Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 2448010, 11 pages
https://doi.org/10.1155/2022/2448010

Research Article

Intrusion Detection Model for Wireless Sensor Networks Based on MC-GRU

Zhou Jingjing,[1] **Yang Tongyu**,[1] **Zhang Jilin**,[2] **Zhang Guohao**,[1] **Li Xuefeng**,[1] **and Pan Xiang**[1]

[1]*School of Information and Electronic Engineering, Zhejiang Gongshang University, Hangzhou 310018, China*
[2]*School of Computer Science, Hangzhou Dianzi University, Hangzhou 310018, China*

Correspondence should be addressed to Zhou Jingjing; zhoujingjing@zjgsu.edu.cn

Received 15 June 2022; Accepted 18 August 2022; Published 5 September 2022

Academic Editor: Chenglu Jin

A crucial line of defense for the security of wireless sensor network (WSN) is intrusion detection. This research offers a new MC-GRU WSN intrusion detection model based on convolutional neural networks (CNN) and gated recurrent unit (GRU) to solve the issues of low detection accuracy and poor real-time detection in existing WSN intrusion detection algorithms. MC-GRU uses multiple convolutions to extract network data traffic features and uses the high-level features output after convolution operations as input parameters of the GRU network, which strengthens the learning of spatial and time series features of traffic data and improves the detection performance of the model. The experiment results based on the WSN-DS dataset show that the overall detection accuracy of the four types of attack of black hole, gray hole, flooding, and scheduling and normal behaviors reaches 99.57%, and it is also better than the existing WSN intrusion detection algorithms in real-time performance and classification ability.

1. Introduction

The use of WSN has grown in popularity across many industries, including aviation, industry, and the environment, as a result of the quick advancement of wireless communication and sensor technologies, breaking the limitations of traditional methods to monitor and collect data in harsh environments [1]. However, the security problem of WSN brings new threats. Intrusion attacks against WSN can cause great damage to the safety of individual or collective life and property. Accurate detection of various types of attacks in WSN can provide a reliable security guarantee for the network. As a result, the WSN intrusion detection method has emerged as a major area of study in the field of network security today.

A distributed wireless communication network made up of management, sink, and sensor nodes is known as a WSN. Because wireless signals are divergent and sensor nodes are also limited by their own computing power, storage capacity, and wireless communication capabilities, WSN is facing security threats such as data leakage and data forgery [2]. Existing research generally adopts a two-layer defense mechanism to ensure the security of WSN. The first layer of the defense mechanism includes data encryption, data authentication, and security protocols, but with the continuous breakthrough of network attack technology, the effect of the first layer of the defense mechanism gradually becomes less than ideal. As the second layer defense mechanism to protect WSN security, intrusion detection technology can effectively compensate for the deficiency of the first layer defense mechanism and reduce losses caused by network attacks [3].

Because WSN has low computing and communication capabilities, traditional network intrusion detection algorithms are not suitable for directly using in WSN. At present, most research on WSN intrusion detection uses traditional machine learning methods to analyze network traffic data. Due to the growth in both the network's size and its user

base, the WSN network will generate high-dimensional traffic data, and the traditional machine learning approach would encounter issues like poor feature extraction and detection accuracy, which cannot meet such an application environment [4].

Compared to machine learning methods for detecting intrusions, deep learning-based intrusion detection can reduce computational complexity and increase the ability to learn the characteristics of data traffic, which can improve the precision of the detection model [5].

The MC-GRU intrusion detection algorithm, based on CNN and GRU, is suggested in this paper. It takes into account the detection accuracy and feature selection of the intrusion detection model in considerable detail. MC-GRU extracts the basic characteristics of network data traffic through CNN, uses the advanced features output after the convolution operation as the input parameters of the GRU network for time series feature learning, and then uses the dropout mechanism to suppress the occurrence of overfitting of the detection model and improve the generalization ability of the WSN intrusion detection model, and finally, the softmax function is used for multiclassification. Compared to the existing WSN intrusion detection model, it can increase the detection accuracy, real-time detection, and various multiclassification capabilities of various types of WSN attack. The experimental results show that MC-GRU is superior to existing WSN intrusion detection algorithms in terms of detection accuracy, real-time performance, and classification ability and is an effective solution to the second-layer defense mechanism of WSN.

The following describes the organizational structure of this paper. Section 1 describes the background of WSN intrusion detection research and shows the MC-GRU implementation process. Section 2 summarizes related domestic and international research on WSN intrusion detection. Section 3 describes the structure and related principles of MC-GRU. The results of the MC-GRU experimental data are displayed and analyzed in the fourth section, and the fifth section summarizes this paper.

2. Related Work

In recent years, an abundance of papers have carried out research on multiclassification of traffic types in WSN intrusion detection. Paper [6] designs the corresponding intrusion detection algorithm based on the difference in node resources and uses the lightweight random forest algorithm for WSN intrusion detection in the cluster head node with relatively scarce resources. The deep random forest algorithm further detects attack behavior that cannot be detected by the cluster head node, improving the real-time detection and accuracy of the WSN intrusion detection model, but the multiclassification effect still needs to be improved. In paper [7], the data density and the feature distance are added to the fuzzy clustering algorithm, and the fuzzy membership obtained is used as the fuzzy factor of the fuzzy support vector machine, which improves the detection efficiency of the model and improves the multiclassification effect. Paper [8] combines the self-encoding network and support vector machine (SVM) to realize the detection of WSN intrusion, which is beneficial for the extraction of high-dimensional spatial information, but the precision of multiclassification needs to be improved. Paper [9] proposes an adaptive AP clustering algorithm based on the adaptive AP algorithm and the clustering algorithm, which reduces the consumption of sensor node storage space and improves clustering efficiency, but the detection accuracy needs to be improved. Paper [10] uses SVM kernel functions such as RBF, PLOY, and sigmoid for data classification, and the best detection effect is 91%, and still room for improvement with the performance. Paper [11] uses a deep neural network (DNN) with different layers to verify the detection performance on the WSN-DS dataset. Overall, multiclassification performance is better, but the false positive rate needs to be improved. For DNN traffic with layers 1 to 5, the average false positive rates for the types were 2.34%, 4.20%, 3.4%, 4.98%, and 2.7%, respectively. Paper [12] extracts the output of each level from the trained deep CNN and implements a linear SVM and a classifier with a nearest neighbor (1-NN), which improves the detection accuracy of attack types with a small sample size in the dataset. However, the detection rate of the model needs to be improved. The K-nearest neighbor node (KNN) classification algorithm used in the paper [13] uses the compressed proximity algorithm to reduce and cluster the original data to locate the sample's center of gravity, which can result in a higher detection rate and relatively less error. However, the detection effect of some multiclassification needs to be improved.

Other studies detect a certain type of attack or do not classify the attack types. Paper [14] uses the K-means algorithm based on enhanced particle swarm optimization to detect spoofing attacks according to the strength of the signal received from the physical layer. Paper [15] uses the mini batch K-means algorithm and SVM to achieve WSN intrusion detection and uses randomly generated small batch data samples for clustering, which improves the convergence speed of the model and greatly reduces the calculation time; it is suitable for WSN environment with large sample size, but the algorithm cannot detect specific attack types. In order to detect flooding attacks, the paper [16] proposes a KNN-based WSN intrusion detection system that compares each node's cutoff value and distance function to identify aberrant nodes. Paper [17] fakes a destination node in WSN to induce a black hole node attack, finds the black hole node through identity verification and location information of the attacking node, and removes it from WSN.

As mentioned above, WSN intrusion detection has seen significant advancements in research, but there are still certain issues, such as poor detection accuracy, low real-time detection performance, and poor multiclassification effect. Meanwhile, with the development of networks and big data, the data to be detected will be more complex, and the traditional WSN intrusion detection method cannot anymore meet the current network environment.

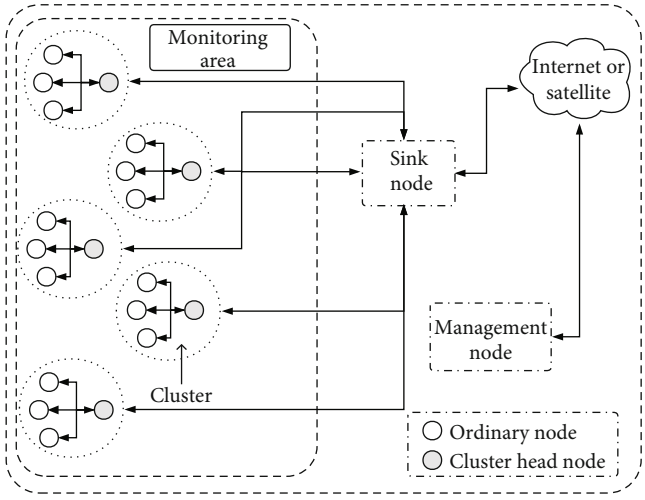

Figure 1: WSN structure [18].

3. WSN Intrusion Detection Model

3.1. Background of Problem

3.1.1. WSN Structure. The WSN MC-GRU intrusion detection model proposed in this paper is based on the layered structure in the topology of the WSN. As depicted in Figure 1, in the layered structure, the wireless sensor nodes are separated into ordinary sensor nodes, cluster head nodes, sink nodes, and management nodes [18], and the node performance improves in turn. The ordinary sensor nodes in the monitored area are responsible for completing the data monitoring and collection tasks issued by the management node and sending the collected data to the cluster head node. The data gathered by the ordinary sensor nodes in the cluster is first preprocessed by the cluster head node before being sent to the sink node. The WSN MC–GRU intrusion detection model in the sink node performs intrusion detection on the data from the cluster head node and then sends the detection results and data to the management node.

3.1.2. Type of Attack. The MC-GRU model suggested in this paper is primarily intended for the detection of the following four types of attacks.

(1) Black Hole Attack. The black hole node discards all data packets from the source node and blocks the communication service with the destination node. The specific description is shown in Figure 2 [17]. The essence of a black hole attack is a routing attack. The source node *S* needs to communicate with the destination node *D* through one or more nodes and will initiate a routing request. At this time, the black hole node will indicate that it is the most suitable relay node to the destination node, but in the data transmission process, it discards all data packets from the source node *S*, resulting in transmission holes.

(2) Gray Hole Attack. The gray hole node also discards the data packets from the source node, but not all of them, only discard a certain type of data packet or discards the data

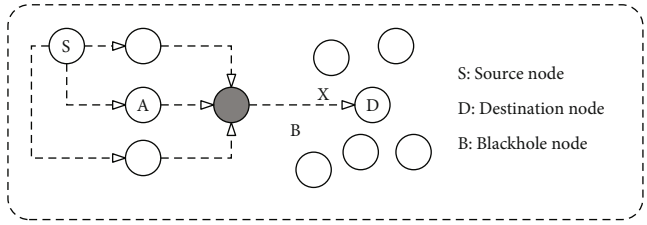

Figure 2: Black hole attack [17].

packets immediately and prevent the data packets from being forwarded to the base station.

(3) Flooding Attack. Flood nodes send or broadcast a high quantity of worthless routing request packets or data packets, consuming the limited resources of WSN nodes, occupying bandwidth meaninglessly, and making WSN communication unable to keep smooth. In addition, abnormal nodes in flood attack route request (RREQ) messages are sent more frequently than normal nodes [16].

(4) Scheduling Attack. A scheduling attack occurs in the initialization phase of the low energy adaptive clustering hierarchy (LEACH) protocol when WSN starts to randomly select the cluster head node; then, the scheduling node pretends to be the cluster head node, and the scheduling node gives all ordinary sensor nodes the same time stamp for sending data. Finally, data conflict between sensor nodes is lost [7].

3.2. MC-GRU Model. Assuming that the WSN dataset that needs anomaly detection is $P = \{x_1, x_2, \cdots, x_N\}$, the preprocessed eigenvalues of the i-th traffic data in the dataset are expressed as $x_i = \{x_i^1, x_i^2, \cdots, x_i^M\}$. The eigenvalue of each piece of traffic data obtains the corresponding probability value through the operation of the MC-GRU model, thus judging the type of the piece of traffic. Among them, M is the number of characteristics that each traffic data sample possesses, and N denotes the total number of traffic data samples that are included in the dataset.

The structure of the WSN MC-GRU intrusion detection model established in this paper is shown in Figure 3. The model contains multiple convolutional layers (MC) and a GRU layer. There are also a pooling layer and a batch normalization layer (BN) in between. The MC uses a convolutional neural network with three layers and multiple convolution kernels to extract features from the data to obtain the deep features of the data stream. The pooling layer compresses the data obtained from the convolutional layer through pooling calculation to improve the processing efficiency of the lower network and accelerate the model convergence. The BN improves the nonlinear expression ability of the network model. To further improve the feature learning ability and processing efficiency of the model, an improved GRU layer based on long short-term memory (LSTM) is added after the batch normalization layer to learn the context and time series features in the data. The dropout layer removes some neurons in a certain proportion to reduce the complex coadaptive relationship between

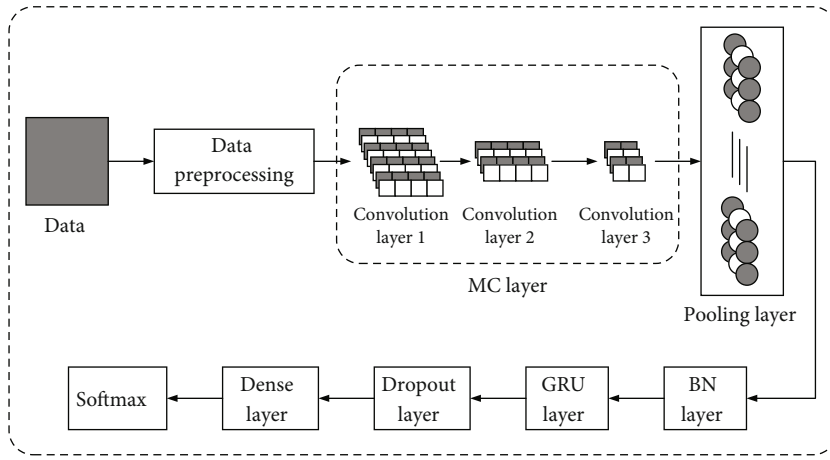

Figure 3: MC-GRU model structure.

neurons. Finally, the processed vector features are inputted into the dense layer for feature fusion, and the softmax logistic regression layer is used for final classification and output classification results.

3.2.1. Data Preprocessing. The nonnumerical properties of the dataset used in the experiment are numericalized and normalized to obtain an input format that can conform to the MC-GRU model.

3.2.2. MC Layer. With the development of wireless sensor networks, the detected traffic data will become large in sample size and complex in features. The sample data is used as the input of the CNN model, and each filter can be used to perform convolution operations on it. Performing feature extraction to obtain advanced features will greatly improve the feature extraction capability of the WSN intrusion detection model for complex traffic data. MC-GRU contains consecutive 3 layers of convolution. The number of convolution kernels is 128, 64, and 64. Iteratively extracts traffic features using multiple convolutional networks to obtain deeper and more complex features of the global data flow. All three-layer convolutional networks use the linear rectification function ReLU as the activation function. In the process of network-based intrusion detection, the sample data of WSN intrusion detection is not necessarily completely linear, and the output obtained by the signature function is a linear combination of the input. Therefore, the rectified linear unit ReLU activation function is selected instead of the sigmoid function. The rule activation function can also reduce the calculation of the model. It can improve training and detection efficiency [19], as shown in the expression:

$$\mathrm{ReLu}(x) = \max(x, 0). \tag{1}$$

The convolutional network's first layer's output is then as follows:

$$x_1 = \begin{cases} b_1 + w_1 * \mathrm{x} & b_1 + w_1 * x > 0, \\ 0 & b_1 + w_1 * x \le 0. \end{cases} \tag{2}$$

The output of the second- and third-layer convolutional networks is as follows:

$$x_m = \begin{cases} b_m + w_m * \mathrm{x}_{m-1} & b_m + w_m * x_{m-1} > 0, \\ 0 & b_m + w_m * x_{m-1} \le 0. \end{cases} \tag{3}$$

Among them, x in formula (2) is the eigenvalue of each piece of detected and preprocessed traffic data, which will be input into the MC-GRU model; b_1 and w_1 are the bias and weight matrices of the first-layer convolutional network; in formula (3), x_{m-1} is the output of the previous layer of the convolutional network; b_m and w_m are the bias and weight matrices of each layer of the convolutional network, $m = 2$, 3; "$*$" represents the convolution operation.

3.2.3. Pooling Layer. The pooling layer is used to extract the output features from the previous layer. It can reasonably reduce the dimension of the current detected data traffic feature vector, which can reduce the complexity of the entire WSN intrusion detection model and reduce the calculation after the pooling layer. The maximum value in the pooling filter is taken for the input feature vector, that is, the strongest feature part is retained. The calculation process is as follows:

$$\begin{cases} H_{\mathrm{out}} = \dfrac{h_{\mathrm{in}} - h_{\mathrm{filter}}}{T+1}, \\ W_{\mathrm{out}} = \dfrac{w_{\mathrm{in}} - w_{\mathrm{filter}}}{T+1}. \end{cases} \tag{4}$$

Among them, H_{out} and W_{out} are the height and width of the feature vector output after calculation by the pooling layer, T is the step size of the pooling filter scan, h_{in} and h_{filter} are the feature vector output from the previous layer and the height of the pooling filter, respectively, w_{in}, and w_{filter} are the feature vector output from the previous layer and the width of the pooling filter, respectively.

3.2.4. BN. When training the MC-GRU model, the parameters are updated, except that the data from the first input

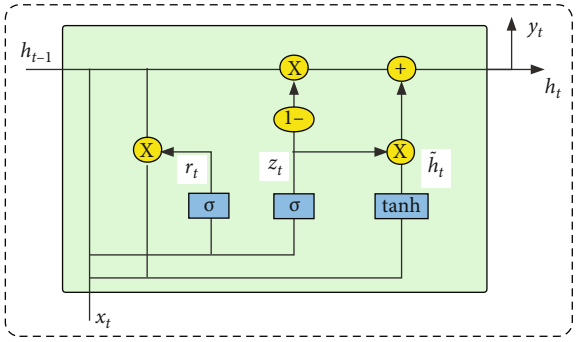

Figure 4: The structure of the GRU memory cell [21].

layer of the model are normalized, the input data distribution of each layer of the model will continue to change, and the network will learn new data distributions, which will reduce the convergence speed of the model. Therefore, batch normalization is added between the MC layer and the GRU layer to normalize the WSN detection model, so that the input samples are not correlated, and the data distribution of the output value of the MC layer and the input value of the GRU layer is closer to the data distribution of the original sample, which improves the convergence speed of the model and prevents the appearance of gradient explosion [20].

3.2.5. GRU Layer. Taking into account the computing power, detection accuracy, real-time requirements of wireless sensor nodes, and the further improvement of the classification ability of the WSN intrusion detection model for various attack categories, an improved GRU network based on LSTM is introduced to learn the contextual features of data flow and timing information [21]. There are only two gates in the GRU model: update gate z_t and reset gate r_t. The specific structure is shown in Figure 4.

The function of the reset gate is to forget the information h_{t-1} of the hidden layer unit at the previous moment:

$$r_t = \sigma(W_r \cdot [h_{t-1}, x_t], b_r). \tag{5}$$

After forgetting, h_{t-1} remaining information: $r_t \cdot h_{t-1}$.

The function of the update gate is to control the balance between the hidden layer state h_{t-1} at the previous moment and the current input information:

$$z_t = \sigma(W_z \cdot [h_{t-1}, x_t], b_z). \tag{6}$$

Enter information, here is the $r_t \cdot h_{t-1}$ after forgetting:

$$\tilde{h}_t = \tanh\left(W_{\tilde{h}_t} \cdot [r_t * h_{t-1}, x_t], b_h\right). \tag{7}$$

h_t after balance:

$$h_t = (1 - z_t) * h_{t-1} + z_t * \tilde{h}_t, \tag{8}$$

where σ is the sigmoid activation function, and tanh is the hyperbolic tangent function:

$$\text{sigmoid}(x) = \frac{1}{1 + e^{-x}}, \tag{9}$$

$$\text{Tanh}(x) = \frac{1 - e^{-2x}}{1 + e^{2x}}. \tag{10}$$

3.2.6. Dropout Layer. Remove some neurons according to a certain proportion to reduce the complex coadaptation relationship between neurons [19]. In a neural network model, if the model has too many parameters and too few training samples, the resulting model will overfit. Overfitting significantly affects how well the model performs, so using dropout in the WSN intrusion detection model can improve the overall performance of the model to some extent.

In the last layer of the proposed MC-GRU network model, softmax function is used as the classifier, and the type of traffic is judged according to the probability value obtained. The mathematical expression is expressed as follows:

$$\text{softmax}(x_i) = \frac{e^{x_i}}{\sum_{j=1}^{n} e^{x_j}}. \tag{11}$$

The configuration of the specific parameter of the MC-GRU model is shown in Figure 5.

3.2.7. Adam. The Adam optimizer proposed by Kingma and Lei Ba can iteratively update the weights of the network model based on training data. It is implemented simply and computed efficiently, it uses less memory, and the scaling change of the gradient has no impact on the updating of its parameters. It is appropriate for cases involving a lot of data and parameters, such WSN intrusion detection.

3.2.8. Categorical_Crossentropy. The difference between the probability distribution obtained by the present training and the genuine distribution is assessed using the cross-entropy loss function. Typically, it works in conjunction with the softmax function to achieve multiclassification.

3.3. WSN Intrusion Detection Framework. The WSN intrusion detection framework based on MC-GRU is shown in Figure 6. According to the resources of each node, the corresponding data operations are shared. This hierarchical structure can disperse the energy overhead, reduce the communication burden, and achieve energy savings. The WSN intrusion detection model based on MC-GRU can be divided into three steps:

Step 1. In the data collection stage, common sensors are distributed in the monitoring area to perceive the environment and collect data. Because common sensor resources are limited, common sensor nodes can only perform some simple processing of the collected data before sending them to the corresponding cluster head node.

Step 2. In the data preprocessing stage, the cluster head node has richer resources than ordinary sensor nodes and is used

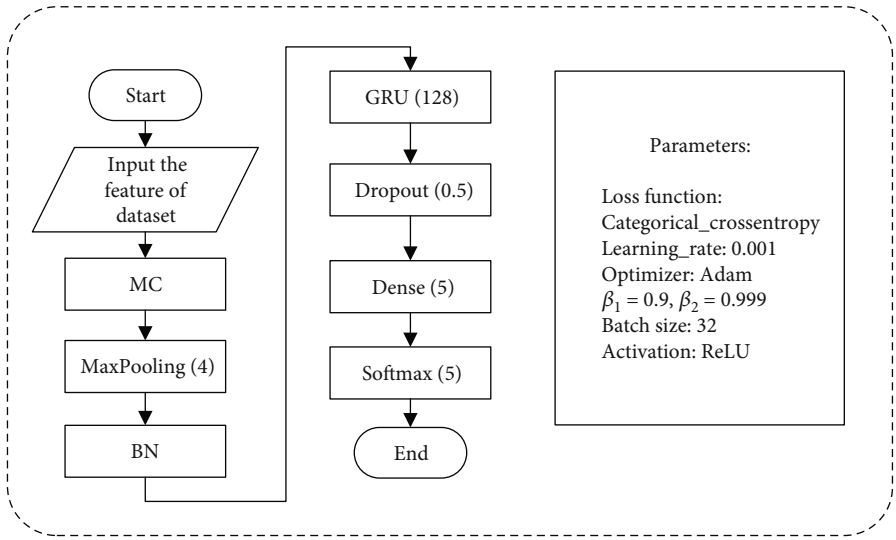

Figure 5: MC-GRU model flow chart and related configuration.

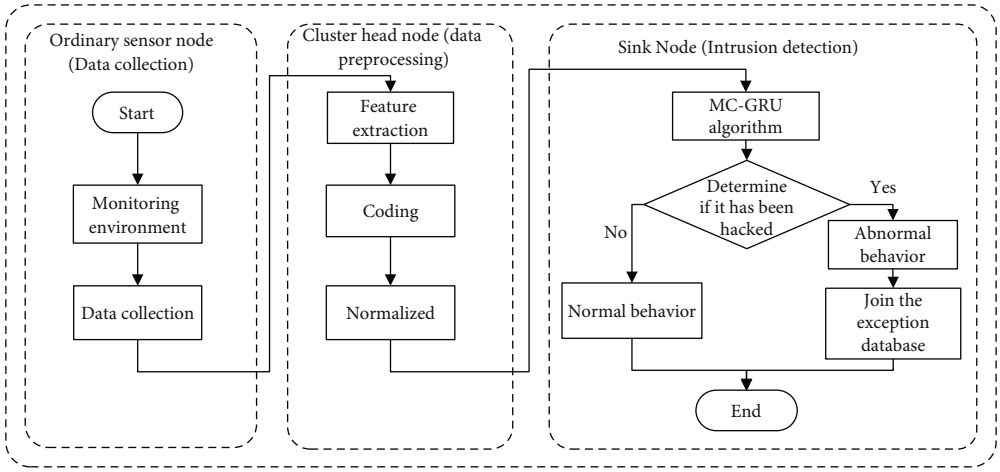

Figure 6: WSN intrusion detection process.

to perform data preprocessing operations such as feature extraction, character encoding, and data normalization on the data samples sent by common sensor nodes in the cluster and send the processed data to the sink node for intrusion detection.

Step 3. In the intrusion detection stage, deploy the trained MC-GRU model at the sink node. The sink node has more abundant resources and stronger computing power than ordinary sensor nodes and cluster head nodes and is suitable for processing cluster head nodes. The completed data are subjected to intrusion detection.

4. Experimental Results and Analysis

4.1. Experimental Data. The operating system used in this experiment is Windows 10, the processor is Intel(R) Core(TM) i5-8500 CPU@3.00GHz, the memory is 16 GB, python 3.7 is used to run through the whole scheme, numpy and pandas are used for data processing, and tensorflow is used. Build the model architecture with the keras framework and finally use matplotlib for visualization.

WSN-DS is an intrusion detection dataset for WSN constructed by Almomani et al. to describe normal behavior and four types of DoS attacks in WSN. The dataset is obtained by simulating the wireless sensor network environment using the NS-2 simulator. Each attribute in the dataset is based on the features analyzed by the LEACH hierarchical routing protocol. By tracking and analyzing the hierarchical routing protocol, it can well reflect the work of the current network environment condition. Each data record in this dataset consists of 18 inherent attributes and 1 class identifier [22]. In addition to normal behavior, the class identifier has 4 possible values: black hole, gray hole, flooding, and scheduling attacks, as shown in Table 1. The WSN-DS dataset has 374661 traffic data points in total. Take 80% and 20% of the WSN-DS dataset and divide it into training and test sets, with 20% of the

Table 1: WSN-DS dataset class distribution.

Type of attack	Number
Normal	340066
Black hole	10049
Flooding	3312
Gray hole	14596
Scheduling	6638

Table 2: Experimental division of WSN-DS dataset.

Type of attack	Training set (80%, of which 20% is a validation set)	Test set (20%)
Normal	272101	67965
Black hole	8006	2043
Flooding	2681	631
Gray hole	11611	2985
Scheduling	5329	1309
All	299728	74933

training set serving as the validation set. Table 2 displays how many of each type there are.

Since the eigenvalues of the WSN-DS wireless sensor dataset used in this paper are all numerical, the feature encoding process is omitted, and the data normalization operation is performed directly. Normalization of traffic data can eliminate the difference between data of different dimensions. To ensure the reliability of the training results, these characteristics are assigned to $[0, 1]$. In this article, the min-max normalize method [23] of the following formula is used to process the data, which only compresses the data and does not change the initial information of the data samples.

$$x^* = \frac{x - x_{\min}}{x_{\max} - x_{\min}}. \tag{12}$$

Among them, x is the sample value, the sample data's greatest value is $x_{\max}$, and its smallest value is $x_{\min}$.

4.2. Evaluation Indicators. The results of intrusion detection include the following four types: true positive (TP) indicates that it is actually normal behavior, the prediction is also the number of normal behavior, and false positive (FP) indicates that it is actually abnormal behavior and is predicted to be normal behavior. The number of true negatives (TN) is actually abnormal behavior, correctly predicted as abnormal behavior, and false negative (FN) represents the number of normal behaviors that are misidentified as abnormal behavior [24]. Details are shown in Table 3. According to the above four detection results, the accuracy rate, false positive rate, and recall rate are further evolved, which are used as evaluation indicators for intrusion detection technology in this paper.

(1) The accuracy rate indicates the ratio of the number of samples that correctly identify abnormal samples and normal samples to the total number of samples. The calculation formula is as follows:

Table 3: Confusion matrix.

Predicted	True	
	Positive	Negative
Positive	TP	FP
Negative	FN	TN

$$\text{Acc} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FN} + \text{FP} + \text{TN}}. \tag{13}$$

(2) The false positive rate (FPR) indicates that among the samples whose true values are abnormal, the probability of being predicted to be a normal sample is calculated as:

$$\text{FPR} = \frac{\text{FP}}{\text{TN} + \text{FP}}. \tag{14}$$

(3) The recall rate (true positive rate, TPR) indicates that the true value is in the normal sample, and the probability of being predicted to be a normal sample is calculated as:

$$\text{TPR} = \frac{\text{TP}}{\text{TP} + \text{FN}}. \tag{15}$$

4.3. Analysis of Results. In the deep learning model, the learning rate is a hyperparameter which controls the degree to which we adjust the network weights according to the loss gradient. To choose an optimal learning rate, this article first selects different learning rate values for comparison experiments, as shown in Figure 7, these reflect the detection accuracy of the MC-GRU model under different learning rates. According to Figure 7's analysis of the experimental findings, relatively speaking, when the learning rate is 0.001, the detection accuracy of the model is relatively high, reaching 0.9957. Therefore, in this article, the model's learning rate is set to 0.001.

Figure 8 depicts the correlation between the accuracy and the number of iterations, with training acc denoting the accuracy of the training set and validation acc denoting the accuracy of the validation set.

According to Figure 9, there is a correlation between the number of iterations and the loss value, where the training loss corresponds to the loss value of the training set and the validation loss to the loss value of the validation set.

Observing the curves of the two images in Figures 8 and 9, it is clear that the overall trend of the accuracy of the

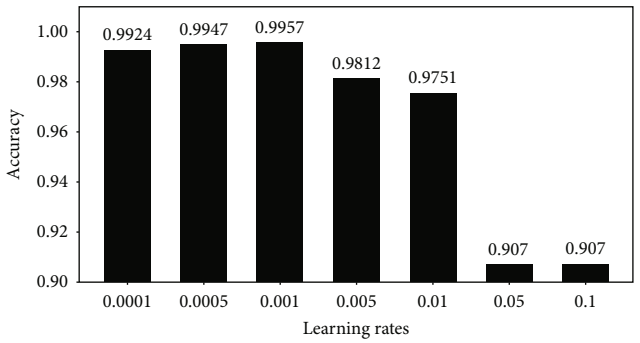

Figure 7: MC-GRU detection accuracy with different learning rates.

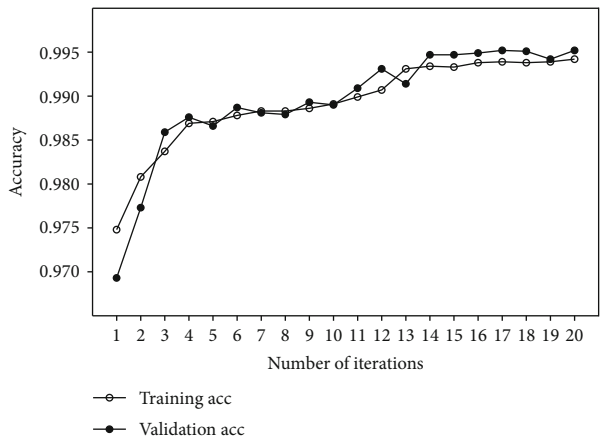

Figure 8: Accuracy curve.

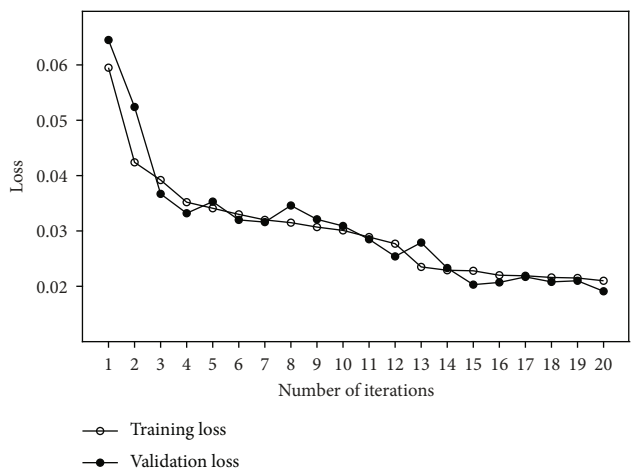

Figure 9: Loss curve.

training set and the validation set rises with each increment in the number of iterations. In cases when the epoch is more than 13, the accuracy of testing and verification tends to be stable, reaching a maximum of 0.9957, while the loss curve gradually decreases, and it can be concluded that the model has converged to the best state.

Table 4: Multiclassification results.

Performance	Normal	Black hole	Gray hole	Flooding	Scheduling
TPR	0.998	0.953	0.989	0.904	0.996
FPR	0.017	0.0014	0.0004	0.0009	0.00006
Acc	0.999	0.992	0.957	0.995	0.930

This article is mainly for the classification and identification of black hole, gray hole, flooding, scheduling attacks, and normal traffic data in the WSN-DS dataset, as shown in Table 4. Accuracy, false positive, and recall are for several types of data traffic. It is obvious from Table 4 that the detection accuracy of black hole, gray hole, flooding, scheduling, and normal types is all above 0.93; and the overall detection accuracy has reached 99.57%. It shows that the scheme proposed in this paper has a good multiclass detection effect for these types of data traffic in wireless sensor networks.

The real-time detection performance of the overall WSN intrusion detection system can be enhanced by increasing the intrusion detection rate of the traffic data model. As can be observed, the MC-GRU model took 2064.10 s to train, which is less than the training time of other models. It is clear that the model suggested in this paper has a low level of temporal complexity. The test time is 8.89 s, and the average detection time of a piece of traffic data is $8.89/74933 = 1.186 \times 10^{-4}$s, so the real-time detection performance of the MC-GRU model is high. It can also be proved that although the MC-GRU-based WSN intrusion detection model has a more complex model structure and more parameters, the training speed does not decrease with the deepening of the model but improves the real-time detection.

To be able to prove the effect of the MC-GRU algorithm on WSN intrusion detection, as shown in Figures 10–12, it is given that in the case of all using the WSN-DS dataset, some algorithms are selected for experimental comparison, including Naive Bayes (NB), SVM, KNN, and CNN, in addition to CNN-LSTM based on CNN and LSTM, to compare the accuracy, false positive, and recall of these intrusion detection algorithms.

Figure 10 shows the accuracy comparison between MC-GRU and the comparison algorithm. In contrast to the comparison algorithm, the accuracy rates of the MC-GRU algorithm proposed in this paper for detecting the five behaviors are 0.999, 0.992, 0.957, 0.995, and 0.930, respectively. The accuracy of black hole attack, gray hole attack, flood attack, and normal behavior detection is the best. Overall, the accuracy of the MC-GRU beats that of other algorithms.

Figure 11 shows the recall comparison results between MC-GRU and the comparison algorithm. In contrast to the comparison algorithm, the recall rates of the MC-GRU algorithm proposed in this paper for detecting five behaviors are 0.998, 0.953, 0.989, 0.904, and 0.996, respectively, and the accuracy in the detection of gray hole attacks and scheduling attacks is the best. SVM-RBF has a somewhat greater recall rate than MC-GRU when detecting normal behavior

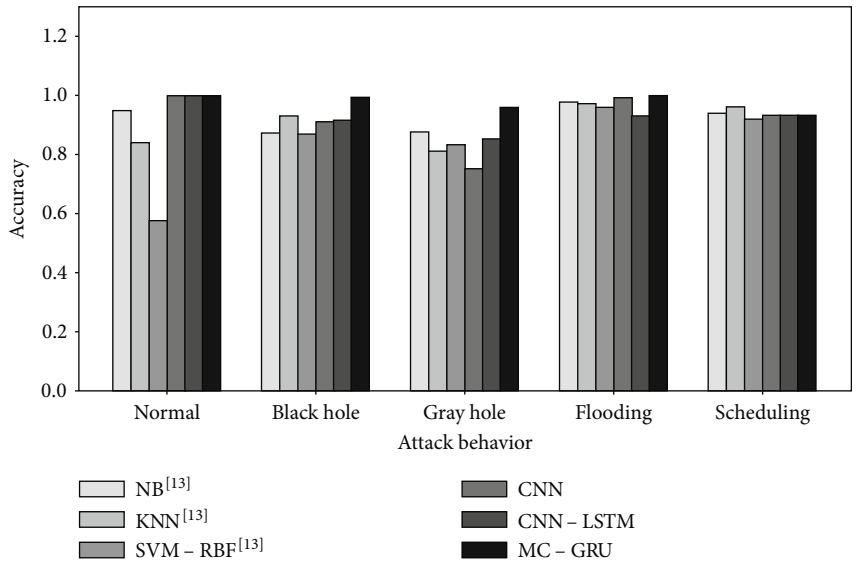

Figure 10: Comparison of the accuracy of six classification algorithms.

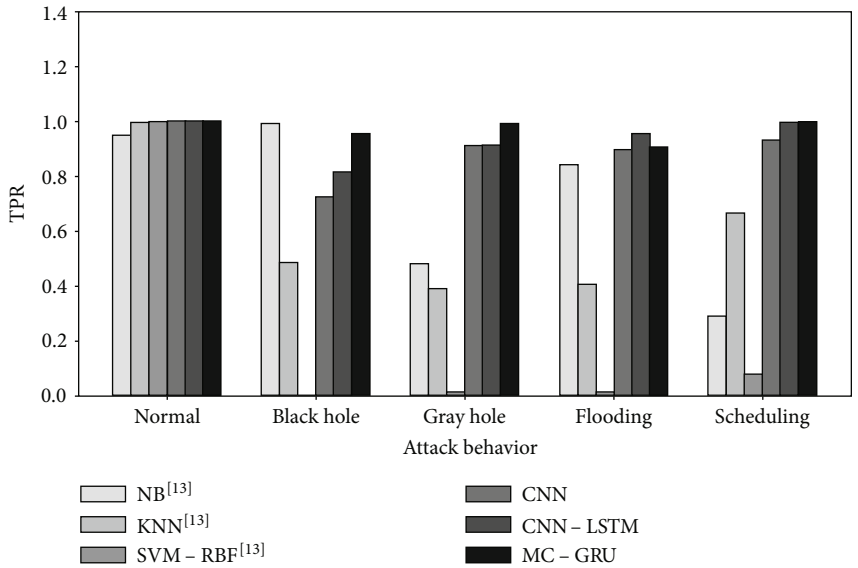

Figure 11: Comparison of recall rates of six classification algorithms.

and black hole attacks. For the detection of flooding attacks, the recall rate of CNN-LSTM is slightly higher than that of MC-GRU, but when combined with Table 5, it is found that the detection rate of MC-GRU is much higher than that of CNN-LSTM. As can be seen in the picture, MC-GRU outperforms other algorithms in terms of recall.

Figure 12 compares the false positive rate results between MC-GRU and the comparison algorithm. In contrast to the comparison algorithm, the recall rates of the MC-GRU algorithm proposed in this article to detect the five behaviors are 0.017, 0.0014, 0.0004, 0.0009, and 0.00006, respectively. The false positive rate is optimal in the detection of different behaviors. Although the false positive rate of SVM-RBF for detecting black hole attacks, gray hole attacks, flooding attacks, and scheduling attacks is similar to that of MC-GRU, the false positive rate for normal behavior detection reaches 0.922, and the overall false positive rate is too high.

In summary, the detection performance of MC-GRU for various traffic types in the WSN-DS dataset is significantly better than that of other models. When the MC-GRU model detects complex traffic attack types, it uses multiple convolutions to extract features from the original data and then introduces GRU to learn the context and time series features of the data, which makes the model more capable of extracting data flow features to speed up the convergence of the model. Therefore, compared to other models, MC-GRU has higher detection accuracy, faster detection rate, and better multiclassification effect.

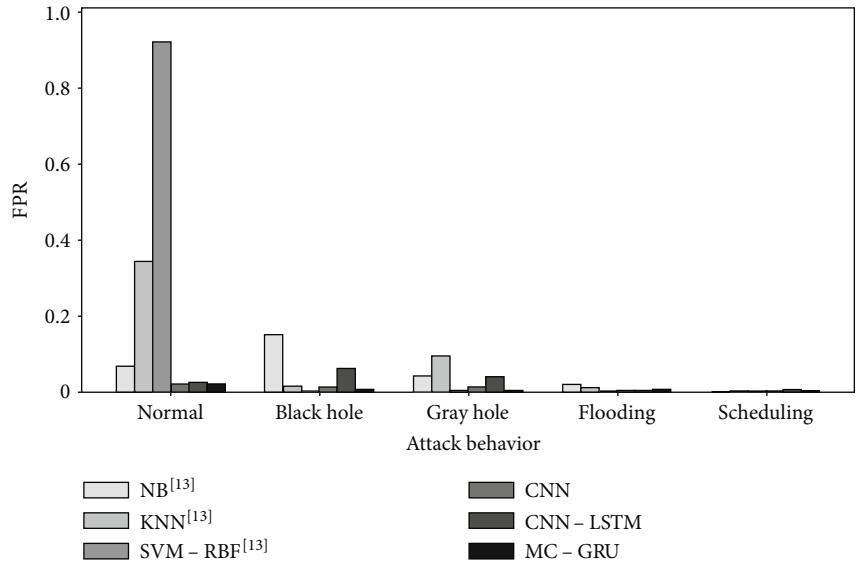

Figure 12: Comparison of false alarm rates of six classification algorithms.

Table 5: Model detection real-time comparison.

Model	Training time/s	Detecting time of each data/s
SVM	1837.18	5.404×10^{-4}
Simple RNN	2101.21	6.927×10^{-4}
CNN-LSTM	4283.63	2.461×10^{-4}
MC-GRU	2064.10	1.186×10^{-4}

5. Summary

Targeting the variety of current WSN traffic attack types, a WSN MC-GRU intrusion detection model is proposed. The experiment's findings demonstrate that the MC-GRU model's test set detection accuracy is 99.57%, and it can identify black hole attacks, gray hole attacks, flooding attacks, scheduling attacks, and normal behavior traffic types with high accuracy. Compared with other detection models, it significantly improves the ability of multiclassification of WSN attack types. At the same time, the detection rate is not slowed down due to the deepening of the model, which ensures the real-time detection of the model.

Data Availability

The data set WSN-DS used in this article can be obtained at https://gitee.com/he-feifan/matlab_workspace/blob/master/WSN-DS.csv.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This paper is funded by the project of Natural Science Foundation of Zhejiang Province (no. LY19F020006)

References

[1] J. S. Pan, F. Fan, S. C. Chu, H. Q. Zhao, and G. Y. Liu, "A lightweight intelligent intrusion detection model for wireless sensor networks," *Security and communication Networks*, vol. 2021, Article ID 5540895, 15 pages, 2021.

[2] G. Kalnoor and S. Gowrishankar, "Minimizing energy consumption for intrusion detection model in wireless sensor network," in *Applications of Artificial Intelligence and Machine Learning*, pp. 527–537, Springer, Singapore, 2021.

[3] T. Zhang, D. Han, M. D. Marino, L. Wang, and K. C. Li, "An evolutionary-based approach for low-complexity intrusion detection in wireless sensor networks," *Wireless Personal Communications*, vol. 8, pp. 1–24, 2021.

[4] Y. Yan, L. Qi, J. Wang, Y. Lin, and L. Chen, "A network intrusion detection method based on stacked autoencoder and LSTM," in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pp. 1–6, Dublin, Ireland, 2020.

[5] M. Mittal, C. Iwendi, S. Khan, and A. Rehman Javed, "Analysis of security and energy efficiency for shortest route discovery in low-energy adaptive clustering hierarchy protocol using Levenberg-Marquardt neural network and gated recurrent unit for intrusion detection system," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 6, article e3997, 2021.

[6] D. O. Rui-hong, Y. A. Hou-hua, Z. H. Qiu-yu, and L. I. Xue-yong, "Distributed WSN intrusion detection model based on deep forest algorithm," *Journal of Lanzhou University of Technology*, vol. 46, no. 4, p. 103, 2020.

[7] L. Fu-cai, W. Fei, C. Qian, H. Jindong, and K. Liang, "Machine learning-based intrusion detection technology for wireless sensor networks," *Journal of Harbin Engineering University*, vol. 41, no. 3, pp. 433–440, 2020.

[8] N. Gao, L. Gao, Y. Y. He, and H. Wang, "A lightweight intrusion detection model based on autoencoder network with feature reduction," *ACTA Electonica Sinica*, vol. 45, no. 3, p. 730, 2017.

[9] J. Jiang, Z. F. Wang, T. M. Chen, C. C. Zhu, and B. Chen, "Adaptive AP clustering algorithm and its application on

intrusion detection," *Journal on Communications*, vol. 36, no. 11, pp. 118–126, 2015.

[10] M. A. Hamzah and S. H. Othman, "A review of support vector machine-based intrusion detection system for wireless sensor network with different kernel functions," *International Journal of Innovative Computing*, vol. 11, no. 1, pp. 59–67, 2021.

[11] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. al-Nemrat, and S. Venkatraman, "Deep learning approach for intelligent intrusion detection system," *IEEE Access*, vol. 7, pp. 41525–41550, 2019.

[12] M. M. Chowdhury, F. Hammond, G. Konowicz, C. Xin, H. Wu, and J. Li, "A few-shot deep learning approach for improved intrusion detection," in *2017 IEEE 8th annual ubiquitous computing, electronics and Mobile communication conference (UEMCON)*, pp. 456–462, New York, NY, USA, 2017.

[13] L. Wang, J. Li, U. A. Bhatti, and Y. Liu, "Anomaly detection in wireless sensor networks based on KNN," in *International Conference on Artificial Intelligence and Security*, pp. 632–643, Cham, 2019.

[14] L. Tao and Z. Sun, "KIPSO spoofing attack detection model in wireless sensor networks," *Journal of Transduction Technology*, vol. 29, no. 7, pp. 1049–1055, 2016.

[15] O. Xiao-qin and W. Qiu-hua, "An intrusion detection scheme based on mini batch K-means and SVM in wireless sensor networks," *Software Guide*, vol. 19, no. 3, pp. 204–209, 2020.

[16] W. Li, P. Yi, Y. Wu, L. Pan, and J. Li, "A new intrusion detection system based on KNN classification algorithm in wireless sensor network," *Journal of Electrical and Computer Engineering*, vol. 2014, Article ID 240217, 8 pages, 2014.

[17] W. Jun, Z. Zhi-wei, and L. Jun-jie, "Detection and defense method for blackhole attacks in wireless sensor networks," *Computer Science*, vol. 46, no. 2, pp. 102–108, 2019.

[18] O. U. Maheswari and S. Jayasankari, "Secure communication in wireless sensor network using intrusion detection system for agriculture," *International Journal of Modern Agriculture*, vol. 10, no. 2, pp. 1829–1845, 2021.

[19] R. Lohiya and A. Thakkar, "Intrusion detection using deep neural network with antirectifier layer," in *Applied Soft Computing and Communication Networks*, pp. 89–105, Springer, Singapore, 2021.

[20] X. Gong and Y. Xiao, "A skin cancer detection interactive application based on CNN and NLP," *Journal of Physics: Conference Series*, vol. 2078, no. 1, article 012036, 2021.

[21] A. B. Abhale and S. S. Manivannan, *Deep Learning Algorithmic Approach for Operational Anomaly Based Intrusion Detection System in Wireless Sensor Networks*, 2021.

[22] N. Singh, D. Virmani, and X. Z. Gao, "A fuzzy logic-based method to avert intrusions in wireless sensor networks using WSN-DS dataset," *International Journal of Computational Intelligence and Applications*, vol. 19, no. 3, article 2050018, 2020.

[23] R. N. Asha, "Data mining based intrusion detection system for securing wireless sensor network," *Harbin Gongye Daxue Xuebao/Journal of Harbin Institute of Technology*, vol. 53, no. 10, pp. 22–32, 2021.

[24] W. Yang, S. Wang, and M. Johnstone, "A comparative study of ML-ELM and DNN for intrusion detection," in *2021 Australasian Computer Science Week Multiconference*, Dunedin New Zealand, 2021.