Journal on Big Data
DOI:10.32604/jbd.2021.017299
Article

Design of Cybersecurity Threat Warning Model Based on Ant Colony Algorithm

Weiwei Lin[1,2,*] and Reiko Haga[3]

[1]School of Electronic and Information Engineering, Fujian Polytechnic Normal University, Fuqing, 350300, China
[2]Engineering Research Center for ICH Digitalization and Multi-Source Information Fusion, Fujian Province University, Fuqing, 350300, China
[3]CommScope Japan KK, Nagatacho, Tokyo, 100-0014, Japan
[*]Corresponding Author: Weiwei Lin. Email: linww_cn@hotmail.com
Received: 11 May 2021; Accepted: 25 June 2021

Abstract: In this paper, a cybersecurity threat warning model based on ant colony algorithm is designed to strengthen the accuracy of the cybersecurity threat warning model in the warning process and optimize its algorithm structure. Through the ant colony algorithm structure, the local global optimal solution is obtained; and the cybersecurity threat warning index system is established. Next, the above two steps are integrated to build the cybersecurity threat warning model based on ant colony algorithm, and comparative experiment is also designed. The experimental results show that, compared with the traditional qualitative differential game-based cybersecurity threat warning model, the cybersecurity threat warning model based on ant colony algorithm has a higher correct rate in the warning process, and the algorithm program is simpler with higher use value.

Keywords: Ant colony algorithm; cybersecurity threats; warning model; index system

1 Introduction

After the advent of the Internet era, crimes involving cybersecurity have also emerged in endlessly. The cybersecurity of international organizations and countries, as well as the cybersecurity of enterprises or individuals, is always at risk of being attacked and harassed by hackers. And because most people do not have the ability to defend against network intrusion, they are helpless in the face of cybersecurity threats and can only let Trojan horses attack the network [1]. In order to solve cybersecurity problems, to face the increasingly complex network situation in the future, and to improve the ability to solve cybersecurity threats, warning of cybersecurity threats has become a subject of widespread concern. In the past warning models of cybersecurity threats, some cannot achieve the warning effect well, and some have complex structures and poor computing effects. Therefore, based on the ant colony algorithm, a warning model of cybersecurity threats is designed to improve the warning model of cybersecurity threats that cannot achieve the desired effect in the past. Both the ant colony algorithm and the improved ant colony algorithm that is gradually designed and improved can be used to find the best path. It is an algorithm that can gradually approach the global optimal solution by enhancing the better solution. Therefore, the ant colony algorithm is widely used in the computer field [2]. First, the structure of the ant colony algorithm is designed to find a local optimization model that can realize the warning function of cybersecurity threats. Second, the indicator system of cybersecurity threat warning is comprehensively judged and designed from the three perspectives of relevant policies, warning capabilities and final warning effects. Third, a cybersecurity threat warning model based on ant colony algorithm is designed. Finally, an experiment is designed to verify that the designed cybersecurity threat warning model based on ant colony algorithm is better than

the previous cybersecurity threat warning models, and the algorithm has low redundancy and practicality.

2 Establishment of Cybersecurity Threat Warning Model Based on Ant Colony Algorithm

2.1 Ant Colony Algorithm Structure Design

Ant colonies in nature usually secrete a chemical substance in the process of foraging so that other ants nearby can detect this pheromone and find the shortest path from the starting point to the ending point based on the pheromone [3–4]. In the process of finding the optimal path, ants will also release this pheromone, so the more ants behind, the higher the probability of choosing the optimal path. Moreover, the unique pheromone of this ant colony is very adaptable. Even if an obstacle suddenly appears in the middle of the path, the ant colony can quickly find a new shortest path [5]. Based on this existing optimal path finding method in nature, some scholars in the computer field have proposed an ant colony algorithm to find the optimal solution. The mechanism of ant colony algorithm in computer can be roughly summarized as the following process. First, when the artificial ants in the computer solve problems with each other, they need to find a better solution according to the guidance of pheromone. In the process of finding a better solution, these artificial ants will also leave behind the same pheromone. According to the iterative effect of the algorithm, the artificial ants at the rear can enhance the better solution based on these increasingly rich pheromones to obtain a better solution. In this way, a positive feedback mechanism of information is formed, enabling artificial ants to find solutions that are getting closer and closer to the optimal solution. Finally, at the end of the iteration, an approximate optimal solution can be obtained [6].

In the iteration, assuming that the number of iterations is t, the probability of the ant choosing the path (i, j) is:

$$p_{ij}(t) = \begin{cases} \frac{[\tau_{ij}(t)]^{\alpha}[\eta_{ij}(t)]^{\beta}}{\sum_{l \in N_i^k}[\tau_{il}(t)]^{\alpha}[\eta_{il}(t)]^{\beta}}, \text{if } j \in N_i^k \\ 0, otherwise \end{cases} \tag{1}$$

where, $p_{ij}(t)$ represents the probability of choosing the path (i, j) when the artificial ant moves from the starting point i to the end point j during the t-th iteration; N_i^k represents a collection of places that artificial ants can pass through at point i; $\tau_{ij}(t)$ represents the pheromone concentration left by artificial ants ahead when they pass the (i, j) path during the t-th iteration [7]; $\eta_{ij}(t)$ represents the heuristic information constructed by the path (i, j) and the pheromone of the artificial ant during the t-th iteration; Both α and β represent the weight factors of pheromone and heuristic information emitted by artificial ants [8].

When the artificial ant has traversed all the paths from point i to point j (that is, after traversing all the paths), it is necessary to update the pheromone everywhere in theN_i^k set, and then a local optimization model can be obtained.

2.2 Establishment of Indicator System for Cybersecurity Threat Warning

To establish a cybersecurity threat warning model based on ant colony algorithm, it is also necessary to design a cybersecurity threat warning indicator system [9]. The network structure is a complex system, as shown in Fig. 1.

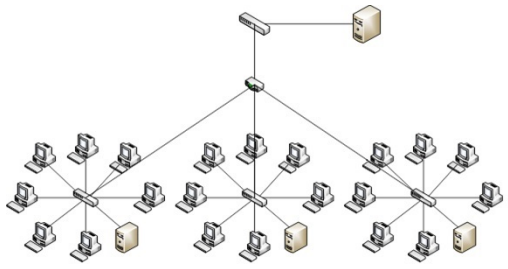

Figure 1: Schematic diagram of network structure

At present, there are few research on the indicator system of cybersecurity threat warning, and the research framework and weight judgment are different. Based on the research of a large number of cybersecurity related research documents, the cybersecurity threat warning indicator system is designed, and details are shown in the following table.

Table 1: Cybersecurity threat warning indicator system

Overall index	First-level index	Second-level index	Index description
Cybersecurity threat warning U	Related policy U1	Strategic completeness u1	Cybersecurity threat warning policy
		Advanced management u2	Regulations on Warning Management of Cybersecurity threats
		Engineering maturity u3	Cybersecurity threat warning implementation strategy
		Technical validity u4	Cybersecurity threat warning measures
	Warning ability U2	Detect u5	Network security threat detection capabilities
		Warning u6	Network security threat warning capability
		Defend u7	Network security threat defense capabilities
	Warning effects U3	Status monitoring u8	The overall status monitoring of the computer system
		Safety limit u9	Minimum requirements for safe operation of computer systems
		Warning effect u10	Cybersecurity threat warning effect
		Warning benefits u11	Social and economic benefits

According to Table 1, the warning indicators for cybersecurity threats are mainly judged from three perspectives: relevant policies, warning capabilities, and final warning effects. National policies and regulations on cybersecurity threat warning, methods and technical measures in the specific implementation process, the detection, warning, and defense capabilities of cybersecurity threat warning, and the effects and benefits of cybersecurity threat warning are comprehensively considered [10–11].

2.3 Cybersecurity Threat Warning Model Construction Based on Ant Colony Algorithm

Through the use of ant colony algorithm, the network security threat early warning model established based on the above network security threat early warning indicator system pays more attention to the weight evaluation of various indicators [11]. The specific model building steps are shown in the figure below.

As shown in the Fig. 2, first, the model structure of the ant colony algorithm is built inside the computer, and then the obtained optimal solution is substituted into the initial network security threat warning indicator system matrix to calculate the comprehensive impact matrix. The centrality and cause degree of indicators are determined according to the comprehensive influence matrix, and finally the weight of each indicator is determined [12–14]. Then the comprehensive evaluation value is solved based on the weight value, the evaluation value can indicate whether a network data stream is threat data [15–18]. If the evaluation value is higher than the dangerous value, it is dangerous data and warning is issued; if the evaluation value is lower than the dangerous value, it is safety data and no warning is required [19–20].

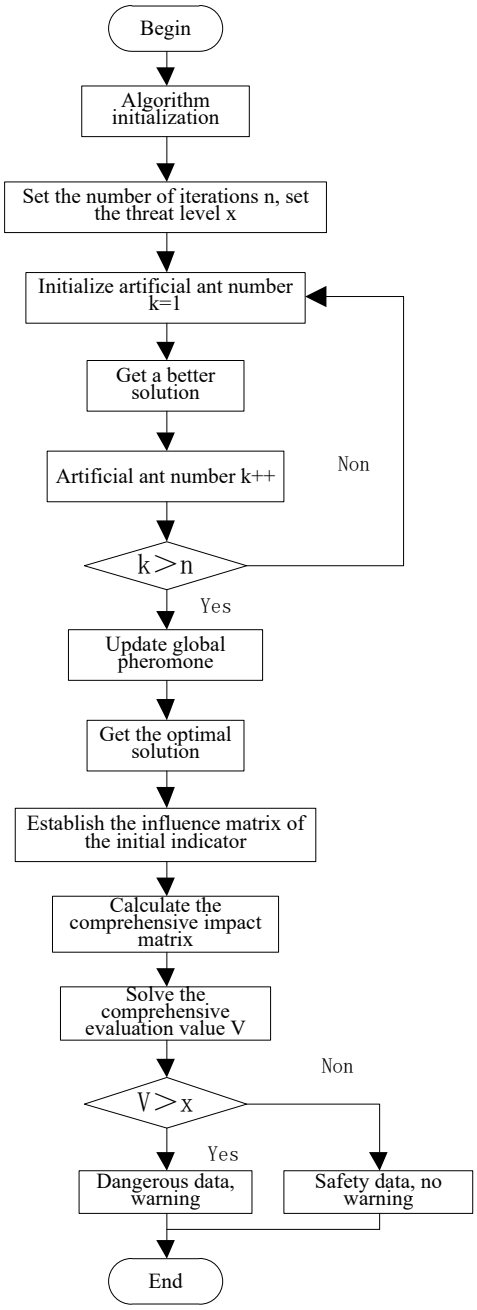

Figure 2: Flow chart of cybersecurity threat warning model

3 Experimental Design

In order to judge whether the designed cybersecurity threat warning model has a better cybersecurity threat warning function, whether the algorithm structure is more concise and clear, the cybersecurity threat warning model based on ant colony algorithm and the cybersecurity threat warning model based on qualitative differential game are compared and analyzed.

3.1 Experiment Preparation

First, the experimental environment needs to be set up. The software and hardware settings required for the experiment are shown in the Table 2.

Table 2: Experimental environment settings

	Name	Parameters
Hardware	Model	(Lenovo) Y7000p
	Processor	Lenovoi7-10875 @ 5.10 GHz eight core
	Graphics card	192 bit 6 GB Set display + independent display
	Motherboard	Asus P8Z68-V LX
	Running memory	32 GB
Software	Operating system	Windows 10 64 bit
	Code writing	Visual Basic 6.0
	Simulation tool	Scalable Simulation Framework 2.0
	Calculation tool	Matlab 6.0

Then it is necessary to establish a data set of cybersecurity threat to test the functions of the design model and the cybersecurity threat warning model based on qualitative differential games. 10,000 pieces of network-related data are collected, including 100 pieces of data with threats, and the ratio of security data to threat data is 99:1. The 10,000 pieces of network data are randomly divided into 10 data groups with different security data and threat data, and the designed cybersecurity threat warning model based on ant colony algorithm and the cybersecurity threat warning model based on qualitative differential game are used respectively for detection. The accuracy and detection time of the two models in the detection process are compared to determine the warning effect and algorithm redundancy of the two models.

3.2 Analysis of Results

The experimental data are analyzed through Matlab software, and the experimental results obtained are shown in the Table 3.

Table 3: Experimental results

Data group	Model designed in this paper		Traditional model	
	The warning accuracy	Running time	The warning accuracy	Running time
1	100%	14s	98%	26s
2	100%	16s	100%	27s
3	98%	23s	98%	30s
4	100%	25s	96%	31s
5	98%	20s	96%	32s
6	100%	21s	98%	30s
7	100%	19s	100%	29s
8	100%	18s	100%	28s
9	100%	13s	100%	33s
10	100%	25s	96%	35s

As shown in the Table 3, Fig. 3 and Fig. 4, the established network security threat early warning model based on ant colony algorithm has a correct probability of 80%, while the traditional network security threat early warning model based on qualitative differential game has a correct probability of only 40%, which is far less accurate than the established one. In terms of running time, the designed warning model takes an average of 19.4 s, while the calculation time of the traditional warning model is 30.1 s, which is about 1.5 times that of the designed warning model. Therefore, it can be known that the designed cybersecurity threat warning model has better threat detection methods, can enhance the warning accuracy of traditional models, and the program algorithm is more concise and clear.

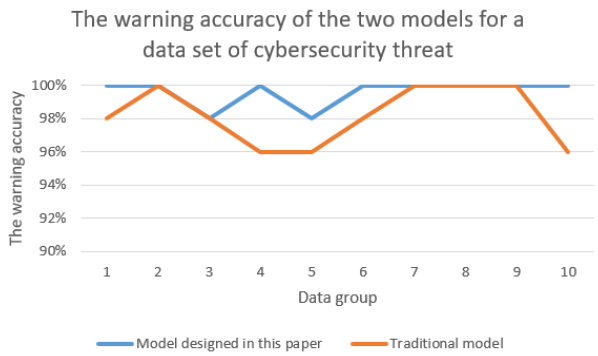

Figure 3: Experimental results of the warning accuracy

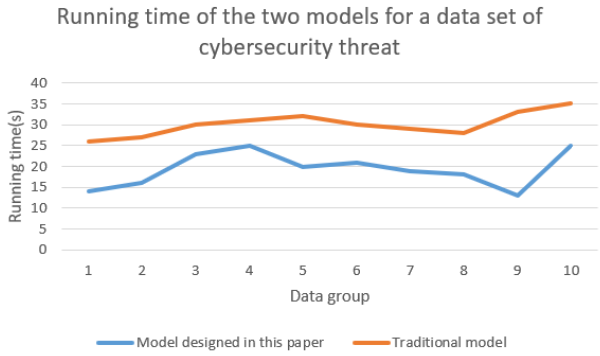

Figure 4: Experimental results of running time

4 Conclusion

According to the ant colony algorithm, the cybersecurity threats are screened by variables, and a cybersecurity threat warning model based on ant colony algorithm is constructed through the cybersecurity threat index system. There are 11 indicator factors in this model, and the selection of variables is more comprehensive. Through comparative experiments, it can be judged that, compared with the cybersecurity threat warning model based on qualitative differential game, the cybersecurity threat warning model based on ant colony algorithm has better computational effect and data simplicity.

Funding Statement: This work was supported by the Natural Science Foundation of Fujian Province, China; Research on Network Risk Assessment Method Based on Dynamic Attack Behavior (Grant No. 2019J01889), the Education-Scientific research Project for Middle-Aged and Young of Fujian Province, China; Research on Analysis System of Malicious Code Based on API Relevance (Grant No. JT180626).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Y. L. Yu, D. Q. Yang, Q. Dian and D. L. Guo, "Multi-index intuitionistic fuzzy comprehensive evaluation model for early warning level of internet public opinion," *Journal of Sanming University*, vol. 37, no. 4, pp. 11–20, 2020.

[2] Y. Wang, J. Q. Sun and R. H. Huai, "Research on civil aviation network security situation awareness technology based on the perspective of Business + Data," *Journal of Information Security Research*, vol. 6, pp. 549–554, 2020.

[3] S. R. Huang, H. W. Zhang, J. D. Wang and R. Y. Dou, "Network security threat early warning method based on qualitative differential game," *Journal on Communications*, vol. 39, no. 8, pp. 29–36, 2018.

[4] D. L. Liu, X. Liu, H. Zhang, H. Yu, L. Ma *et al.,* "Research and application of network security situation awareness and active defense technology based on big data," *Computer Measurement and Control*, vol. 27, no. 10, pp. 229–233, 2019.

[5] J. L. Liang, J. S. Huang, S. J. Bai, P. Wang and R. Li, "An early warning model of APT attacks on power data networks based on ant colony algorithm," *Computer and Modernization*, vol. 1, pp. 95–100, 2019.

[6] X. A. Gu, B. Q. Wang and W. Q. Li, "Research on the improvement of early warning correction rate of logistic financial early warning model—analysis of introducing earnings management variables," *Journal of Nanjing Audit University*, vol. 15, no. 4, pp. 45–52, 2018.

[7] Z. J. Mu, Y. D. Li and D. H. Yan, "Design and implementation of a learning early warning system based on learning behavior data in a hybrid learning environment," *Journal of Distance Education*, vol. 36, no. 3, pp. 55–63, 2018.

[8] Z. Y. Zhao and X. M. Ji, "Research on fusion model of intelligent network security threat perception," *Netinfo Security*, vol. 4, pp. 87–93, 2020.

[9] W. Tang, "Research on network security early warning and supervision platform based on trapping technology," *Cyberspace Security*, vol. 10, no. 6, pp. 9–14, 2019.

[10] Z. Y. Liu, "An empirical study on the causes of network security information early warning system and the correlation elements of the construction path," *Network Security Technology and Application*, vol. 231, no. 3, pp. 13–18, 2020.

[11] W. Fang, L. Pang and W. N. Yi, "Survey on the application of deep reinforcement learning in image processing," *Journal on Artificial Intelligence*, vol. 2, no. 1, pp. 39–58, 2020.

[12] W. Han, Z. Tian, Z. Huang, L. Zhong and Y. Jia, "System architecture and key technologies of network security situation awareness system YHSAS," *Computers, Materials & Continua*, vol. 59, no. 1, pp. 167–180, 2019.

[13] D. F. Zu, "Critical information infrastructure network security protection system," *China Computer & Communication*, vol. 407, no. 13, pp. 198–199, 2018.

[14] G. Yang, M. Yang, S. Salam and J. Zeng, "Research on protecting information security based on the method of hierarchical classification in the era of big data," *Journal of Cyber Security,* vol. 1, no. 1, pp. 19–28, 2019.

[15] Z. Zhang, Y. D. Chen and J. J. Tang, "Research on dynamic defense of network security based on threat," *Confidential Science and Technology*, vol. 6 pp. 22–31, 2020.

[16] I. You, C. Choi, V. Sharma, I. Woungang and B. K. Bhargava, "Advances in security and privacy technologies for forthcoming smart systems, services, computing, and networks," *Intelligent Automation & Soft Computing*, vol. 25, no.1, pp. 117–119, 2019.

[17] Z. G. Ke, Y. B. Yang and S. W. Mai, "Network security situational awareness solution based on big data," *Information Technology & Standardization*, vol. 9, pp. 21–22, 2019.

[18] W. Fang, F. Zhang, Y. Ding and J. Sheng, "A new sequential image prediction method based on LSTM and DCGAN," *Computers, Materials & Continua*, vol. 64, no. 1, pp. 217–231, 2020.

[19] W. H. Jiang, "Research on the strategies of building an intelligent early warning system for network security in large enterprises," *Electronics World*, vol. 552, no. 18, pp. 61–62, 2018.

[20] Z. J. Hu, "Application thinking of network security situation awareness platform based on big data," *Financial Technology Time*, vol. 10, pp. 44–46, 2019.