Abnormal Traffic Detection Scheme Based on RBF Fuzzy Neural Network and Attention Mechanism in Robot Environment

Jintao Liu, Zhenxing Hao, Jiyue Wang, and Xi Zhang
(Corresponding author: Jintao Liu)

College of Mechanical Engineering, Zhengzhou University of Science & Technology
Zhengzhou Henan 450064, China
Email: aqiufenga@163.com

(Received July 19, 2023; Revised and Accepted Oct. 1, 2023; First Online Oct. 10, 2023)
The Special Issue on Data Fusion, Deep Learning and Optimization Algorithms for Data Privacy Protection
Special Editor: Prof. Shoulin Yin (Harbin Institute of Technology)

Abstract

The rapid increase in terminal devices in the robot environment has brought many security risks. Detecting abnormal traffic efficiently has become an essential task in robot safety research. The existing detection methods have the problem of high computational cost. They cannot explicitly capture the relationship and structure of traffic data, so it is difficult to deal with new network attacks. This paper proposes a novel abnormal traffic detection scheme based on an RBF fuzzy neural network in a robot environment. Fuzzy rules are used to simulate the relationship between factors. The incremental fuzzy neural network training method and batch fuzzy neural network training method are combined to train the network. The risk level derived from the fuzzy rules is de-blurred to get the risk index of the information system. On this basis, the attention module is introduced to enhance the extraction of key features, enhance the interpretability of the model, and further improve the detection accuracy. Experimental results on the open data set CTU-13 show that the proposed method can detect traffic effectively and save more time than other advanced methods.

Keywords: Abnormal Traffic Detection; Attention Module; RBF Fuzzy Neural Network; Robot Environment

1 Introduction

With the development of the robot ecosystem, a large number of intelligent terminal devices are widely used in a number of IoT application fields, such as smart home [17, 18], smart healthcare, smart transportation 4.0 and so on. However, the sharp increase in the number of robot terminal equipment has brought many serious security risks, and the complex network environment makes the data generated by robot equipment easy to be leaked, attacked or interrupted [11, 29, 39]. On the one hand, the robot terminal equipment is often limited by computing, memory, bandwidth and other resources, and its own limitations bring higher security challenges to the robot. On the other hand, there is a close correlation between robot devices. Once a device is invaded, it may lead to user privacy data disclosure, network infrastructure failure, network congestion or paralysis, etc., and even cause huge economic and social losses, seriously threatening enterprise and national security [40, 41].

In the past few years, the rise and development of machine learning and deep learning have promoted the research in the field of Internet of Things security [19, 20, 28], and various types of neural networks (such as convolutional neural networks [6], long short-term memory networks [37], and auto-encoders [31]) have been extensively applied in the intrusion detection of Internet of Things. Reference [2] proposed a hierarchical intrusion detection system based on three different classifiers (decision tree, JRP algorithm, random forest). The first two classifiers run in parallel and feed the results to the third classifier, achieving good results in the IDS2017 data set, but the system model was relatively simple and the accuracy and false positive rate are not ideal. In order to solve the problem of unbalanced samples, a CNN-FDC method based on convolutional neural network was proposed in reference [30]. After converting KDD-CUP99 data set into gray image, the original loss function was replaced with focal length loss, which weakened the influence caused by fewer attack samples. However, this model often had low accuracy in the face of high-dimensional data. Reference [10] proposed a hybrid deep learning model CNN-LSTM, which used long short-term memory network to learn the time features of high-dimensional traffic data. Compared with other advanced intrusion detection algorithms [13, 14], although the accuracy of the model was 99.03%, the main disadvantage was that the method based on back-propagation random gradient was used to update the weight, which required a long time for training and updating, could not meet the low time ductility requirements of the Internet of Things system, and the operation cost was large. In reference [35], Transformer, a popular method in the field of natural language processing, was introduced to improve the model combined with the traffic data set, which improved the detection accuracy and reduced the delay. However, the trained sample was a statistic-based attack sample, and the detection effect was poor when it encountered propagating attacks, which could not meet the high dynamic requirements of the Internet of Things system [8, 9, 21, 24, 25].

Machine learning and deep learning methods are mostly applied to Euclidian Spaces with fixed neighbor nodes, but in real IoT scenarios, a large number of edge devices and sensors are connected together in a complex, non-linear manner, thus forming a non-Euclidian space with non-fixed neighboring nodes [15, 27, 38]. However, most of the traditional methods are shallow learning methods, which only analyze the anomalies of the traffic data of a single node from a statistical point of view, and do not explicitly learn the existing relationships or structures between variables [12, 32]. Therefore, the performance of conventional deep learning methods in processing non-European spatial data is still difficult to be satisfactory. Some cunning intruders will launch attacks with low-intensity and highly targeted abnormal traffic, in which the packets are very similar to legitimate traffic and do not cause significant changes at the level of statistical analysis [34], and such new attacks are often difficult to detect by traditional methods.

Based on neural network, this paper proposes a distributed abnormal traffic detection scheme for robot environment. RBF neural network is used to remove the message passing module in the network. The distributed traffic anomaly detection architecture will perform anomaly detection at the active node of each robot. The attention mechanism is introduced to calculate the attention of each adjacent node, and the detection accuracy of the model is further improved by optimizing the weight selection process of each fully connected layer.

2 Abnormal Network Traffic Detection Model

This paper considers deploying an AI distributed detection module on the side of the fog node or on the SDN edge transponder to replace the detection methods running on the virtual server or the cloud. These detection modules are implemented by a low-power AI processor on the edge transponder. Each distributed unit focuses on a subset of the data transmission business, including the detection of module information and abnormal status of neighboring nodes, and ultimately the localization of abnormal traffic detection.

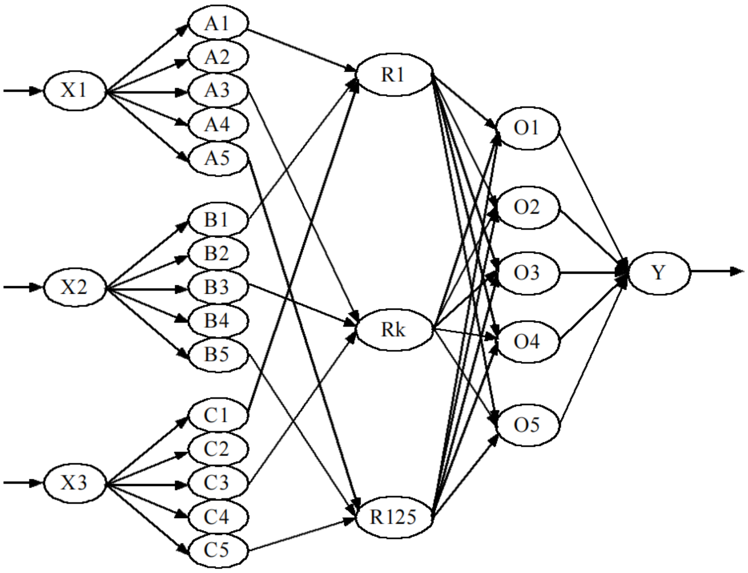

Figure 1: RBF fuzzy neural network structure

According to the basic principle of information security risk assessment and the characteristics of RBF fuzzy neural network [4, 23], the information structure diagram shown in Figure 1 is constructed, which is composed of five layers, namely, input layer, membership function layer, regularization layer, result layer and defuzzifying output layer.

First layer. Input layer, whose input is consistent with output. The three inputs are the factors that affect the information security risk level including the probability of threat occurrence, the value of assets, and the severity of vulnerability.

$$In_1(i) = out_1(i) = X = [x_1, x_2, x_3]. \tag{1}$$

Second layer. The blurring layer, for each input factor, is divided into 5 levels. For example, factor 1 is divided into $A_j (j \in [1, 5])$, which respectively represents high, high, medium, low and very low, and the other two factors are similarly divided into B_j and $C_j (j \in [1, 5])$. These factors belong to different levels according to different membership degrees. Here, the membership function adopts Gaussian radial basis function. c_{ij} and b_{ij} by are the center and base width of the membership function of the $j-th$ fuzzy set of the $i-th$ input variable, respectively.

$$out_2(i, j) = e^{\frac{(out_1(i)-c_{ij})^2}{(b_{ij})^2}}. \tag{2}$$

Third layer. In the rule layer, each node in layer 3 is only connected to a single level node of each factor in layer 2, then the number of nodes in layer 3 is 125, which is expressed as $R_i, i \in [1, 125]$. That is, each rule is determined by three factors, and the input is the result of the multiplication of the three.

$$Out_3(k) = out_2(1, j_1) \times out_2(2, j_2) \times out_2(3, j_3). \tag{3}$$

Fourth layer is the result layer. The nodes are represented by $O_i, i \in [1, 125]$. All rules produce different results with different combinations of weights. Each node of this layer is connected to the third layer. w_{kj} is the weight from the $k-th$ node of the third layer to the $j-th$ node of the fourth layer. The transfer function uses the $logsig()$ function to compress the output value between 0 and 1.

$$in_4(j) = \sum_{k=1}^{125} in_3(k) w_{kj}. \tag{4}$$

$$out_4(j) = logsig(in_4(j)). \tag{5}$$

The fifth layer is the deblurring layer. This layer has only one node, which is represented by Y. The 5 level values are combined according to certain weights to produce the final output result. w_j represents the weight of the fifth node of the fourth layer to the output layer, and the output function uses $logsig()$ function that compresses the output value between 0 and 1.

$$in_5 = \sum_{j=1}^{5} w_j^*(j). \tag{6}$$

$$out_5 = logsig(in_5). \tag{7}$$

As shown in Figure 2, this paper presents two independent models for updating the attributes of nodes and their corresponding edges. Based on this, a distributed detection unit deployed on the edge transponder is constructed. The core module of the architecture consists of edge RBF and node RBF, which are used to classify the state of nodes and edges respectively, and update the attributes of nodes and their corresponding edges. Edge detection units are used to classify features and predict the probability of anomalies on adjacent nodes, while node detection units are used to update features of nodes and calculate the probability of causing their own abnormal state.

Different from the conventional RBF neural network model, a communication channel is implemented in this paper, and the information exchange neighborhood is established in the channel, which is used to combine the information of edge RBF and node RBF. The inputs to the model represent three properties of the edge feature and five properties of the node feature, and each neuron is connected by a one-way link. In detail, the input and output are defined: suppose there is a node j and its adjacent nodes $i = 1, 2, \cdots, N$. The input of the edge is composed of the edge feature vector corresponding to the neighbor, the information of the node itself and the edge feature vector corresponding to the neighbor. Update the edge feature vector through the output of the fully connected layer. At the same time, the node RBF module also updates the node's own feature representation according to the collected information, and then concatenates the updated edge feature vector with the features of the $i-th$ node as the input of Softmax classifier [16,42], and finally gets the anomaly probability of node j through classification. Compared with other centralized intrusion detection systems, this way of information exchange does not require explicit message passing and effectively reduces the resource occupation.

In the forward propagation of RBF, node information that plays an important role should be paid attention to, while node information that plays a secondary role should be ignored. In order to further improve the detection accuracy, this paper adds the attention mechanism module before the last layer classification. When each node updates the output of the hidden layer, different weights are assigned to each adjacent node by calculating the attention of adjacent nodes, and nodes with higher weights are taken as the focus of the neural network. The introduction of the attention mechanism reduces the computational burden of processing high-dimensional data, and makes the detection system more focused on finding significant relevant and useful information in the data, thus improving the output quality.

3 Experimental Results and Analysis

3.1 Experimental Environment

In order to evaluate the detection performance of the scheme in this paper, Python, NumPy, Pandas, Pytorch and other tools are used. Simulation experiments were performed on a 64-bit computer using Intel i9-9700K 16GB RAM, Nvidia GeForce RTX2080Ti 32GB and version 10.2 of CUDA.

3.2 Experimental Data

The data set used in this paper is CTU-13 [5,33], which is a botnet traffic dataset captured at CTU University in 2011. The dataset contains 13 different attacks, with each packet containing information about various clients and servers. The network consists of 30 transponders and 170 iot devices that exchange data based on distributed devices in the CTU.

3.3 Evaluation Index

The performance index of abnormal traffic detection depends on the confusion matrix. In the confusion matrix, the true class (TP) is the correctly classified abnormal traffic instances; False positive class (FP) is a misclassified normal traffic instance; True and inverse class (TN)

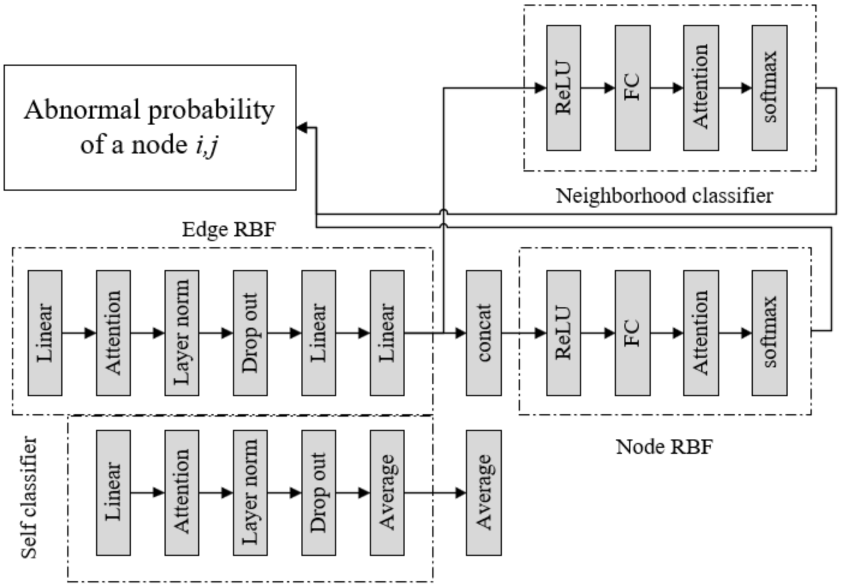

Figure 2: Structure of traffic anomaly detection

is a correctly classified normal traffic instance; False anti-class (FN) is an abnormal traffic instance that is misclassified. These 4 items are used to generate the following performance evaluation indicators [7].

Accuracy, that is, the ratio of the number of samples correctly classified by the model to the total number of samples, is calculated as follows:

$$Accuracy = \frac{TP+TN}{TP+FN+FP+TN}. \tag{8}$$

Precision, that is, the ratio of the number of normal samples correctly classified by the model to the total number of normal samples, is calculated as follows:

$$Precision = \frac{TP}{TP+FP}. \tag{9}$$

Recall, that is, the ratio of the number of intrusion samples correctly classified by the model to the total number of correctly classified samples, is calculated as follows:

$$Recall = \frac{TP}{TP+FN}. \tag{10}$$

False Positive Rate (FPR) is the ratio of the number of normal samples wrongly reported as intrusions to the total number of normal samples. The formula is as follows:

$$FPR = \frac{FP}{FP+TN}. \tag{11}$$

3.4 Analysis of Experimental Results

In order to prove the advantages of the proposed scheme, classical machine learning algorithms and deep learning methods were used for experimental comparison on dataset CTU-13, including three machine learning methods and three deep learning methods. The Adam optimizer is used to train the model, uniformly setting the batch size to 1024, the learning rate to 0.0001, the batch to 30, and the dropout to 0.5. Pytorch is used to build a detection model, and the performance indicators of the experiment are shown in Table 1. The results show that the accuracy rate, accuracy rate, recall rate and false positive rate in the CTU-13 dataset are up to 0.9995, 0.9831, 0.9964 and 0.0041. This is due to the fact that the improved RBF neural network model in this paper can better learn complex features in large data sets, because the larger the data set, the more complex the communication mode, the more IP nodes and interaction edges. Compared with other methods, the improved model in this paper can more easily play an advantage and detect abnormal traffic more accurately. In addition, the introduction of attention mechanism also further improves the detection effect, making the detection performance of the proposed scheme better than other schemes.

Table 1: Detection comparison with different schemes/%

Scheme	Accuracy	Precision	Recall	FPR
Decision tree [1]	0.7884	0.7492	0.7789	0.1845
Naive Bayes [3]	0.8089	0.8175	0.8764	0.1553
SVM	0.8575	0.9028	0.9226	0.0774
PCA-SSH [36]	0.9587	0.9044	0.9360	0.0293
BGA [22]	0.9194	0.9217	0.9517	0.0171
DAE-GAN [26]	0.9726	0.9815	0.9705	0.0097
Proposed	0.9995	0.9831	0.9964	0.0041

Table 2: Computational complexity comparison of different schemes

Method	Number of trainable parameters/10^3	Training time/s	Testing time/s
PCA-SSH	18.7	168.4	10.41
BGA	23.3	172.6	12.51
C	43.7	266.2	18.61
DAE-GAN	6.4	98.4	9.27

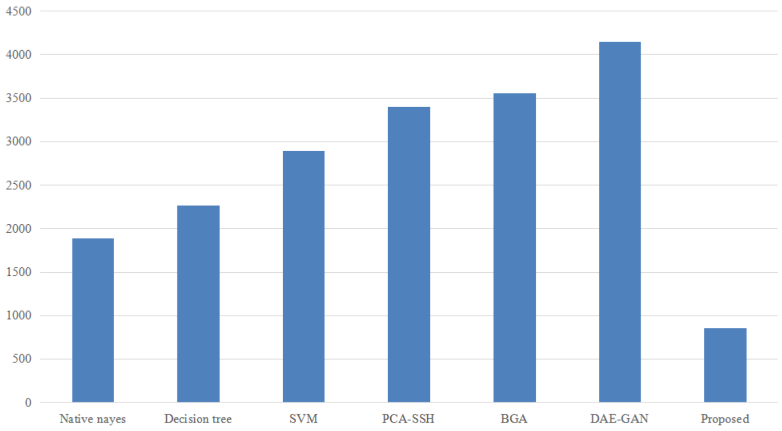

Figure 3: Bandwidth comparison of different schemes

To validate the advantages of deploying distributed detection units over centralized IDS, the paper also compares the performance of different schemes in terms of resource consumption and time overhead. The bar chart shows the resource consumption between different schemes, as shown in Figure 3. According to the data, it is not difficult to see that the minimum bandwidth consumption of the proposed scheme is only 856kb/s. Compared with other mainstream methods, the resource consumption is significantly reduced, because distributed anomaly detection does not need to transmit data to the IDS of the cloud server for calculation, and each detection unit reduces the resource consumption of centralized IDS with less bandwidth occupation.

Table 2 shows the number of training parameters and running time of the proposed scheme and other comparison schemes, using GPU to speed up the training of all models. It can be seen that by improving the message passing module of traditional RBF, the scheme in this paper has achieved a good improvement in time overhead, and the training time and training speed have been reduced. At the same time, there are few trainable parameters in the algorithm, which can realize efficient parallel computation.

4 Conclusions

In this paper, a distributed abnormal traffic detection scheme is proposed based on the complex characteristics of device nodes in robot environment and the requirement of low delay and high precision detection. The RBF convolutional neural network is optimized to replace the existing messaging module with an improved multi-layer perceptron to learn, making the model more suitable for iot environment. On this basis, combined with numerous characteristics of robot nodes, node RBF and edge RBF are designed to implement distributed traffic anomaly detection, realize localized abnormal traffic detection, and introduce attention mechanism to further improve the detection effect of the model. The experimental results show that the proposed scheme not only improves the detection accuracy effectively, but also reduces the overhead of network communication and speeds up the detection speed. The next step will be to perform graph structure analysis on more types of traffic datasets to train and test the model in a wider range of scenarios.

Acknowledgments

This work was supported by the Applied Research Program from Henan Provincial Department of Education, project No.23B460011. Key scientific research project plan of colleges and universities in Henan Province, project No.23B480003. Key scientific research project of Higher Education Department of Henan Province "Research on Obstacle Avoidance Detection and Safety Control of Industrial Robots" project No. 21B460017 and research on Vibration Analysis and Control of Chemical Fiber High-speed Winding Head Based on Particle Damping Project No. 182102210553. The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] A. Aboah, M. Shoman, V. Mandal, S. Davami, Y. Adu-Gyamfi and A. Sharma, ”A Vision-based System for Traffic Anomaly Detection using Deep Learning and Decision Trees,” in *2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Nashville, TN, USA*, pp. 4202-4207, 2021.

[2] A. Ahmim, L. Maglaras, M. A. Ferrag, M. Derdour and H. Janicke, ”A Novel Hierarchical Intrusion Detection System Based on Decision Tree and Rules-Based Models,” in *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini, Greece*, pp. 228-233, 2019.

[3] A. Alsaleh and W. Binsaeedan, ”The Influence of Salp Swarm Algorithm-Based Feature Selection on Network Anomaly Intrusion Detection,” *IEEE Access*, vol. 9, pp. 112466-112477, 2021.

[4] C. Ai, L. Jia, M. Hong and C. Zhang, ”Short-Term Road Speed Forecasting Based on Hybrid RBF Neural Network With the Aid of Fuzzy System-Based Techniques in Urban Traffic Flow,” *IEEE Access*, vol. 8, pp. 69461-69470, 2020.

[5] A. Bansal, S. Mahapatra, ”A comparative analysis of machine learning techniques for botnet detection,” *Proceedings of the 10th international conference on security of information and networks*, pp. 91-98, 2017.

[6] L. Chen, J. Cao, K. Wu, Z. Zhang, ”Application of generalized frequency response functions and improved convolutional neural network to fault diagnosis of heavy-duty industrial robot,” *Robotics and Computer-Integrated Manufacturing*, vol. 73, pp. 102228, 2022.

[7] S. Chowdhury, M. Khanzadeh, R. Akula, F. Zhang, S. Zhang, H. Medal, M. Marufuzzaman, L. Bian, ”Botnet detection using graph-based feature clustering,” *Journal of Big Data*, vol. 4, pp. 1-23, 2017.

[8] T. H. Feng, W. T. Li, M. S. Hwang, “False data report filtering scheme in wireless sensor networks: A survey”, *International Journal of Network Security*, vol. 17, no. 3, pp. 229-236, 2015.

[9] T. H. Feng, N. Y. Shih, M. S. Hwang, “A safety review on fuzzy-based relay selection in wireless sensor networks”, *International Journal of Network Security*, vol. 17, no. 6, pp. 712-721, 2015.

[10] L. Fu, Q. Tang, P. Gao, J. Xin, J. Zhou, ”Damage identification of long-span bridges using the hybrid of convolutional neural network and long short-term memory network,” *Algorithms*, 2021, 14(6): 180.

[11] M. Hajiabbasi, E. Akhtarkavan and B. Majidi, ”Cyber-Physical Customer Management for Internet of Robotic Things-Enabled Banking,” *IEEE Access*, vol. 11, pp. 34062-34079, 2023.

[12] W. P. Hu, C.-B. Lin, J.-T. Wu, C.-Y. Yang, and M. S. Hwang, ”Research on Privacy and Security of Federated Learning in Intelligent Plant Factory Systems,” *International Journal of Network Security*, vol. 25, no. 2, pp. 377-384, 2023.

[13] C. H. Ling, W. F. Hsien, M. S. Hwang, “A double circular chain intrusion detection for cloud computing based on adjointVM approach”, *International Journal of Network Security*, vol. 18, no. 2, pp. 397-400, 2016.

[14] L. C. Huang, M. S. Hwang, “Study of intrusion detection systems”, *Journal of Electronic Science and Technology*, vol. 10, no. 3, pp. 269-275, 2012.

[15] M. S. Hwang, C. C. Chang, K. F. Hwang, “Digital watermarking of images using neural networks”, *Journal of Electronic Imaging*, vol. 9, no. 4, pp. 548–555, Jan. 2000.

[16] Z. Jiang, Z. Wang and E. -H. Kim, ”Noise-Robust Fuzzy Classifier Designed With the Aid of Type-2 Fuzzy Clustering and Enhanced Learning,” *in IEEE Access*, vol. 11, pp. 8108-8118, 2023.

[17] C. H. Lee, M. S. Hwang, W. P. Yang, “A novel application of the phone card and its authentication in mobile communications”, *Journal of Information Science and Engineering*, vol. 15, no. 4, pp. 471-484, 1999.

[18] C. H. Lee, M. S. Hwang, W. P. Yang, “Phone card application and authentication in wireless communications”, in *The International Federation for Information Processing*, pp. 323-329, 1996,

[19] C. T. Li, M. S. Hwang, “A lightweight anonymous routing protocol without public key en/decryptions for wireless ad hoc networks”,*Information Sciences*, vol. 181, no. 23, pp. 5333-5347, 2011.

[20] C. T. Li, M. S. Hwang and Y. P. Chu, “An efficient sensor-to-sensor authenticated path-key establishment scheme for secure communications in wireless sensor networks”, *International Journal of Innovative Computing, Information and Control*, vol. 5, no. 8, pp. 2107-2124, Aug. 2009.

[21] C. T. Li, C. C. Yang, M. S. Hwang, “A secure routing protocol with node selfishness resistance in MANETs”, *International Journal of Mobile Communications*, vol. 10, no. 1, pp. 103-118, 2012.

[22] H. Li, H. Ge, H. Yang, J. Yan and Y. Sang, ”An Abnormal Traffic Detection Model Combined BiIndRNN With Global Attention,” *IEEE Access*, vol. 10, pp. 30899-30912, 2022.

[23] R. Li, Y. Yang and Q. Zhang, ”Neural Network Based Adaptive SMO Design for TCS Fuzzy Descriptor Systems,” *IEEE Transactions on Fuzzy Systems*, vol. 28, no. 10, pp. 2605-2618, 2020.

[24] W. T. Li, T. H. Feng, and M. S. Hwang, “Distributed detecting node replication attacks in wireless sensor networks: A survey,” *International Journal of Network Security*, vol. 16, no. 5, pp. 323–330, 2014.

[25] W. T. Li, C. H. Ling, M. S. Hwang, “Group rekeying in wireless sensor networks: A survey”, *International*

Journal of Network Security, vol. 16, no. 6, pp. 400-410, 2014.

[26] Z. Li, S. Chen, H. Dai, D. Xu, C. -K. Chu and B. Xiao, "Abnormal Traffic Detection: Traffic Feature Extraction and DAE-GAN With Efficient Data Augmentation," *IEEE Transactions on Reliability*, vol. 72, no. 2, pp. 498-510, 2023.

[27] I. C. Lin, H. H. Ou, M. S. Hwang, "A user authentication system using back-propagation network", *Neural Computing & Applications*, vol. 14, pp. 243-249, 2005.

[28] C. H. Ling, C. C. Lee, C. C. Yang, and M. S. Hwang, "A secure and efficient one-time password authentication scheme for WSN", *International Journal of Network Security*, vol. 19, no. 2, pp. 177-181, Mar. 2017.

[29] M. C. Lucas-Esta, B. Coll-Perales and J. Gozalvez, "Redundancy and Diversity in Wireless Networks to Support Mobile Industrial Applications in Industry 4.0," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 1, pp. 311-320, 2021.

[30] Y. Ma, Q. Yang, Y. Gao, "An internet of things intrusion detection method based on cnn-fdc," in *2021 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS). IEEE*, pp. 174-177, 2021.

[31] M Maimaitimin, K Watanabe, S Maeyama, "Stacked convolutional auto-encoders for surface recognition based on 3d point cloud data," *Artificial Life and Robotics*, vol. 22, pp. 259-264, 2017.

[32] A. Massing, M. G. Larson, A. Logg, "Efficient implementation of finite element methods on nonmatching and overlapping meshes in three dimensions," *SIAM Journal on Scientific Computing*, vol. 35, no. 1, pp. C23-C47, 2013.

[33] M. Putra, D. Hostiadi, T. Ahmad, "Botnet dataset with simultaneous attack activity," *Data in Brief*, vol. 45, pp. 108628, 2022.

[34] G. Stafford and L. L. Yu, "An Evaluation of the Effect of Spam on Twitter Trending Topics," in *2013 International Conference on Social Computing, Alexandria, VA, USA*, pp. 373-378, 2013.

[35] L. Tao, Z. Xie, D. Xu, K. Ma, Q. Qiu, S. Pan, B. Huang, "Geographic Named Entity Recognition by Employing Natural Language Processing and an Improved BERT Model," *ISPRS International Journal of Geo-Information*, vol. 11, no. 12, pp. 598, 2022.

[36] Z Wang, D Han, M Li, H Liu, M Cui, The abnormal traffic detection scheme based on PCA and SSH," *Connection Science*, vol. 34, no. 1, pp. 1201-1220, 2022.

[37] D. Wu, Y. Zhang, M. Ourak, K. Niu, J. Dankelman and E. V. Poorten, "Hysteresis Modeling of Robotic Catheters Based on Long Short-Term Memory Network for Improved Environment Reconstruction," *IEEE Robotics and Automation Letters*, vol. 6, no. 2, pp. 2106-2113, 2021.

[38] H. J. Wu, Y. H. Chang, M. S. Hwang, I. C. Lin, "Flexible RFID location system based on artificial neural networks for medical care facilities", *ACM SIGBED Review*, vol. 6, no. 2, pp. 1-8, 2009.

[39] Y. Wu, M. Li, G. Li and Y. Savaria, "Persistence Region Monitor With a Pheromone-Inspired Robot Swarm Sensor Network," *IEEE Internet of Things Journal*, vol. 9, no. 14, pp. 12093-12110, 2022.

[40] S. Yin, H. Li, A. A. Laghari, S. Karim, A. K. Jumani, "A Bagging Strategy-Based Kernel Extreme Learning Machine for Complex Network Intrusion Detection," *EAI Endorsed Transactions on Scalable Information Systems*, vol. 21, no. 33, e8, 2021.

[41] S. Yin, L. Wang, M. Shafiq, L. Teng, A. A. Laghari and M. F. Khan, "G2Grad-CAMRL: An Object Detection and Interpretation Model Based on Gradient-Weighted Class Activation Mapping and Reinforcement Learning in Remote Sensing Images," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 16, pp. 3583-3598, 2023.

[42] Q. Zhu and X. Zu, "A Softmax-Free Loss Function Based on Predefined Optimal-Distribution of Latent Features for Deep Learning Classifier," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 33, no. 3, pp. 1386-1397, 2023.

Biography

Jintao Liu biography. Jintao Liu is with College of Mechanical Engineering & Zhengzhou University of Science & Technology. Research interests are Mechanical design, robotics, data security analysis.

Zhenxing Hao biography. It is required by the Zhenxing Hao is with College of Mechanical Engineering & Zhengzhou University of Science & Technology. Research interests are Mechanical design, robotics, data security analysis.

Jiyue Wang biography. Jiyue Wang is with College of Mechanical Engineering & Zhengzhou University of Science & Technology. Research interests are Mechanical design, robotics, data security analysis.

Xi Zhang biography. Xi Zhang is with College of Mechanical Engineering & Zhengzhou University of Science & Technology. Research interests are Mechanical design, robotics, data security analysis.