International Journal of Information Security and Privacy
Volume 18 • Issue 1

Network Information Security Monitoring Under Artificial Intelligence Environment

Longfei Fu, Lanzhou Institute of Technology, China
Yibin Liu, Lanzhou Institute of Technology, China
Yanjun Zhang, Lanzhou Institute of Technology, China
Ming Li, Information and Communication Branch of State Grid Anhui Electric Power Co., Ltd., China*

ABSTRACT

At present, network attack means emerge in endlessly. The detection technology of network attack must be constantly updated and developed. Based on this, the two stages of network attack detection (feature selection and traffic classification) are discussed. The improved bat algorithm (O-BA) and the improved random forest algorithm (O-RF) are proposed for optimization. Moreover, the NIS system is designed based on the Agent concept. Finally, the simulation experiment is carried out on the real data platform. The results showed that the detection precision, accuracy, recall, and F1 score of O-BA are significantly higher than those of references [17], [18], [19], and [20], while the false positive rate is the opposite ($P < 0.05$). The detection precision, accuracy, recall, and F1 score of O-RF algorithm are significantly higher than those of Apriori, ID3, SVM, NSA, and O-RF algorithm, while the false positive rate is significantly lower than that of Apriori, ID3, SVM, NSA, and O-RF algorithm ($P < 0.05$).

KEYWORDS

Bat Algorithm, Network Attack, Network Information Security, Random Forest Algorithm

With the rapid development of internet technology, network security issues are increasingly prominent, and network information security (NIS) is facing enormous challenges. Various information security incidents, including webpage tampering, computer viruses, illegal system intrusions, data leaks, website fraud, service paralysis, and illegal exploitation of vulnerabilities, have brought significant threats and losses to people. Therefore, exploring how to detect and defend against network attacks has become an urgent problem to be solved.

Network attack detection is an important means of ensuring NIS security. It includes two stages: feature selection and traffic classification. In terms of feature selection, traditional algorithms have lower processing efficiency for network data. Traffic classification is also limited by the complexity of feature dimensions and classifiers. Therefore, how to improve the efficiency and accuracy of feature selection and traffic classification is an important research task.

This article proposes improved bat algorithms and random forest (RF) algorithms for optimizing network attack detection. These two algorithms are applied to feature selection and traffic classification,

DOI: 10.4018/IJISP.345038
*Corresponding Author

respectively. Specifically, this article proposes a NIS system based on outlier-based behavioral analysis (O-BA) and outlier-based RF (O-RF) algorithms, which can effectively detect and defend against denial-of-service (DOS) attacks and detection attacks. To verify the performance of the proposed algorithm and system, simulation experiments were conducted on a real data platform. The experimental results show that the proposed algorithm and system can significantly improve the effectiveness of network attack detection and maintain good detection efficiency. Therefore, this has important practical significance for the detection and defense of current network attacks.

LITERATURE REVIEW

NIS is a comprehensive discipline involving computer science, network technology, communication technology, cryptography, information security technology, applied mathematics, number theory, and information theory. It mainly means that information systems (including hardware, software, data, humans, the physical environment, and infrastructure) are protected from damage, change, and disclosure due to accidental or malicious reasons (Rzym et al., 2024). The system operates continuously, reliably, and normally, and the information service is not interrupted.

Finally, business continuity is realized. With the rapid development of internet technology and the diversification of hacker attack methods, NIS is facing a huge threat in recent years. Information security incidents such as web page tampering, computer viruses, illegal system intrusion, data disclosure, website fraud, service paralysis, and illegal exploitation of vulnerabilities occur from time to time (Andrade-Hoz et al., 2024). Therefore, how to detect and defend network attacks has become a topic of concern. Network attacks generally attack the system and resources by using loopholes and security defects in the network information system (Yun et al., 2024).

Threats are mainly divided into man-made threats and natural threats. Natural threats come from various natural disasters, harsh site environments, electromagnetic interference, natural aging of network equipment, etc. Man-made threats are man-made attacks on the NIS. By looking for the weakness of the system, the purpose of destroying, cheating, and stealing data and information is achieved in an unauthorized way (Palma et al., 2024). In contrast, many types of well-designed man-made attack threats are difficult to prevent. These are the attacks prevention efforts should focus on.

Network attack detection is the primary concern for NIS, and the resulting network attack detection systems are diverse, such as open-source HIDS security, Snort, Huawei NIP series intrusion detection system, Venustech IDS, and NSFOCUS NIDS, all with their own characteristics (Kong et al., 2024).

Although the research on network attack detection has never stopped, there are still deficiencies in the face of the same endless attack methods. From the perspective of communication, any new network information technology is bound to be accompanied by new attack modes and characteristics, making it more difficult to automatically extract network attack characteristics, which results in the loss of effectiveness of network attack detection technology through fixed rule matching (Casado-Vara et al., 2024). Moreover, in the real environment, real-time response to network attack means is required, so there is not enough time to slowly mark the attack samples. Under the condition of capturing a small number of samples, the detection system needs to accurately find the intrusion virus (Kan & Fang, 2024). The emergence of new attack technologies greatly tests the real-time performance of the system. In addition, artificial intelligence (AI) technology based on deep learning has developed rapidly in recent years and has been applied to network attack technology by hackers. This has made attack methods more and more intelligent, requiring the use of AI technology as part of the continuous updating of defense technology (Hasas et al., 2024).

In summary, NIS has always been a topic of concern for scholars. The detection technology of network attacks must be constantly updated and developed to better face the various network attack methods, and the use of AI technology is a new development trend.

A covert channel is used to ex/infiltrate classified information from legitimate targets; consequently, this manipulation violates network security policy and privacy. Cao Pan, and Zou