Hindawi
Computational Intelligence and Neuroscience
Volume 2022, Article ID 7512289, 10 pages
https://doi.org/10.1155/2022/7512289

Research Article

Application of Bayesian Algorithm in Risk Quantification for Network Security

Lei Wei

School of Criminal Justice, Shanghai University of Political Science and Law, Shanghai 201701, China

Correspondence should be addressed to Lei Wei; weilei@shupl.edu.cn

Received 24 February 2022; Revised 22 May 2022; Accepted 17 June 2022; Published 8 July 2022

Academic Editor: Shahid Mumtaz

Network security risk quantification involves both technical and management aspects. Risk quantification has great uncertainty and cannot be fully quantified. Therefore, the fully objective realization of network information security risk quantification is not yet mature. This paper analyzes and quantifies the network security risks caused by various threat sources through a network security risk quantification model based on the Bayesian algorithm. By combining expert knowledge, the conditional probability matrix under the inference rule of the Bayesian algorithm is clarified, and the subjective judgment information of experts on the damage degree of the target information system is synthesized into the prior information system of network security threat. The Bayesian algorithm is used to realize the observation node of objective assessment information and combining subjective security threat levels to achieve continuity and accumulation of security assessments. The error is about 3%, which has a very good effect on the quantification of network security risk.

1. Introduction

With the continuous development of network information and the Internet of Things, especially the continuous growth of the Internet information industry in recent years, the quantification of network security risks on the Internet has become more and more important [1, 2]. Problems existing in adopting changes to traditional solutions cannot obtain effective parameters, which leads to the low quantification precision of cybersecurity risk quantification quantitative model, and the optimization of network security risk quantitative parameters is studied by the numerical simulation method. For the host risk calculation, the risk vector is defined according to the state of the host, and a reasonable weight function is obtained through weighted calculation, and the direct risk value and indirect risk value of the host are combined to obtain the host risk value. While communication between different computer networks can increase efficiency, it also presents an opportunity for cyberattacks, a new attack method for systemic security vulnerabilities, widely used by intruders and hackers. In addition, the dangers and threats to information system security are gradually eliminated. Information system security has always been the focus of attention. A large number of intrusions on the Internet make computer users and many organizations face potential network security risks. Therefore, there is a strong need to prevent network systems, organizations, and government agencies from being attacked [3]. An intrusion can be interpreted as an attempt to break into an information system and disrupt various aspects of the system's integrity, availability, confidentiality, or service performance. Organize some preventive measures to protect network systems, servers, and confidential data from intrusion, such as using passwords, firewalls, or strict access control mechanisms to verify the identity of users. These protections are not completely protective because they fail to detect malicious attacks from ill-intentioned workers and cyberattacks, for example, buffer flooding attack, which exploit application feeble and provide great security. The issue of cybersecurity has been a high concern in every country, especially in military needs. The advantage of using a cybersecurity system for evaluation is the wide range of system accuracy postulates. Blurred set theory and blurred logic have become effective methods for quantitatively

representing and dealing with inaccurate choices. A blurred set or blurred number can properly represent inexact parameters and can be manipulated by various operations on the fuzzy set or fuzzy number. The comprehensive assessment mode of computer network communication security is a matter of collective efforts. Group decision-making (i.e., multiple experts) is typical decision-making behavior. Using this expert can alleviate some decision-making difficulties caused by complex and uncertain problems [4–6]. Group decision-making problems tend to follow a general solution consisting of two phases: the aggregation phase and the development phase. Many aggregation operators and methods have been developed to solve group decision problems with linguistic information. It can effectively avoid information loss and false positives in the process of language information processing. The Bayesian algorithm embodies the simple statement of conditional independence that each variable is an autonomous nondescendant in the graph given its parent state. This feature can be used to reduce (sometimes greatly) the number of various parameters required to characterize a variable. Such an algorithm provides an efficient way to calculate the posterior probability. Effective decision-making and quantitative assessment of network information security risks are one of the effective ways to solve security problems in information systems. Information security assessment is the application of risk assessment theory and method in the information system. Including fault tree analysis, AHP (analytic hierarchy process), and fuzzy comprehensive evaluation, information security assessments have been used by reviewers. Through the assessment, let the masses discover the problems and contradictions in information security, and the methods and measures to solve these problems. Therefore, the information security evaluation is very important to improve the security significance of the information system. However, to date, the impact of human factors and management measures in the area of information systems have not been fully considered. Meanwhile, information security threat assessment involves both technical and management aspects. The assessment is subject to significant uncertainty and cannot be fully quantified. As such, it is difficult to achieve a fully objective cybersecurity risk assessment. This research integrates subjective and objective cybersecurity assessment messages and establishes a quantitative model of network security threat assessment based on the Bayesian algorithm. First, the decision-making method fully draws on the experience and evaluation by every decision maker to evaluate the target intelligence system, which largely makes up for the singularity of the decision-maker's individual judgment; second, compared with neural network, Bayesian network (BN) can completely describe human reasoning process. Dynamically reflect the risk of the system, and if the attack firewall is blocked by the firewall, it will not affect the internal network. Even if the internal network is imperfect, there is no risk under the protection of the external firewall, which ensures the security of the network to the greatest extent. For different network settings of different matrix parameters, different risk assessment results will be obtained after setting the state transition matrix, observation matrix,

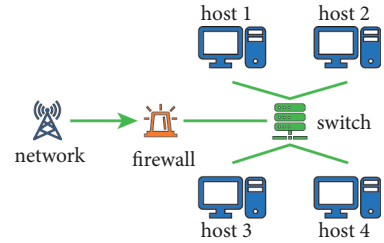

Figure 1: Study network system structure.

and initial state, which can adapt to different network environments and is universal. The calculation amount of the model is very small, and the calculation process can be completed in a very short time, which ensures the real-time assessment and real-time reflection of network risk. However, it is difficult to control the size of the observation matrix and associate the observation matrix with the state transition matrix. The safety evaluation based on the Bayesian algorithm can not only explain the safety evaluation process quantitatively, but also embody the accumulation and continuity of safety evaluation [7–9]. Therefore, the information security quantitative model based on the Bayesian algorithm can fully taking into account the subjective judgment data of various decision makers, and it can also prove the continuity and accumulation of safety assessment. In addition, the confidence of the prior information of the Bayesian algorithm is improved.

2. Network Security Risk Quantification

In recent years, with the rapid development of electronic communication technology and networks, the national security boundary is not limited to geographic space, but extends to information networks. The network is becoming an increasing number of important in people's lives, and the issue of network security issues cannot be ignored. Nowadays, the network system needs to ensuring the security of network communication, and first of all, it is necessary to make a correct assessment of the network risk. In order to quantify the network risk value and evaluate the threats in the process of network operation, optimizing real-time cybersecurity risk quantification methods were invented. In the past, it was set manually, and now the new method is to set the parameter matrix. The set parameter matrix simplifies the complexity of the configuration. Network security has become an important issue closely related to national security. Therefore, how to accurately quantify the security risks existing in the network, take defensive measures accordingly, as shown in Figure 1, and minimize the losses caused by network security risks as much as possible have become the key issue of relevant scholars' research, and its research has a high degree of importance value. Generally speaking, the measurement of network security risks was achieved through establishing a model. It was impossible to obtain reasonable and effective important factors, and the result of measurement was not reliable. In view of the disadvantages of the traditional methods, some of them introduced the artificial intelligence into the study of

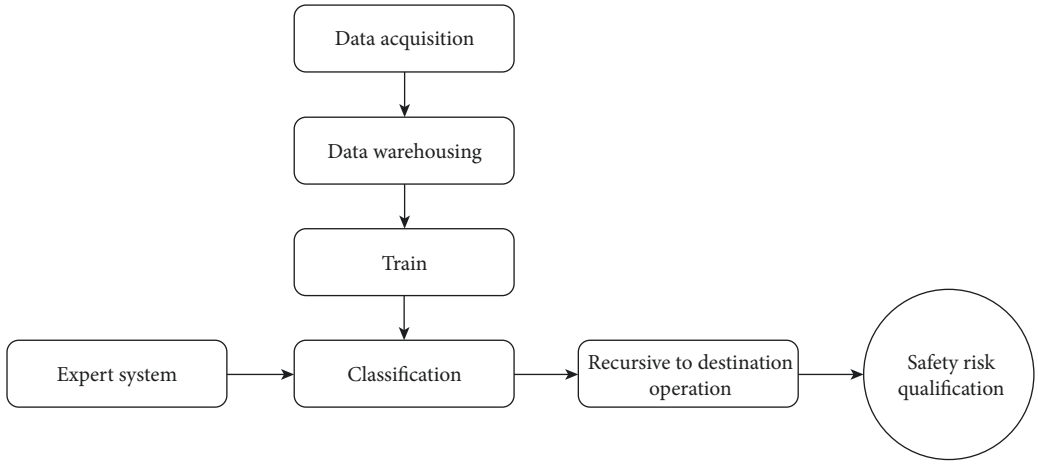

Figure 2: Discussion on the research roadmap.

network security risks, mainly including the methods of the artificial nerve network and the methods of the support machine. The artificial neural network method has a good approximation ability to nonlinear functions. It is realized on the basis of assuming that the empirical risk is minimized [10–12]. However, the risk cannot be minimized. It has certain defects in theory, which is not good for the quantitative results. It will also cause a certain delay. The support vector machine method is better than the artificial neural network method in solving this kind of problem and has a good expansion ability, but its parameters are relatively large, and the problem can be solved by optimizing the parameters. In view of this, according to the characteristics of the nonlinear characteristics of network security risk, the delay parameter is introduced, and the important parameters of the support vector machine model are optimized through numerical simulation, so as to improve the quantization accuracy. The experimental test is used to verify the performance of the network security risk quantification model after parameter optimization on the actual network security risk quantification.

Based on the Bayesian model, the quantification and optimization of the network security risk assessment method are realized, and based on the Bayesian model, the network security risk quantification method is described in real time, the shortcomings are analyzed, and optimization measures are proposed. The innovation and practicability of this method are presented. It is proved that the risk description rule base can get the optimal solution and can be well used for risk assessment. The research roadmap of this paper is shown in Figure 2. Bayes' rule offers a way to calculate the hypothesis probability with the priori probability. The best assumption is the most likely hypothesis because there are prior probabilities for various hypotheses h on the data D to be observed, and h is the hypothesis space that contains the objective function. The Bayesian algorithm (BA) has many probability classes method and an optimal method for predicting the class of unknown samples [13–15], widely used in data deep search, image processing, bioinformatics and multitarget retrieval of information, and other fields. Look at how the conditions are collected in the data set, and find out which data belong to the different categories using how the conditions are collected. Based on a comprehensive analysis of current research challenges, this time a new algorithm was adopted that uses the Bayesian algorithm to solve problems such as classification rate and false positive rate [16, 17]. Bayesian networks (BN) are used to represent dependencies between nodes using Bayesian theory, which can be represented by variables. BN consists of nodes, arcs, and a node probability table (NPT). Arcs represent causal relationships, and NPTs represent probability tables that summarize the probabilities of occurrence between causal nodes [18, 19]. BN is very useful for solving problems such as insufficient information, a posteriori inference, and the change from qualitative to quantitative problems by learning new knowledge about the relationship between posterior and prior probabilities.

Bayesian networks (BN), also known as directed acyclic graph models (or simply Bayesian network), consist of a series of combinations that express causal rules, and BN corresponds to another GM structure called Directed Acyclic Graph (DAG), belonging to the model series of probability graphics [20–22]. This structure is very popular in statistics, machine learning, artificial intelligence, etc. Bayesian networks can efficiently represent and compute a joint probability distribution (JPD) over a set of random variables. These structures were used to express the places with relative uncertainty. From the picture, it could be seen that each node represented a random variable, and the boundaries between the probability of each node corresponded to the random variable were relevant. The conditions in the picture depended on the estimation, and they usually used the known statistics and calculation techniques. Therefore, Bayesian theory combines principles such as graph theory, probability theory, computer science, and statistics, and GMs with undirected edges are often referred to as Markov random fields or Markov networks. These networks are based on the concept of Markov chains, which provide a simple definition of independence, that is, between any two different nodes [23–26]. The formulas for calculating the mean relative error MAPE and the root mean square error RMSE are as follows:

$$\text{MAPE} = \frac{1}{n}\sum_{i=1}^{n}\frac{\left|y'_{\text{true}} - y_{\text{estimate}}\right|}{y_{\text{true}}} \times 100\%,$$
$$\text{RMSE} = \sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(y'_{\text{true}} - y_{\text{estimate}}\right)^2}, \quad (1)$$

where n is the total number of samples, y'_{true} is the true value, and y_{estimate} is the estimated value.

The set u is the mathematical expectation assigned to the weight vector $\omega = (1/n, 1/n, \ldots, 1/n, 1/n)$, σ is the standard deviation between u and ω, and there are

$$u_n = \frac{1}{n}\frac{n(n+1)}{2} = \frac{n+1}{2},$$
$$\sigma_n = \sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(i - u_n\right)^2},$$
$$\omega'_n = \frac{1}{\sqrt{2\pi\sigma_n}}e^{\left(i-u_n\right)^2/2\sigma\pi}, \quad (2)$$
$$\omega = \frac{\omega'}{\sum_{i=1}^{n}\omega'}.$$

In the above formula, u_n is the mathematical expectation, σ_n is the standard deviation, ω'_n is the distribution function, and ω is the importance quantification value.

3. Analysis of Bayesian Model Results

Network security means that the hardware or software of the network and the data in its system are protected from property loss and personal safety due to accidental or malicious damage, so as to maintain the continuous and reliable operation of the system. Network security should include enterprise (company) security system, transmission security, data security, firewall security, server security, etc. If you want to realize that the personal information (such as bank account number and ID card information) or login information transmitted on the network will not be found by others, you must ensure that the system software, application software, and database have certain self-protection functions, and ensure that these applications cannot be accessed without authorization. In the real world, there is no absolute network security. Especially, in the case of developed network technology, it is a major issue that must be carefully considered to prevent all forms of hacker attack. Everyone has the same definition of network security, but from different perspectives. For enterprises, if there are network security problems, it may cause heavy losses to enterprises; for the country, it may damage national security. To solve these network security problems, programmers need to make great breakthroughs in technology and improve and deal with all kinds of sudden software security problems in time.

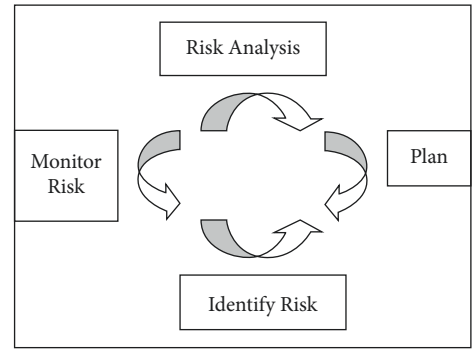

Figure 3: Risk quantification diagram.

The characteristics of the new network security risk are as follows: all kinds of homogeneous and heterogeneous data are widely collected, stored, analyzed, and applied, and data have increasingly become an important strategic resource and new production factor. Information systems and platforms show the characteristics of huge data storage scale, diverse data types, fast data generation speed, and high data value. These valuable data will become the target of criminals' crimes, and the problem of data security will become more prominent in the era of big data. In the context of the Internet and cloud platforms, information virtualization not only promotes the development of the "four new economies" but also makes network security risks more hidden. For example, online pyramid schemes, online drug trafficking, virtual currency, and ransomware based on the Internet platform are characterized by strong concealment, fast transmission speed, virtualization, difficulty in obtaining evidence, a wide range of cases involved, and strong anonymity. The Internet, industrial Internet, and Internet of Things have become "new infrastructure." The network environment under the new infrastructure is becoming more and more complex and heterogeneous. Although personalized services can be provided according to users and business needs, with the increasing of various network attack means, the need for security is increasing in all key links of heterogeneous networks. The innovation of artificial intelligence technology promotes the development of "four new economies," and interweaves the traditional network security risks with the new network security risks. The relationship diagram is shown in Figure 3. Information and intelligent technology are a double-edged sword, which not only brings new network security risks, leads to the increase of new intelligent network attack means, but also promotes the formation of new network security governance means.

Different from traditional risks, network security risks are systematic and interdependent and have both high-frequency low-loss and low-frequency large losses. However, traditional risk assessment methods can still be used for reference, and network security risks have been preliminarily described. The probability of reaching the final result gives several relevant evidence variables. The final result possibly encoded into the model along with the probability of occurrence of the evidence variable [27–29]. Assuming that the final result is

generated, the probability of the evidence variable is independent of the probability of other evidence variables giving the final result, and the decision-making group is composed of four experts, and the evaluation target is the highest TL [30, 31]. Assuming that the target TL is high, medium, and low, the quantitative judgment information provided by the four decision makers is as follows:

$$\begin{aligned} U_1 &= (0.3, 0.5, 0.3), \\ U_2 &= (0.2, 0.5, 0.3), \\ U_3 &= (0.37, 0.2, 0.3), \\ U_4 &= (0.3, 0.6, 0.33). \end{aligned} \tag{3}$$

In the formula, U_1, U_2, U_3, U_4 represent the matrix value under different attack strategies. According to the equation, the operator weight vector w can be obtained:

$$w = (0.123, 0.367, 0.432). \tag{4}$$

Among them, w is the arithmetic weight operator.

Then, the TL evaluation value U of the decision-making group is

$$U = (0.245, 0.356, 0.352). \tag{5}$$

In the formula, U represents the combined attack value.

As shown in Figure 4, the state collection of the variables in the model looks as follows:

$$\begin{aligned} \mathrm{TL} &= \{\mathrm{High}, \mathrm{Medium}, \mathrm{Low}\}, \\ C &= \{\mathrm{Big}, \mathrm{Middle}, \mathrm{Small}\}, \\ T &= \{\mathrm{High}, \mathrm{Midium}, \mathrm{Low}\}. \end{aligned} \tag{6}$$

In the above formula, the threat level is TL, and C and T are state variables.

The average risk value of the entire network at time t is

$$\overline{R(t, j)} = \frac{1}{L} \sum_{l=1}^{L} R_l(t, j), \quad 1 \le j \le 10. \tag{7}$$

The host risk value is recorded as $R_l(t, j)$, L is the number of units, and $\overline{R_l(t, j)}$ is the average host risk.

The risk-independent situation is the same. In the risk-dependent situation, with the increase of the confidence level, the VaR value and ES value of network security incident losses gradually increase. When the confidence level is low, as shown in Figure 5, the splice distribution and the mixed distribution have smaller basic VaR and ES values in describing the loss of network security events, so they are better than the thick-tailed distribution in describing the loss of network security events. When the confidence level is high, the splicing distribution and the thick-tailed distribution are basically the same in describing the loss of network security risk; that is, the VaR value and the ES value are in the same order of magnitude, while the mixed distribution has a smaller VaR value. Therefore, under the condition of network risk dependence, when the confidence was high, the mixed distribution could better describe the loss risk of network security events.

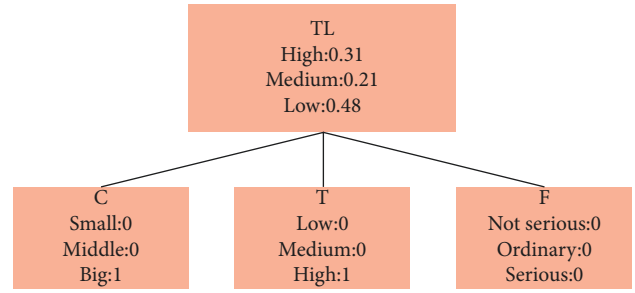

Figure 4: State collection diagram of variables in the model.

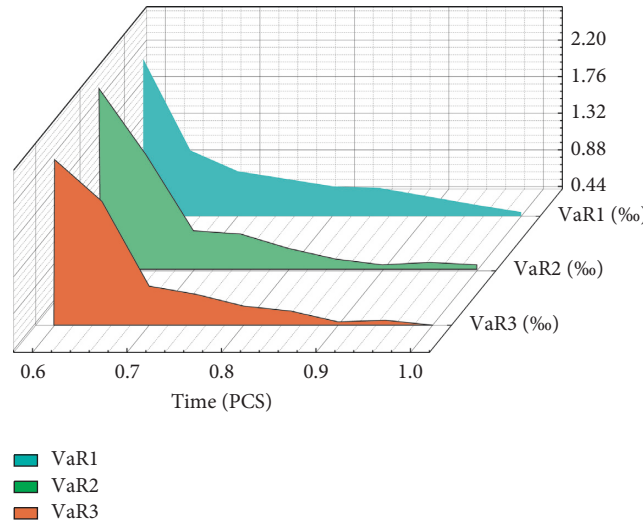

Figure 5: VaR values in different states.

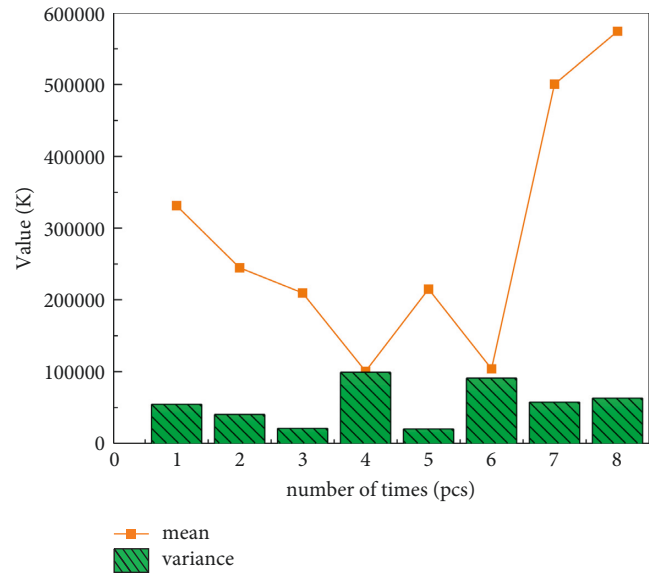

Figure 6: Unequal variance curve.

Network security incidents originate from threats and vulnerabilities. The possibility of incidents can be determined by evaluating threats and vulnerabilities of information via algorithms. At the same time, the impact of

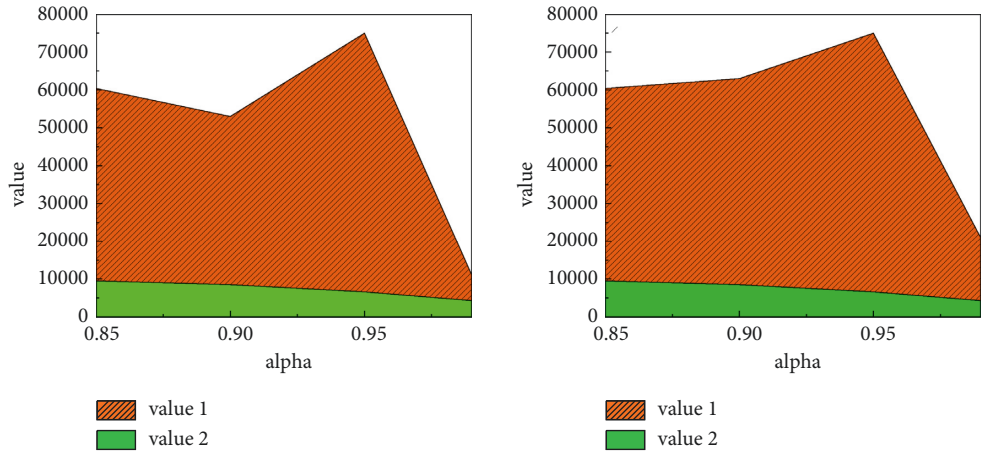

Figure 7: Quantitative value of network security risk.

network information protection incidents is related to funding, and conclusions can be drawn through funding assessment. As shown in Figure 6, information security risk can be regarded as the impact on capital. To simplify the model, only the following factors are considered: impact on capital, frequency of threats to capital, vulnerability of capital F, and threat level TL. In this case, a quantitative evaluation model of information security based on the Bayesian algorithm is established.

There are many hosts in a network. Due to the different importance of the location, the services provided, and the importance of storing and processing data, the importance of the hosts must be different. If an ordinary host at the edge of the network is attacked or completely damaged, there should be no significant impact on the risk status of the network [32]. The impact of network risk was also great. Therefore, in order to figure out the different impact of different host on the network risk and more accurately describe the network risk, the relative importance of the host was introduced, and the traditional calculation method of network risk was modified and weighted. In this way, the risk changes of the entire network can be reflected more realistically, and focused remedial measures can be taken to improve the efficiency of developing security policies.

Analysis of Figure 7 shows that, compared with the comparative literature methods and methods, the method in this paper is most consistent with the quantification value and time results of network security risk, and there are only few differences, while the risk quantification results of different methods and the actual results are very different. The main reason is that the parameters optimized by the method in this paper are the most reasonable, which can make the quantitative results tend to the actual values. Through a more objective analysis of the reliability of the method in the network security risk quantification results, the optimization performance of the method in this paper for important parameters is verified.

The spliced distribution is more sensitive to the change of the shape parameter. When the shape parameter becomes larger, its mean, variance, VaR, and ES values increase exponentially, while the results of the thick-tailed distribution

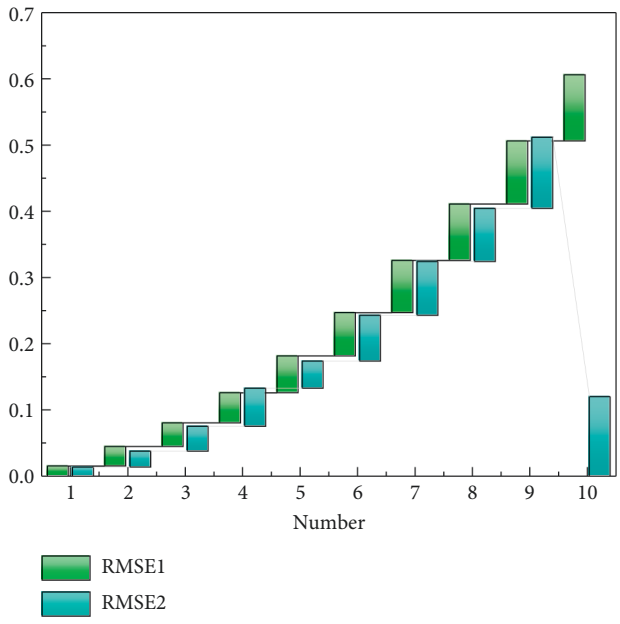

Figure 8: RMSE values under different parameters.

and the mixed distribution are relatively stable, like Figure 8. For thick-tailed distribution, when the shape parameter increases, its mean, variance, VaR, and ES values increase; for mixed distribution, when the shape parameter increases, its mean, variance, VaR, and ES values change slightly mildly, so the mixed distribution has good robustness in parameter setting. Figure 9 compares and analyzes the probability distribution of network security risk losses under risk dependence and risk independence.

Figure 10 shows that under risk independence, the splicing distribution can better reflect the possibility of the extreme importance of the network security event, but the extreme importance of the splicing distribution is still lower than the possible extreme value of the mixed distribution. Figure shows that, under the risk dependence, both the spliced distribution and the mixed distribution show good thick-tailed and extreme value characteristics. Based on the

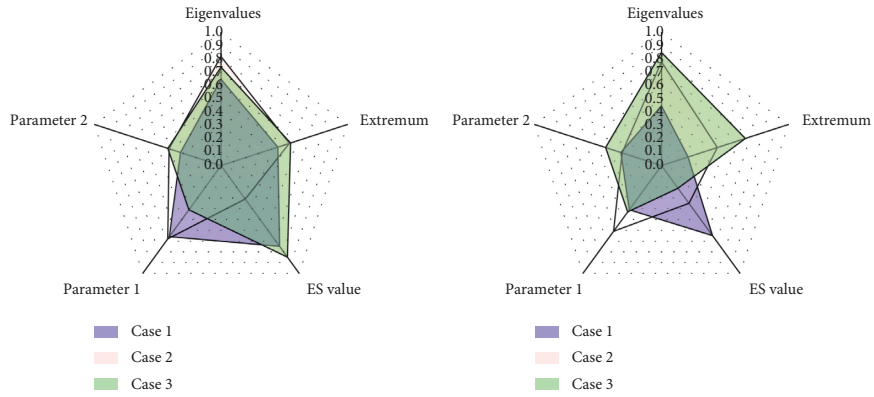

Figure 9: Different parameter values under risk independence.

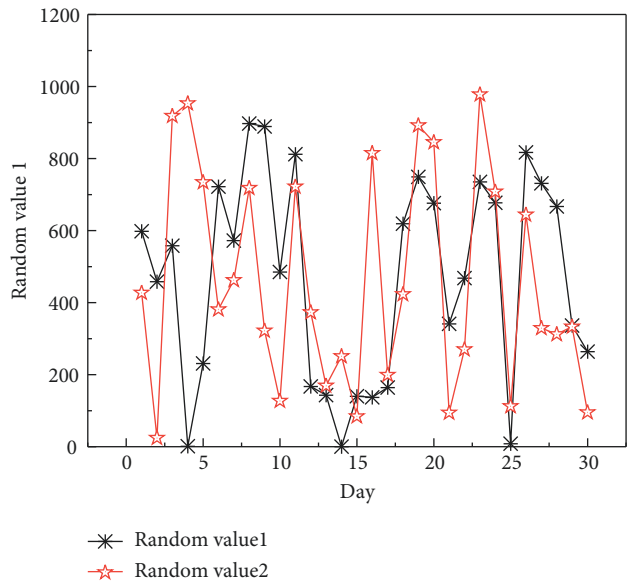

Figure 10: Random number of network attacks.

average risk value at a certain moment, a qualitative model of network security was established by using the support machine with time delay. Then, the important factors in the model were optimal with the combination of the ant group method and the simulation method. The test results show that the method has excellent parameter optimization performance and high network security risk quantification accuracy.

Compared with the change of network risk, the change of risk value calculated by the traditional method is relatively gentle, like Figure 11. The disadvantage of this quantitative method is that network administrators will only notice that it is too late to adopt remedial strategies when the network risk value exceeds the alert value. As shown in Figure 12, the average risk value of the network calculated by the method in this paper varies greatly from time to time. The reason is that the absolute value of the risk of relatively important hosts in the network does not change much, but because of its high weight, it can be caused by the new calculation method. Therefore, the advantage of the method in this paper is that it can detect significant changes in network risks as early as possible, highlight the impact of important hosts on network risks, and achieve focused protection, which is of great significance for improving the security of the entire network and adopting corresponding security strategies in a timely manner.

Most of the existing network security risk measures are qualitative analysis or single loss distribution representation, but this way of thinking ignores the characteristics of system city, interdependence, and network security risk with both high-frequency and low-frequency losses and low-frequency huge losses. Based on the Bayesian method, this paper quantitatively evaluates the network security risk loss. The research results show that the network security risk loss has thick tail characteristics, and the splicing distribution can better describe the extreme events of the network security risk than the single distribution; and the mixed distribution is better than the splicing. Distribution is more advantageous in risk assessment and safety capital preparation. In the case of

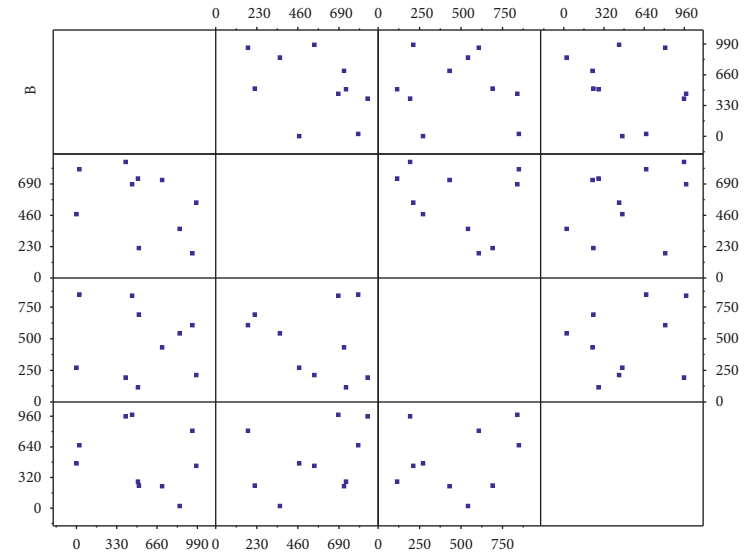

Figure 11: Network random frequency statistics.

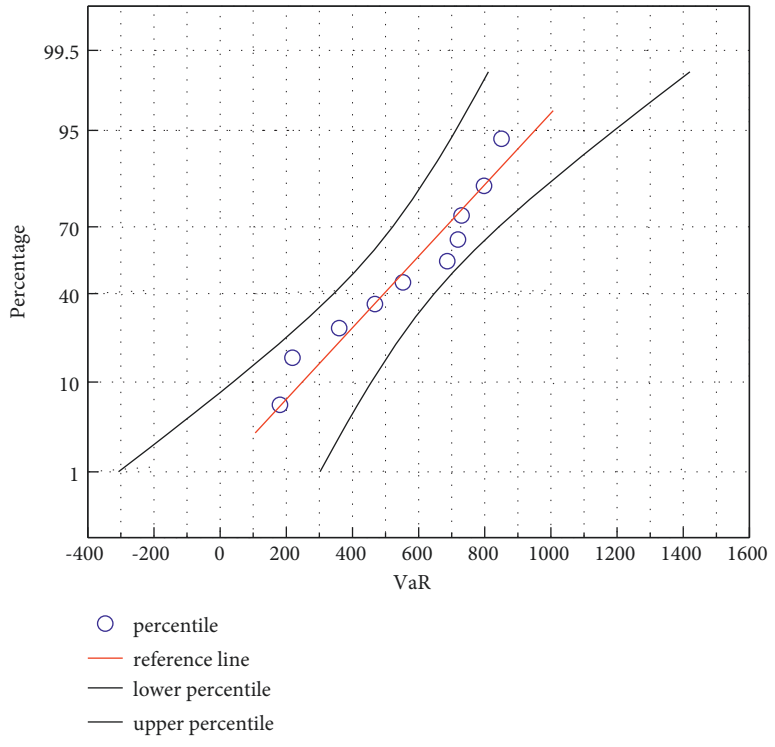

Figure 12: Statistics of network security risk value.

independent risk, the spliced distribution can better estimate the loss of network security risk; while in the case of dependent risks, the mixed distribution can better describe the loss of network security risk. In addition, the parameter sensitivity analysis of the distribution shape shows that the mixed distribution has good stability, and the distribution can better describe the extreme value and thick-tailed characteristics of network security risk loss. The Bayesian model is an effective method to quantitatively analyze network security risk losses, and its results can guide enterprises to conduct corresponding network security risk management.

4. Conclusion

Cybersecurity risk quantification is the basis and premise of network system security management. Aiming at the problem of ignoring the correlation and difference of nodes in traditional quantitative assessment methods, a node-related network security risk quantification method is proposed. In this method, the network node correlation is introduced into the quantitative assessment process based on the hidden Markov model, which solves the problem that the node correlation is generally ignored in the existing

quantitative assessment methods of network security risk, characterizes the differences in the contribution of different hosts to network risk. The early network security risk quantification model did not take into account the relatively personal threat evaluation information given by decision makers in professional experience. This is a loss of information for the overall evaluation model. Based on the systematic analysis of information security threat factors, this model combines subjective TL judgment information and objective situation information to establish a network information security risk quantification model based on Bayesian operator. The actual process of information security risk quantification can more accurately reflect the real TL. Bayesian network has been widely used in the field of prediction evaluation. Many scholars use the Bayesian network to conduct network security prediction evaluation research, and gradually become practical. However, the Bayesian network still has the following problems to be solved when it is used in the field of prediction evaluation: (1) in reality, the Internet is constantly changing, but the standard Bayesian network is a static model. Therefore, how to make the standard Bayesian network predict dynamic network security is a worthy research direction. (2) In the study of Bayesian network knowledge synthesis, we maintain the network structure unchanged; that is, we assume that the network structure can describe the problem domain well. However, when the uncertainty knowledge is not consistent with the network structure and comes from unreliable data sources, it may not reflect the problem model realistically. How to combine the related algorithms of Bayesian network structure and realize the synthesis of uncertainty knowledge by modifying the network structure is also a very meaningful research direction. (3) In Bayesian network prediction, efforts are still needed to encode expert knowledge. That is, the Bayesian network needs to be solved. On the one hand, it overcomes the static limitations of the expert system, and it is better to realize knowledge storage, acquisition, and update. The new and more reliable probability knowledge updates the existing Bayesian network and enhances the practical significance of the Bayesian network. The method of quantifying network security risk in real-time provides an effective method for network administrators to manage the network. You can monitor the status of the network at any time, discover network risks, and solve them in time. This paper makes some optimizations and improvements on the basis of the Bayesian method, which makes this method simpler to use and more reliable in parameter setting and evaluation. In the research, it is found that the algorithm of threat degree can classify the types of attacks, and by sorting the degree of threat, the attention of the network maintenance system to irrelevant attacks can also be reduced. The threat algorithm is subject to further modification and testing. With the rapid development of the network, the speed of maintaining network security cannot keep up with the speed of network development. In the future research, it is necessary to reduce network risk, strengthen the research of network risk identification and self-healing, realize the automation of network system maintenance, and meet the needs of most network users. Combined with the relevant algorithms of Bayesian network structure, the uncertainty in network security quantification is realized by modifying the network structure.

Data Availability

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

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] W. Kejin, S. Wenhui, and Z. Aichun, "Research on the application of electronic information technology in the Internet of things," *Journal of Physics: Conference Series*, vol. 1570, no. 1, Article ID 012067, 2020.

[2] I. Cholissodin, D. S. Seruni, J. A. Zulqornain et al., "Development of big data app for classification based on map reduce of naive Bayes with or without web and mobile interface by RESTful API using Hadoop and spark," *Journal of Information Technology and Computer Science*, vol. 5, no. 3, pp. 302–312, 2020.

[3] X. Ai, H. Chen, K. Lin, Z. Wang, and J. Yu, "Nowhere to hide: efficiently identifying probabilistic cloning attacks in large-scale RFID systems," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 714–727, 2021.

[4] F. Jin, M. Cao, J. Liu, L. Martínez, and H. Chen, "Consistency and trust relationship-driven social network group decision-making method with probabilistic linguistic information," *Applied Soft Computing*, vol. 103, no. 3, p. 107170, 2021.

[5] M. Yazdani, A. Mohammed, C. Bai, and A. Labib, "A novel hesitant-fuzzy-based group decision approach for outsourcing risk," *Expert Systems with Applications*, vol. 184, p. 115517, 2021.

[6] M. Najafzadeh, A. Etemad-Shahidi, and S. Y. Lim, "Scour prediction in long contractions using ANFIS and SVM," *Ocean Engineering*, vol. 111, pp. 128–135, 2016.

[7] Y. Li, G. Huang, C. Wang, and Y. Li, "Analysis framework of network security situational awareness and comparison of implementation methods," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, pp. 1–32, 2019.

[8] P. G. George and V. R. Renjith, "Evolution of safety and security risk assessment methodologies towards the use of bayesian networks in process industries," *Process Safety and Environmental Protection*, vol. 149, pp. 758–775, 2021.

[9] F. Chen, C. Wang, J. Wang, Y. Zhi, and Z. Wang, "Risk assessment of chemical process considering dynamic probability of near misses based on Bayesian theory and event tree analysis," *Journal of Loss Prevention in the Process Industries*, vol. 68, p. 104280, 2020.

[10] F. Saberi-Movahed, M. Najafzadeh, and A. Mehrpooya, "Receiving more accurate predictions for longitudinal dispersion coefficients in water pipelines: training group method of data handling using extreme learning machine conceptions," *Water Resources Management*, vol. 34, no. 2, pp. 529–561, 2020.

[11] T. Poggio, A. Banburski, and Q. Liao, "Theoretical issues in deep networks," *Proceedings of the National Academy of Sciences*, vol. 117, no. 48, pp. 30039–30045, 2020.

[12] H. Hong, Z. Zhang, A. Guo et al., "Radial basis function artificial neural network (RBF ANN) as well as the hybrid method of RBF ANN and grey relational analysis able to well predict trihalomethanes levels in tap water," *Journal of Hydrology*, vol. 591, p. 125574, 2020.

[13] K. Gundersen, G. Alendal, A. Oleynik, and N. Blaser, "Binary time series classification with bayesian convolutional neural networks when monitoring for marine gas discharges," *Algorithms*, vol. 13, no. 6, p. 145, 2020.

[14] M. S. Siddiqui, C. Coppola, and G. Solak, "Discovering stable robot grasps for unknown objects in presence of uncertainty using bayesian models," *Towards Autonomous Robotic Systems*, vol. 13, no. 54, pp. 46–55, 2021.

[15] T. V. Hoang and H. G. Matthies, "An efficient computational method for parameter identification in the context of random set theory via Bayesian inversion," *International Journal for Uncertainty Quantification*, vol. 11, no. 4, pp. 1–18, 2021.

[16] D. Mei and Q. Liu, "A new algorithm for analysis of MiRNA expression profiles—svm-RFE-FKNN," *Journal of Imaging Science and Technology*, vol. 65, no. 3, pp. 1–8, 2020.

[17] W. Alhakami, A. ALharbi, S. Bourouis, R. Alroobaea, and N. Bouguila, "Network anomaly intrusion detection using a nonparametric Bayesian approach and feature selection," *IEEE Access*, vol. 7, pp. 52181–52190, 2019.

[18] R. Kaya and B. Yet, "Building Bayesian networks based on DEMATEL for multiple criteria decision problems: a supplier selection case study," *Expert Systems with Applications*, vol. 134, pp. 234–248, 2019.

[19] P. P. Mondal, P. M. Ferreira, S. G. Kapoor, and P. N. Bless, "Monitoring and diagnosis of multistage manufacturing processes using hierarchical bayesian networks," *Procedia Manufacturing*, vol. 53, no. 5, pp. 32–43, 2021.

[20] A. P. C. Chan, F. K. W. Wong, C. K. H. Hon, and T. N. Y. Choi, "A Bayesian network model for reducing accident rates of electrical and mechanical (E&M) work," *International Journal of Environmental Research and Public Health*, vol. 15, no. 11, p. 2496, 2018.

[21] C. E. Graafland and J. M. Gutiérrez, "Learning complex dependency structure of gene regulatory networks from high dimensional micro-array data with Gaussian Bayesian networks," p. 55, 2021, http://arxiv.org/abs/2106.15365.

[22] F. Delussu, F. Imran, C. Mattia, and R. Meo, "Fuel prediction and reduction in public transportation by sensor monitoring and bayesian networks," *Sensors*, vol. 21, no. 14, p. 4733, 2021.

[23] B. Mihaljević, C. Bielza, and P. Larrañaga, "Bayesian networks for interpretable machine learning and optimization," *Neurocomputing*, vol. 456, pp. 648–665, 2021.

[24] A. El-Awady and K. Ponnambalam, "Integration of simulation and Markov chains to support Bayesian Networks for probabilistic failure analysis of complex systems," *Reliability Engineering & System Safety*, vol. 211, p. 107511, 2021.

[25] G. F. de Arruda, F. A. Rodrigues, and Y. Moreno, "Fundamentals of spreading processes in single and multilayer complex networks," *Physics Reports*, vol. 756, pp. 1–59, 2018.

[26] H. Cherifi, G. Palla, B. K. Szymanski, and X. Lu, "On community structure in complex networks: challenges and opportunities," *Applied Network Science*, vol. 4, no. 1, pp. 1–35, 2019.

[27] N. Killoran, T. R. Bromley, J. M. Arrazola, M. Schuld, N. Quesada, and S. Lioyd, "Continuous-variable quantum neural networks," *Physical Review Research*, vol. 1, no. 3, p. 033063, 2019.

[28] K. Masmoudi, L. Abid, and A. Masmoudi, "Credit risk modeling using Bayesian network with a latent variable," *Expert Systems with Applications*, vol. 127, pp. 157–166, 2019.

[29] N. J. Venhuizen, M. W. Crocker, and H. Brouwer, "Expectation-based comprehension: modeling the interaction of world knowledge and linguistic experience," *Discourse Processes*, vol. 56, no. 3, pp. 229–255, 2019.

[30] K. Topuz and D. Delen, "A probabilistic Bayesian inference model to investigate injury severity in automobile crashes," *Decision Support Systems*, vol. 150, p. 113557, 2021.

[31] H. Wang, A. Núñez, Z. Liu, D. Zhang, and R. Dollevoet, "A Bayesian network approach for condition monitoring of high-speed railway catenaries," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 10, pp. 4037–4051, 2019.

[32] A. R. Abdou, P. C. Van Oorschot, and T. Wan, "Comparative analysis of control plane security of SDN and conventional networks," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3542–3559, 2018.