AMS Intrusion Detection Method Based on Improved Generalized Regression Neural Network

Yuhong Wu[1*], *Xiangdong Hu*[2]

[1] *College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, China*
[2] *College of Automation, Chongqing University of Posts and Telecommunications, China*
wuyuhong_2021@126.com, huxiangdong2021@126.com

Abstract

The smart grid integrates the computer network with the traditional power system and realizes the intelligentization of the power grid. The Advanced Measurement System (AMS) interconnects the power system with the user, realizes the two-way interaction of data and information between the power supplier and the user, and promotes the development of the smart grid. Therefore, the safe operation of AMS is the key to the development of the smart grid. As smart grids and computer networks become more and more closely connected, the number of cyberattacks on AMS continues to increase. Currently, AMS intrusion detection algorithms based on machine learning are constantly being proposed. Machine learning algorithms have better learning and classification capabilities for small sample data, but when faced with a large amount of high-dimensional data information, the learning ability of machine learning algorithms is reduced, and the generalization ability is reduced.

To enhance the AMS intrusion detection algorithm, this paper uses a Generalized Regression Neural Network (GRNN) to identify attack behaviors. GRNN has strong non-linear mapping ability, is suitable for unstable data processing with small data characteristics, has good classification and prediction ability, and has been widely used in power grid systems. Aiming at the existing problems, this paper proposes an upgraded generalized regression neural network AMS intrusion detection method DBN-DOA-GRNN. Based on the feature extraction and dimensionality reduction of the data by DBN, GRNN is used for data with less feature information in learning classification. In addition, to improve the detection effect of the method, the Drosophila Optimization Algorithm (DOA) is used to optimize the parameters of GRNN to reduce the influence of random parameters on the detection results, improve the detection accuracy of this method on small-scale sample data, and thereby improve the detection performance of the AMS intrusion detection algorithm. The proposed method archives an accuracy of 87.61%, 3.10% false alarm rate, and 96.9 precision rate.

Keywords: Deep belief network, Intrusion detection, Extreme learning machine, Generalized regression neural network

1 Introduction

The General Regression Neural Network (GRNN) is a quadratic fully convolutional decentralized network on the RBFNN framework developed by American researcher Specht in 1990. The GRNN network has a high degree of convergence, it can converge to the best value without too many training samples, and it has better detection ability for unstable and incomplete data [1]. Since it allows to identify and react to hostile traffic, a networking intrusion detection system (NIDS) is essential for cybersecurity. The real advantage of malware detection is that it alerts IT, professionals, whenever an attacker or networking incursion is suspected.

1.1 GRNN Network Structure

The GRNN network consists of a 4-layer network consisting of an input layer, a pattern layer, a summation layer, and an output layer. A version of radial basis neural networks is the generalized regression neural network (GRNN) [2-3]. It is a nonlinear regression-based machine learning approach that has been enhanced. Each knowledge management is considered to show an average toward a nonlinear activation synapse. The characteristics of GRNN are single-pass understanding eliminates the need for back propagation, prediction results are valid due to the usage of Gaussian functions, it can cope with noise in the inputs, it merely necessitates a smaller amount of information. Convolution models of unit operations make up an appropriate GRNN design (input, pattern, summation, and output neurons). The information is sent to the pattern layer via the input nodes, which accept the original input X. The patterning layer's neurons then create an outcome 'h' and deliver it to the accumulation level. As shown in Figure 1, the network input samples are: $X=\{x_1,x_2,\ldots,x_i\}$,The output sample is:$Y=\{y_1,y_2,\ldots,y_k\}$.

(1) Input layer

The input layer is a simple linear unit, which is the entrance for sample data to enter the network. The number of neurons is set equal to the dimension of the input information. In this paper, the data information after feature extraction through DBN (Deep Belief Network) is input into this layer.

(2) Mode layer

The model layer is frequently referred to as the hidden

*Corresponding Author: Yuhong Wu; E-mail: wuyuhong_2021@126.com
DOI: 10.53106/160792642023032402029

regression layer. Hidden layers are necessary for artificial neural networks therefore if information should be segregated non-linearly. Every algorithm can be applied towards the former layer with every level (frequently a linear conversion shadowed through a squashing nonlinearity). The sources are transformed into whatever activation function is utilized by the convolution nodes. The obtained data is sent from the input layer towards the mode layer. This layer's units correlate to every learning algorithm. The transfer function of each function of this layer is:

$$P_i = \exp\left[\frac{-(x-x_i)^T(x-x_i)}{2\sigma^2}\right], i = 1,2,...,n. \quad \textbf{(1)}$$

The input sample value in formula (1) is the distinctive factor of AMS intrusion detection, x- sample value, x_i- training sample equivalent to the ith neuron, and the model output is as follows:

$$D_i^2(x-x_i)^T(x-x_i). \quad \textbf{(2)}$$

(3) Summation layer

In the summation layer, there are two units. The weighted sum of the mode layer's outcome is calculated in one unit, as well as the total of the mode layer's data is calculated in the other. The first layer's frequency response is shown in:

$$S_D = \sum_{i=1}^{i=n} P_i. \quad \textbf{(3)}$$

S_D is the output value of the neuron pattern layer of this layer.

The connection weight of the neurons of this layer and the upper pattern layer is 1, and the transfer function of the second layer of neurons is as follows:

$$S_{Nj} = \sum_{i=}^{i=n} P_i Y_{ij}, j = 1,2,...,k. \quad \textbf{(4)}$$

S_{NJ} is the output value of the neuron pattern layer of this layer.

This layer performs a weighted summation of the output values of the pattern layer, where y_{ij} is the weight of the i-th neuron and the jth neuron of the summation layer.

(4) Output layer

The activation function separates the two kinds of neural components in the summation layer as the numerator and denominator, respectively, to form the transfer function. The final element's number of neurons matches the proportions of the dataset, as well as the extracted features is as regards:

$$Y_j = \frac{S_{Nj}}{S_D}, j = 1,2,...,n. \quad \textbf{(5)}$$

Where, $Y_{j\_}$ is the weight of the jth neuron.

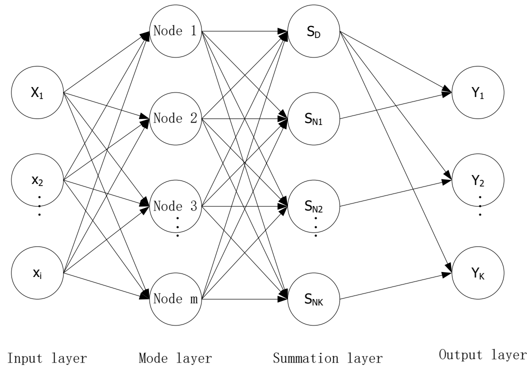


Figure 1. GRNN network structure diagram

1.2 Basic theory of GRNN

In the GRNN network, let $f(x, y)$ be the joint probability density of the network, x, and y as the independent variables, the training data as the x value, and y as the output value. The regression expression of y relative to x is:

$$E(y\,|\,x) = \hat{y}(x) = \int_{-\infty}^{+\infty} yf(x,y)dx \Big/ \int_{-\infty}^{+\infty} yf(x,y)dy. \quad \textbf{(6)}$$

The majority of non-parametric analyses are only assumption testing, with no determination of an influence magnitude or a credibility range. The majority of non-parametric approaches work by ordering a variable's frequencies in the order of increasing and then computing a normality test depending on the summation of these scores. An approach for nonparametric multivariate data that may also be used during categorization is Parzen windows categorization. The approach uses the standard accumulation of distributions centered on the observed points to simulate a particular test set probability utilizing a specified linear model. Suppose the sample data set is: $\{x_i, y_i\}_{i=1}^n$, use the Parzen non-parametric estimation method to estimate the training set, the sample density function can be evaluated as: $\hat{f}(x,y)$, the formula is as follows:

$$\hat{f}(x,y) = \frac{\sum_{i=1}^{n} e^{-d(x,x_i)} \times e^{-d(y,y_i)}}{2n\pi^{\frac{p+1}{2}}\sigma^{p+1}}. \quad \textbf{(7)}$$

Among them, $d(x,x_i) = \frac{(x-x_i)(x-x_i)^T}{2\sigma^2}$ and $d(y,y_i) = \frac{(y-y_i)^2}{2\sigma^2}$, n is the number of samples, p is the dimension of x, and σ is the smoothing factor (standard deviation of the Gaussian function).

By exchanging integral and summing, we get:

$$y(x)=\frac{\sum_{i=1}^{n}e^{-d(x,x_i)}\int_{-\infty}^{+\infty}ye^{-d(y,y_i)}dy}{\sum_{i=1}^{n}e^{-d(x,x_i)}\int_{-\infty}^{+\infty}e^{-d(y,y_i)}dy}. \quad \textbf{(8)}$$

In the GRNN network, only the smoothing factor σ has a significant impact on the network performance. But if the value of σ is much big, $y(x_0)$ is nearer towards the estimated factor of entire samples, then the factor of d(x, x_i) is close to 0; if the value of σ is too low, $y(x_0)$ is near to the dataset. The value of σ is the only random factor in GRNN, then the size of σ precisely involves the generalization capability of GRNN.

The main contribution of the paper is discussed as follows:

A Generalized Regression Neural Network is used to improve the AMS intrusion detection algorithm in this paper. GRNN has a high non-linear mapping capability and is well suited for unstable data processing with limited data features. The GRNN parameters are optimized using the Drosophila Optimization Algorithm (DOA).

2. Improved Generalized Regression Neural Network Algorithm

The choice of the smoothing factor σ in the GRNN is a difficult process, and the improper selection of σ value can easily fall into the issue of local optimum. A neural group is a combination of techniques that attempts to detect hidden patterns in a piece of information using a method that is similar to how the brain processes information. Because neural networks can react to new information, they can produce the desired outcome without requiring the outcome parameters to be redesigned.

Whenever the smoothing factor σ is huge, the output result is nearer to the average value of the entire sample. At the time of σ value is low; the learning ability is enhanced as well as the detection outcome is enhanced. This section uses the DOA to optimize the smoothing factor in the GRNN network globally.

2.1 Drosophila Optimization Algorithm (D0A) Optimizes GRNN network

The DOA is a new global optimization algorithm proposed by Taiwanese scholar Pan Wenchao in 2011 dependent on the foraging behavior of drosophila [4]. It has become widely employed in subsequent years in a variety of sectors, including surveillance, prediction, and categorization. Drosophila's sense of taste and eyesight are better than that of other organisms. Drosophila's olfactory function collects various odors floating in the air, they can even smell food sources 40 kilometers away. Drosophila's olfactory system, which is very basic but sensitive, is used to induce a range of behavioral behaviors in reaction to odors. The olfactory functioning of a growing group of mutants has been discovered to be faulty. Then, after flying close to the food location, it can also use intense visualization to detect the location where the food besides the companions gathers, then fly in that direction. The search technique is illustrated in Figure 2.

The Fruit Fly Optimization Algorithm (FFOA) is a novel approach for determining an optimal solution that is predicated on certain fruit flies 'nutrition behavior. It is a novel stochastic optimization approach that focuses on the feeding habits of fruit flies that has been demonstrated to be comparable with established optimization computation like particle swarm optimization (PSO). The stages of the drosophila evolutionary algorithms are as follows, based on the efficiency properties of the drosophila method:

(1) Randomly set the starting position of the drosophila group as: (X_{axis}, Y_{axis}), According to the foraging characteristics of drosophila, the direction and distance of drosophila searching for food are set at random.

$$\begin{cases} X_i = X_{axis} + Random \\ Y_i = Y_{axis} + Random \end{cases}. \quad \textbf{(9)}$$

In formula (9), Random is the search radius of drosophila.

(2) Calculate the current position of the drosophila as: (X_{axis}, Y_{axis}) ,and the distance from the starting position is: (Dist)，the distance can be known from equation (10):

$$D_i = \sqrt{X_{axis}^2 + Y_{axis}^2}. \quad \textbf{(10)}$$

(3) Set the taste concentration judgment value S_i as the reciprocal of the distance between the drosophila's current position and the initial position, as shown in equation (11):

$$S_i = 1/D_i. \quad \textbf{(11)}$$

(4) Bring the taste judgment value into the Fitness function, and find the individual position concentration of the drosophilaSmile (i), as shown in formula (12):

$$Smile(i) = Function(S_i). \quad \textbf{(12)}$$

(5) Find the drosophila individuals with the upper most sensitivity attentiveness in the drosophila populace, as shown in formula (13):

$$[bestSmellbestindex] = \max(Smell). \quad \textbf{(13)}$$

Among them, the best Smell is the best concentration value; the best index is the position of the drosophila.

(6) The coordinate data of the optimal concentration factor is retained, and the drosophila colony utilizes visualization to fly there.

$$\begin{cases} Smellbest = bestSmell \\ X_{axis} = X(bestindex) \\ Y_{axis} = Y(bestindex) \end{cases}. \quad \textbf{(14)}$$

(7) Iteratively repeat (2) ~ (5) until the drosophila colony finds food location and completes the optimal process of drosophila foraging.

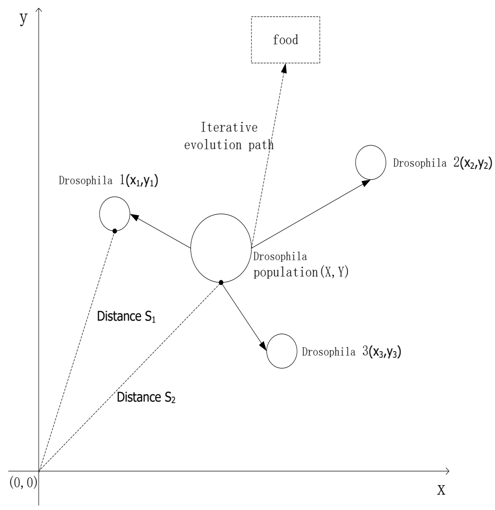


Figure 2. Schematic diagram of the optimization of the drosophila population

The foraging gene in Drosophila melanogaster is a well-known illustration of a genotype having significant impacts on behavior and variability. Because it was identified and designated for this characteristic, this genome is mainly remembered for underpinning the approaches of roving and seated forage caterpillars. The Drosophila Optimization Algorithm (DOA) optimizes the overall σ in formula (7), and the σ value corresponding to the best concentration value (RMSE minimum) is the optimal parameter value, as shown in Figure 3 for the DOA improved GRNN Algorithm flow.

The specific steps for selecting the smoothing factor σ are as follows:

Step 1: Initialize the position of the drosophila population, the population size of 30, the number of iterations of 100, the search direction, and the preliminary spot of the drosophila;

Step 2: Put the DBN matrix factorization learning algorithm into the system, set the drosophila foraging location at arbitrary, then compute the distance (Dist) among the actual populace's placement as well as the beginning point (Dist) to get the flavor intensity judgement rating;

Step 3: Bring in the taste determination concentration determination function to find the individual position concentration of the drosophila;

Step 4: Find the drosophila with the highest taste concentration in the drosophila population, keep the best concentration value and coordinates, and fly the drosophila to the place;

Step 5: Enter iterative optimization, after the iteration, the optimal smoothing factor is output, the GRNN detection model is established, and the training set data is trained.

2.2 Improved Generalized Regression Neural Network Algorithm Framework

This article first uses DBN to remove characteristics, in addition, diminish the dimensionality of the information. The DBN parameters are set to establish an AMS intrusion detection model of DBN-DOA-GRNN. As shown in Figure 4.

(1) Data preprocessing: the data set is digitized and normalized, and the data set is processed into a unified type.

(2) DBN feature extraction: put the pre-processed data set into the DBN network for pre-training and fine-tuning of weights, extract the main features of the data, and eliminate redundant features [5].

(3) DOA-GRNN classifier classification: input the reduced-dimensional training set into the GRNN network, use the group optimization algorithm DOA to optimize the smoothing factor in GRNN and obtain the optimal smoothing factor σ through multiple iterations to complete GRNN Network construction [6-7]. The attack samples of the training set are trained and learned, and the attack recognition result of AMS intrusion detection is obtained through detection.

3. Experimental Research

3.1 Experimental Parameter Design

Orientation of arriving estimate is a major study field in signal analysis and numerous technical areas, including mobile technology, meteorology, radar systems, acoustics, navigational, motion detection, seismic, healthcare, and certain other immediate assistance equipment that rely on it. In the process of DOA algorithm optimization, three factors require to be set, namely the number of iterations, the population size as well as the search step.

(1) Drosophila algorithm search step size

The search stage size alluded towards the optimization area of the drosophila system. When the optimization radius is small, the optimization accuracy is high, but the optimization process tends to fall into local optimization problems; whenever the optimization radius is much high, the optimization range becomes larger and the optimization is optimized. The distribution is uniform, which greatly reduces the local optimal problem, so the setting of the search step value is very important [8-9]. By consulting related experiments, experiments were carried out on the three-step sizes of [-5, 5], [-10, 10], and [-20, 20]. The results showed that training for ten thousand pieces of data, [-20, 20] is more suitable for the algorithm requirements of this article.

(2) Drosophila Population Size (DPS)

In the process of optimizing the drosophila population, the larger the population size and the uniform distribution, the higher the probability of finding the ideal value. In this experiment, the quantity of iterations is set to 30, the search step size is [-20, 20], then the population size is set to 10, 20, and 30 pairs of research drosophila optimization process, as shown in Figure 5.

From Figure 5(a), Figure 5(c), Figure 5(e), it can be seen that as the population size continues to increase, the drosophila optimization convergence curve gradually becomes smoother, and it keeps approaching the convergence value, and the convergence effect becomes better. It employs an adaptive method to reduce a specified dispersion imperfection. As a result, a "community" of GMMs is treated via several repetitions and stages that alter, classify (selection), as well as reassemble the GMMs. From Figure 5(b), Figure 5(d), Figure 5(f), it can be seen that as the population size increases, the drosophila optimization trajectory tends to a straight line. This process shows that the population size is too small, the optimization distribution is uneven, and it is simple to fall into the local optimum, and the increase in population size can effectively avoid such problems [10]. However, with the increase of the group size, the computational complexity is high, and the training takes a long time. Therefore, the determination of the population size needs to increase the population size under the premise of ensuring optimization efficiency. Through consulting literature and experiments, this article adopts the population size as 30 [10-14].

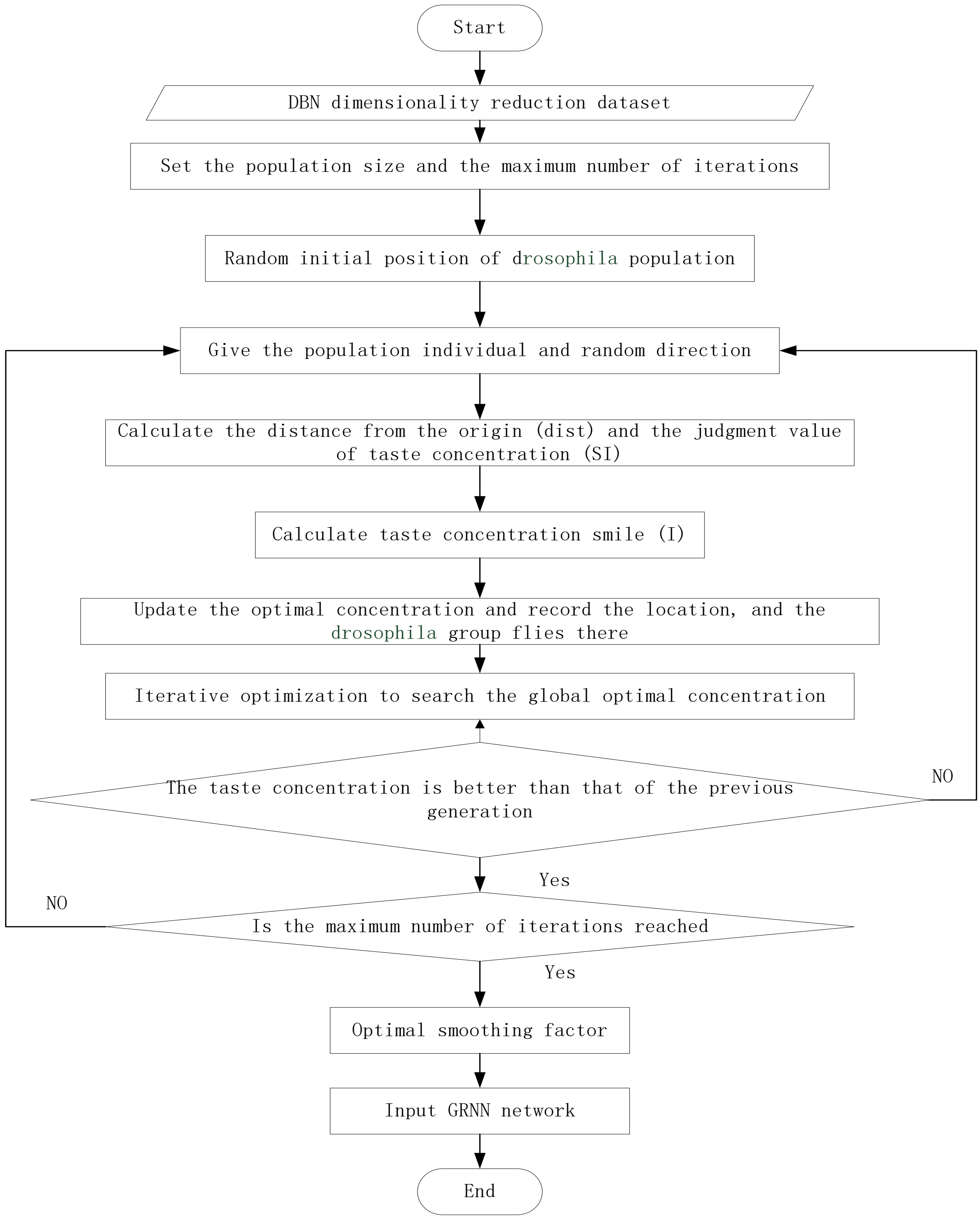


Figure 3. DBN-DOA-GRNN training flowchart

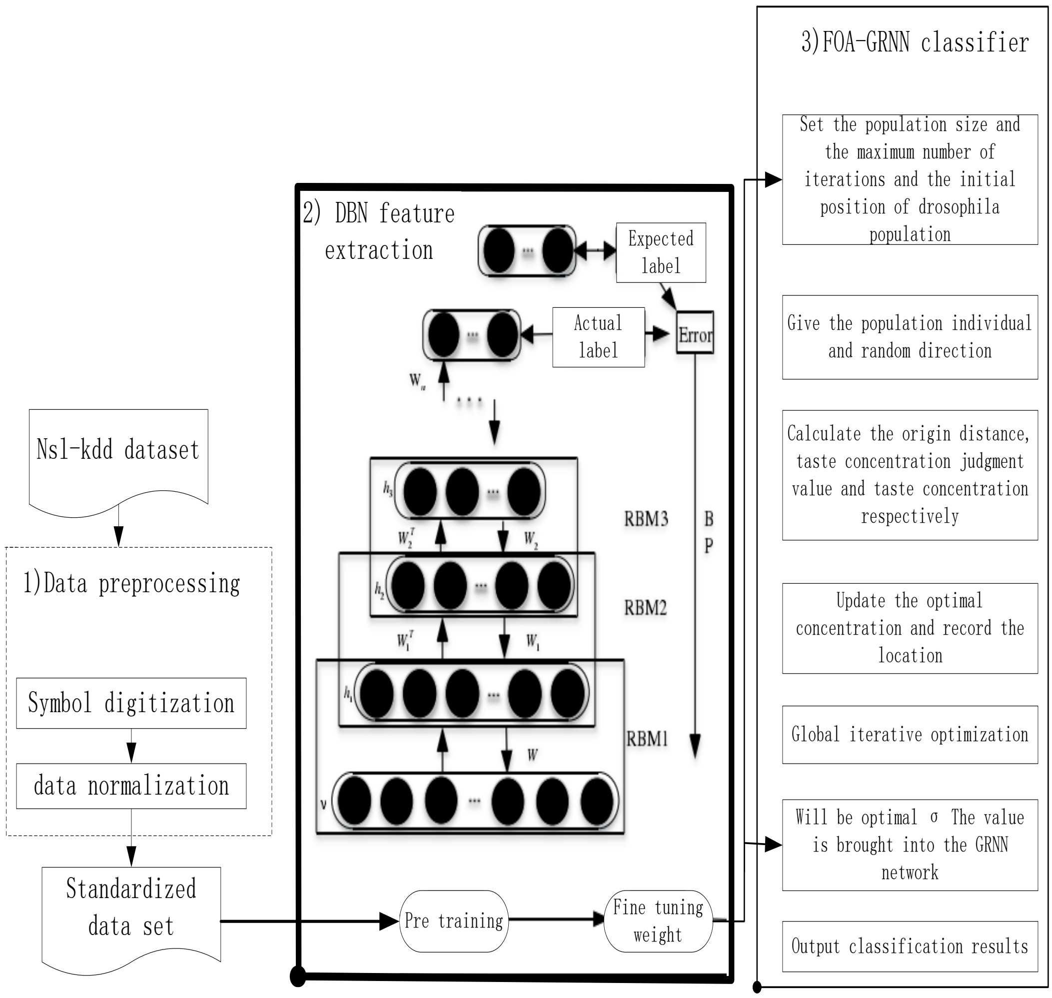
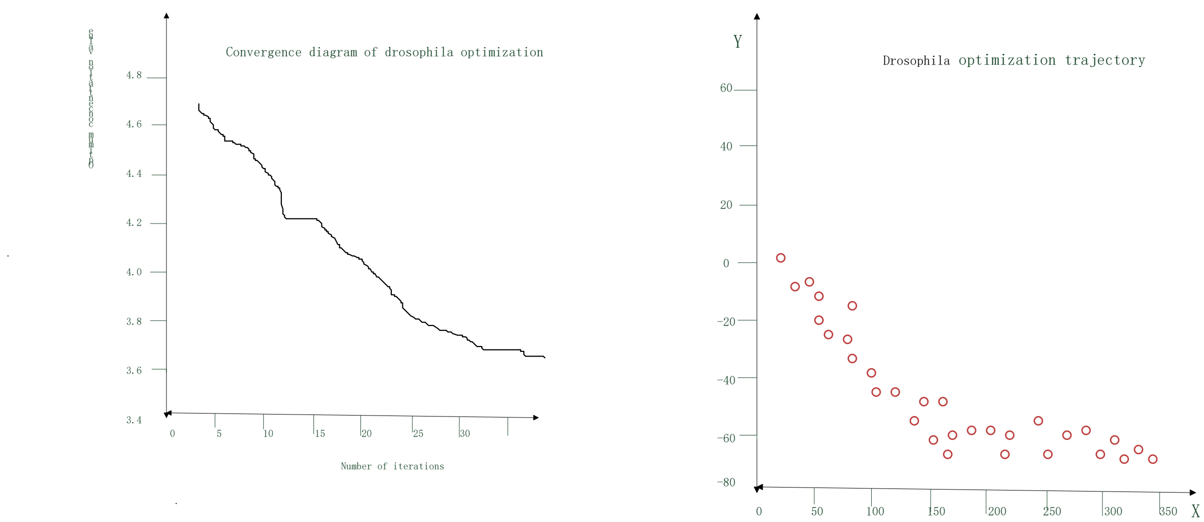
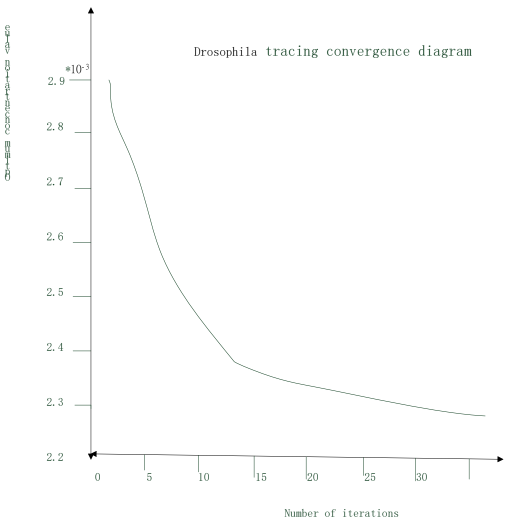


Figure 4. DBN-DOA-GRNN training flowchart

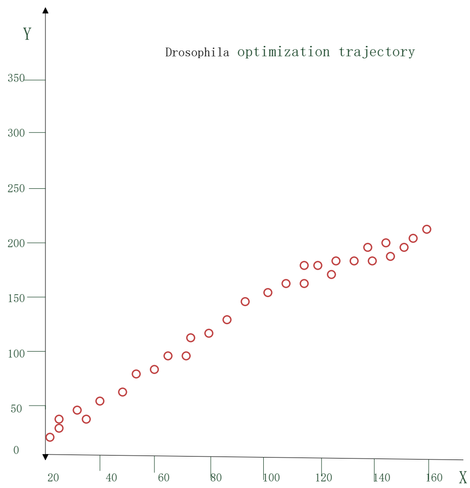


(a) Convergence graph of Drosophila optimization when SP=10

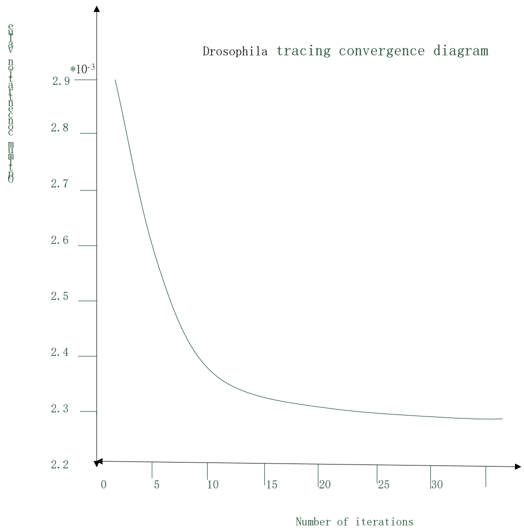
(b) Optimal trajectory of drosophila when SP=10



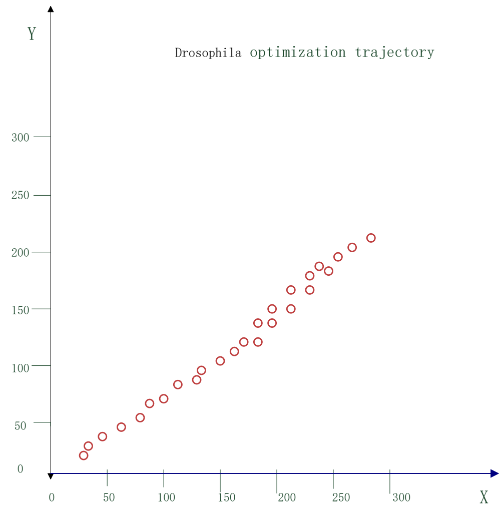
(c) Convergence graph of Drosophila optimization when SP=20



(d) Optimal trajectory of drosophila when SP=20

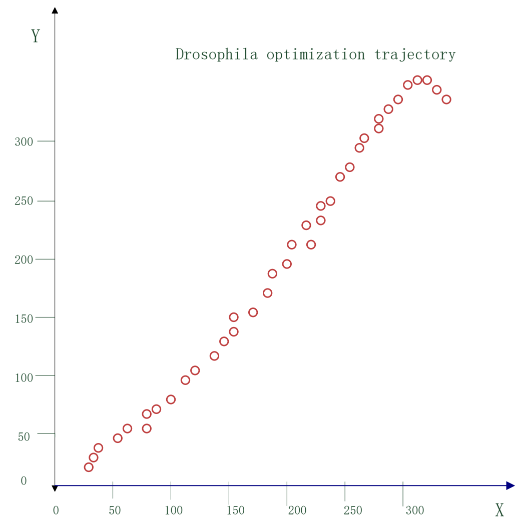


(e) Convergence graph of drosophila optimization when SP=30

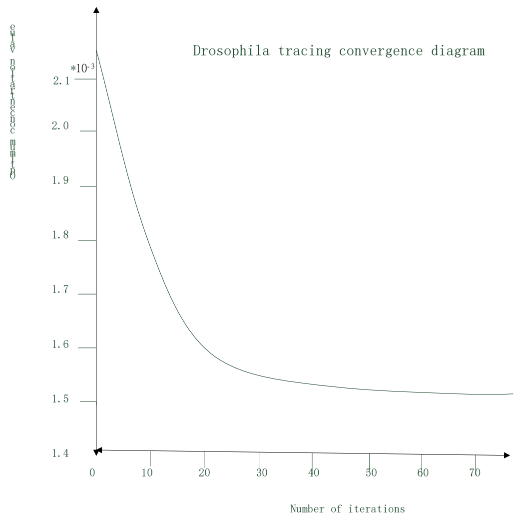


(f) Optimal trajectory of drosophila when SP=30

Figure 5. Diagrams of optimizing drosophila under different population sizes



(a) Drosophila optimization trajectory diagram



(b) Convergence graph of optimal concentration value

Figure 6. Drosophila algorithm optimization result graph

(1) Number of iterations

The number of iterations determines whether the optimization result falls into a local optimum. The greater the number of iterations, the more accurate the optimal value obtained, but it also comes with the high computational complexity of multiple iterations [14]. In this experiment, the population size is set to 30, the number of iterations is set to 50, and the random distance of flight is [-20, 20]. Figure 6(a) shows the activity trajectory diagram of drosophila optimization, and Figure 6(b) shows the best Convergence of the concentration value.

After 100 iterations of DOA, it can be seen from Figure 6(a) that the optimal position of the drosophila population is (329.7411, 347.4114), and iterate to the 47th time to determine the optimal concentration value, after which the curve tends to be flat. The selection of the number of iterations needs to reduce the number of iterations while ensuring that the optimal value is selected. The number of iterations in this article is 50.

3.2 Analysis of Experimental Results

In this paper, an intrusion detection method of DBN-DOA-GRNN is proposed. The training set KDDtrain+ then the test set KDDtest+ in the NSL-KDD data set is utilized as experimental information for the investigationalstudy. Utilize the accuracy rate (ACC), false alarm rate (FAR), and precision (PRE) in formulas (15), (16), and (17) as the evaluation basis of the experiment. The evaluation technique of each evaluation indicator is as follows: where TP is the quantity of properly categorized positive samples, FN denotes a set of misclassification negative samples, FP denotes the number of incorrectly classified positive samples, and addition to TN denotes the number of correctly classified negative datasets [15].

$$Acc = \frac{TP + TN}{TP + FN + FP + TN}. \tag{15}$$

$$PRE = \frac{TP}{TP + FP}. \tag{16}$$

$$FAR = \frac{FN}{TP + FN}. \tag{17}$$

The experiment in this section randomly selects 20000 pieces of data from the KDDtrain+ training set as the training set. The training set is divided into two groups for cross-validation to protect over-fitting problems throughout the training procedure. Through many experiments, this article chooses the population size to be 30, the number of iterations is 50, the flying random distance is [-20, 20], then the best smoothing factor σ is 0.0023. The test information is put into the enhanced GRNN model for training and acquired to categorize occurrences.

To authenticate the interruption detection capability of the algorithm model in the face of a variety of unknown attacks, 20,000 preprocessed training data sets are randomly selected, and normal data, as well as attack information, are mixed. Table 1 illustrates the intrusion detection consequence of the algorithm when the attack is unidentified.

Table 1 depicts the intrusion detection outcomes of five algorithms: BP, SVM, GRNN, DBN-GRNN, and DBN-DOA-GRNN when the attack type is indefinite. Among them, the smoothing factor in GRNN that has not been improved by the DOA algorithm is set to the default value 1, the number of hidden layers of the BP network is 5, and the number of iterations is set to 30. It can be seen from Table 1 that the GRNN network after the data is reduced by DBN has an accuracy rate of 4.9% higher than that of directly using the GRNN network, and the false alarm rate is reduced by 4.98%.

Table 1. Intrusion detection results of various attacks (unknown attack type)

Algorithm	ACC	FNR	PRE
BP	79.97%	7.34%	95.68%
SVM	74.5%	12.65%	93.22%
GRNN	71.14%	10.88%	91.12%
DBN-GRNN	75.01%	7.9%	92.10%
DBN-DOA-GRNN	87.61%	3.10%	96.9%

Secondly, the intrusion detection accuracy rate of the DBN-DOA-GRNN algorithm after the optimization of the smoothing factor by the DOA algorithm is increased by 11.57%, and the false alarm rate is reduced by 7.78%. Compared with the BP and SVM algorithms, the DBN-DOA-GRNN algorithm has obvious advantages in improving detection accuracy. Finally, the DBN-DOA-GRNN algorithm has a small improvement in accuracy compared to the other four algorithms, but it still maintains a certain advantage. Experiments show that the effect of DBN feature extraction is significant, and it has better learning ability than traditional machine learning methods. The smoothing factor in the GRNN network is shown in Figure 6(b). It can be seen that the convergence curve of the DOA algorithm is smooth and the convergence speed is fast. It can be seen that the DOA algorithm has better global optimization performance, and the GRNN network performance after optimization is improved, which improves the intrusion detection performance of the network. In general, the DBN-DOA-GRNN algorithm is better than the BP and SVM machine learning algorithms. 20,000 input image information were obtained to test the application's access control capacity in the presence of several assaults. User to Root (U2R) Attack is the attacker requests a standard user identity, and then exploits the program's weaknesses to acquire administrative privileges. While Root to Local (R2L) attack is an adversary that acquires administrator rights through leveraging communication weaknesses and delivering messages to a distant system.

As Table 2 shows, which can be observed that the improved GRNN has a certain enhancement in detection accuracy compared to the standard GRNN network, and has a certain improvement in the small sample data U2R data. The DBN-DOA-GRNN algorithm has a certain progression over the SVM algorithm. Experiments show that the DBN-DOA-

GRNN algorithm has a certain development in the intrusion detection recognition rate by comparing with traditional methods such as GRNN and SVM. GRNN learning is rather straight forward. Because GRNN is an association network, the number of nodes following learning is equivalent to the total of training instances.

Table 2. Intrusion detection results of various attacks (with known attack types)

Classification algorithm	ACC (%)				
	Normal	Dos	U2R	R2L	Probe
SVM	95.29	78.4	9.5	15.5	61.88
BP	97.22	73.65	5.6	9.53	67.20
GRNN	96.1	74.48	5.4	19.30	57.87
DBN-DOA-GRNN	96.69	76.05	10.23	25.37	67.68

The detection effect of the small sample data U2R & R2L in the experiment is generally because the sample categories in the data set are unbalanced, the small sample data is too small in the training set, and the small sample data features obtained in the DBN extraction process are too few, which makes the classification results biased for large sample data, small sample U2R and R2L attack classification results are not good. On the whole, the accomplishment of the DBN-DOA-GRNN machine learning method outperforms the BP and SVM algorithms.

To ensure that the intrusion detection system is working properly, capabilities of the DBN-DOA-GRNN algorithm and the DBN-OS-RKELM algorithm against multiple attacks with incomplete data characteristics, 20,000 pieces of data were randomly selected from the KDD train+ training set, and normal data and attack data were mixed. Table 3 depicts the intrusion detection of the system when the attack is unknown.

Whenever the assault method is uncertain, Table 3 illustrates the network security performance of the different techniques, DBN-DOA-GRNN and DBN-OS-RKELM. The recognition rate of the DBN-DOA-GRNN technique is 3.58 percent greater than that of the DBN-OS-RKELM method whenever the size of the data sampling is 20,000, as shown in the table, and the associated false positive rate and precision have evident benefits. The experiment shows that when the data feature information is less, the DBN-DOA-GRNN algorithm has a better learning ability for the data, and has certain benefits in the detection precision of the attack datasets. This algorithm makes up for the low detection accuracy of the DBN-OS-RKELM algorithm when the data feature information is less.

Table 3. Intrusion detection outcomes of the two algorithms in multiple attacks (unknown attack type)

Algorithm	ACC	FNR	PRE
DBN-DOA-GRNN	87.61%	3.10%	96.9%
DBN-OS-RKELM	84.03%	99%	84.93%

4 Conclusion

The electrical grid is the country's comprehensive development, as well as the smart grid is the way an enlightened society will grow in the future. AMS is a critical component in achieving power system two-way connectivity. Current intrusion detection for AMS can no longer encounter the needs of present intrusion detection.

To resolve the issue that the existing intrusion detection algorithm has low detection accuracy when the data feature information is less, this paper proposes a generalized regression neural network and a drosophila swarm optimization algorithm. Based on the GRNN algorithm, DBN is utilized to remove the features of the information. GRNN is used as a classifier, and the drosophila algorithm is used to optimize the σ value of GRNN. Artificial neural networks have a lot of benefits, such as the capacity to track the complicated dynamic correlation between various factors without mandating detailed statistical instruction, the required to recognize all interrelations among regression models, as well as the accessibility of different instructional methodologies. An enhanced generalized regression neural network AMS intrusion detection technique DBN-DOA-GRNN is proposed. Compare this method with BP, SVM, GRNN, and DBN-OS-RKELM algorithm, by using accuracy rate (ACC), precision (PRE), and false alarm rate (FNR) as evaluation indicators, it verifies that the technique developed in this paper is comparable compared with the traditional BP, SVM and GRNN algorithms, it has certain advantages in intrusion detection. At the same time, it is proved that when the data feature information is less, the DBN-DOA-GRNN algorithm makes up for the problem of low detection accuracy of the previous algorithms.

Acknowledgements

Scientific Research Program of Chongqing Municipal Education Commission (KJ1602201); Joint Fund of MOE and China Mobile (MCM20150202).

References

[1] E. Al-Shaer, M. A. Rahman, *Security and resiliency analytics for smart grids*, *Advances in Information Security*, Springer, 2016.

[2] V. Giordano, F. Gangale, G. Fulli, M. S. Jimenez, I. Papaioannou, A. Colta, K. I. Onyeij, A. Mengolini, T. Ojala, I. Maschio, E. Alecu, *Smart Grid projects in Europe: lessons learned and current developments*, Jrc Reference Reports, EUR 24856 EN, 2011.

[3] A. Alazab, M. Hobbs, J. Abawajy, A. Khraisat, M. Alazab, Using Response Action with Intelligent Intrusion Detection and Prevention System against Web Application Malware, *Information Management & Computer Security*, Vol. 22, No. 5, pp. 431-449, November, 2014.

[4] P. Tao, Z. Sun, Z. Sun, An improved intrusion detection algorithm based on GA and SVM, *Ieee Access*, Vol. 6,

pp. 13624-13631, March, 2018.

[5] M. Idhammad, K. Afdel, M. Belouch, Dos detection method based on artificial neural networks, *International Journal of Advanced Computer Science and Applications*, Vol. 8, No. 4, pp. 465-471, 2017.

[6] N. Gao, L. Gao, Q. Gao, H. Wang, An Intrusion Detection Model Based on Deep Belief Networks, *Second International Conference on Advanced Cloud and Big Data*, Huangshan, China, 2014, pp. 247-252.

[7] R. U. Khan, X. Zhang, M. Alazab, R. Kumar, An Improved Convolutional Neural Network Model for Intrusion Detection in Networks, *2019 Cybersecurity and Cyberforensics Conference (CCC)*, Melbourne, VIC, Australia, 2019, pp. 74 -77.

[8] P. Singh, A. Shankar, A novel optical image denoising technique using convolutional neural network and anisotropic diffusion for real-time surveillance applications, *Journal of Real-Time Image Processing*, Vol. 18, No. 5, pp. 1711-1728, October, 2021.

[9] M. A. Faisal, Z. Aung, J. R. Williams, A. Sanchez, Securing Advanced Metering Infrastructure Using Intrusion Detection System with Data Stream Mining, *Pacific Asia Conference on Intelligence & Security Informatics*, Kuala Lumpur, Malaysia, 2012, pp. 96-111.

[10] Y. Zhang, L. Wang, W. Sun, R. C. Green II, M. Alam, Distributed intrusion detection system in a multi-layer network architecture of smart grids, *IEEE Transactions on Smart Grid*, Vol. 2, No. 4, pp. 796-808, December, 2011.

[11] K. Wang, M. Du, S. Maharjan, Y. Sun, Strategic honeypot game model for distributed denial of service attacks in the smart grid, *IEEE Transactions on Smart Grid*, Vol. 8, No. 5, pp. 2474-2482, September, 2017.

[12] X. Liu, P. Zhu, Y. Zhang, K. Chen, A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure, *IEEE Transactions on Smart Grid*, Vol. 6, No. 5, pp. 2435-2443, September, 2015.

[13] Y. Li, R. Qiu, S. Jing, Intrusion detection system using Online Sequence Extreme Learning Machine (OS-ELM) in advanced metering infrastructure of smart grid, *PLoS ONE*, Vol. 13, No. 2, Article No. e0192216, February, 2018.

[14] P. Ponmurugan, C. Venkatesh, M. D. Priyadharshini, S. Balamurugan, Intrusion Detection Strategies in Smart Grid, in: D. Goyal. S. Balamurugan, S.-L. Peng, O. P. Verma (Eds.), *Design and Analysis of Security Protocol for Communication*, Scrivener Publishing, 2020, pp. 211-233.

[15] K. Song, P. Kim, V. Tyagi, S. Rajasekaran, *Artificial Immune System (AIS) Based Intrusion Detection System (IDS) for Smart Grid Advanced Metering Infrastructure (AMI) Networks*, CS 4624: Multimedia, Hypertext, and Information Access [196], May, 2018.

Biographies

Yuhong Wu, Female, born in 1981, associate professor, now a doctoral candidate. In recent years, her main research directions include industrial control system security, artificial intelligence technology, intelligent intrusion detection technology, big data, etc.

Xiangdong Hu, male, born in 1971, is a professor. He has published more than 60 SCI, EI and Chinese core papers, and presided over a number of national patents, His main research interests are intelligent perception, network measurement and industrial information security.