ISSN 1330-3651 (Print), ISSN 1848-6339 (Online) https://doi.org/10.17559/TV-20230808000860
Original scientific paper

Illegal Intrusion Detection of Internet of Things Based on Deep Mining Algorithm

Xingjuan FAN, Hui LI*, Xinglong LIU, Fangtong GUO, Hongjing MA

Abstract: In this study, to reduce the influence of The Internet of Things (IoT) illegal intrusion on the transmission effect, and ensure IoT safe operation, an illegal intrusion detection method of the Internet of Things (IoT) based on deep mining algorithm was designed to accurately detect IoT illegal intrusion. Moreover, this study collected the data in the IoT through data packets and carries out data attribute mapping on the collected data, transformed the character information into numerical information, implemented standardization and normalization processing on the numerical information, and optimized the processed data by using a regional adaptive oversampling algorithm to obtain an IoT data training set. The IoT data training set was taken as the input data of the improved sparse auto-encoder neural network. The hierarchical greedy training strategy was used to extract the feature vector of the sparse IoT illegal intrusion data that were used as the inputs of the extreme learning machine classifier to realize the classification and detection of the IoT illegal intrusion features. The experimental results indicate that the feature extraction of the illegal intrusion data of the IoT can effectively reduce the feature dimension of the illegal intrusion data of the IoT to less than 30 and the dimension of the original data. The recall rate, precision, and F1 value of the IoT intrusion detection are 98.3%, 98.7%, and 98.6%, respectively, which can accurately detect IoT intrusion attacks. The conclusion demonstrates that the intrusion detection of IoT based on deep mining algorithm can achieve accurate detection of IoT illegal intrusion and reduce the influence of IoT illegal intrusion on the transmission effect.

Keywords: data classification; deep mining algorithm; extreme learning machine; feature extraction; illegal intrusion detection; IoT

1 INTRODUCTION

The Internet of Things (IoT) technology has been widely used in various industries. The IoT is a technology that connects various devices and people, realizes information interaction, and improves people's work and life [1-5]. The resulting IoT security problems are also emerging one after another. In particular, some criminals use illegal techniques to infiltrate the IoT for personal interests, steal IoT data, and attack related IoT devices during IoT communication, resulting in IoT paralysis and major losses to the security of enterprise and personal information.

Illegal intrusion detection is the key to the security of the IoT. This mechanism can determine the presence of an illegal intrusion in the IoT by comparing certain information, such as user behavior and network usage rate, with normal behavior. The illegal intrusion attacks of the IoT include malicious use attacks, malicious response injection attacks, denial of service attacks, and other attacks, among which denial of service attack is the main attack behavior. Hu et al. [6] developed a stackable denoising convolutional autoencoding network, extracted key features, combined the convolutional neural network and de-noising auto-encoder to enhance the feature recognition ability, improved the pooling operation to increase the adaptive processing ability, and adopted Adam algorithm to obtain the optimal parameters during the model training to complete the intelligent intrusion detection of the industrial IoT based on deep learning. Lv et al. [7] used the Hadoop distributed computing system to complete the deployment of an online integration model and realize the IoT intrusion detection of smart homes based on the edge cloud collaborative environment. Li et al. [8] combined the perception ability of deep learning with the decision ability of reinforcement learning to achieve effective detection of various types of network attacks on the industrial IoT.

There may be various types of illegal intrusion behaviors involved in the Internet of Things environment, such as network attacks, device tampering, etc. How to design effective deep mining algorithms for different types of intrusions has become an important issue. IoT data typically has high-dimensional and complex features, and traditional machine learning methods may have certain limitations when processing these data. Therefore, it is necessary to explore deep mining algorithms and models suitable for high-dimensional data. Illegal intrusion behavior in the Internet of Things environment has concealment and complexity, and traditional security defense methods often cannot identify new intrusion and attack methods. Therefore, studying illegal intrusion detection methods for the Internet of Things has important practical significance and challenges. By conducting in-depth research on illegal intrusion detection methods in the Internet of Things, the security and risk resistance of IoT systems can be improved. An effective illegal intrusion detection system can help detect and prevent intrusion activities in a timely manner, enhance the security protection capabilities of IoT systems, and protect user privacy and data security.

In recent years, deep mining algorithms have shown excellent performance as a powerful machine learning technology in many fields. In the field of information security, deep mining algorithms are playing an increasingly important role in illegal intrusion detection. However, research on the issue of illegal intrusion detection in the Internet of Things, especially the application research based on deep mining algorithms, is still in its early stages. Deep mining algorithms, such as Deep Neural Networks and Convolutional Neural Networks, can learn advanced feature representations from large-scale data through multi-level neural network structures, with strong pattern recognition and data mining capabilities. This makes deep mining algorithms have great potential in the field of illegal intrusion detection. Although some studies have explored deep mining algorithms for illegal intrusion detection in traditional network environments, there is still relatively little research on their application in IoT environments. The special properties of the Internet of Things, such as high-dimensional data, dynamic network topology, and device

heterogeneity, bring new challenges to the application of deep mining algorithms. Therefore, conducting research on illegal intrusion detection in the Internet of Things based on deep mining algorithms has important practical significance and theoretical value. In this work, the illegal intrusion detection of IoT based on the deep mining algorithm is to accurately detect the illegal intrusion of the IoT, reduce the influence of illegal intrusion on the transmission effect of the IoT, and ensure the operation security of the IoT.

2 STATE OF THE ART

Several scholars in related fields have conducted in-depth research on the difficulty and low efficiency of illegal intrusion detection of the IoT. Saheed et al. [9] applied intrusion detection system (IDS) based on the ML supervision algorithm to the IoT. The concept of minimum–maximum normalization was used for feature scaling on the UNSW-NB15 dataset to limit the information leakage of test data. Yao et al. [10] studied network intrusion detection based on the combination of parameter t-distribution random neighbor embedding and hierarchical neural network. The unsupervised dimension reduction algorithm was used to reduce the dimension of multiple data to complete the detection. This method was applied in a small number of data sets with better-concentrated effects. Elmenshawy et al. [11] studied the clustering-based IoT context anomaly detection method and divided IoT context attributes into two different categories, namely, context and behavioral attributes. The K-Means clustering technology was applied to context and behavior attributes, and the intersection between context and behavior clustering was used to detect context anomalies. Dong et al. [12] constructed an intrusion detection model of wireless sensor networks based on the information gain ratio and Bagging algorithm. In this model, the information gain ratio method was used to select the characteristics of traffic data of sensor nodes. Then, the Bagging algorithm was used to construct an ensemble classifier to train multiple improved C4.5 decision trees. The parameters of the ensemble classifier were optimized by 10 iterations, and a dynamic pruning process was introduced. Finally, the classification results of C4.5 decision trees were classified and tested by the majority voting mechanism. Zhang [13] took IDS as the research object and established an IDS model based on data mining to realize network vulnerability intrusion detection based on data mining. The experimental results indicate that the intrusion detection system based on data mining has better network security performance and stronger detection ability for network vulnerability intrusion. The aforementioned system provides a new way for the research of intrusion detection of network protection security vulnerabilities. Khan et al. [14] proposed a new intrusion detection method based on ensemble voting classifier, which combined multiple traditional classifiers as the basic learner and voted on the prediction of traditional classifiers to obtain the final prediction. They conducted experiments on a group of seven different IoT devices to test the effectiveness of the proposed method and the binary and multi-class attack classification. The experimental results demonstrated that the method could fully detect binary and multi-class attack classification with good practical application effects. Tian et al. [15] suggested a two-stage intrusion detection method for the SD IoT network. The variation mechanism of the differential evolution algorithm was used to improve the firefly algorithm to solve various problems, such as slow convergence speed, easily falling into the local optimum, and low precision in complex problems. This mechanism adopted the wrapper-based feature selection method to send the selected features to a new ensemble classifier, which was composed of a C4.5 decision tree, a multi-layer perceptron, and instance-based learning. The weighted voting method was used to determine whether the network traffic is abnormal to realize the two-stage intrusion detection method of the SD IoT network. Roy et al. [16] proposed an intrusion detection model based on machine learning to effectively detect network attacks and anomalies in a resource-constrained IoT network. The model can use less training data and training time in identifying the most important features of intrusion detection through a series of optimizations, including the removal of multicollinearity, sampling, and dimension reduction. The experimental results indicated that the model has a high detection rate, low false alarm rate, and good practical application effect. Mudgerikar et al. [17] proposed an intrusion detection method for system-level device edge separation IDS for IoT devices. IDS configures IoT devices in an autonomous, efficient, and scalable manner by using system-level information based on their behavior and detecting abnormal behavior that represents an intrusion. Modular design and unique device edge segmentation architecture allow for effective attack detection on IoT devices with minimal overhead to ensure the quality and efficiency of IoT attack detection.

The original data of IoT intrusion detection are characterized by high dimensions, large number of data sets, and uncertainty of network intrusion behaviors. However, the above-mentioned methods have poor processing ability for massive data sets. Moreover, the detection process will suffer from overfitting due to the complex environment of IoT and redundant data information, resulting in low detection accuracy. The deep mining algorithm can excavate valuable information from massive data and improve the information utilization rate. Therefore, IoT intrusion detection is studied based on the deep mining algorithm.

The remaining structure of this study is as follows: Section 3 provides the method design for achieving illegal intrusion detection in the IoT. Section 4 discusses the experimental design results and analysis.

3 METHODOLOGY

This study sets up an IoT illegal intrusion detection model of the deep mining algorithm to improve the illegal intrusion detection efficiency of the IoT. The overall structure of the method is shown in Fig. 1. To effectively use the deep mining algorithm to detect the illegal intrusion detection of the IoT, collect data, and conduct normalized pre-processing of the collected original data, an IoT data training set is set up, an improved sparse auto-encoder neural network is used to extract the illegal intrusion features of IoT data training set, and the IoT illegal

intrusion features are classified through extreme learning machine. The classification result is the outcome of IoT illegal intrusion detection.

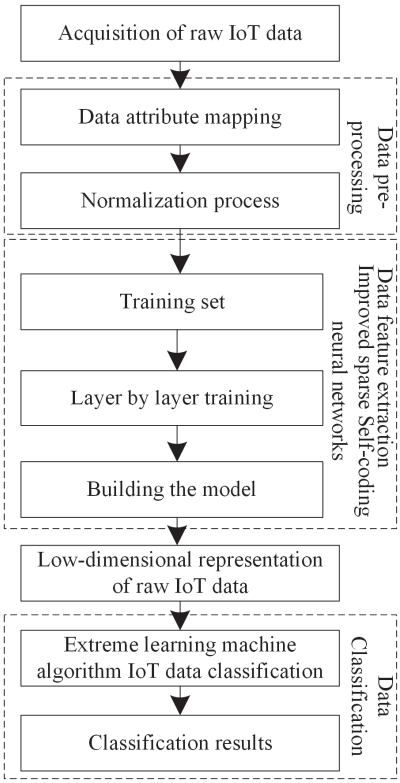

Figure 1 The overall structure of the IoT illegal intrusion detection method

3.1 IoT Data Pre-Processing Method

This mechanism collects IoT data through data packets, such as network traffic, IP address, and connection attributes, and pre-processes the collected data to meet the format of the sparse auto-encoder. The steps of the IoT data pre-process are as follows:

In data attribute mapping, the character information is converted into numerical information.

The IoT data is standardized and normalized to reduce the influence of the large number of different feature values on the training of the illegal intrusion detection model of IoT [18, 19]. The interval of data normalization is [0, 1]. The IoT data standardization formula is shown as follows:

$$y_1 = (y - \bar{y}) / \sigma \tag{1}$$

where $\bar{y}$ is the average characteristic value of IoT data, y_1 denotes the standardization results of the IoT data, y represents the IoT data characteristic value, and σ is the standard deviation of the IoT data.

The IoT data normalization formula is expressed as follows:

$$y_2 = (y_1 - y_{1\min}) / (y_{1\max} - y_{1\min}) \tag{2}$$

where y_2 represents the result after IoT data normalization; and $y_{1\min}$ and $y_{1\max}$ are the minimum and maximum characteristic values after the IoT data normalization, respectively.

(3) To solve the problem of unbalanced distribution of a few types of IoT data, the regional adaptive oversampling algorithm is adopted to optimize this type of data and obtain the training set of the IoT data.

3.2 Improve the Extraction of Illegal Intrusion Features from the Sparse Auto-Encoder Neural Network

Sparse autoencoders can extract advanced features by learning the sparse representation of input data. Sparse representation means that only a few neurons are activated when encoding input data, which helps to capture important information in the input data. Compared to traditional autoencoders, the improved sparse autoencoder can better represent subtle differences in input data. The IoT data training set constructed by the pre-processed data is used as the input of the improved sparse auto-encoder neural network. The neural network extracts the IoT illegal intrusion characteristics as the basis for IoT illegal intrusion detection. The auto-encoder is an input neural network, which is composed of an encoder and a decoder that attempt to reconstruct. The network can realize the conversion between the input and the encoded signals through the encoder to reduce the original data dimension. The sparse auto-encoder is generated by adding a new penalty factor into the network loss function. The neuron nodes of the sparse auto-encoder are greatly affected by subjective experience, resulting in poor adaptability. Therefore, the improvements are implemented on the basis of sparse auto-encoder to ensure the stability of the illegal intrusion feature extraction process of IoT. The improvement process of the sparse auto-encoder is as follows:

(1) Implement initial training for neural network. During training, the dimension of the neural network data set and the total number of neuron nodes at each layer must remain the same [20, 21].

(2) Improve the penalty factor, and generate an improved sparse auto-encoder neural network. To achieve the optimal loss function, the suppressed nodes are searched, and the constraint of the hidden layer neurons is strengthened by adding penalty factors. The penalty factor is the entropy between q_i and M_i. The improvement of the penalty factors is expressed as follows:

$$\sum_{i=1}^{1} q_i \log\left(\frac{q_i}{M_i}\right) + (1-q_i)\log\left[\frac{(1-q_i)}{1-M_i}\right] \tag{3}$$

where M_i is the average output activity of the fourth neuron, q_i is a random variable, and l is the number of hidden layer neurons.

(3) Train the improved network with the optimal penalty factor loss function as the training objective [22].

(4) Make clear the hidden layer neuron nodes.

An improved sparse auto-encoder illegal intrusion feature extraction model of the IoT is constructed on the basis of the layer-by-layer greedy training strategy. The training principle is as follows: first, train one hidden layer network; second, take the training results as the inputs of the next training; third, continue training two hidden layer networks; finally, obtain the optimal solution through cycle training [23].

The process of improving the sparse auto-encoder illegal intrusion feature extraction model of the IoT is as follows:

Step1: Input the original data through the standardized IoT, and obtain the new hidden layer of the auto-encoder neural network using the above-mentioned improved process.

Step 2: The improved sparse auto-encoder neural network method is adopted to obtain a new hidden layer from the auto-encoder neural network. The offset value and the number of nodes of the hidden layer are used to obtain an auto-encoder neural network. After training the original data of the IoT after data processing [24], the output value is the input of the new hidden layer.

Step 3: The improved sparse auto-encoder neural network method is adopted to obtain the next new hidden layer. After the new auto-encoder neural network is obtained from training the previous two steps, the output value is obtained as the input of the new hidden layer.

Step 4: The previous operation is repeated. The termination condition of the network training is that a new hidden layer cannot be obtained by using only the improved sparse auto-encoder neural network method.

The improved sparse auto-encoder neural network model can be obtained according to the above-mentioned process, as shown in Fig. 2. In Fig. 2, the encoder represents the IoT illegal intrusion feature extraction model, and the numbers in the model represent the features of the IoT dataset, that is, the dimensions of the data. After the improved sparse auto-encoder neural network model is used to reduce the dimension of IoT data, it can obtain the high sparse IoT illegal intrusion feature vector y_i.

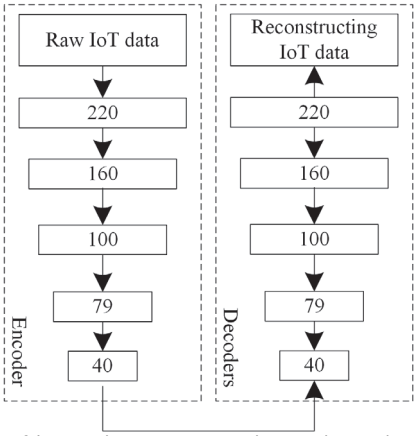

Figure 2 Improved sparse auto-encoder neural network model

3.3 IoT Illegal Intrusion Feature Classification Based on Extreme Learning Machine Algorithm

The high sparse feature vector y_i extracted by the improved sparse auto-encoder neural network is used as the input of the extreme learning machine classifier to realize the classification and detection of IoT illegal intrusion features. The extreme learning machine algorithm process is as follows: the new sample (y_i, t_i) consists of feature vector $y_i = [y_{i1}, y_{i2}, ..., y_{in}]^{\mathrm{T}} \in R^n$ and label vector $\boldsymbol{t}_i = [t_{i1}, t_{i2}, ..., t_{in}]$, a single hidden layer neural network with l hidden layer nodes:

$$u_j = \sum_{i=1}^{1} g(W_i y_i + b_i)\alpha_i, j = 1, 2, ..., n \tag{4}$$

where W_i is the input weight, $W_i = [w_{i,1}, w_{i,2}, ..., w_{i,n}]^{\mathrm{T}}$; $W_i y_i$ denotes the inner product of W_i and y_i; α_i is the output weight; b_i is the i hidden layer unit, $g(x)$ is the activation function; n is the number of feature vectors of the IoT samples; and u_i is the output value corresponding to the j input IoT feature vector sample.

The intrusion detection results with the minimum output target loss error can be obtained through the classification learning of the single hidden layer neural network of extreme learning machine, as shown in the following formula:

$$\sum_{j=1}^{N} u_j - t_j = 0 \tag{5}$$

where t_j is the j IoT feature vector sample corresponding to the actual output value.

When b_i, W_i, and α_i are known values:

$$t_j = \sum_{i=1}^{L} g(W_i X_i + b_i)\alpha_i, j = 1, 2, ..., n \tag{6}$$

The actual output matrix of IoT feature vector sample is as follows:

$$T = H * \alpha \tag{7}$$

where T is the actual output of the IoT illegal intrusion detection result, H is the node output matrix of the hidden layer, and α is the output weight.

b_i, W_i, and α_i can be obtained through the training of a single hidden layer neural network. Thus, the minimum loss function of the illegal intrusion detection of the IoT is:

$$\left\| H(W_i, b_i)\alpha_i - T \right\| = \min_{W, b, \alpha} H\alpha(W_i, b_i)\alpha_i - T \tag{8}$$

where $i = 1, 2, ..., n$. The output weight α of Eq. (8) is expressed as follows:

$$\alpha = T * H^{+} \tag{9}$$

where H^{+} is the H generalized inverse.

The output weight α and the IoT illegal intrusion detection results with the least loss can be obtained according to the above equation.

4 RESULT ANALYSIS AND DISCUSSION

The experiment selects the IoT of a logistics and warehousing company that consists of a perception layer, a network layer, and an application layer as the experimental object. The company covers an area of about 200 000 m^2 and is divided into three office areas: A, B and C. The IoT has covered all areas of each district and is mainly responsible for the warehousing, distribution, and

equipment management of international goods. The company's IoT collects data through various sensors, cameras, REID tags, and other devices in the perception layer and transmits to the application layer after being transmitted and processed through the limited wireless network and cloud computing platform in the network layer. The method in this study is used to detect the illegal intrusion of the logistics and warehousing company's IoT and tests its application effect. The IoT data set is selected as the experimental data set, which includes five types of IoT illegal intrusion data and one type of normal data.

Table 1 Data set

Type	Training set/unit	Testing set/unit
Illegal access to remote machine (R2L)	58	300
Malicious Status Command Injection (MSCI)	789	123
Denial of Service Attach (Dos)	46987	4456
Complex Malicious Response Injection (CMRI)	14566	3656
Port Scanning and Detection Attach (Probe)	11756	2306
Normal Access Data (Normal)	65465	2356

Statistics on the training loss curve of the single hidden layer neural network are conducted using the extreme learning machine to verify the method's IoT illegal intrusion classification effect in this study. The training loss results are shown in Fig. 3. Fig. 3 indicates that the neural network training loss of the extreme learning machine significantly decreases when the training times are 300. When the training times are more than 750, the training loss curve is in a slow and stable downward trend, and the training loss tends to zero, indicating that the method in this study applies extreme learning machine to the classification detection of illegal intrusion in the IoT with good convergence and can improve the efficiency of intrusion detection.

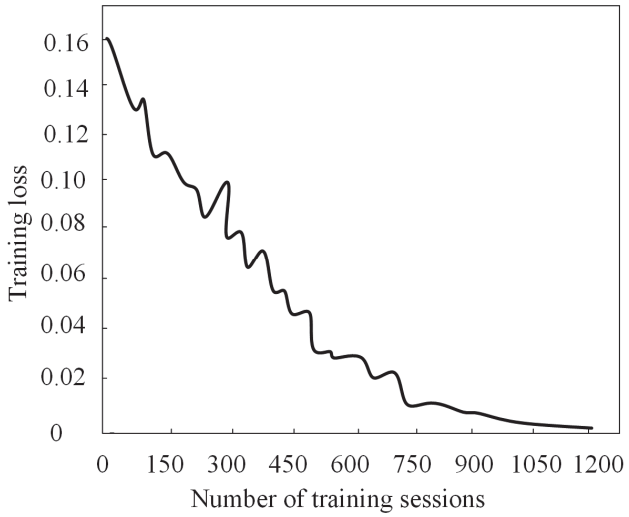

Figure 3 Training loss result

The method in this study is used to extract the features of five types of illegal intrusion data of the IoT. The dimension reduction effect of the method in this work is analyzed by comparing the dimensions of the original data and the extracted characteristic data, as shown in Fig. 4. The aforementioned figure indicates that the original data dimensions of five types of IoT illegal intrusion are all over 70. The method in this study is used to extract the features of five types of IoT illegal intrusion data and reduce the feature dimension of each type of IoT illegal intrusion data to less than 30. The finding demonstrates that the method in this study can reduce the dimension of the original data through feature extraction, obtain the high sparse low-dimensional illegal intrusion feature vector of the IoT, and use it for the classification of IoT illegal intrusion detection to improve the accuracy and efficiency of the IoT illegal intrusion detection.

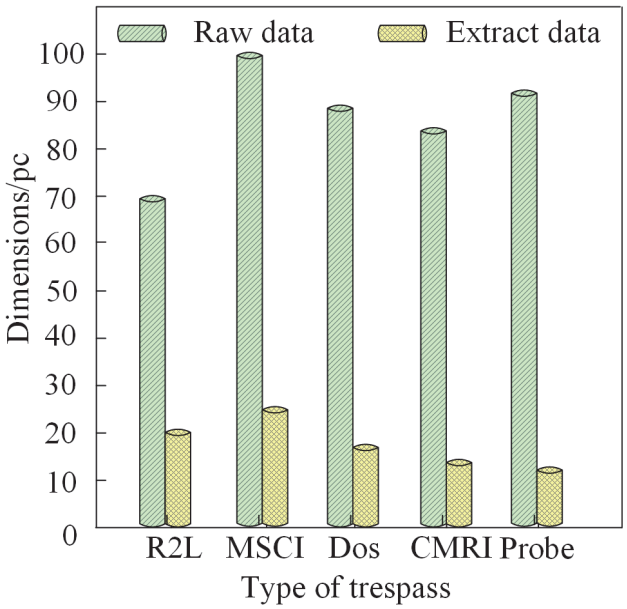

Figure 4 Feature extraction result

The recall rate, precision, and F1 value are selected as the evaluation indexes of the illegal intrusion detection effect of the method in this work. The intrusion detection effect of this method is evaluated, as shown in Tab. 2. The aforementioned table indicates that the results of the various IoT illegal intrusion detection indicators of the method in this work are relatively good. The recall rate is 98.3%, the precision is 98.7%, and the F1 value is 98.6%, verifying that the detection effect of the method in this work is good, and that it can accurately detect the illegal intrusion attack behavior of the IoT.

Table 2 Intrusion detection effect evaluation of the method in this work

Type	Recall rate	Precision	F1 value
Illegal access to remote machine (R2L)	0.982	0.993	0.991
Malicious Status Command Injection (MSCI)	0.962	0.971	0.965
Denial of Service Attach (Dos)	0.984	0.982	0.994
Complex Malicious Response Injection (CMRI)	0.991	0.995	0.986
Port Scanning and Detection Attach (Probe)	0.996	0.995	0.996

The method in this work is used to detect the abnormal situation of the IoT in Area A of the logistics and warehousing company 24 h/day. Statistically, 10 illegal invasion attacks on the IoT in Area A of the logistics and warehousing company in 24 h are detected by using the method in this study. The attack time is mainly between 8:00 and 18:00, among which denial of service attack (Dos) most frequently occurs, indicating that the method in this work has a good effect on the detection of illegal intrusion

of the IoT and can accurately detect illegal intrusion behaviors of the IoT, with strong applicability.

The packet loss of the IoT during the transmission of different numbers of data packets under the two scenarios with or without illegal intrusion is counted to test the transmission performance of the IoT network after the application of the method in this study. The results are shown in Tab. 3.

Table 3 Testing result of the IoT transmission performance after the application of the method in this work

Different scenarios	Sent data packets/unit	Received data packets/unit	Whether packet loss occurred	Number of packet loss/unit
With illegal intrusion	10698	10698	No	0
	453722	453722	No	0
	759326	759326	No	0
	1112365	1112360	Yes	5
	6223353	6223346	Yes	7
Without illegal intrusion	10668	10668	No	0
	56263	56263	No	0
	136640	136640	No	0
	620126	620126	No	0
	3656201	3656201	No	0

The aforementioned table indicates that the number of packets received and sent by network ports is the same in the case of no illegal intrusion after the application of the method in this work. Moreover, the data transmission effect of the IoT is good without packet loss. In the case of illegal intrusion, only when the number of sent packets exceeds one million levels, the IoT transmission will appear packet loss, and the number of packet loss is considerably small, indicating that the application of the method in this study can effectively reduce the influence of illegal intrusion on the transmission effect of the IoT. The application of the method in this study for the illegal intrusion detection of the IoT can ensure the safe transmission of the IoT data.

5 CONCLUSION

Nowadays, the increasing illegal intrusions of the IoT seriously threaten the interests of enterprises and individuals. The illegal intrusion behavior of the IoT is hidden and varied. The original illegal intrusion detection technology cannot meet the current demand for the illegal intrusion of the IoT. Accordingly, an illegal intrusion detection method based on deep mining algorithm is proposed to improve the current security defense capability of the IoT. The conclusions indicate that:

(1) The feature extraction of the illegal intrusion data of the IoT can effectively reduce the feature dimension of the illegal intrusion data of the IoT to less than 30 and the dimension of the original data.

(2) The recall rate, precision, and F1 value of the IoT intrusion detection are 98.3%, 98.7%, and 98.6%, respectively, which can accurately detect IoT intrusion attacks.

(3) This method can reduce the dimensionality of IoT data and extract optimal data features, with high detection accuracy, making it more suitable for detecting abnormal attacks in complex IoT networks.

Although the method proposed in this study has achieved good application results, there are still many issues worth further research. If the effectiveness of our method is tested through, a large number of experiments on different datasets and other deep mining methods are introduced to meet the real-time requirements of illegal intrusion detection in logistics networks.

Acknowledgements

This study is supported by the Hebei Provincial Education Department Foundation (No. ZC2021253, Z2020217), Hebei Development and Reform Commission Foundation (No. Z20210039) and Shijiazhuang Federation of Social Sciences Foundation (No. Z20210063).

6 REFERENCES

[1] Rane, S. B. & Thakker, S. V. (2020). Green procurement process model based on blockchain - IoT integrated architecture for a sustainable business. *Management of Environmental Quality: An International Journal*, *31*(3), 741-763. https://doi.org/10.1108/MEQ-06-2019-0136

[2] Balakrishnan, S. & Vinoth Kumar, K. (2023). Hybrid Sine-Cosine Black Widow Spider Optimization based Route Selection Protocol for Multihop Communication in IoT Assisted WSN. *Tehnicki vjesnik-Technical gazette*, *30*(4), 1159-1165. https://doi.org/10.17559/TV-20230201000306

[3] Acko, B., Weber, H., Hutzschenreuter, D., & Smith, I. (2020). Communication and validation of metrological smart data in IoT-networks. *Advances in Production Engineering & Management*, *15*(1), 107-117. https://doi.org/10.14743/apem2020.1.353

[4] Xing, S. (2022). Layout and Location of Water IoT Device Based on Few-Shot Reinforcement Learning. *Tehnicki vjesnik-Technical gazette*, *29*(4), 1184-1192. https://doi.org/10.17559/TV-20220225044110

[5] Wang, N., Li, X. J., & Nie, H. (2021). Digital Production Control of Manufacturing Workshop Based on Internet of Things. *International Journal of Simulation Modelling*, *20*(3), 606-617. https://doi.org/10.2507/IJSIMM20-3-CO15

[6] Hu, X. D. & Zhou, Q. (2020). IoT intelligent intrusion detection based on deep learning. *Computer Systems & Applications*, *29*(9), 47-56. https://doi.org/10.15888/j.cnki.csa.007620

[7] Lv, Z. L., Duan, L., Zhu, L. et al. (2022). Intrusion detection method of internet of things for smart home in edge-cloud collaborative environments. *Mobile Communications*, *46*(5), 106-112. https://doi.org/10.3969/j.issn.1006-1010.2022.05.017

[8] Li, B. B., Song, J. R., Du, Q. Y. et al. (2021). DRL-IDS: Deep reinforcement learning based intrusion detection system for industrial Internet of Things. *Computer Science*, *48*(7), 47-54. https://doi.org/10.11896/jsjkx.210400021

[9] Saheed, Y. K., Abiodun, A. I., Misra, S., Holone, M. K., & Colomo-Palacios, R. (2022). A machine learning-based intrusion detection for detecting internet of things network attacks. *Alexandria Engineering Journal*, *61*(12), 9395-9409. https://doi.org/10.1016/j.aej.2022.02.063

[10] Yao, H., Li, C., & Sun, P. (2020). Using parametric t-distributed stochastic neighbor embedding combined with hierarchical neural network for network intrusion detection. *International Journal of Network Security*, *22*(2), 265-274. https://doi.org/10.6633/IJNS.202003 22(2).10

[11] ElMenshawy, D., Helmy, W., & El-Tazi, N. (2019). A clustering based approach for contextual anomaly detection in internet of things. *Journal of Computer Sciences*, *15*(8), 1195-1202. https://doi.org/10.3844/jcssp.2019.1195.1202

[12] Dong, R. H., Yan, H. H., & Zhang, Q. Y. (2020). An intrusion detection model for wireless sensor network based on information gain ratio and bagging algorithm. *International Journal of Network Security*, *22*(2), 218-230. https://doi.org/10.6633/IJNS.202003 22(2).05

[13] Zhang, J. (2019). Detection of network protection security vulnerability intrusion based on data mining. *International Journal of Network Security*, *21*(6), 979-984. https://doi.org/10.6633/IJNS.201911 21(6).11

[14] Khan, M. A., Khan Khattk, M. A., Latif, S., Shah, A. A., Ur Rehman, M., Boulila, W., Driss, M., & Ahmad, J. (2022). Voting classifier-based intrusion detection for iot networks. *Advances on Smart and Soft Computing: Proceedings of ICACIn 2021*, 313-328. https://doi.org/10.48550/arXiv.2104.10015

[15] Tian, Q., Han, D., Hsieh, M. Y., Li, K. C., & Castiglione, A. (2021). A two-stage intrusion detection approach for software-defined IoT networks. *Soft Computing*, *25*, 10935-10951. https://doi.org/10.1007/s00500-021-05809-y

[16] Roy, S., Li, J., Choi, B. J., & Bai, Y. (2022). A lightweight supervised intrusion detection mechanism for IoT networks. *Future Generation Computer Systems*, *127*, 276-285. https://doi.org/10.1016/j.future.2021.09.027

[17] Mudgerikar, A., Sharma, P., & Bertino, E. (2020). Edge-based intrusion detection for IoT devices. *ACM Transactions on Management Information Systems*, *11*(4), 1-21. https://doi.org/10.1145/3382159

[18] Yao, R., Fei, Y., Ding, Y., Wang, H. L., & Tian, L. (2022). Research on engineering data information prediction model based on intelligent data mining algorithm. *Electronic Design Engineering*, *30*(7), 63-67. https://doi.org/10.14022/j.issn1674-6236.2022.07.013

[19] Nimbalkar, P. & Kshirsagar, D. (2021). Feature selection for intrusion detection system in Internet-of-Things (IoT). *ICT Express*, *7*(2), 177-181. https://doi.org/10.1016/j.icte.2021.04.012

[20] Shi, Y. & Shen, H. (2020). Anomaly detection for network flow using immune network and density peak. *InternationalJournalof Network Security*, *22*(2), 337-346. https://doi.org/10.6633/IJNS.20200322(2).18

[21] Qiu, M., Dai, W., & Vasilakos, A. V. (2016). Loop parallelism maximization for multimedia data processing in mobile vehicular clouds. *IEEE Transactions on Cloud Computing*, *7*(1), 250-258. https://doi.org/10.1109/TCC.2016.2607708

[22] Bakhshi, T. & Ghita, B. (2021). Anomaly Detection in Encrypted Internet Traffic Using Hybrid Deep Learning. *Security and Communication Networks*, *2021*, 5363750. https://doi.org/10.1155/2021/5363750

[23] Mohamed, M. R., Nasr, A. A., Tarrad, I. F., & Abdulmageed, M. Z. (2019). Exploiting incremental classifiers for the training of an adaptive intrusion detection model. *International Journal of Network Security*, *21*(2), 275-289. https://doi.org/10.6633/IJNS.201903 21(2).12

[24] Aveleira-Mata, J., Luis Munoz-Castaneda, A., Teresa Garcia-Ordas, M., Benavides-Cuellar, C., Alberto Benitez-Andrades, J., & Alaiz-Moreton, H. (2021). IDS prototype for intrusion detection with machine learning models in IoT systems of the Industry 4.0. *Dyna*, *96*(3), 270-275. https://doi.org/10.6036/10011

Contact information:

Xingjuan FAN, Master, Associate Professor
Department of Intelligent Engineering,
Shijiazhuang Posts and Telecommunications Technical College,
No. 318 Tiyu South Street, Hebei, Shijiazhuang, China
E-mail: Fanxingjuan1977@163.com

Hui LI, Master, Lecturer
(Corresponding author)
Department of Intelligent Engineering,
Shijiazhuang Posts and Telecommunications Technical College,
No. 318 Tiyu South Street, Hebei, Shijiazhuang, China
E-mail: Lihui_197907@163.com

Xinglong LIU, Master, Lecturer
School of Information Science and Technology,
Hebei Agricultural University,
Hebei, Baoding, China
E-mail: liuxinglong1976@163.com

Fangtong GUO, Master, Lecturer
Founder Software Vocational and Technical College,
Peking University,
Beijing, China
E-mail: guofangtong@pfc.cn

Hongjing MA, PhD, Lecturer
Department of Intelligent Engineering,
Shijiazhuang Posts and Telecommunications Technical College,
No. 318 Tiyu South Street, Hebei, Shijiazhuang, China
E-mail: ww2008_ww@163.com