International Journal on Semantic Web and Information Systems
Volume 20 • Issue 1

A Network Intrusion Detection Method for Various Information Systems Based on Federated and Deep Learning

Qi Zhou, School of Artificial Intelligence, Guangdong Open University, Guangzhou, China*
Chun Shi, School of Electronic and Information, Guangdong Polytechnic Normal University, Guangzhou, China

ABSTRACT

Under the premise of ensuring data privacy, traditional network intrusion detection (NID) methods cannot achieve high accuracy for different types of intrusions. A NID method combining transformer and federated learning (FedL) is proposed for this purpose. First, a multi-party collaborative learning framework was built based on FedL, which achieved data exchange and sharing. Then, by introducing the self-attention mechanism (AttM) to improve the traditional transformer, it could quickly converge. Finally, an NID model integrating transformer and FedL was constructed by combining DNN, GRU, and an encoder module composed of improved transformer, achieving accurate detection of network intrusion. The proposed NID method was compared with the other three methods. The results show that the proposed method has the highest NID accuracy and F1 score on the NSL-KDD and UNSW-NB15 dataset, with the highest accuracy reaching 99.65% and 89.25%, while the F1 score has the highest accuracy, reaching 99.45% and 88.13%, outperforming the other three comparative algorithms in terms of performance.

KEYWORDS

DNN, Federated Learning, GRU, Network Intrusion Detection, Transformer

INTRODUCTION

In recent years, the large-scale popularization and rapid development of the internet have brought great convenience to the development of enterprises and personal lives, followed by a series of network security issues and challenges (Hamad et al., 2020; Wang, et al., 2021; Fan et al., 2020). Bad actors often exploit network vulnerabilities, Trojan viruses, and other means to steal confidential information and valuable personal information. Network attacks can have wide coverage and endanger many areas of public production and security, causing huge burdens and losses. Research shows that sudden network attacks reveal that the existing basic network security protection technologies cannot flexibly adapt to resist complex network attacks. Therefore, there is an urgent need to propose network security technologies to address network security threats (Wang et al., 2020; Park et al., 2020; Wang et al., 2022).

DOI: 10.4018/IJSWIS.335495 *Corresponding Author

At present, the complexity of network threats is increasing, and the means of attack are becoming increasingly diverse, making the security protection of network systems particularly important. Firewalls, spam filters, and antivirus software are all tools used to protect network security. But currently the most widely used and powerful network security technology is NID systems. It is the most crucial link in the attack defense chain and can be used as the first or second defense mechanism for threats or attacks (Liu et al., 2020; Qin et al., 2020; Sharafaldin et al., 2021). The ultimate goal of the NID system is to quickly and accurately detect different types of attacks that may occur in the network, such as denial of service, port scanning, malware, distributed denial of service, or ransomware, by investigating network traffic (Meidan et al., 2022; Lin et al., 2021; Sattler et al., 2022).

The goal of NID is to detect abnormal behavior that damages the host as much as possible without interfering with the normal use of the network. The key to implementing NID is to find an effective detection algorithm to analyze network traffic (Yang et al., 2022; Cheng et al., 2020; Cheng et al., 2021).

Traditional machine learning (ML) technology has been proven to effectively identify important patterns in Internet of things (IoT) traffic, thus effectively targeting attacks. At present, the public is becoming increasingly sensitive to data privacy, and there is a risk of privacy leakage during data transmission (Zhu, et al., 2023; Cui, et al., 2023; de Caldas et al., 2023). Therefore, the data collected and transmitted from the device will be subject to legal regulatory limitations, which may lead to deviations in NID's task results. The delay generated by training based on global data and returning the results to edge nodes is relatively large, which is unacceptable for some delay sensitive applications (Ling & Hao 2022; Ling & Hao., 2022; Tembhurne, et al., 2022).

In 2016, Google proposed a distributed ML framework called FedL that can protect privacy, which is used to protect user privacy and information security during data exchange. FedL provides a collaborative and secure learning protocol that enables efficient learning among multiple participants while ensuring legal compliance (Srivastava, et al., 2022; Rahman, et al., 2020). Under this framework, each edge device can contribute to global model training while retaining the training data locally. In the FedL environment, edge devices typically collect sensing data from IoT nodes, typically time series data, and capture the behavior and operational status of IoT nodes through computational analysis (Mourad, et al., 2020; Abbas, et al., 2021).

This article solves the issues of sensitive information protection and incomplete data in training data by applying transformer and FedL to NID and improves the accuracy of NID. Compared with traditional methods, the proposed method provides the following innovations:

1. It utilizes sparse stacked autoencoders for feature dimensionality reduction and extracting deep level features of traffic using DNN. Using GRU to extract temporal features of traffic, the two feature maps are combined to ensure the comprehensiveness of the extracted features.
2. By introducing self AttM, the traditional transformer network has been improved to achieve fast convergence under massive computational data.
3. A multi-party collaborative learning framework was built based on FedL, and a NID model was constructed by combining DNN module, GRU module, and encoder module composed of improved transformer.

RELATED WORK

NID

The NID system is an important component of network security research. It detects intrusion behavior through proactive defense technology and takes emergency measures such as alerting and terminating the intrusion. Therefore, with the rapid development of learning technology, people have developed

Deriving Competitive Foresight Using an Ontology-Based Patent Roadmap and Valuation Analysis

Amy J.C. Trappey, Charles V. Trappey, Ai-Che Changand Jason X.K. Li (2019). *International Journal on Semantic Web and Information Systems (pp. 68-91).*
www.irma-international.org/article/deriving-competitive-foresight-using-an-ontology-based-patent-roadmap-and-valuation-analysis/223109