions.

1.1. Related Work. A machine learning-based intrusion detection system's effectiveness and efficiency in detecting threats to organizations and other network users are interesting and valuable. Because cyber threats fall into a variety of categories, certain machine learning algorithms may not be able to detect them on a computer network. The data fusion model was initially introduced by cyber situation awareness (CSA), which then improved and adjusted the original model, established the CSA model, and clarified the CSA's purpose [10]. The CSA model is well developed and mature as of 2016, related research has not advanced significantly since then, the CSA's primary duty is evaluation, and it conducts extensive research in this area. The objective of the mathematical model (MM) method, which comprehensively takes into account various situational factors, is to assess the network situation from various angles [11]. Situation assessment was the first application of the MM approach. It integrates several systems and concentrates on various elements that influence the network state. The situation factor reflects the situation's status from several angles, but MM only addresses multiattribute fusion and excludes the fusion of multisource data, and the model it employs is fixed [12]. The knowledge reasoning (KR) method emerged if just specific assessment findings could be reached, neglecting the uncertainty aspect to overcome the two main difficulties of MM. On the one hand, KR processes ambiguous information using fuzzy sets, probability theory, evidence theory, etc. [13]. On the other hand, the reasoning is used to obtain knowledge that has multiple sources and multiple attributes. A popular area of study is the KR approach as represented by Bayesian networks [14]. Numerous documents have surfaced, and further research is important. The largest problem facing KR is how to get inference rules and prior probabilities, particularly for a novel research area like CSA. To address this challenge, the pattern recognition (PR) method was developed. With its significant capacity for learning, the PR has been educated to use historical data or practice samples to mine the situation mode division's knowledge methodically and scientifically since 2005 [14, 15]. The majority of the already used evaluation techniques will essentially introduce data mining, which also illustrates the tendency of a thorough application of numerous techniques the examination of the idea that "problems appear to solve issues" is embodied in the creation of evaluation methodologies. Research on the representation of knowledge is uncommon and only recently has it begun [4]. The crucial position of CSA has been simultaneously formed by network management requirements and broad application prospects, and associated research has continued to advance. The preliminary examination of existing CSA revealed the following characteristics of relevant research: (i) other aspects of network security situational awareness, such as traffic, faults, topology, and survivability, are infrequently studied; (ii) system architecture is the subject of study and is at a relatively advanced stage. It accepts data from joint directors of laboratories (JDL), despite variations. (iii) The representation of the network system is based on a hierarchical structure; the representation of uncertain information is primarily simple grading and turned into discrete data; the design principles of the fusion model and the Endsley situational awareness model. (iv) Weight analysis is the basic foundation for the method's evaluation [4, 16]. The mathematical data fusion method has been attempted to be incorporated into CSA in some studies. Other issues still need to be resolved in the CSA research, which has attracted attention [12]. Figure 2 displays the situational awareness indicator system in cyberspace. Figure 3 contains several variables that have an impact on the situational security awareness system.

1.2. Study Characteristics and Problems. The existing research has focused mostly on the network management technologies already in use, failed to take into account the security situation in each unit, and is unable to provide a thorough analysis and presentation of the whole situation [17], owing to the absence of thorough and organized research on the entire CSA system. Second, the knowledge representation is inadequate. The term "situation" is too limited and does not adequately capture the general and macroscopic properties of the scenario. Although it is straightforward and obvious to use a hierarchical structure to depict a network system, it cannot reveal the intricate

Figure 2: Cyber security situation awareness attributes.

relationships between network pieces. Relationships prevent the potential situational information in multisource and multiattribute data from being mined [18]. Concerning data representation, research needs to be done on how to choose and expand the feature measurement employed for situation evaluation and create a fair and comprehensive indicator system. Third, there is no single standard for scenario assessment. This is partially attributable to the fact that a scenario is an abstract idea [19]. What kind of circumstance qualifies as good, and how good is it? Both grading and scoring are unreliable and lack a scientific foundation. However, the fundamental causes are neither persuasive nor evident. There cannot be agreement on the scenario and the situation assessment due to the formal definition of the situation and the absence of indications and techniques to gauge the benefits and drawbacks of the evaluation results. However, there are several distinct evaluation techniques. Nearly all theoretical data fusion approaches have been applied to the scenario appraisal stage, and new ways are constantly being developed. This entails extensive, recurring research, and sometimes even the application of specific mathematical techniques to deepen the theory. Only the standards for evaluation are consistent. Accurately, the goals and directions of the study on evaluation methods are well defined [19, 20]. Fourth, the available research is comparatively unconnected and only addresses the situation itself. There is a lack of integration between levels on the vertical (level 1/3) and horizontal (level 4/5/6) axes. It is not incorporated into the system for fusing data. The research framework in Figure 3 separates the research of each layer from one another and makes it difficult to directly apply level 1 because the current three main research areas are level 2 integration, the key technology of integration, without involving communication, interaction, system management, etc. The fusion's output is utilized as the starting point for measuring situational awareness features; it does not meet the requirements for fusion at levels 3 and higher, which is better for threat analysis and decision-making [3, 20]. It has attracted widespread interest from the academic community and is currently a hot topic in the data fusion sector. However, the majority of studies only focus on one component of CSA and are still in the theoretical exploratory stage. The focus of present and future research efforts is comprehensive and in-depth theoretical research and the deployment of actual applications, and the most pressing requirement is to build a unified assessment system [3, 7].

1.3. System Evaluation Index. The ultimate goal of situational awareness in cyberspace is to protect the security of network information and to provide an integrated situational awareness system in cyberspace. The regulatory authorities can understand the operation status of the network and lay a strategic foundation for the development of cyberspace [21]. The potential sense of network space states is shown as $F = \mathrm{G}(x) = \mathrm{g}_1(x_1)$ and $g_2(x_2)$ and $\cdots . g_n(x_n)$, where F is the quantitative evaluation result, G represents the application of the fusion algorithm, x represents the evaluation index set, $x_1, x_2 \cdots, x_{\mathrm{n}}$ denotes the specific analysis index, $g_1, g_2 \cdots, g_n$ represents the performance of various fusion algorithms and represents the integration process of the evaluation system. The

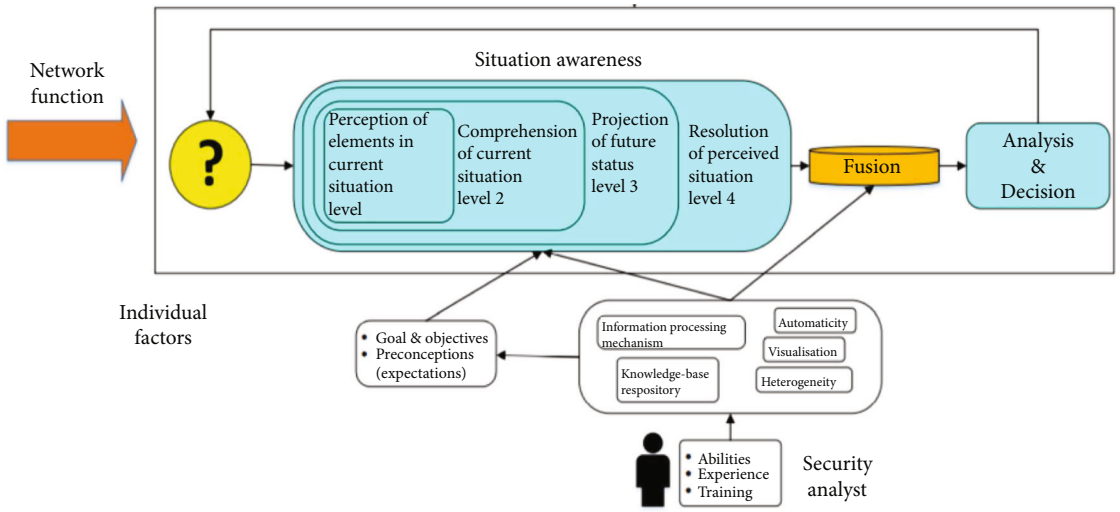

Figure 3: Network security situational awareness.

mode of situational awareness in cyberspace and description of the nature of situational awareness in cyberspace from four aspects is started. It covers the information entities in the network and fully reflects the status quo of situational awareness in cyberspace. These four aspects are, respectively, weakness, victimization, risk, and stability. The number of data parameters (weakness, victimization, risk, and stability indexes) of the definition reflects the network space situational awareness [9]. According to the four dimensions of situational awareness in cyberspace, this study established an index system of perceived security status. The results show that in the current network state, the system can calculate the trend of network quantitative analysis, to realize real-time network monitoring and control [21].

In this study, the occurrence of network space is divided into four levels, that is, risk, weakness, stability, and victimization. The first level index is described in two levels. According to the national first aid emergency plan and combined with the characteristics of network hazard elements, cyberspace is divided into five levels. The interval [0, 1] is used to describe the weight of indicators at several levels, as listed in Table 1. The grade matrix of the four first-level indicators and cyberspace situation is listed in Table 2, and the security level of first-level indicators is listed in Table 3. This study demonstrates the superiority of a multiclassifier ensemble over a single classifier.

2. Propose Optimization Approach

2.1. ANN-BP Algorithm. The BP neuron (input n) node through the weighted value W_i $(i = 1, 2 \cdots, n)$ input parameter x_i $(i = 1, 2 \cdots, n)$, neural element threshold θ, excitation function f, and the output parameter y is expressed.

$$y = f\left(\sum_{i=1}^{n} w_i x_i - \theta\right). \tag{1}$$

The hidden layer of ANN-BP requires a continuous excitation function, and the excitation function is selected as a sigmoid function at this time. The ANN-BP model includes the following two steps, information transmission and reverse correction of errors [22, 23]. The ANN-BP tends to fall into local minima, and the simulated annealing algorithm can fill this shortcoming [22]. During the first step set the starting temperature t_0, the starting state $s_0 = x_0$, the lowest temperature min, the optimal solution $s^* = s_0$, and the current target value $E(s_0)$. While on the second step, if the pretemperature is higher than $t_{\min}$, the number of iterations is the dimension of the initial solution. News* is produced in each iteration, and the calculated function value $E(s^*)$ and the phase ortho error difference $\Delta E = \Delta E(s^*) - \Delta E(s)$. If $\Delta E < 0$, the current state value is taken as the optimal solution of the current iteration, that is, $s^* * = s^*$. If ΔE is greater than or equal to 0; then, this step size adjustment increases the error, because it will be settled with p probability. Select the Metropolis criterion to calculate $p = \exp(-\Delta E/T)$ after iteration the optimal solution s^* and its state value $E(s^*)$ are obtained. The final step, first annealing optimization, detempering process $T = t_0/LG(1 + T)$. If $E(s^*)) < E(s^*)$, then $s^* = s^*$; on the contrary, it indicates that the global optimal solution is the current optimal solution. The situation awareness assessment process of the ANN-BP is optimized, as shown in Figure 4. The ANN-BP model is optimized and used to observe the current network condition, and the network grade difference is compared to determine whether it affects the current network condition. ANN-BP was a situational awareness evaluation process and a decision tree (DT).

2.2. Situational Assessment. Ten experts are selected to evaluate the system, which ensured the accuracy of the method. Recurrent back propagation in data mining is fed forward until a fixed value is achieved. After that, the error is computed and propagated backwards.

The main difference between both of these methods is that the mapping is rapid instatic back propagation while it

Table 1: Situational awareness level in cyberspace.

Situation index values	0.0 ~ 0.15	0.15~0.35	0.35~0.65	0.65~0.85	0.85~1.0
Threat level	*	**	***	****	*****
Description	Normal operation	The network is slightly attacked	Network operation is greatly affected	The network is attacked more seriously	The network is invaded by a large number of viruses
Description	Intrusion behavior	Loss is not big	System vulnerability is more	More seriously	Serious alert

*Safe, **medium threat, ***high threat, ****most threat, *****it indicates that the network is normal, and intrusion behavior does not exist.

Table 2: Primary indicators and network situation grade matrix.

Grade	High	Medium	Threat	Safe
Threat	*	**	***	***
Frailty	*	*	**	*
Victimization	*	***	***	***/**
Stabilization	***	***/**	**/*	*

*Low, **medium, and ***high.

Table 3: Primary index safety grade.

Grade	High	Medium	Low
Threat index	0 ~ 0.375	0.375~0.685	0.675~1.0
Vulnerability index	0 ~ 0.275	0.275~0.585	0.585~1.0
Disaster tolerance index	0 ~ 0.375	0.485~0.785	0.785~1.0
Stability index	0 ~ 0.275	0.275~0.675	0.685~1.0

is nonstatic in recurrent back propagation. The condition of the system is as follows:

$$E_i = \frac{1}{n}\sum_{j=1}^{n} a_j, i = 1, 2.\cdots, m. \tag{2}$$

The dispersion of the expert opinion is as follows:

$$\sigma_i = \sqrt{\frac{1}{n-1}\sum_{j=1}^{n}\left(a_j - E_i\right)^2} \quad i = 1, 2, .. \cdots, m, \tag{3}$$

where a_j is the score taught by the j position, according to the state potential special point, the full $E_i \le 1$, $\Delta i \le 0.6$ is the second-level evaluation index, which is constructed into the expected output of the second-level evaluation. This experiment has 100 samples, 20 of which are test sets, and 80 of which are training sets. The network (Honeywall) topology diagram is presented in Figure 5.

Figure 6 shows the first layer inputs the divine meridian element n, that is, the n-dimensional vector $X \in R^n$, where $X = (x_1, x_2 \cdots, x_n)^T$; the output of l neurons in the hidden layer is $X^* \in RL$, $X* = (x_1^*, x_2^* \cdots, x_n^*)^T$, threshold θ_i, $i \in (1, l)$; $Y \in R^m$, $Y = (y_1, y_2 \cdots, y_m)^T$, threshold θ_i^*, $i \in (1, m)$. The weight from the input layer to the hidden layer can be an $n \times l$ matrix, i.e., $Wij\{i \in (1, n), j \in (1, l)$. Similarly, the weight matrix from the hidden layer to the output layer is $W_{ij}^*\{i \in (1, n), j \in (1, l)\}$. Each element of the neural network output is

$$x_j^n = f\left(\sum_{i=1}^{n} w_i x_i - \theta\right) i = 1, .. \cdots, l, \tag{4}$$

$$y_i = f\left(\sum_{i=1}^{k} w_i x_i - \theta_i\right) i = 1, .. \cdots, m. \tag{5}$$

When the training sample s is sent to the output layer, it is compared with the expected:

$$E^{(i)} = \frac{1}{2}\sum_{i=0}^{m-1}\left(d_i^{(s)} - y_i^{(s)}\right)^2. \tag{6}$$

The sum of training sample errors is the total error, where E is the sigma count $s = 1$, $E(s)$ is the 1, 2 sigma count $s = 1$ sigma $m - 1$:

$$E = \sum_{s=1}^{\text{count}} E^{(s)} = \frac{1}{2}\sum_{s=1}^{\text{count}}\sum_{i=0}^{m-1}\left(d_i^{(s)} - y_i^{(s)}\right)^2, \tag{7}$$

where the "count" is the total number of samples.

According to equation (4), if $E_i(1) \le \varepsilon(I = 1, 2 \cdots, m)$ (ε is the specified minimum error number), then, the bundle formation is trained, and the threshold value and corresponding weight of the neuron are determined. Adjust the weight along the negative gradient direction, that is

$$\Delta W_{ij} = -\eta\frac{\partial E}{\partial W_{ij}}, \tag{8}$$

where η is called the learning coefficient, equation (6) is transformed into

$$\Delta W_m^{l,l-1} = -\eta\delta_m^l \gamma_j^{l-1}, \tag{9}$$

where l is the number of layers, δ_m^l is the neuron in the layer γ_j^{l-1} is the output of the j neuron in the layer: l = level , while l < level.

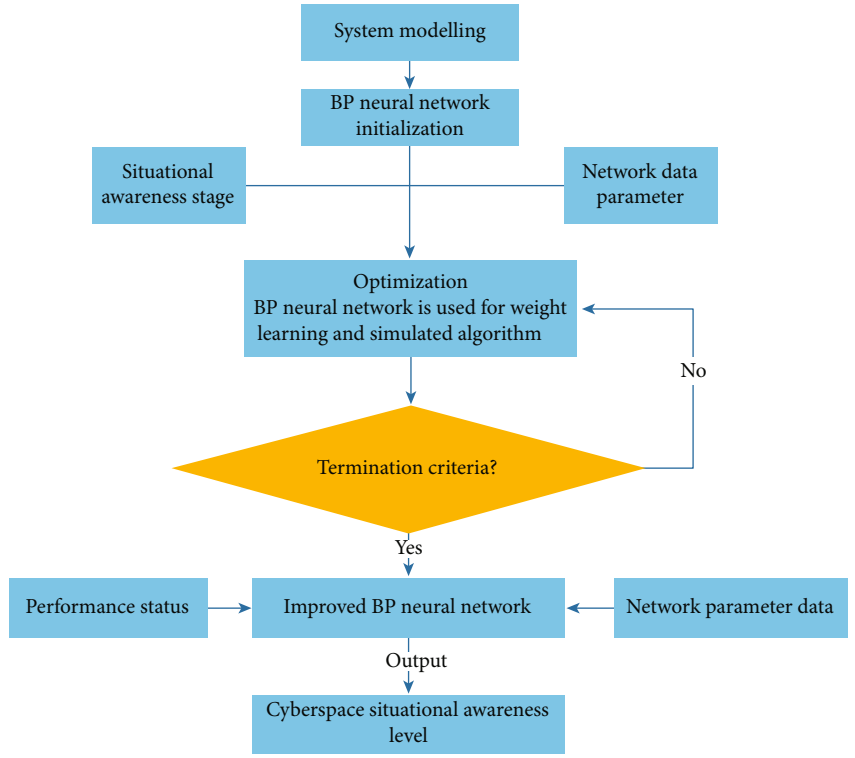

Figure 4: Optimized ANN-BP situational awareness assessment process.

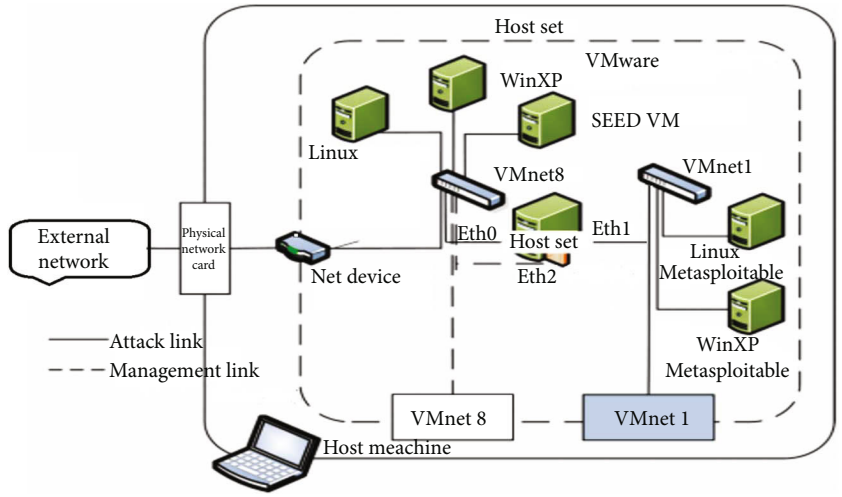

Figure 5: Network (Honeywall) topology.

$$\delta_m^l = \begin{cases} \left(\gamma_m^l - d_m\right) f'\left(I_m^l\right), \\ \sum_m \delta_{mj}^{l+1,k} f'\left(I_m^l\right). \end{cases} \tag{10}$$

3. Results and Discussion

The specific steps of the experiment include Honeypot installation and configuration, Honeywell shut down construction and configuration, installation, my SQL database login, and information collection. This experiment uses software to build virtual simulation, and the Matlab platform is employed to implement the standard ANN-BP. Table 4 shows the results of a comparison between the output of several test samples and the expected output. The input data is preprocessed by $\Delta x_i = (x_i - \min)/(X \max - \min)$, and the data is quantified to the interval [0, 1]. The traditional method of performing hyperparameter optimization has been grid search, or parameter swap, which is simply a complete search through a manually specified subset of the hyperparameter space of the learning algorithm. Where x_i

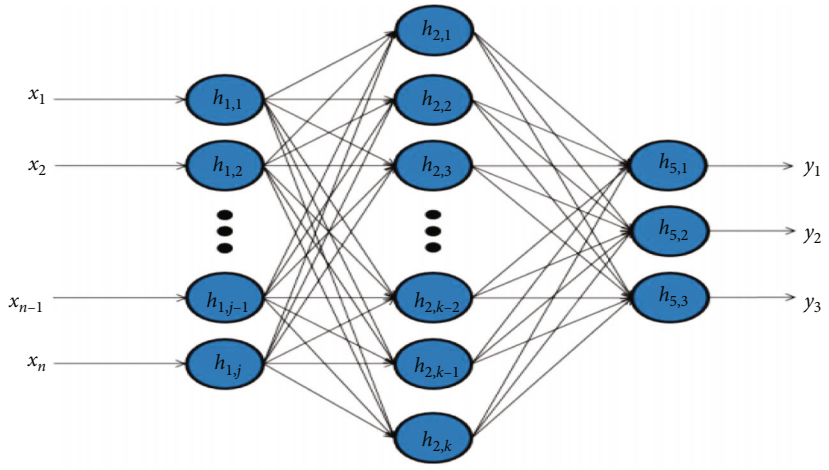

Figure 6: Multilayer structure diagram of ANN-BP algorithm.

Table 4: Actual output of test data.

Actual output	0.70	0.75	0.62	0.53	0.45	0.32	0.33	0.36	0.45	0.35
Expected output	0.72	0.74	0.67	0.51	0.40	0.36	0.29	0.35	0.40	0.30
Actual threat	***	***	**	**	**	***	*	*	**	*
Level	***	***	**	**	**	**	*	*	*	*

*low, **medium, and ***high.

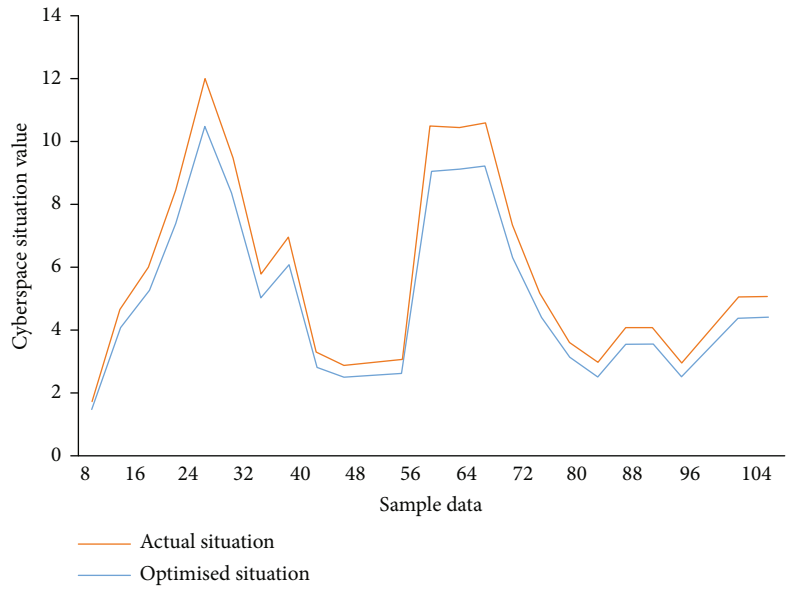

Figure 7: Comparison between the situation value and the actual value of the ANN-BP assessment.

is the datum of the generation table, min is the minimum value, and max is the maximum value. Figure 7 is the comparison result between the situation value evaluated by the ANN-BP and the actual situation value. The ANN-BP algorithm can evaluate the situation of situational awareness in cyberspace, which weakens the human factor and improves the objectivity and authority of the results and can deal with nonlinear questions very effectively. The experimental results show that not only do the 80 training sets based on the ANN-BP model meet the evaluation of experts and professors but also the 20 test sets are consistent with the actual situation. The ANN-BP algorithm can evaluate the situation of situational awareness in cyberspace, which weakens the human factor improves the objectivity and authority of the results and can deal with nonlinear questions very effectively. The experimental results show that the modified BP

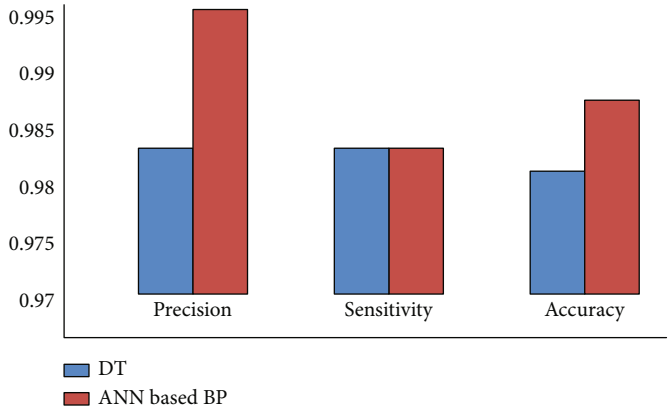

Figure 8: Performance comparison of ANN-BP and a decision tree.

oracle network can accurately evaluate the situational awareness system in cyberspace. In this study, the ANN-BP algorithm is used to quantitatively evaluate the level of situational awareness in network space. First, the requirements of situational awareness assessment in network space are analyzed. Then, in Figure 8, performance comparison of ANN-BP and a decision tree the shortcomings of traditional ANN-BP are introduced, and the defiring optimization method is used for improvement. When these different models are employed to make major predictions, stakeholders are seeking more transparency and explanation. Results depicting the output of ML models are crucial in cybersecurity, as specialists expect substantially more information from the model than a simple binary output for their analysis.

4. Conclusion

In this study, an ANN-BP creates a robust cyber situation awareness model that enhanced cybersecurity by improving intrusion prediction. A machine learning-based intrusion detection system's effectiveness and efficiency in detecting threats to organizations and other network users are interesting and valuable. Because cyber threats fall into a variety of categories, certain machine learning algorithms may not be able to detect them on a computer network. The relationship between the level of cyber situational awareness and the perceptual parameters quantitatively evaluates the situation of situational awareness. The variable step size learning strategy and simulated annealing method are used for optimization to build a virtual network environment, after the construction and modelling of a threat detection prediction model, which suggests a safe system than a single classifier. They are data-oriented, which makes it easier to detect patterns in the datasets using the IDS classifiers. The proposed work offers better precision (0.989) and 0.984 sensitivity, while its accuracy was useful at 98.7% than the DT classifiers. It seems a small difference but important to note that there is a difference. This system has importance for the computer network administrator. Future work can introduce multiensemble algorithms in the perception phase to improve IDS accuracy.

Data Availability

Data has been cited inside the paper and also available upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

The authors appreciate the research facilities and library access of affiliated institutes/universities. This research was funded by NSFC (nos. 61972106 and 62072131), the Key R&D Program of Guangdong Province (no. 2019B010136003), the National Key Research and Development Plan (Grant no. 2019QY1406), and Science and Technology Projects in Guangzhou (no. 202102010442).

References

[1] S. Li, L. Jiang, Q. Zhang, Z. Wang, Z. Tian, and M. Guizani, "A malicious mining code detection method based on multi-features fusion," *IEEE Transactions on Network Science and Engineering*, 2022.

[2] O. Altay, T. Gurgenc, M. Ulas, and C. Özel, "Prediction of wear loss quantities of ferroalloy coating using different machine learning algorithms," *Friction*, vol. 8, no. 1, pp. 107–114, 2020.

[3] M. Ulas, O. Altay, T. Gurgenc, and C. Özel, "A new approach for prediction of the wear loss of PTA surface coatings using artificial neural network and basic, kernel-based, and weighted extreme learning machine," *Friction*, vol. 8, no. 6, pp. 1102–1116, 2020.

[4] S. Li, Q. Zhang, X. Wu, W. Han, and Z. Tian, "Attribution classification method of APT malware in IoT using machine learning techniques," *Security and Communication Networks*, vol. 2021, Article ID 9396141, 12 pages, 2021.

[5] S. Li, Y. Li, W. Han, X. Du, M. Guizani, and Z. Tian, "Malicious mining code detection based on ensemble learning in cloud computing environment," *Simulation Modelling Practice and Theory*, vol. 113, article 102391, 2021.

[6] P. Mishra, E. S. Pilli, V. Varadharajan, and U. Tupakula, "Intrusion detection techniques in cloud environment: a survey," *Journal of Network and Computer Applications*, vol. 77, pp. 18–47, 2017.

[7] C. S. Rao, R. S. Shankar, and K. Murthy, "Cyber-physical system—an overview," *Smart Intelligent Computing and Applications*, pp. 489–497, 2020.

[8] S. M. Aslam, A. K. Jilani, J. Sultana, and L. Almutairi, "Feature evaluation of emerging E-learning systems using machine learning: an extensive survey," *IEEE Access*, vol. 9, pp. 69573–69587, 2021.

[9] M. Ulas, O. Aydur, T. Gurgenc, and C. Ozel, "Surface roughness prediction of machined aluminum alloy with wire electrical discharge machining by different machine learning algorithms," *Journal of Materials Research and Technology*, vol. 9, no. 6, pp. 12512–12524, 2020.

[10] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," *Internet of Things*, vol. 7, p. 100059, 2019.

[11] I. H. Sarker, "Deep cybersecurity: a comprehensive overview from neural network and deep learning perspective," *SN Computer Science*, vol. 2, no. 3, pp. 1–16, 2021.

[12] E. Grechishnikov, M. M. Dobryshin, S. S. Kochedykov, and V. I. Novoselcev, "Algorithmic model of functioning of the system to detect and counter cyber attacks on virtual private network," *Journal of physics: conference series*, vol. 1203, p. 012064, 2019.

[13] M. Aledhari, R. Razzak, and R. M. Parizi, "Machine learning for network application security: empirical evaluation and optimization," *Computers & Electrical Engineering*, vol. 91, p. 107052, 2021.

[14] M. Putyato, A. Makaryan, and M. Evsyukov, "Conceptual approach to implementation of adaptive protection of operational cybersecurity centers," in *Computer science on-line conference*, Cham, 2021.

[15] E. Vitenburg and A. Nikishova, "Algorithm of software package of intellectual decision support when designing cyber security system at the enterprise," *Vestnik of Don State Technical University*, vol. 20, no. 2, pp. 178–187, 2020.

[16] O. Milov, A. Voitko, I. Husarova et al., "Development of methodology for modeling the interaction of antagonistic agents in cybersecurity systems," *Eastern European Journal of Advanced Technologies*, vol. 2, no. 9 (98), pp. 56–66, 2019.

[17] C. K. Shiva, B. Vedik, R. Kumar, S. Mahapatra, and S. Raj, "Impacts of computational techniques for wireless sensor networks," *Nature-Inspired Computing for Smart Application Design*, p. 87, 2021.

[18] B. Uchendu, J. R. C. Nurse, M. Bada, and S. Furnell, "Developing a cyber security culture: current practices and future needs," *Computers & Security*, vol. 109, p. 102387, 2021.

[19] J. Yao, X. Fan, and N. Cao, "Survey of network security situational awareness," in *International Symposium on Cyberspace Safety and Security*, Springer, 2019.

[20] G. Kou, S. Wang, and G. Tang, "Research on key technologies of network security situational awareness for attack tracking prediction," *Chinese Journal of Electronics*, vol. 28, no. 1, pp. 162–171, 2019.

[21] I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," *Journal of Big data*, vol. 7, no. 1, pp. 1–29, 2020.

[22] I. R. Shareef, "Design and implementation of smart security system based on artificial neural network," *Journal of Engineering and Applied Science*, vol. 11, no. 9, 2016.

[23] H. Yang, S. Li, X. Wu, H. Lu, and W. Han, "A novel solutions for malicious code detection and family clustering based on machine learning," *IEEE Access*, vol. 7, pp. 148853–148860, 2019.