IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received August 24, 2019, accepted September 7, 2019, date of publication September 12, 2019,
date of current version September 30, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2940822

Quantitative Assessment of Wireless Connected Intelligent Robot Swarms Network Security Situation

WEIHONG HAN[1], ZHIHONG TIAN[1], ZIZHONG HUANG[2], DONGQIU HUANG[1], AND YAN JIA[2]
[1]Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou 510006, China
[2]Computer School, National University of Defense Technology, Changsha 410073, China

Corresponding author: Zhihong Tian (tianzhihong@gzhu.edu.cn)

This work was supported in part by the NSFC under Grant 61972106 and Grant U1636215, in part by the National Key Research and Development Plan under Grant 2019QY1406, and in part by the Guangdong Province Key Research and Development Plan under Grant 2019B010137004.

ABSTRACT The wirelessly connected intelligent robot swarms are more vulnerable to be attacked due to their unstable network connection and limited resources, and the consequences of being attacked are more serious than other systems. Therefore, the quantitative assessment of wireless connected intelligent robot swarms network security situation is very important. Factors determining the state of wireless connected intelligent robot swarms network security have characteristics such as mass and diversity, which constantly evolve with time. In fact, network security measurement has multi-level, multi-dimensional, and multi-granularity characteristics. Therefore, properly selecting wireless connected intelligent robot swarms network security measurement parameters and reducing and converging them to quantitative values such that they can enable a true and objective reflection of the network security state is a very challenging problem. However, deep learning is a novel solution to the abovementioned problems; its algorithm gets rid of the dependence on feature engineering and automatically builds a quantitative assessment model of a network security situation with dynamic adjustment as well as self-adaptive and self-learning characteristics. In this study, we propose a quantitative assessment method of wireless connected intelligent robot swarms network security situation based on a convolutional neural network (CNN). Generally, the convolutional layer is used to locally detect and deeply extract features, and the pooling layer is used to rapidly shrink the network scale and highlight the summary features. Using the deep network structure of several hidden layers, the results of quantitative assessment of the network security situation are highly consistent with expert experience. Experimental results show that the quantitative assessment of wireless connected intelligent robot swarms network security situation can be realized by combining the characteristics of a network security index system and CNN. Note that the accuracy rate is 95%, and the calculation results are better than those of other deep learning models.

INDEX TERMS Network security, index system, convolutional neural networks, deep learning.

I. INTRODUCTION

In recent years, robots technology are moving toward modularity, intelligence and systematization. Robot swarm is one of the hottest topics in both robotics and artificial intelligence, and exciting progress is being achieved. Its applications involve agriculture, architecture, disaster prevention, medical care, family services, etc. These are all areas closely related to human activities, and robot swarms have gradually integrated into human society. The wirelessly connected intelligent robot swarms are more vulnerable to be attacked due to their unstable network connection and limited resources, and the consequences of being attacked are more serious than other systems. Therefore, the network security problem of wireless connected intelligent robot swarms should be highly valued. The quantitative assessment of wireless connected intelligent robot swarms network security situation is required to meet the requirements of wireless connected intelligent robot swarms network security. Based on the technology of big data acquisition and storage management of network security,

The associate editor coordinating the review of this manuscript and approving it for publication was Jinming Wen.

a multi-dimensional, multi-level, and multi-granularity study is conducted for the wireless connected intelligent robot swarms network security situation from a micro- to macro-perspective. Then, the quantitatively assessed value is used to provide decision-making support for wireless connected intelligent robot swarms security.

The factors determining the state of wireless connected intelligent robot swarms network security have characteristics such as mass and diversity, which constantly evolve with time. Note that network security measurement has multi-level, multi-dimensional, and multi-granularity characteristics. Therefore, properly selecting wireless connected intelligent robot swarms network security measurement parameters and reducing and converging them to quantitative values to enable them to truly and objectively reflect the network security state is a very challenging problem. However, deep learning is a novel solution to the abovementioned problems, its algorithm gets rid of the dependence on feature engineering and automatically builds a quantitative assessment model of wireless connected intelligent robot swarms network security situation with dynamic adjustment as well as self-adptive and self-learning characteristics. Convolutional neural network (CNN) is a type of feedforward neural network that uses convolution calculations and a deep structure. Moreover, its convolutional layer and pooling layer can effectively compress data and extract key features, as well as conduct translation invariant classification. Therefore, a multi-dimensional, multi-level, multi-granularity, and configurable comprehensive network security situation assessment model that covers various properties of a network can be established via the training and learning of a CNN. The established wireless connected intelligent robot swarms network security situation assessment model has both good expandability and contains the primary event types and security indicators that affect the network system, which can accurately and comprehensively reflect the network security situation in real time.

II. RELATED RESEARCH

Robot swarms are one of the hottest topics in both robotics and artificial intelligence [1]. As the key enablers in practical robot swarms, communication and networking are attracting attention [2], [3]. Most research consider centralized control, reliable communication infrastructure, distributed task allocation, formation control and collision avoidance in robot swarms and so on [4], [5]. But few studies are focus on Robot swarms' network security [6].

In the field of network security, quantitative assessment of a network security situation has always been a research hotspot, and there have been multiple related research results. Wang et al. proposed a network security situation index system based on an analytic hierarchy process (AHP) and grey clustering algorithm [7]. Chen et al. reported an index system for quantitatively assessing of network security situation and provided an example of the evaluation process. Moreover, this index system can be used for assessing softs witch and mobile core network [8]. Tang et al. proposed a quantitative assessment model of network security situation based on situation entropy and developed the calculation method of situation assessment index value of network availability [9]. From the perspective of system security mechanism, Yao et al. reported a method to construct the index system of network security situation elements and developed the method to acquire the data of network availability situation elements and calculate the index value [10]. Li et al. proposed a vulnerability index system construction method based on a knowledge reduction algorithm, which guarantees the accuracy of assessment results and is more objective compared to an AHP weight judgment method [11]. Zhang et al. proposed a configurable network security quantitative assessment model, which generated a corresponding network security situation quantitative assessment model for the dynamic configuration of different requirements [12]. Ming et al. proposed a network survivability evaluation model based on a PDR model and a survivability R3 model [13]. Ou et al. examined the weight allocation method of network security index systems and proposed a method based on Delphi and AHP to calculate the weight value of index [14].

For applying deep learning in the field of network security, the existing studies primarily focused on using deep learning methods for malware detection and intrusion detection. Wenyi and Stokes *et al.* [15] proposed MtNet, which uses multi-task learning and DNN (Deep neural network) to extract features of a malicious code. Kolosnjaji *et al.* [16] constructed a neural network based on a convolutional layer and a recurrent layer to detect malware system call sequences obtained via dynamic analysis. Tobiyama *et al.* [17] simultaneously used RNN (Recurrent Neural Network) and CNN (Convolutional Neural Networks) to extract malware features. Kim *et al.* [18] used LSTM (Long Short-Term Memory) to conduct network intrusion detection on the KDD99 data set and select parameters, thus achieving a high detection rate. Salama *et al.* [19] first applied DBN (Deep Belief Network) as a generation model for data dimensionality reduction in intrusion detection and used SVM (Support Vector Machine) to classify the data after dimensionality reduction. Abolhasanzadeh *et al.* [20] proposed a method for the dimensionality reduction of intrusion detection features using the Bottleneck AE architecture. Alom *et al.* [21] used DBN to classify intrusion detection, digitally encoded features, and to reduce the dimensionality of features via deviation standardization. Aygun *et al.* [22] proposed a random denoising self-encoder for intrusion detection and achieved a good detection rate.

At this stage, to assess network security, we conducted studies by combining the traditional neural network with the calculation of network security indices and obtained good results [23]–[27]. However, when dealing with large-scale input data, the complete connection structure of traditional neural networks is not effective when it is applied to large-scale complex networks because the dimension of hidden layer nodes and input data exponentially increases.

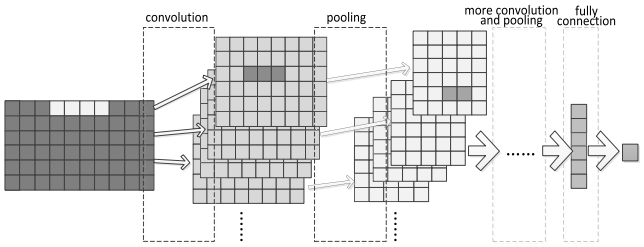


FIGURE 1. Convolution neural network model structure for network security situation assessment.

Moreover, the bias value that is corresponding to each intermediate node will lead to excessive weights in nodes. However, the use of deep learning, particularly CNN, is still being explored for the quantitative assessment of the network security situation.

III. QUANTITATIVE ASSESSMENT MODEL OF WIRELESS CONNECTED INTELLIGENT ROBOT SWARMS NETWORK SECURITY SITUATION BASED ON CNN

A. CONVOLUTIONAL NEURAL NETWORK

As a typical deep learning model, CNN has evolved from a traditional neural network model and is extensively used in image recognition, target detection, speech recognition, text processing and other aspects; moreover, it has achieved remarkable results and effects [28]–[30]. CNN has the characteristic of sharing weights and can effectively reduce the computational complexity of high-dimensional data using convolution and pooling. Moreover, weight sharing on a feature-mapping surface can help in parallel computation, which is conducive for improving the model's efficiency. Furthermore, the role of pooling is reflected when summarizing the statistical characteristics, which can show a better effect for preventing over-fitting. As shown in Figure 1, the convolution kernel, represented by a light color, is used for conducting inner product operation with the training data matrix in the convolution operation of the model; moreover, a feature map is generated via a certain stride movement. Thus, the convolution output is considered as the input of pooling, and then the calculation is performed through similar pooling kernels to reduce the computational complexity, and then the model is constructed by combining multiple convolutions and pooling.

By taking advantage of the abovementioned operational characteristics of CNNs, we can efficiently calculate the required fitting expert assessment results by mining the correlation between the eigenvalues and the non-linear mapping between the input and output eigenvectors.

Generally, network-generated data can be divided into either batch data or stream data; however, the data in the field of network security situation have real-time and time-ordered characteristics, which is a typical stream data. There are bound to be limitations such as the effect of analyzing information at a specific time only. The analysis model should have the ability of online learning, i.e., the stream data generated in real-time should be iteratively processed to update and optimize its learning function. The CNN characteristics agree with this requirement; therefore, they are suitable for network security data analysis of large-scale liquidity.

B. CNN DATA INPUT

According to CNN characteristics, we should analyze the quantified network security data in the form of stream. Therefore, when using convolutional social networks to perform quantitative assessment of the wireless connected intelligent robot swarms network security situation, we are first required to design a wireless connected intelligent robot swarms network security index system; then quantify and standardize the selected index; and then form an equal-length multi-dimensional vector. In this manner, these vectors are combined into a data set $D = \{d1, d2, \ldots, dn\}$, which acts as an input to the model.

1) CONSTRUCTION OF WIRELESS CONNECTED INTELLIGENT ROBOT SWARMS NETWORK SECURITY INDEX SYSTEM

To meet the quantitative assessment requirements of wireless connected intelligent robot swarms network security situation, we designed a hierarchical assessment model of network security index system, which includes three dimensions: a basic operation index to reflect the basic state of wireless connected intelligent robot swarms network as well as certain security information and anti-risk capability; a vulnerability index to reflect the different types of security vulnerabilities existing in wireless connected intelligent robot swarms network and the severity of the impact of security vulnerabilities on network security; and a threat index to reflect the different elements of wireless connected intelligent robot swarms network attacks from outside and the severity of active attacks. To effectively measure the security state of the network from these aspects, it is necessary to further adopt assessment factors with smaller dimensions and assess the security state of the network in various aspects. The specific design is shown in the following figure 2.

a: BASIC OPERATION INDEX

An infrastructure operation index primarily considers whether it is sufficiently robust to perform its own working capacity from the aspects of wireless connected intelligent robot swarms network hardware and software capabilities, as well as security protection capabilities against external threats and actual loads. The basic operation index is used to reflect the basic state of the network and the safe operation of various programs; moreover, it is primarily divided into disaster tolerance and stability.

b: VULNERABILITY INDEX

A vulnerability index primarily considers the vulnerability of wireless connected intelligent robot swarms, i.e., the vulnerability of the network itself without attacks, e.g., how many attacks can the network withstand on its own and how much harm and loss can the attack bring to the network. The vulnerability index is extensively used in many network security index systems. In wireless connected intelligent robot

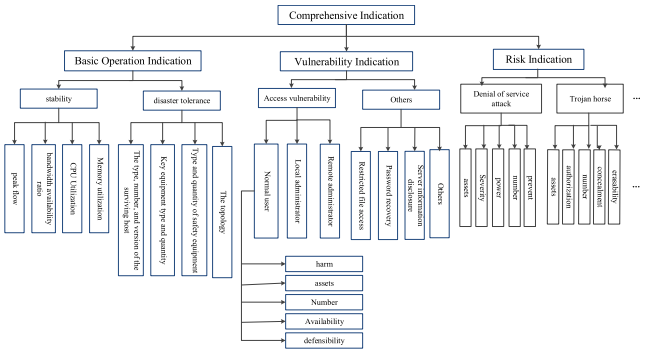


FIGURE 2. Construction of network security index system.

swarms network security index systems, the network disaster tolerance will be considered within the scope of vulnerability index.

c: THREAT INDEX

Threat index refers to quantitative function of the inherent risk brought by valuing assets owned by the network subject, the credibility of external threats, and the ease of exploiting vulnerabilities and security measures. In this study, the impact of threats, i.e., network attacks on wireless connected intelligent robot swarms is primarily considered, and the related index of threat dimension is collectively referred to as threat index. Network attacks exist in the form of network alarms, which are generated by event correlation analysis collected by multiple security devices. The hierarchical structure of the threat index corresponding to many network attacks is shown in the figure 2. Note that because of space constraints, there are many threat indices that have not been shown in the figure 2.

2) DATA QUANTIFICATION OF WIRELESS CONNECTED INTELLIGENT ROBOT SWARMS NETWORK SECURITY INDEX SYSTEM

After determining the wireless connected intelligent robot swarms network security index system, quantifying and normalizing the obtained network security data before it can be used as the input of CNN is necessary.

a: QUANTIFICATION OF BASIC OPERATION INDEX

First, the quantitative data are normalized, and the severity is measured by the overload rate of each index in each time period. The overload rate is defined as follows: $o_{ij} = k_{ij}/l_{ij}$ where i belongs to the integer set $\{1, 2, 3, 4\}$, representing peak traffic, bandwidth utilization, CPU utilization, and memory utilization, respectively; j is the range of node number from 1 to N; l_{ij} represents the threshold of attribute i in node j; k_{ij} represents the real value of attribute i in node j; and o_{ij} is the overload rate of attribute i in node j. Then, the overload rate is qualitatively quantified and divided into five grades according to certain rules, and then each grade is normalized.

For the disaster tolerance quantification of basic operation index, the number of surviving hosts, key equipment, and safety equipment are quantified using a linear normalization method, while the quantification process of other indexes can be qualitatively quantified according to the real environment.

b: QUANTIFICATION OF VULNERABILITY INDEX AND THREAT INDEX

We adopted the network vulnerability index and threat index calculation model based on a hierarchical index. Considering the network vulnerability index as an example, the network vulnerability index of a three-level index basic network is obtained via a hierarchical calculation principle. Then, the network vulnerability index of a secondary index basic network is calculated by a three-level index of the basic network. Finally, using the deep learning network, the final network security index obtained by the vulnerability index of secondary network and other secondary indexes is inputted. Note that the calculation of network vulnerability of a two-level index V is divided into two steps:

First, the secondary network vulnerability index is classified into n categories according to the vulnerability index classification criteria. Then, according to the three-level vulnerability data of each category, the basic vulnerability characteristic indexes $A_1, A_2, A_3, \ldots A_{m-1}, A_m$ of each category are determined. Finally, the corresponding secondary vulnerability index V is calculated from these characteristic indexes.

The secondary vulnerability index V of a certain network at time t is defined as follows:

$$V(t) = f(g(A_1(t)), g(A_2(t)), \cdots g(A_n(t))) \tag{1}$$

where $A_i(t)$ is the numerical value of the index A_i at t time and $g(A_i(t))$ is the normalized value of $A_i(t)$.

Note that function is a type of aggregation function that is used to calculate the vulnerability through the quantization value of characteristics of a class of events. Basically, the most commonly used aggregation function is the weighted sum method, i.e.

$$V(t) = \sum_{i=1}^{m} g(A_i(t)) \times w_i \quad where \ \sum_{i=1}^{m} w_i = 1, \quad w_i \geq 0 \tag{2}$$

where w_i is the weight of the index, and the rationality and accuracy of the weight directly affect the reliability of the evaluation results.

3) DATA INPUT MODE

After quantifying and standardizing the wireless connected intelligent robot swarms network security data, these data should be constructed into multi-dimensional vectors of equal length. Then, these vectors are composed of data set $D = \{d_1, d_2, \ldots, d_n\}$. Finally, it is inputted into the CNN. Note that the data input mode directly affects the training and learning effect of CNN; therefore, we design different data combination input modes and determine its effect via testing.

a: RANDOM DATA COMBINATION INPUT

This is the simplest way of data input. We randomly arranged the data of leaf nodes in the network security index system into analog image data of m rows × n columns. The output is 10 network security levels; however, after normalizing the input data, its value is limited to 0-1, while the output is limited to 0-9.

b: SUBNETTING DATA INPUT MODE

The network security data is divided into n subnets. Therefore, di in $D = \{d_1, d_2, \ldots, d_n\}$ is the network security index data collected in a subnet. Each di is sorted according to three dimensions: basic operation dimension, vulnerability dimension, and threat dimension, i.e., di = (X indexes of basic operation dimension; Y indexes of vulnerability dimension; and Z indexes of threat dimension).

c: GROUPED DATA INPUT MODE

In the training process of CNN, whether the training data of the same batch (i.e., the set of different two-dimensional data sets provided for joint training in a single training) have similar size and weight characteristics will have considerable impact on the training effect of the deep learning network; therefore, we can try to improve the input mode 2. The training data can be grouped in advance, and the data sets with the same characteristics can be considered in the same training batch to try to improve the model's accuracy.

Data input is set to m rows × n columns of analog image data. Note that n columns of data represent n different network subnets, and each row of data represents different collection data of a basic network security index data in n subnets. Furthermore, for the same batch of data, the m rows × n columns of data have similar size characteristics, and the similar security level output can be obtained.

C. CONSTRUCTING THE MODEL STRUCTURE

1) CONVOLUTION

Figure 1 shows that the first layer of convolution operation extracts features from input data by sliding the 1 × n 1D convolution kernel window. Moreover, other deeper convolutions are similar to this operation. Therefore, for the input data x, we defined the convolution calculation of feature map σ of layer m as follows:

$$c_\sigma^m(x) = f\left(\sum w^{(m,\sigma)} p_i^{(m-1)} + b^{(m,\sigma)}\right), \quad \sigma = 1, 2, \cdots, n. \tag{3}$$

$c_\sigma^m(\mathrm{x})$ denotes the output of feature extraction of the upper layer by the convolution kernel σ of the layer m; $w^{(m,\sigma)}$ denotes the weight parameter of convolution kernel σ of the layer m; $p_i^{(m-1)}$ denotes the ith feature map in the layer m-1; $b^{(m,\sigma)}$ is the bias value; and $f(\cdot)$ is the activation function. We have used the ReLU function at this instance.

TABLE 1. Weight training update rules.

1	***while***
2	***do*** Forward propagation of input signal
3	E Calculate the error E between the expected value and the target value
4	***if*** E convergence
5	***end all***
6	***else*** Update the weight w′ of the last layer by using equation 5
7	***do*** E is propagated back to the upper level and w is updated with equation 5
8	***while*** Not reaching the first input layer

2) POOLING

For each convolution feature map, the 1D maximum pooling layer can be used for downsampling.

$$s_\sigma^m = \text{maximum pooling}\left(c_\sigma^{m-1}\right) + b^{(m,\sigma)} \tag{4}$$

The pooling operation is primarily used to rapidly shrink the network scale, better highlight the summary statistical characteristics, reduce noise interference, and effectively overcome over-fitting.

3) OUTPUT

The output is $\mathrm{Pre} = \{\mathrm{pr1}, \mathrm{pr2}, \ldots, \mathrm{prn}\}$, and the input index is converted into the predicted value by function calculation.

4) CALCULATION

The model uses a back propagation algorithm to calculate the weight. For layer m of the network, the calculation weight of the ith input feature and the jth output feature are updated as follows:

$$\Delta w_{ij} = \alpha \delta_j P_i. \tag{5}$$

If the layer m is the last layer, δj in the above equation can be calculated as follows:

$$\delta_j = \left(T - C_j\right) d'(P_i) \tag{6}$$

where $d'(p)$ is the derivative of a function. Moreover, if layer m is not the last layer, δ_j in Equation (5) can be calculated as follows:

$$\delta_j = d'(P_i) \sum_{k=1}^{N_{m+1}} w_{jk} \tag{7}$$

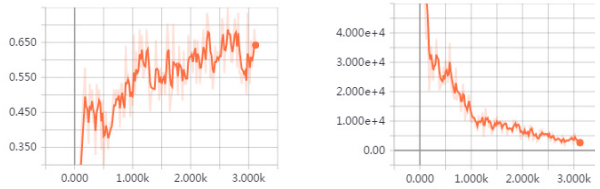
Note that k is the kth output of layer m + 1 and j is the jth output of layer m. Therefore, the training process can be constructed as shown in Table 1:

D. SETTING OF MODEL PARAMETERS

Considering the learning efficiency and the total amount of computation, using smaller convolution kernels can help construct a relatively deep model. Although it seems more complex, this approach works better than the traditional shallow network with additional connections. Thus, we constructed

TABLE 2. Initial setting of model parameters.

Parameters	Setting
Convolution kernel size	1@2@3@ : 1*4 , 4@5@ : 1*3
Number of convolution kernels	64*5
Sliding step of convolution kernel	1
Pooling method	Max
Pooling window size	1*2
Sliding step of pooling window	2
Activation function	Relu
Dropout	0.5
Full connective layer neurons	100
Parametric solution algorithm	Rmsprop
Loss function	Mean_Squared_Error



(a) Precision rat (b) Loss

FIGURE 3. Experiment effect diagrams of random data combination input mode.

a five-layer hidden layer part. To calculate the convolution, the first three layers and the last two layers use 1×4 and 1×3 convolution kernels, respectively. Table 2 lists the key parameters.

IV. EXPERIMENTAL ANALYSIS

A. EXPERIMENTAL DATA

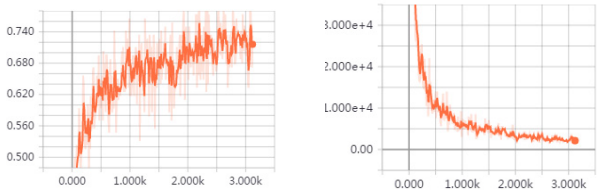
Currently, there is no open test data set for the quantitative analysis of wireless connected intelligent robot swarms network security situation. For this experiment, we used network security data of wireless connected intelligent robot swarms simulation system for 6 months and extracted 3150K of representative manually annotated historical data in our cyber range environment [31]. We selected 28 specific indexes for corresponding preprocessing from the designed index system, and the magnitude of data was unified using the standard normalization method. We used the 3000K data as the training set and the 150K data as the test set.

B. EXPERIMENTAL RESULTS AND ANALYSIS

1) ANALYSIS OF THE INFLUENCE OF DIFFERENT DATA INPUT MODES ON THE LEARNING EFFECT OF CNN

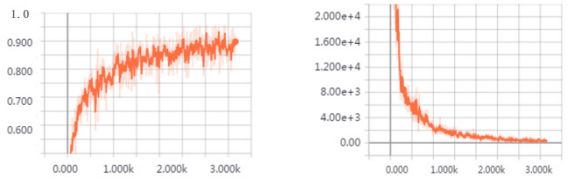
We used the same CNN model and parameter setting in which the batch number of the same input was 64. The effects of the three different data input modes discussed in section "B. CNN Data Input" were compared and tested.

Figure 3 shows the experimental results of the random data combination input mode. The left image is the precision image, the right image is the loss image, the dashed line is



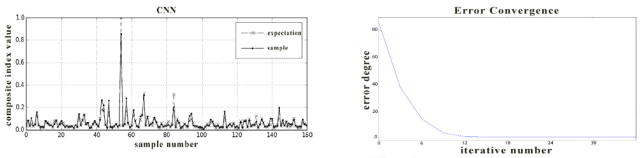
(a) Precision rat (b) Loss

FIGURE 4. Experimental effect diagrams of subnetting data input mode.



(a) Precision rat (b) Loss

FIGURE 5. Experiment effect figure of grouped data input mode.



(a) Fitting of CNN (b) CNN error convergence

FIGURE 6. Calculation results of CNN model.

the direct data result of the actual experiment, and the real line is the data result after smoothing by fitting parameter smoothing (smoothing = 0.6). The highest precision rate of a single test is 74%, and the fluctuation range is considerably large; therefore, the test effect is not good.

Figure 4 shows the experimental results of subnetting data input mode. Note that the highest precision rate can reach 82%. The overall effect is better than the data input mode of random data combination; however, the problem that the training effect fluctuates considerably does exist.

Figure 5 shows the experimental results of grouped data input mode, and the highest precision rate is 95%. From the experiments, we observe that the same batch of training data using data sets of similar size and weight characteristics can effectively reduce the fluctuation of training curve and improve the precision rate. Thus, the experiment effect is generally improved.

2) EFFECT ANALYSIS OF WIRELESS CONNECTED INTELLIGENT ROBOT SWARMS NETWORK SECURITY SITUATION QUANTIFICATION ASSESSMENT BASED ON CNN

We inputted the pre-processed experimental training data into the CNN model using a grouped data input method. After multiple training, the function achieved the self-trained learning artificial evaluation effect. As shown in Figure 6, the function error reached the optimal convergence after the

TABLE 3. Comparison of regression evaluation indexes.

	EVS	MAE	MSE	R2 Score
LR	0.7325	0.0169	0.0007	0.7321
BPNN	0.7920	0.0142	0.0005	0.7920
MLP	0.7594	0.0155	0.0006	0.7567
KRR	0.7092	0.0167	0.0007	0.6986
CNN	0.8011	0.0137	0.0005	0.7913

39th iteration; thus, it automatically stopped the iterative convergence. If we compare the calculated results of the learned function model with the labeled expected values, the results can be fitted well.

3) COMPARISONS BETWEEN CNN AND OTHER DEEP LEARNING MODELS

In this study, to objectively understand the calculation effect of the model, we placed the experimental data into linear regression, back propagation neural network, multi-layer perceptro and kernel ridge regression to compare the computational results using CNN. We used four evaluation indices, i.e., explained variance score, mean absolute error, mean squared error (MSE), and goodness of fit R2 Score, to assess the performance of the regression equation. On comparing multiple models, CNN performs better than other models except for the R2 Score. The experimental results are shown in Table 3.

V. CONCLUSION

The wirelessly connected intelligent robot swarms are more vulnerable to be attacked due to their unstable network connection and limited resources, and the consequences of being attacked are more serious than other systems [32]–[35]. Therefore, the quantitative assessment of wireless connected intelligent robot swarms network security situation is very important. Traditional quantitative assessment methods of network security situation mostly rely on artificial evaluation. Note that the index weight determined by them is fuzzy, the set value fluctuates considerably sometimes, and they lack adaptability when facing different cyberspace and different factors of concern. Therefore, in this study, we present a quantitative assessment method of network security situation based on CNN. We used the convolutional layer to locally detect and deeply extract the feature, and the pooling layer is used to rapidly shrink the network scale and highlight the summary features. Using the deep network structure of several hidden layers, the process of comprehensive quantitative assessment of network security situation by fitting the expert experience is finally realized using adaptive characteristics such as online learning. Moreover, by experimental comparison, in this study, we combine the characteristics of network security index system and CNN to achieve a better quantitative assessment of network security situation. Note that the calculation results are better than those of other models.

REFERENCES

[1] A. F. T. Winfield, W. Liu, A. Martinoli, and J. Nembrini, "Modelling a wireless connected swarm of mobile robots," *Swarm Intell.*, vol. 2, nos. 2–4, pp. 241–266, 2008.

[2] J. D. Bjerknes, A. F. T. Winfield, and C. Melhuish, "An Analysis of emergent taxis in a wireless connected swarm of mobile robots," in *Proc. Swarm Intell. Symp.*, 2007, pp. 45–52.

[3] Z. Tian, S. Su, W. Shi, X. Du, M. Guizani, and X. Yu, "A data-driven method for future Internet route decision modeling," *Future Gener. Comput. Syst.*, vol. 95, pp. 212–220, Jun. 2019.

[4] F. Awad, M. Naserllah, A. Omar, A. Abu-Hantash, and A. Al-Taj, "Collaborative indoor access point localization using autonomous mobile robot swarm," *Sensors*, vol. 18, no. 2, p. 407, 2018.

[5] Z. Tian, X. Gao, S. Su, J. Qiu, X. Du, and M. Guizani, "Evaluating reputation management schemes of Internet of vehicles based on evolutionary game theory," *IEEE Trans. Veh. Technol.*, vol. 68, no. 6, pp. 5971–5980, Jun. 2019.

[6] A. F. T. Winfield and J. Nembrini, "Safety in numbers: Fault tolerance in robot swarms," *Int. J. Model. Identificat. Control*, vol. 1, no. 1, pp. 30–37, 2006.

[7] Y. Wang, J. Wang, H. Li, and Z. Xu, "Assessing cyber-threats situation for electric power information networks," in *Proc. Int. Conf. Natural Comput.*, 2013, pp. 1557–1562.

[8] Q. Chen and H. Ou, "Research on IMS core network security index system," *Telecommun. Sci.*, vol. 8, pp. 12–20, 2014.

[9] X. Cheng, S. Lang, "Research on network security situation assessment and prediction," in *Proc. 4th Int. Conf. Comput. Inf. Sci.*, vol. 11, 2012, 118–127.

[10] Z. Xuan, "Survey of network security situation awareness and key technologies," *Electron. Test*, vol. 8, pp. 3281–3286, 2017.

[11] J. Li, H. Xie, and J. S. Wang, "Construction of wireless network vulnerability evaluation index system based on knowledge reduction," *J. Nanjing Univ. Inf. Technol.*, vol. 1, pp. 58–62, Jan. 2019.

[12] J. Zhang, F. Liu, Y. Jia, P. Zou, and W. Han, "Research and implement of configurable network security index system," in *Proc. Int. Conf. Appl. Robot. Power Ind.*, 2012, pp. 645–648.

[13] L. Ming, D. Wang, L. Zhang, X. Kuang, J. Tang, C. Wang, and L. Zhang, "Index system of network security and survivability," in *Proc. 1st Int. Conf. Instrum., Meas., Comput., Commun. Control.*, 2018, pp. 848–851.

[14] Y. Ou, J. Xie, and J. Ling, "An improved network terminal security evaluation index system," in *Proc. Int. Conf. Manage. e-Commerce e-Government*, 2014, pp. 65–69.

[15] W. Huang and J. W. Stokes, "MtNet: A multi-task neural network for dynamic malware classification," in *Proc. 5th Int Conf. Detection Intrusions Malware, Vulnerability Assessment*. Berlin, Germany: Springer, 2016, pp. 399–418.

[16] B. Kolosnjaji, A. Zarras, G. Webster, and C. Eckert, "Deep learning for classification of malware system call sequences," in *Proc. 30th Australas. Joint Conf. Artif. Intell.* Berlin, Germany: Springer, 2016, pp. 137–149.

[17] S. Tobiyama, Y. Yamaguchi, T. Ikuse, T. Yagi, and H. Shimada, "Malware detection with deep neural network using process behavior," in *Proc. IEEE 8th Int Conf Comput. Softw. Appl.*, Piscataway, NJ, USA, Jun. 2016, pp. 577–582.

[18] J. Kim, J. Kim, H. L. T. Thu, and H. Kim, "Long short term memory recurrent neural network classifier for intrusion detection," in *Proc. IEEE 22nd Int. Conf. Platform Technol. Service*, Piscataway, NJ, USA, Feb. 2016, pp. 49–54.

[19] M. A. Salama, H. F. Eid, A. Darwish, A. E. Hassanien, and R. A. Ramadan, "Hybrid intelligent intrusion detection scheme," in *Soft Computing in Industrial Applications*. Berlin, Germany: Springer, 2011, pp. 293–303.

[20] B. Abolhasanzadeh, "Nonlinear dimensionality reduction for intrusion detection using auto-encoder bottleneck features," in *Proc. IEEE 7th Conf. Inf. Knowl. Technol.*, Piscataway, NJ, USA, May 2015, pp. 26–31.

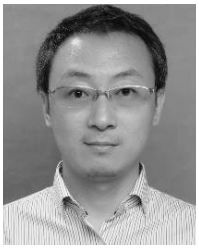
[21] M. Z. Alom, V. Bontupalli, and T. M. Taha, "Intrusion detection using deep belief networks," in *Proc. IEEE 9th Conf. Aerosp. Electron.*, Piscataway, NJ, USA, Jun. 2015, pp. 339–344.

[22] R. C. Aygun and A. G. Yavuz, "Network anomaly detection with stochastically improved autoencoder based models," in *Proc. IEEE 4th Int. Conf. Cyber Secur. Cloud Comput.*, Piscataway, NJ, USA, Jun. 2017, pp. 193–198.

[23] L. Xie, Y. Wang, and Y. U. Jinbo, "Network security situation awareness based on neural networks," *J. Tsinghua Univ.*, vol. 53, no. 12, pp. 1750–1760, 2013.

[24] C. Tang, Y. Xie, X. Wang, R. Zhang, and B. Qiang, "Security situation prediction based on dynamic BP neural with covariance," *Procedia Eng.*, vol. 15, pp. 3313–3317, Aug. 2011.
[25] Z. Tian, W. Shi, Y. Wang, C. Zhu, X. Du, S. Su, Y. Sun, and N. Guizani, "Real-time lateral movement detection based on evidence reasoning network for edge computing environment," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4285–4294, Jul. 2019.
[26] Z. Tian, M. Li, M. Qiu, Y. Sun, and S. Su, "Block-DEF: A secure digital evidence framework using blockchain," *Inf. Sci.*, vol. 491, pp. 151–165, Jul. 2019. doi: 10.1016/j.ins.2019.04.011.
[27] L. Huang, J. Huang, and W. Wang, "The sustainable development assessment of reservoir resettlement based on a bp neural network," *Int. J. Environ. Res. Public Health*, vol. 15, no. 1, p. 146, 2018.
[28] T. N. Sainath, B. Kingsbury, G. Saon, H. Soltau, A.-R. Mohamed, G. Dahl, and B. Ramabhadran, "Deep convolutional neural networks for large-scale speech tasks," *Neural Netw.*, vol. 64, pp. 39–48, Apr. 2015.
[29] C. Ding and D. Tao, "Trunk-branch ensemble convolutional neural networks for video-based face recognition," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 40, no. 4, pp. 1002–1014, Apr. 2018.
[30] Q. Tan, G. Yue, J. Shi, X. Wang, B. Fang, and Z. Tian, "Toward a comprehensive insight into the eclipse attacks of tor hidden services," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1584–1593, Apr. 2019.
[31] Z. Tian, Y. Cui, L. An, S. Su, X. Yin, L. Yin, and X. Cui,"A real-time correlation of host-level events in cyber range service for smart campus," *IEEE Access*, vol. 6, pp. 35355–35364, 2018. doi: 10.1109/ACCESS.2018.2846590.
[32] K. Zhang, Y. Zhu, S. Leng, Y. He, S. Maharjan, and Y. Zhang, "Deep learning empowered task offloading for mobile edge computing in urban informatics," *IEEE Internet Things J.*, to be published.
[33] Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A survey of key management schemes in wireless sensor networks," *Comput. Commun.*, vol. 30, nos. 11–12, pp. 2314–2341, Sep. 2007.
[34] K. Zhang, S. Leng, X. Peng, L. Pan, S. Maharjan, and Y. Zhang, "Artificial intelligence inspired transmission scheduling in cognitive vehicular communications and networks," *IEEE Internet Things*, vol. 6, no. 2, pp. 1987–1997, Apr. 2019.
[35] X. Du and H. H. Chen, "Security in wireless sensor networks," *IEEE Wireless Commun. Mag.*, vol. 15, no. 4, pp. 60–66, Aug. 2008.

WEIHONG HAN received the Ph.D. degree from the Cyberspace Institute of Advanced Technology, Guangzhou University, where she is currently a Professor and Ph.D. Supervisor. From 2002 to 2017, she was with the National University of Defense Technology. Her current research interests include computer networks and network security. She is also a member of the CyberSecurity Association of China.



ZHIHONG TIAN received the Ph.D. degree from the Cyberspace Institute of Advanced Technology, Guangzhou University, where he is currently a Professor, a Ph.D. Supervisor, and the Dean. From 2003 to 2016, he was with the Harbin Institute of Technology. His current research interests include computer networks and network security. He is also the Standing Director of the CyberSecurity Association of China and a member of the China Computer Federation.

ZIZHONG HUANG received the master's degree from the Computer School, National University of Defense Technology, where he is currently a Senior Engineer. His current research interests include big data mining and network security.

DONGQIU HUANG is currently pursuing the master's degree (Fang Binxing Class) with the Cyberspace Institute of Advanced Technology, Guangzhou University. Her tutor is Prof. Z. Tian.

YAN JIA received the Ph.D. degree from the Computer School, National University of Defense Technology, where she is currently a Professor and a Ph.D. Supervisor. Her current research interests include big data mining and network security. She is also the Standing director of the CyberSecurity Association of China and a member of the China Computer Federation.