Journal of Engineering Science and Technology Review 16 (5) (2023) 150 - 155

Research Article

JOURNAL OF
Engineering Science and Technology Review

www.jestr.org

Intelligent Detection Method for Malicious Attacks in Enterprise Internet of Things Based on Graph Neural Network

Wei Liu[1,*] and Xilin Liu[1,2]

[1]*Shenzhen Power Supply Bureau Co., Ltd., 518000, China*
[2]*School of Electrical and Electronic Engineering, North China Electric Power University, Beijing 102206, China*

Received 11 March 2023; Accepted 30 October 2023

Abstract

With the continuous development of Internet of Things (IoT) technology and the widespread application of IoT by enterprises, enterprise IoT is facing increasingly complex and frequent malicious attack threats. To effectively detect malicious attacks in enterprise IoT and timely take corresponding security protection measures, an intelligent detection method was proposed for malicious attacks in enterprise IoT based on graph neural networks. Pre-processing enterprise IoT data, extracting data features, analyzing data packet transmission characteristics, and employing a graph neural network to extract time series features were involved in this method. To mitigate feature gradient disappearance, additional connections were incorporated. Data containing interactive nodes was filtered using these features, and a three-layer model was established for classifying the data, thus facilitating intelligent detection of malicious attacks. Experimental results show that this method can accurately describe the changing characteristics of malicious attacks on enterprise IoT and overcome the shortcomings of current malicious attacks on enterprise IoT. It achieves a 100% accuracy rate on the KDD (Knowledge Discovery and Data Mining) Cup 1999 dataset and enterprise IoT and is consistent with the imported data information. The average malicious node detection rate of this method is 97.26% on the two datasets. The method outperforms node-centered control algorithms, mutual information-based methods, and GWB-LSSVM joint methods. The proposed intelligent detection method exhibits strong feasibility, high accuracy, and important practical application value.

Keywords: Enterprise IoT, Malicious attack, Network attack, Graph neural network, Intelligent detection, Feature gradient

1. Introduction

The Internet of Things (IoT) technology, an extension of Internet technology, connects the Internet with physical objects to enable information exchange among them. The adoption of IoT technology in various business fields has given rise to the concept of enterprise IoT. However, it also introduces the risk of malicious attacks, which can potentially lead to data breaches and significant losses for enterprises. Detecting and mitigating these attacks promptly has become a critical concern in the field.

Current network attack detection methods often fall short in meeting the security maintenance needs of enterprise IoT for several reasons. First, traditional rule-based and feature engineering methods struggle to adapt to dynamically changing attack behaviors [1]. Second, the complexity of topological structures and connection relationships in enterprise IoT environments poses a challenge for traditional machine learning algorithms. Furthermore, existing detection methods frequently require extensive manual involvement and adjustments, resulting in inefficiency and the potential for false positives and false negatives [2].

To address these challenges, this study introduces a novel approach: an intelligent detection method for malicious attacks in enterprise IoT based on graph neural networks. This method leverages graph neural networks to filter and classify data with interactive nodes, thus facilitating the detection of malicious attacks within enterprise IoT. Specifically, the paper models data as a graph structure and utilizes graph neural networks to handle high-dimensional node features and intricate node relationships. By learning the representation of nodes and edges within the graph, these networks effectively capture the patterns and characteristics of malicious attacks. Subsequently, by classifying alerts, the method quickly and accurately identifies malicious behavior and enables the implementation of appropriate defensive measures.

The contribution of this study lies in the introduction of graph neural networks to the realm of enterprise IoT malicious attack detection, presenting a fresh and robust solution. Experimental results demonstrate the method's strong performance in detecting malicious attacks within enterprise IoT, offering effective security maintenance solutions for enterprises. The remainder of this study is structured as follows: first, it presents relevant research findings from scholars in the current field; then, it outlines the intelligent detection method for malicious attacks in the enterprise IoT; finally, it verifies the method's detection performance through simulation experiments.

2. Literature review

Numerous scholars have proposed methods for detecting network attacks. For example, Yi [3] detected network attacks by identifying key behavioral characteristics within network attack data. This approach involves importing classified network traffic data into the model and applying

*E-mail address: chexvtisirgxtdoc@163.com
ISSN: 1791-2377
doi:10.25103/jestr.165.18

mutual information theory to analyze interactions between classified data within the model. This analysis leads to the classification and identification of persistent network attack data, thereby completing the network attack detection process. However, this method suffers from low detection accuracy. Zhao, et al. [4] conducted research based on maritime communication networks, analyzing the characteristics of network attack traffic within this specific network environment. They established a node simulator for malicious traffic based on their analysis results. However, this method has limited applicability beyond the maritime domain. Zhang, et al. [5] conducted research within the power system network domain, analyzing both the information and physical domains within the power system. They integrated these results to create a complex network architecture model of the power system. Unfortunately, this method exhibits poor real-time performance.

Some scholars introduced machine learning methods for attack detection. For example, Arunkumar, et al. [6] improved attack detection accuracy in cloud computing environments by employing supervised and unsupervised machine learning techniques. They used these techniques to detect and prevent attacks effectively. Inayat, et al. [7] used machine learning and deep learning methods for data collection, feature extraction, selection, model training, evaluation, and the identification and prediction of IoT attacks. They employed convolutional neural networks for precise feature extraction and further classification using long short-term memory models.

Deep learning is also gaining prominence in attack detection. For example, Sahu, et al. [8] used convolutional neural networks for feature extraction and subsequently classified the data using long short-term memory models for accurate attack detection. Mohammadpourfard, et al. [9] designed a long short-term memory recurrent neural network that embedded dynamic time-varying power system characteristics, enabling accurate modeling of the power grid's dynamic behavior in response to attacks. This distinguished power grid changes from real-time attacks. Zografopoulos, et al. [10] proposed an integrated method for multi-agent microgrid systems based on the subspace method, enhancing the detection of malicious cyber-physical attacks. They constructed an attack detector using the small-signal model of autonomous/islanded microgrids, effectively identifying stable kernel representations in the absence of attacks. Alkahtani, et al. [11] identified botnet attacks using a hybrid learning algorithm, specifically a combination of convolutional neural networks and long short-term memory algorithms.

Faster attack detection performance can also be achieved through end services. Simpson, et al. [12] proposed a security method based on edge computing and fuzzy logic to reduce cooperative attacks in IoT networks within smart cities. They established a trusted environment by using fuzzy logic for node reputation assessment and malicious node detection. Additionally, computing tasks were offloaded to edge servers to enhance performance and reduce latency, effectively mitigating the impact of attacks.

In the above-mentioned research, some scholars detected network attacks by identifying behavioral characteristics of network attack data, analyzing attack traffic characteristics in specific network environments, and building complex network models. However, these methods have limitations. To improve the accuracy and reliability of network attack detection, many researchers introduced machine learning and deep learning methods. These methods use supervised and unsupervised machine learning techniques to extract and select features from the data and build models to identify malicious behaviors and prevent attacks. With convolutional neural networks and long short-term memory models, feature representations of classified and predicted data can be extracted accurately. These technologies enable great accuracy and feasibility of attack detection. In addition, when implementing attack detection, end services and edge computing are used to improve detection performance. By establishing a trusted environment in edge computing environments, cooperative attacks can be reduced. Moreover, the use of hybrid learning algorithms, such as the combination of convolutional neural networks and long short-term memory algorithms, can help identify botnet attacks.

In summary, network attack detection remains a challenging field, with researchers continually exploring diverse methods and technologies to enhance detection accuracy and reliability. However, further research is required to improve malicious attack detection performance and apply these methods in practical network environments to enhance network security and safeguard user data confidentiality.

3. Design of intelligent detection method for malicious attacks in enterprise IoT

3.1 Preprocessing enterprise IoT data for feature extraction

The following formula is used to comprehensively analyze enterprise IoT traffic data and normalize the initial IoT data:

$$x = \frac{x' - x'_{\min}}{x'_{\max} - x'_{\min}} \tag{1}$$

In the formula, x represents the normalized enterprise IoT data, x' represents the initial IoT data, x'_{max} and $x'_{\min}$ represent the maximum value and minimum value, respectively.

Dimensionality reduction is then performed on the normalized enterprise IoT data to reduce the impact of data dimensions. The dimensionality reduction method is given as follows:

$$L = \frac{\lambda}{2}\left\|\sigma w x^{\lambda} + b\right\|^2 \tag{2}$$

In the formula, L represents the dimensionality reduction divergence, λ represents the regularization parameter, σ represents the response coefficient, w and b represent the row vector and column vector of the data in the space, respectively.

The low-dimensional data is standardized for subsequent unified feature extraction using the following method:

$$X = x_L - \frac{\sum_{x=1}^{a}\eta}{\alpha} \tag{3}$$

In formula (3), X represents standardized data, x_L represents low-dimensional data, η represents the maximum eigenvalue, and represents the bias vector.

The standardized enterprise IoT data is used for a unified data feature extraction process. Based on the maximum eigenvalue of the data, a feature judgment matrix is established, which is expressed as follows:

$$A=\begin{bmatrix} 1 & 2 & 2 & \frac{1}{2} \\ \frac{1}{2} & 1 & 1 & \frac{1}{2} \\ \frac{1}{2} & 1 & 1 & \frac{1}{2} \\ 2 & 2 & 2 & 1 \end{bmatrix} \tag{4}$$

In formula (4), A represents the feature judgment matrix.

The covariance of the data features is calculated through this matrix, that is,

$$c_{(x)}=\frac{\sum_{j=1}^{a}(X-\overline{X})}{a-1}, j \in A \tag{5}$$

In the formula, $c_{(x)}$ represents the data feature covariance, j represents the data feature value, and $\overline{X}$ represents the data feature vector mean.

According to the calculated data feature covariance value, the data features are extracted in order according to the size of the covariance value.

3.2 Graph neural network for filtering enterprise IoT data interaction nodes

The extracted characteristics of enterprise IoT data are deconstructed, and the data packet transmission with different data characteristics in enterprise IoT is analyzed, as shown in Fig.1. The data transmission in enterprise IoT tends to avoid areas with significant data congestion. According to this characteristic, the characteristics of the enterprise IoT data are processed.

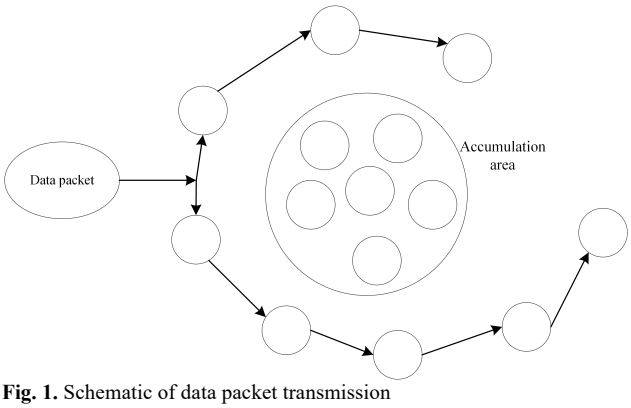

Fig. 1. Schematic of data packet transmission

The graph neural network is used to extract the time series features of data features, as shown in Fig.2. This study uses a graph neural network to add residual connections to the temporal characteristics of the data in the output process, addressing issues related to gradient vanishing.

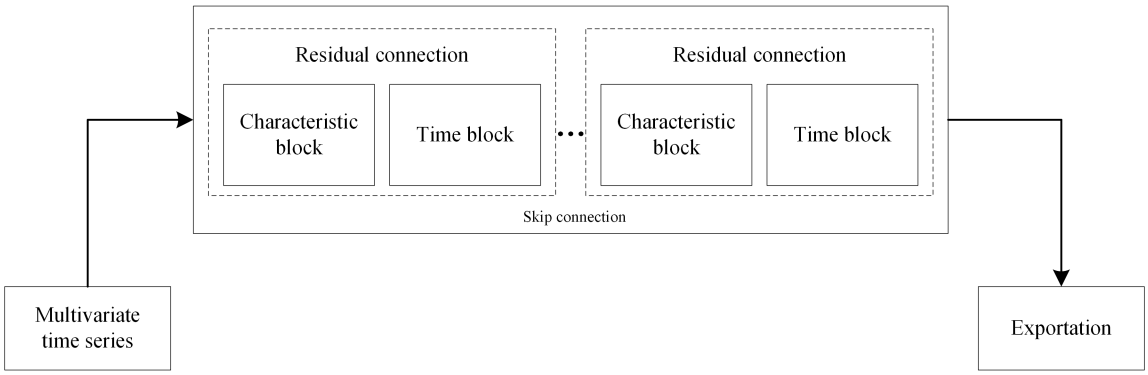

Fig.2. Neural network extracting time series features

According to the extracted time characteristics of the data, the interactive nodes of the data in enterprise IoT are filtered.

$$\hat{y}=R(h\sum_{k=0}^{k}\theta)^{-\frac{1}{2}} \tag{6}$$

In the formula, $\hat{y}$ represents the number of interactive nodes of the data, R represents the layer index, k represents the time characteristics of the data, and θ represents the data transmission parameters.

Using the results of the interactive node count, the data containing interactive nodes in enterprise IoT are filtered out. Data with a calculated result of "0" is eliminated [13], followed by a thorough inspection of the filtered data.

3.3 Intelligent detection of malicious attack nodes in enterprise IoT

Intelligent detection of malicious attack nodes on the filtered enterprise IoT interaction data is performed. A three-layer malicious attack detection model is established [14-16], as shown in Fig.3. The data containing interactive nodes in the enterprise IoT are detected and classified into normal data and suspected attack data in the second-layer architecture [17-19]. The types of malicious attacks on suspected data are classified in the third-layer architecture of the model.

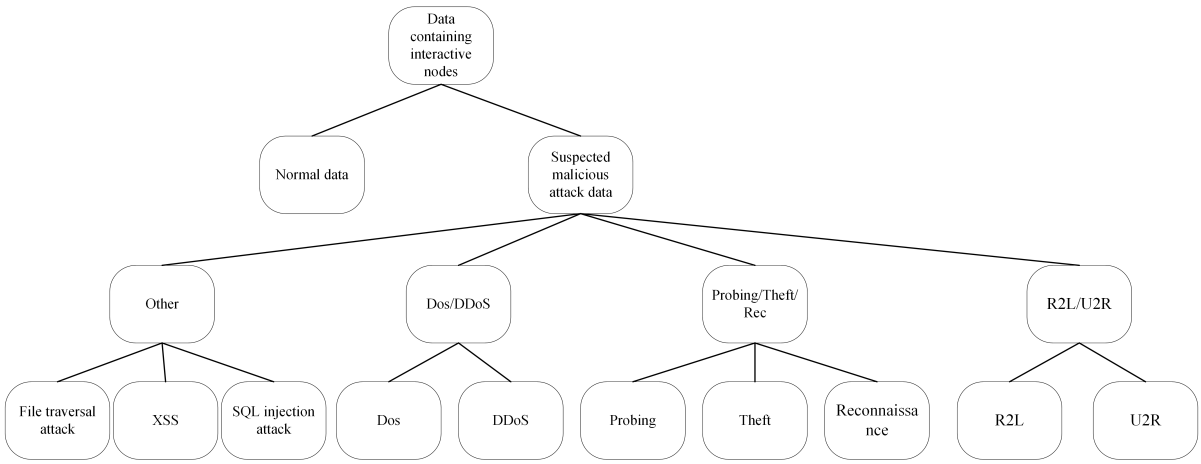

Fig.3. Three-layer malicious attack detection model

The malicious attack data detected by this model are encoded with information timestamps [20] as follows:

$$T = G_{(X)} \cdot t + \delta \tag{7}$$

In formula (7), T represents the information timestamp, $G_{(X)}$ represents the data detected as a malicious attack, t represents the detection time, and δ represents the measured malicious attack category.

The encoded data are fed back to complete the detection of malicious attacks in enterprise IoT.

4. Simulation experiment

To test the feasibility of the intelligent detection method for malicious attacks in enterprise IoT proposed in this study, the corresponding simulated experimental results are observed.

4.1 Experiment settings

To ensure the universality of the results of this experiment, malicious attack detection experiments were conducted on multiple types of enterprise IoT. The categories of enterprises involved are shown in Table 1.

Table 1. Business Categories

Serial Number	Business Category	Serial Number	Business Category
1#	Agriculture	9#	Transportation
2#	Industry	10#	Construction and installation industry
3#	Service industry	11#	medical hygiene
4#	Post and telecommunications	12#	Urban Construction
5#	communication	13#	Tourism
6#	community service	14#	Hotel
7#	wholesale	15#	Catering
8#	retail industry		

The currently recognized IoT architecture was used to build enterprise IoT for different enterprises, as shown in Table 2. The attack detection experiment in the built IoT was then conducted.

Table 2. Enterprise IoT Architecture

Hierarchy of architecture	Architecture function
Application layer	Processing information, human–computer interaction
Perceptual layer	Sensing data collection
Network layer	Transferring data information to the application layer

4.2 Experimental dataset

Two types of datasets were selected for the experiment to test the detection performance under different attack data types. They are the KDD (Knowledge Discovery and Data Mining) Cup 1999 network attack dataset and the Bot-IoT displacement attack dataset. The attack traffic categories of the two datasets are shown in Tables 3 and 4.

Table 3. KDD Cup 1999 Dataset Attack Traffic Categories

Attack traffic category	Quantity
Prob	56517
R2L	49389
U2R	59689
DoS	46637
SQL injection attack	15567
Normal	496968

Table 4. Bot-IoT Dataset Attack Traffic Categories

Attack traffic category	Quantity
DoS	6526
DDoS	2609
Reconnaissance	7496
Theft	4954
XSS	7626
File traversal attack	9426
Normal	16974

4.3 Experimental platform

The two datasets were divided into a 3:1 ratio. The larger portion (3 parts) was used as the training set for algorithm and model training, whereas the smaller part (1 part) served as the test set for conducting malicious attack detection experiments on the enterprise IoT. The main equipment used in the experiment includes peripherals that implement the enterprise IoT architecture, network peripherals that provide wireless connection networks, and a PC. The parameter configuration of the PC is presented in Table 5.

Table 5. PC Parameter Configuration

Parameter item	Parameter configuration
Operating system	Windows 10
CPU	Inter Core i7 – 107000K
Graphics card	NVIDIA RrForce RTX 3080
Internal storage	16 G
Programming language	Python

4.4 Experimental results and analysis

The feasibility of the intelligent detection method for malicious attacks on enterprise IoT, based on graph neural networks was evaluated. The KDD Cup 1999 dataset and agricultural-type enterprise IoT were used for the evaluation. A 2D spatial distribution of enterprise IoT data was created to visualize the test results. The results are shown in Figure 4. The IoT data's 2D distribution closely aligns with the imported data information. This preliminary assessment suggests that the method proposed in this study can effectively detect malicious attacks on enterprise IoT and is indeed feasible.

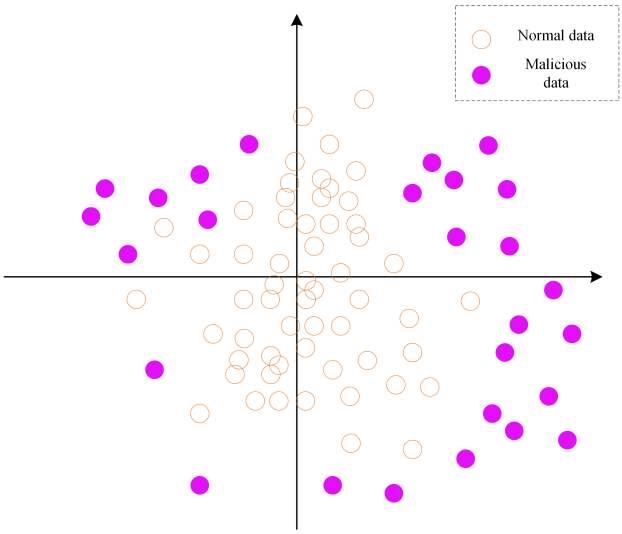

Fig. 4. Intelligent detection of malicious attacks in enterprise IoT

To provide a more quantitative assessment of the method's effectiveness, quantitative index evaluation and analysis of the experimental detection results were conducted. The effectiveness of different detection methods was determined by comparing the index calculation results of different deployment methods. Attack data and normal data were treated as malicious nodes and legitimate nodes, respectively. The evaluation index of this experiment was set as the malicious node detection rate. The calculation formula is

$$\xi = \frac{N_a}{N_A} - \frac{N_{la}}{N_l} \tag{8}$$

In formula (8), ξ represents the detection rate of malicious nodes, N_a represents the number of detected malicious nodes, N_A represents the number of malicious nodes, N_{la} represents the number of legitimate nodes detected as malicious nodes, and N_l represents the number of legitimate nodes [14-15].

The calculation results of the malicious node detection rate can effectively reflect the overall performance of the malicious attack detection method for the enterprise IoT. The higher the calculated malicious node detection rate, the higher the accuracy and credibility of the detection results.

The comparative analysis method was used to analyze the effectiveness of the experimental results, and the network attack methods proposed by the node-centered control algorithm and the joint method based on mutual information and GWB-LSSVM were used for comparison. The malicious attack detection performance of enterprise IoT under the two datasets was tested. The serial numbers shown in Table 1 were used to detect different types of enterprise IoT. To reduce experimental errors, this detection experiment was conducted multiple times. The detection results of different methods are shown in Fig.5. In the malicious attack detection experiment on different types of enterprise IoT using two datasets, the method proposed in this study achieves an average malicious node detection rate of 97.26%. The average detection rates of malicious nodes of the node-centered control algorithm and the method combined with GWB-LSSVM are 74.66% and 56.79%, respectively. This experimental comparison demonstrates that the method proposed in this study significantly improves the accuracy of malicious attack detection on enterprise IoT, yielding highly accurate detection results.

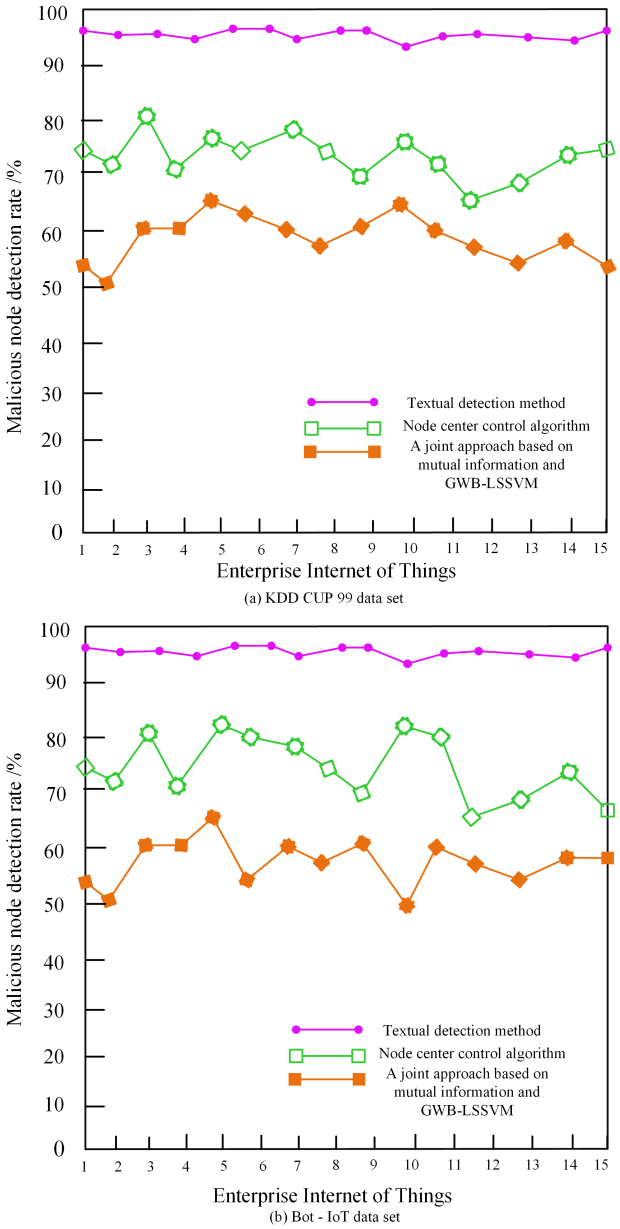

Fig. 5. Detection results of different methods

In summary, the comparative analysis results of the experiment demonstrate that the proposed method yields a relatively high detection performance for malicious attacks on enterprise IoT. The obtained detection results are highly credible.

5. Conclusion

Ensuring the security of data information in the operation of enterprise IoT and preventing the leakage of sensitive enterprise information is of paramount importance. This study has introduced an intelligent detection method for malicious attacks on enterprise IoT based on graph neural networks, leading to the following research findings:

(1) This method incorporates graph neural networks with residual connections to the temporal characteristics of data during the output process. This approach effectively mitigates the issue of gradient vanishing and enhances the success rate of malicious attack detection.

(2) This method achieves good results on the KDD Cup 1999 dataset and within the context of enterprise IoT. In visualizing a 2D spatial distribution of enterprise IoT data, the method's detection results for malicious attacks on enterprise IoT closely align with the imported data information. This finding indicates the method's robust feasibility in effectively detecting malicious attacks on IoT.

(3) Using two datasets, KDD Cup 1999 and Bot-IoT datasets, for malicious attack detection rate analysis and comparison with other literature methods, the proposed method achieves an average malicious node detection rate of 97.26%, significantly surpassing the performance of other literature methods. This outcome underscores the method's capability for accurate malicious attack detection.

Although this study has yielded valuable research findings, it also highlights several challenges and avenues for future exploration. As the scale of enterprise IoT continues to expand, in-depth research into detecting malicious attacks in large-scale network environments is necessary. Additionally, the development of more precise and efficient models and algorithms to counter new malicious attack methods is an important direction for future research. Strengthening the formulation of IoT security standards and policies, as well as fostering collaboration between industry and academia, will play a pivotal role in advancing the innovation and application of IoT security technology.

References

[1] L. Liu, Q. C. Zhao, R. F. Zheng, Z. Y. Tian and S. Q. Sun. "Method for automatically generating intrusion detection rules based on threat intelligence, " *Comput. Eng. Des.,* vol. 43, no. 1, pp. 1-8, Jan. 2022.

[2] J. J. Chen, B. Z. Peng, and P. Z. Wu. "Malicious code detection method based on dynamic behavior and machine learning," *Comput. Eng.,* vol. 47, no. 3, pp. 166-173, Mar. 2021.

[3] M. Yi. "Design of malicious attack detection system for maritime communication network traffic," *Ship. Technol. Res.,* vol. 43, no. 2, pp.175-177, Jan. 2021.

[4] J. Zhao, L. Gu, and Y. Wu. "Network attack detection model based on MI-GWB-LSSVM," *Meas. Sci. Technol.,* vol. 45, no.24, pp.98-104, Dec. 2022.

[5] B. Zhang, X. Liu, Z. C. Yu, W. B. Wang, Q. Q. Jin, and W. J. Li. "Review on artificial intelligence-based network attack detection in power systems," *High Volt. Eng.,* vol. 48, no. 11, pp. 4413-4426, Nov. 2022.

[6] M. Arunkumar, K. Ashok Kumar. "Malicious attack detection approach in cloud computing using machine learning techniques," *Soft Comput.,* vol. 26, no. 23, pp. 13097-13107, Feb. 2022.

[7] U. Inayat, M. F. Zia, S. Mahmood, H. M. Khalid, and M. Benbouzid. "Learning-based methods for cyber attacks detection in IoT systems: A survey on methods, analysis, and future prospects," *Electronics,* vol. 11, no. 9, pp. 1502, May.2022.

[8] A. K. Sahu, S. Sharma, M. Tanveer, and R. Raja. "Internet of Things attack detection using hybrid Deep Learning Model," *Comput. Commun.,* vol. 176, pp. 146-154, Aug. 2021.

[9] M. Mohammadpourfard, A. Khalili, I. Genc, and C. Konstantinou. "Cyber-resilient smart cities: Detection of malicious attacks in smart grids," *Sustain. Cities Soc.,* vol.75, Dec. 2021, Art. no.103116.

[10] I. Zografopoulos and C. Konstantinou. "Detection of malicious attacks in autonomous cyber-physical inverter-based microgrids," *IEEE Trans. Ind. Electron.,* vol. 18, no. 9, pp. 5815-5826, Dec. 2021.

[11] H. Alkahtani and T.H.H. Aldhyani. "Botnet attack detection by using CNN-LSTM model for Internet of Things applications," *Secur. Commun. Netw.,* vol. 2021, Sep. 2021, Art. no. 3806459.

[12] S.V. Simpson and G. Nagarajan. "A fuzzy based co-operative blackmailing attack detection scheme for edge computing nodes in MANET-IOT environment," *Futur. Gener. Comp. Syst.,* vol. 125, pp.544-563, Dec. 2021.

[13] D. Grattarola and C. Alippi. "Graph neural networks in tensorflow and keras with spektral [application notes]," *IEEE Comput. Intell. Mag.,* vol. 16, no. 1, pp.99-106, Feb. 2021.

[14] F. Hussain, et al. "A framework for malicious traffic detection in IoT healthcare environment," *Sensors,* vol. 21, no. 9, pp. 3025, Apr. 2021.

[15] U. Inayat, M. F. Zia, S. Mahmood, H. M. Khalid, and M. Benbouzid. "Learning-based methods for cyber attacks detection in IoT systems: A survey on methods, analysis, and future prospects," *Electronics,* vol. 11, no. 9, pp. 1502, May. 2022.

[16] I. A. Kandhro, *et al.* "Detection of real-time malicious intrusions and attacks in IoT empowered cybersecurity infrastructures," *IEEE Access,* vol. 11, pp. 9136-9148. Jan. 2023.

[17] T. D. Diwan, *et al.* "Feature entropy estimation (FEE) for malicious IoT traffic and detection using machine learning," *Mob. Inf. Syst.,* vol. 2021, Dec. 2021, Art. no. 8091363.

[18] A. Khraisat and A. Alazab. "A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges," *Cybersecurity,* vol. 4, pp.1-27, Mar. 2021.

[19] M. S. Abdalzaher, M. Elwekeil, T. Wang, and S. Zhang. "A deep autoencoder trust model for mitigating jamming attack in IoT assisted by cognitive radio," *IEEE Syst. J.,* vol. 16, no. 3, pp. 3635-3645, Sep. 2021.

[20] V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha, and G. Srivastava, "Federated-learning-based anomaly detection for IoT security attacks". *IEEE Internet Things J.,* vol. 9, no. 4, pp.2545-2554, May, 2021.