DOI: 10.53469/jtpes.2025.5(01).04

Application of Security Situation Awareness in Network Attack Defense

Haoxuan Lu

Shunde Polytechnic, Foshan, Guangdong, 712000

Abstract: ***In the computer network technology system, the development and application of a security situational awareness model and software system can accurately adapt to the application requirements of attack and defense business functions in the computer network. The network attack defense system which is based on security situational awareness technology can reshape all kinds of network attacks, and analyze the vulnerability of computer network security vulnerabilities in the region, so it presents a visual security situation. This paper will focus on the application points of network attack defense based on security situational awareness.***

Keywords: Safety; Situational awareness; Network; Attack defense.

1. INTRODUCTION

There are relatively many security risk factors in the computer network environment, which can pose a serious threat to the accuracy and reliability of various data information resources. Therefore, in the process of building a computer network security supervision system, it is necessary to efficiently use multi-source data fusion network security situational awareness models and big data processing and analysis methods to further improve the automatic warning efficiency and situational prediction accuracy of computer networks, and fully guarantee the security of various virtual assets in computer network systems.

2. OVERVIEW OF SECURITY SITUATION AWARENESS TECHNOLOGY

In the field of computer network security, the widespread application of security situational awareness technology and data models can significantly improve the risk perception level of computer network space, and can selectively screen security vulnerabilities and illegal attack behaviors. Security situational awareness technology can perform secure encryption operations on key communication facilities in the data layer, physical layer, business layer, and network layer on the basis of the original computer network architecture. It can also perform security audits and vulnerability scans on decentralized computer network topologies and other basic system operations. Security situational awareness technology and corresponding data models can significantly improve the security monitoring efficiency of computer networks in this region, and quantitatively analyze data sources and communication links under abnormal conditions, quickly identify and locate network communication link numbers with security risk factors, and so on. However, in the process of building a computer network security situational awareness system, it is inevitable to be disturbed by many force majeure factors, but it is also necessary to comprehensively evaluate the practical application scenarios of different levels of protection mechanisms. By fully utilizing security situational awareness technology and data models, the security risk assessment results in many computer network architecture systems will be significantly reduced.

Liu et al. (2024) introduced the Promoted Osprey Optimizer as a solution for the Optimal Reactive Power Dispatch (ORPD) problem, considering the integration of electric vehicles [1]. Li (2025) focused on optimizing clinical trial strategies for anti-HER2 drugs, utilizing Bayesian optimization and deep learning [2]. Huang et al. (2024) explored the contribution of federated learning to trustworthy and responsible AI [3], while another study by Huang et al. (2024) investigated a multi-agency collaboration system for medical image analysis and classification based on federated learning [4]. Chen et al. (2022) presented a one-stage object referring method with gaze estimation in computer vision [5]. Liang and Chen (2019) contributed to network security with a hierarchical authentication mechanism for IPv6 addresses and a high-performance dynamic service orchestration algorithm in hybrid NFV networks [6]. Xie et al. (2024) advanced legal citation text classification using a Conv1D-based approach [7], and Xu et al. (2024) enhanced automated surveillance with real-time detection of Crown-of-Thorns Starfish via YOLOv5 [8]. Xu et al. (2024) also worked on improving user experience and trust in LLM-based conversational agents [9]. Liu (2024) optimized supply chain efficiency using cross-efficiency analysis and inverse DEA models [10]. Lin et al. (2024) applied AI to electroencephalogram analysis for optimizing anesthesia depth [11]. Wang et

al. (2024) researched autonomous robot navigation based on reinforcement learning [12]. Wu et al. (2024) proposed a lightweight GAN-based image fusion algorithm for visible and infrared images [13]. Ren (2024) presented enhancements to Seq2Seq models for role-oriented dialogue summary generation and a novel feature fusion-based model for smoking detection [14]. Fan et al. (2024) investigated optimizing real-time data processing in high-frequency trading algorithms using machine learning [15].

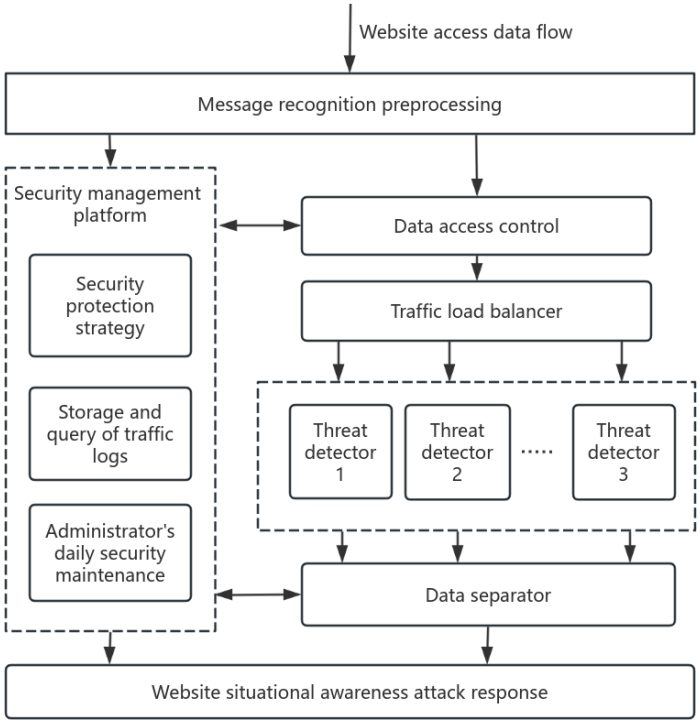

Figure 1: Network Security Situation Awareness Technology Framework

3. THE PROBLEMS FACED IN NETWORK ATTACK DEFENSE

3.1 Fragmentation Development Issues

For computer network security protection technology systems of different scales, there are generally significant differences in defense measures against unknown network attacks, and the overall protection effect varies. The passive defense mode on different computer network nodes generally exhibits the basic application characteristics of fragmentation, which indirectly limits the automation efficiency of many security awareness models [16]. Many decentralized computer network architectures commonly use three-layer attack protection technology systems, but they cannot fully restore illegal attack targets and sources, which can indirectly generate many potential security risk factors. Many network attack incidents are becoming increasingly covert, and the transmission routes and communication links are more difficult to track and trace. Therefore, fragmented network attack behavior is not conducive to improving the overall protection and defense level of local networks. The fragmented development of computer network attack defense technology system cannot strictly follow the requirements of relevant technical specifications and standards for precise traceability, and will also show a trend of discrete and decentralized network technology development. In addition, many computer network practitioners have not strictly reviewed the accuracy of various illegal attack defense systems, and there are generally many gaps and gaps between theory and practice, which increases the risk factor of computer network security monitoring [17].

3.2 Passive interception problem

Among numerous computer network attack defense models, the problem of passive interception is still quite common and can indirectly affect the precise traceability of various illegal network access and background attack behaviors. It also cannot perform encryption and decryption operations quickly, missing the best interception time. Especially in the process of backing up and managing the operation logs of computer network systems, it will have

a certain impact on various passive interception operation modes, and cannot fully match the internal data information resources of the security situational awareness model. It is easy to present an unstable predictive analysis state, and the sensitivity to network attack behavior will also be significantly reduced [18]. Especially after setting up network whitelists and blacklists, passive interception problems become more common and can cause irreversible losses, seriously affecting the stable operation of computer system equipment and network monitoring nodes. The passive interception problem can not only be reflected in technical aspects such as network attack defense, but also cause certain interference to the normal data information collection process of various security monitoring facilities.

3.3 Single point defense issue

There are relatively many types and quantities of network security related products and hardware facilities on the market, but they cannot accurately adapt to the differentiated attack defense needs of computer networks. The issue of single point defense is one of the easily overlooked computer network security risk factors, and can indirectly affect the accuracy and security effectiveness of the network data communication connection process. In the process of building a single point of defense technology system, it is necessary to break down barriers such as information barriers and inconsistent security standards between different operators as much as possible in order to quickly perform basic operations such as information sharing and multi-source data fusion. Especially after determining a certain attack prevention measure, it is necessary to objectively analyze and predict the technical and economic risks in the single point defense process in order to further define the potential security risk levels in the computer network architecture system in this region. The operator networks are all in a state of independent operation, and the only network security defense effect that can be achieved is single point defense. Therefore, in the process of dealing with single point defense issues, the correlation between discrete network security monitoring data information cannot be ignored, and it is also necessary to focus on identifying and judging whether it affects the security link status of different data communication links.

3.4 Unknown Attack Results

In the case where the outcome of a network attack is unknown, management personnel are unable to predict the final outcome of the network attack; In the case where the results of a network attack are known, although managers can provide early warning and attack interception by identifying the attacker's network attack status, they still cannot attack the target and determine whether the target attack is successful. Many classic network attack defense models are prone to generating a lot of misjudgment information in the process of identifying and judging illegal network attack behaviors, which can affect the final decision-making results of network security managers. Especially for IP addresses and source code that are confusing, many network attacks have a relatively long latency and the destructive process is very covert. Under the condition of unknown attack results, many passive defense methods cannot accurately determine and identify the data sources and system devices that need additional protection, and will also waste a lot of network data information resources. The problem of unknown attack results can not only seriously affect the quality and efficiency of data communication transmission between the local local area network and the Internet, but also indirectly generate security risks such as redundant data, and can not accurately identify and locate the key operation results in the system log, nor can it quickly judge and analyze defense targets and objects.

4. NETWORK ATTACK DEFENSE MODEL BASED ON SECURITY SITUATION AWARENESS

4.1 Data source selection and feature extraction

The network attack defense model based on security situational awareness requires precise identification and automated judgment and analysis of the categories and quantities of data information sources in NSSA technology, in order to further define the number and categories of explicit and implicit security risk factors in a certain testing network environment. In the NSSA model, it is necessary to centrally screen the data sources at the three core business levels of service, host, and network, and perform correlation analysis on the corresponding relationships between heterogeneous sensor devices and heterogeneous data information resources, constructing a decentralized association rule matrix. To ensure the diversity and integrity of data networks, it is necessary to use data multivariate fusion methods to perform multivariate fusion and real-time processing of data information, and then establish a network security system based on the Network Security Situation Awareness (NSSA) model. In the NSSA model, the number of nodes and eigenvalues in the input layer, hidden layer, and output layer are crucial

data sources and can indirectly affect the data information transmission efficiency and security performance indicators of various heterogeneous security aware devices. In the process of applying BP network and ant colony algorithm for optimization selection, it is necessary to conduct multidimensional training and simulation prediction on specific computer network security testing environments and predictive analysis results, and feedback the output results to the input layer for verification training. In the process of feature selection, the number of nodes and continuity function can be uniformly selected based on the three-layer data transmission architecture of the BP neural network, but it is necessary to ensure that the calculation results of the weight values and expected output values in the neurons meet the calculation requirements of the continuity function.

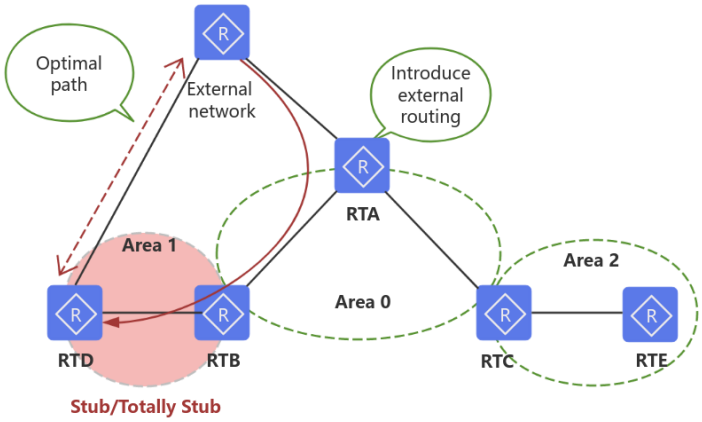

Figure 2: NSSA's network data source

4.2 Service Security Situation Awareness

In the process of building the NSSA security perception model, quantitative analysis can be conducted on different perception levels to target and predict security threat factors in the service layer (business layer), host layer, and network layer, and further define the specific operational status of local network services. In the service security situational awareness module, quantitative statistical analysis of independent variables such as the intensity, weight, and number of illegal network attacks is required, which can indirectly determine the active defense level and traceability goals at the network security service level. In addition, in the process of situational awareness and quantitative statistical analysis of network service security, it is necessary to moderately adjust the adaptive coefficient and learning rate, and directionally adjust the protection level corresponding to network attacks. Especially for most heterogeneous data information resources, in the process of conducting service security situational awareness operations, it is not possible to ignore whether there are abnormal control nodes and data flows in the relevant system operation processes at the business service level. It is also necessary to conduct targeted monitoring and statistical analysis of the transmission status of different communication links in the computer network. Based on the perception and predictive analysis of service security situation, computer network security managers can adjust the backend defense level in a visual screen and conduct time series analysis on key data indicators such as attack numbers and threat weight coefficients. In the process of building a BP network model for service security situational awareness, it is necessary to objectively evaluate and quantitatively analyze the data results of the output layer and the number of hidden layer nodes.

4.3 Host Security Situation Awareness

In the NSSA model, the perception data results of host security situation are crucial and can indirectly affect the calculation results of various service situations, service quantities, and weighting coefficients. After normalization, network security threat data indicators of host devices can be obtained. In BP neural networks, the input layer, hidden layer, and output layer of host security situational awareness results can indirectly affect the risk assessment level of network services and indirectly limit the passive and active defense modes of host network security. However, in the process of selecting host security risk factors and feature values, the relative consistency of importance weight coefficient indicators cannot be ignored. It is also necessary to review and verify the correctness of security threat calculation results to avoid affecting the accuracy of the overall assessment of network security situation.

4.4 Network Security Situation Awareness

The network security situational awareness function requires precise integration with the above two situational awareness results, and accurate calculation of situational awareness feature values and host weighting coefficients. In the process of calculating the results of network security situational awareness, it is necessary to normalize the importance weight values and focus on screening the high-dimensional features of data fusion. According to the network security situation trend map at different time nodes, it is necessary to accurately judge and identify the number of services and time series analysis results of a specific host, and ensure that the fusion perception methods in different network topologies can present system compatibility, and accurately classify the training and testing data in the dataset. In the process of integrating the results of network security situational awareness, it is necessary to accurately classify the security risk levels of computer networks with different topology structures, normalize and statistically analyze the fusion rate, detection rate, and false alarm rate of the perception results, and define the range of event detection values for different data sources uniformly.

5. CONCLUSION

With the increasing importance of cybersecurity, research and application of cybersecurity situational awareness are receiving more and more attention. Network security situational awareness is an environmentally based, dynamic, and holistic ability to perceive security risks. Research on network security situational awareness is of great significance for improving network monitoring capabilities, emergency response capabilities, and predicting network security development trends.

REFERENCES

[1] Liu, Z., Jian, X., Sadiq, T., Shaikh, Z. A., Alfarraj, O., Alblehai, F., & Tolba, A. (2024). Promoted Osprey Optimizer: a solution for ORPD problem with electric vehicle penetration. Scientific Reports, 14(1), 28052.

[2] Li, T. (2025). Optimization of Clinical Trial Strategies for Anti-HER2 Drugs Based on Bayesian Optimization and Deep Learning.

[3] Huang, S., Liang, Y., Shen, F., & Gao, F. (2024, July). Research on Federated Learning's Contribution to Trustworthy and Responsible Artificial Intelligence. In Proceedings of the 2024 3rd International Symposium on Robotics, Artificial Intelligence and Information Engineering (pp. 125-129).

[4] Huang, S., Diao, S., Wan, Y., & Song, C. (2024, August). Research on multi-agency collaboration medical images analysis and classification system based on federated learning. In Proceedings of the 2024 International Conference on Biomedicine and Intelligent Technology (pp. 40-44).

[5] Chen, J., Zhang, X., Wu, Y., Ghosh, S., Natarajan, P., Chang, S. F., & Allebach, J. (2022). One-stage object referring with gaze estimation. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 5021-5030).

[6] Liang, X., & Chen, H. (2019, July). A SDN-Based Hierarchical Authentication Mechanism for IPv6 Address. In 2019 IEEE International Conference on Intelligence and Security Informatics (ISI) (pp. 225-225). IEEE.

[7] Liang, X., & Chen, H. (2019, August). HDSO: A High-Performance Dynamic Service Orchestration Algorithm in Hybrid NFV Networks. In 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS) (pp. 782-787). IEEE.

[8] Xie, Y., Li, Z., Yin, Y., Wei, Z., Xu, G., & Luo, Y. (2024). Advancing Legal Citation Text Classification A Conv1D-Based Approach for Multi-Class Classification. Journal of Theory and Practice of Engineering Science, 4(02), 15–22. https://doi.org/10.53469/jtpes.2024.04(02).03

[9] Xu, G., Xie, Y., Luo, Y., Yin, Y., Li, Z., & Wei, Z. (2024). Advancing Automated Surveillance: Real-Time Detection of Crown-of-Thorns Starfish via YOLOv5 Deep Learning. Journal of Theory and Practice of Engineering Science, 4(06), 1–10. https://doi.org/10.53469/jtpes.2024.04(06).01

[10] Xu, Y., Gao, W., Wang, Y., Shan , X., & Lin, Y.-S. (2024). Enhancing user experience and trust in advanced LLM-based conversational agents. Computing and Artificial Intelligence, 2(2), 1467. https://doi.org/10.59400/cai.v2i2.1467

[11] Liu, M. (2024). Optimizing Supply Chain Efficiency Using Cross-Efficiency Analysis and Inverse DEA Models.

[12] Lin, S., Hu, K., Ye, T., Wang, Y., & Shen, Z. (2024). Artificial Intelligence and Electroencephalogram Analysis Innovative Methods for Optimizing Anesthesia Depth. Journal of Theory and Practice in Engineering and Technology, 1(4), 1–10. https://doi.org/10.5281/zenodo.14457933

[13] Wang, Z., Yan, H., Wang, Z., Xu, Z., Wu, Z., & Wang, Y. (2024, July). Research on autonomous robots navigation based on reinforcement learning. In 2024 3rd International Conference on Robotics, Artificial Intelligence and Intelligent Control (RAIIC) (pp. 78-81). IEEE.

[14] Wu, Z., Chen, J., Tan, L., Gong, H., Zhou, Y., & Shi, G. (2024, September). A lightweight GAN-based image fusion algorithm for visible and infrared images. In 2024 4th International Conference on Computer Science and Blockchain (CCSB) (pp. 466-470). IEEE.

[15] Z. Ren, "Enhancing Seq2Seq Models for Role-Oriented Dialogue Summary Generation Through Adaptive Feature Weighting and Dynamic Statistical Conditioninge," 2024 6th International Conference on Communications, Information System and Computer Engineering (CISCE), Guangzhou, China, 2024, pp. 497-501, doi: 10.1109/CISCE62493.2024.10653360.

[16] Z. Ren, "A Novel Feature Fusion-Based and Complex Contextual Model for Smoking Detection," 2024 6th International Conference on Communications, Information System and Computer Engineering (CISCE), Guangzhou, China, 2024, pp. 1181-1185, doi: 10.1109/CISCE62493.2024.10653351.

[17] Fan, Y., Hu, Z., Fu, L., Cheng, Y., Wang, L., & Wang, Y. (2024). Research on Optimizing Real-Time Data Processing in High-Frequency Trading Algorithms using Machine Learning. arXiv preprint arXiv:2412.01062.

[18] Junhong Liu, Qi Zhang, Wenfeng Wei, Chunyan Jiang Application of Artificial Intelligence in Network Security Situation Awareness of Electric Power Enterprises [J]. Network Security and Informatization, 2021 (12): 126-130