Efficient Intrusion Detection Based on Multiple Neural Network Classifiers with Improved Genetic Algorithm

Yuesheng Gu
Department of Computer Science, Henan Institute of Science and Technology, Xinxiang 453003, China
College of Computer Science and Technology, Wuhan University of Technology, Wuhan 430070, China
Email: hz34567@126.com

Yongchang Shi
College of Computer Science and Technology, Pingdingshan University, Pingdingshan 467000, China
Email: tsjksyc@163.com

Jianping Wang
Department of Computer Science, Henan Institute of Science and Technology, Xinxiang 453003, China
Email: xunji2002@163.com

***Abstract*—The security of computer network is one of the most important issues for all the users. Intrusion may lead to terrible disaster for network users. Therefore, it is imperative to detect the network attacks to protect the information security. The intrusion patter identification is a hot topic in this research area. Using artificial neural networks (ANN) to provide intelligent intrusion recognition has been received a lot of attentions. However, the intrusion detection rate is often affected by the structure parameters of the ANN. Improper ANN model design may result in a low detection precision. To overcome these problems, a new network intrusion detection approach based on improved genetic algorithm (GA) and multi-ANN classifiers is proposed in this paper. The improved GA used energy entropy to select individuals to optimize the training procedure of the BPNN, RBF, PNN and Fuzzy-NN. Then, the satisfactory ANN models with proper structure parameters were attained. In addition, to alleviate the complexity of the input vector, the principal component analysis (PCA) has been employed to eliminate redundant features of the original intrusion data. The efficiency of the proposed method was evaluated with the practical data, and the experiment results show that the proposed approach offers a good intrusion detection rate, and performs better than the standard GA-ANN method.**

***Index Terms*—intrusion detection, artificial neural network, improved Genetic Algorithm, PCA**

I. INTRODUCTION

Network security is a world hot topic in computer security and defense. Intrusion may lead to absence of the internet service and even cripple the whole system for weeks. Hence, it is very important to detect the intrusion in time to prevent broken-downs. Advanced machine learning algorithm, including evolution algorithm, intelligent artificial neural network (ANN) and support vector machine (SVM) and so on, are all appear in the intrusion detection of the networks [1-2]. Among them, ANN [3] is the most extensive used method. However, ANN detection performance is mainly determined by its structural parameters. It is often difficult to determine the ANN parameters without a large number of trials. Although [4] and [5] using GA to tune the ANN structures to improve the network attack detection accuracy, but without considering the GA individual selection adjustment, and just using the KDD dataset to validate their methods, not for practical applications. Therefore, to improve the GA optimization process and to test the real dataset will have important significance for the ANN based intrusion detection [6-10].

In order to solve the above problems, this paper proposed a new intrusion detection method. This method has been marked to achieve multi-ANNs' parameter optimization using improved GA. Moreover, the PCA has been used to the feature selection. It indicates that the feature selection is very essential in the intrusion detection because the original feature space have many useless features to influence the intrusion identification. Eliminate these redundant ones can enhance the intrusion detection rate significantly. By using the practical dataset for experimental analysis, the analysis results show that the proposed new method can detect the network attack efficiently and the detection rates is higher than the standard GA based method.

This paper is organized as follows. In Section 2, the proposed hybrid intelligent method for network intrusion detection based on the combination of PCA, GA and ANNs is described. The application of the proposed method is presented for network intrusion detection in Section 3. The performance of the feature selection using PCA, as well as the network intrusion detection performance is described. The effectiveness of the

doi:10.4304/jsw.7.7.1641-1648

proposed method is valued by analyzing the real data. Conclusions are drawn in Section 4.

II. New Intelligent Model

Due to the interference of inside and external excitations, the network intrusion is a kind of typical non-stationary signal. The different signal components of the network intrusion data exhibit various characteristics, and make a difference between the normal and intrusions. One of the most important procedures in the network intrusion detection is to find out distinguished features to differentiate the intrusion cases from the large amount date sets. However, it is always difficult in choosing an effective feature. Fortunately, the PCA is a powerful tool to select most distinct features from a large amount of characteristics. Therefore, the PCA has been adopted to improve the feature extraction ability of the original data. Meanwhile, ANN is an intelligent approach to deal with non-stationary signal. With its strong learning ability, the ANN is quite suitable for practical intrusion detection. However, its identification efficiency depends on the structure design. This is why the GA optimization is applied to the ANN design. By doing so, satisfactory ANN detection model can be gotten, and consequently the detection rate can be improved.

A. Principal Component Analysis (PCA)

Given sample space $X = \{x_1, x_2, ..., x_n\}$, $x_k \in R^m$ is an *m* dimension column, *n* is total sample number. Suppose the linear transform for X is [11]

$$F_i = a_i^T X = a_{1i}X_1 + a_{2i}X_2, \cdots + a_{ni}X_n, \quad i = (1, 2, \cdots n). \tag{1}$$

Then the covariance matrix for *F* is that

$$\bar{C} = a_i^T \sum a_j \ (i, j = 1, 2, \cdots n). \tag{2}$$

According to $\lambda V = \bar{C}V$, it can calculate the Eigen value λ and eigenvector *V* for Eq. (2), so

$$V = \sum_{i=1}^{n} \alpha_i x_i, \tag{3}$$

$$\lambda = x_k \cdot \bar{C}V. \tag{4}$$

Arrange Eigen value λ in the descending order, then the high dimension space *X* can be transformed in a linear space *Y*:

$$Y = V^T X, \tag{5}$$

According to the 85% criteria, select the first *p* components ($p < m$) in *Y* as principal components, thus realize the dimension reduction for data *X*.

B. Improved GA

Standard GA [12] involves the following procedures: coding, selection, crossover, and mutation. In the selection, standard GA only searches individuals with adaptive value. The diversity of the population is constrained, which may lead to premature convergence of the GA optimization [13]. To deal with this situation, the energy entropy based selection is employed to increase the diversity of population. As GA selects according to the individuals' energy, it need to calculate each individual *z*. The individual energy entropy can be expressed as

$$E(t) = In(\frac{1}{p_t}), \tag{6}$$

Where, p_t denotes energy probability at lever *t*. By the annealing selection, we can derive the individual selection probability [14]

$$P(z_i) = e^{-(E(z_i)+\beta f(z_i))} / \sum_{i=1}^{n} e^{-(E(z_i)+\beta f(z_i))}, \tag{7}$$

where, $P(z_i)$ denotes the probability of individual z in new population, $E(z_i) + \beta f(z_i)$ denotes fitness value of individual z.

After the energy entropy based individual selection procedure, the link between individuals is connected and hence to maintain the diversity of population.

C. Back Ppropagation Neural Network (BPNN)

A neural network has a natural propensity for storing experiential knowledge and making it available for use. Then the Input-Output Mapping property and capability can be provided by the ANNs [15-20]. One of the most commonly used supervised ANN model is BPNN. BPNN is the multilayer feed forward network trained according to error back-propagation algorithm. BP can learn and store a lot of input-output model mapping relationship without revealing and describing the mapping mathematical equation in advance. Its learning rule is by using steepest descent method, through back-propagation to adjust the weights and threshold continuously, thus to make the minimum network error quadratic sum [20]. The structure of BPNN is arranged into different layers: input layer, middle layer and output layer, as illustrated in Fig 1.

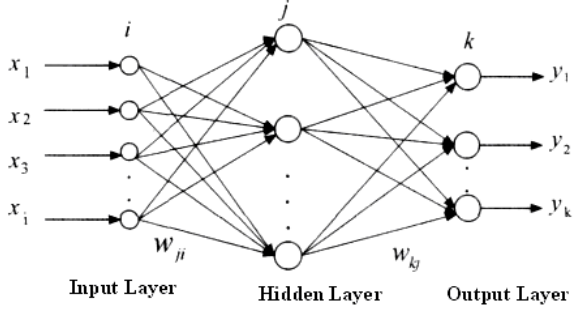

Figure 1. Structure of BP neural network.

When multi-layer network learns algorithm by using BP, in fact, it contains two stages: forward propagation and back propagation. In the forward propagation process, the input information is processed layer by layer: from input layer to hidden layer, and then transmitted to the output layer. The neurons of each layer only affect those on next layer. If the desired output cannot be gotten on the output layer, it will turn to back propagation, the error signal will return along the original channel. By modifying the neuron weights of each layer to decrease the error signal until it reaches the required precision.

D. Probabilistic neural network (PNN)

Probabilistic neural network (PNN) is predominantly a classifier [21]. A PNN is an implementation of a statistical algorithm called kernel discriminate analysis in which the operations are organized into a multilayered feed forward network with four layers: the input layer, pattern layer, summation layer and output layer, as illustrated in Fig 2.

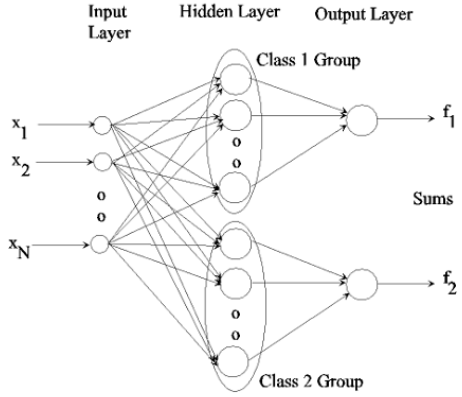

Figure 2. Structure of Probabilistic neural network.

The input nodes are the set of measurements. The second layer consists of the Gaussian functions formed using the given set of data points as centers. The third layer performs an average operation of the outputs from the second layer for each class. The fourth layer performs a vote, selecting the largest value. The associated class label is then determined. Each hidden node in the group for class *k* corresponds to a Gaussian function centered on its associated feature vector in the *k*th class (there is a Gaussian for each exemplar feature vector). All of the Gaussians in a class group feed their functional values to the same output layer node for that class, so there are *K* output nodes.

Once the PNN is defined, then we can feed vectors into it and classify them as follows:

(1) Read input vector and feed it to each Gaussian function in each class;

(2) For each group of hidden nodes, compute all Gaussian functional values at the hidden nodes;

(3) For each group of hidden nodes, feed all its Gaussian functional values to the single output node for that group;

(4) At each class output node, sum all of the inputs and multiply by constant;

(5) Find maximum value of all summed functional values at the output nodes.

E. Radial Basis Function (RBF)

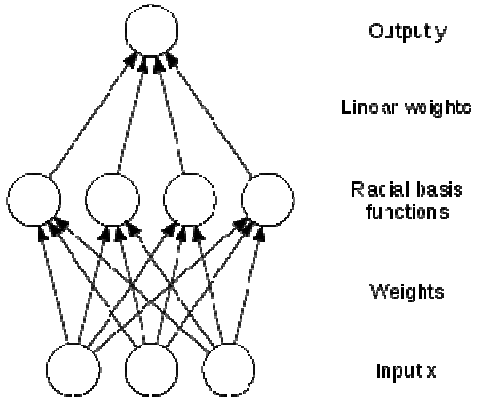

Figure 3. Structure of RBF neural network.

Radial basis function (RBF) neural network adopts supervised learning and is good at modeling nonlinear data and can be trained in one stage rather than using an iterative process [22]. The RBF network has a feed forward structure consisting of three layers, as illustrated in Fig 3.

Input layer – there is one neuron in the input layer for each predictor variable. In the case of categorical variables, N-1 neurons are used where N is the number of categories. Hidden layer – this layer has a variable number of neurons (the optimal number is determined by the training process). Each neuron consists of a radial basis function centered on a point with as many dimensions as there are predictor variables. Summation layer – the value coming out of a neuron in the hidden layer is multiplied by a weight associated with the neuron (W_1, W_2, ...,W_n) and passed to the summation which adds up the weighted values and presents this sum as the output of the network.

The following parameters are determined by the training process:

(1) The number of neurons in the hidden layer.

(2) The coordinates of the center of each hidden-layer RBF function.

(3) The radius (spread) of each RBF function in each dimension.

(4) The weights applied to the RBF function outputs as they are passed to the summation layer.

F. Fuzzy Neural Network (FNN)

Since the integrated fuzzy logic and ANN provides more powerful learning ability, we use the fuzzy-artificial neural network (FNN) to detect the intrusion in this paper.

Fuzzy method is used in various problems. However, the determination of membership functions depends on human experts and experiences, resulting in time-consuming and lack of self-adaptation. To overcome this problem, the artificial neural network (ANN) has been applied to auto-tune the membership functions of the fuzzy inference. The structure of fuzzy neural network is shown in Fig. 4.

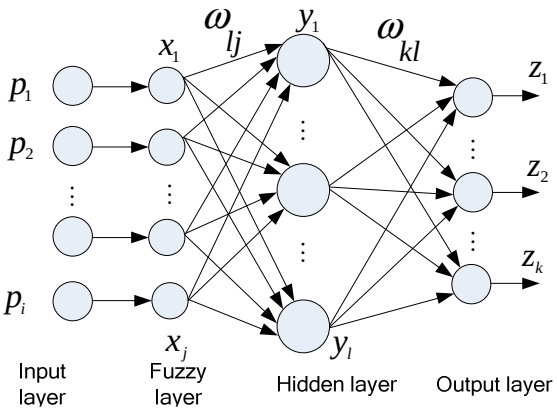

Figure 4. Structure of fuzzy neural network.

The FNN consists of four layers. The input layer connects with input feature vector $P=[p_1, p_2,..., p_i]^T$. The fuzzy layer is used to fuzz each input p_i to get corresponding fuzzy membership values $x_j=\mu_{Aij}(p_i)=[q_{1j}, q_{2j},..., q_{ij}]^T$. The Gaussian function was adopted as the fuzzy membership function, that is

$$\mu_{Aij}(p_i)=\exp[-(\frac{p_i-a_{ij}}{b_{ij}})^2], \quad (8)$$

where a_{ij} is the center of membership function and b_{ij} is the width of the function. Hence, the output of the fuzzy layer is $\mathbf{X}=[x_1, x_2,..., x_j]$. In the hidden layer, for the l neuron nodes, the weights ω_{lj} were used as the fuzzy relation matrix to perform fuzzy inference rules. Then the singleton output of the lth fuzzy rule is

$$y_l(x_j)=\omega_j x_j. \quad (9)$$

The fourth layer outputs the fuzzy decision of the FNN. The weighted average method for inverse fuzzy was used in this paper. It can be noticed that the main purpose of the FNN is to optimize the coefficients of a_{ij}, b_{ij}, ω_{lj} and ω_{kl}.

III. The Proposed Detection Model

In recent years, artificial neural networks (ANN) are proven to be an alternative way to simulate complex nonlinear problems. Once trained, ANN can provide predictions and generalizations with satisfactory performance. However, ANN may not guarantee the global optimal solution [7]. Hence, the hybrid ANN with other approaches has been proposed to search for better performance. These combinations include fuzzy logic, wavelet transform and genetic algorithm (GA), etc. Among them, the GA solves the optimization problem by mimicking the principle of biological evolution, and it is also cost-effective and less time consuming technique. Therefore, GA optimized ANN can form an efficient method for predicting and optimizing any complex process parameters. In the light of this advantage, in this paper the multi-ANNs with improved GA optimization have been used for the network intrusion detection.

The improved GA was used to optimize the structural parameters of the ANNs. The GA begins with random population defined by the problem at hand. Hereby, the neuron number of the above four ANNs' hidden layers and their weight coefficients. The operation processing is followed by the series of GA activities, such as encoding, fitness evaluation, selection, and genetic operations (reproduction, crossover and mutation). However, before the GA optimization, the PCA is used to reduce the dimension of the ANN inputs. By doing so, the training calculation may be decreased.

Usually, the intrusion data contains many features that indicate the intusion activities. The famous data sets are the KDD 99 data, for example. The data sets are recorded by the US defense advanced research (DARPA) plan alliance for intrusion detection system evaluation. The data are divided into training sets and testing sets, and each dataset contains five types of test data: Normal, DoS, Probe, R2L and U2R. Each data describes 41 attribute of the network connection, such as: duration, service type, the bytes issued from source to destination, the bytes from destination to source, etc. However, the high dimension of the 41 features may lead to large training computation and the training result may not as good as desired. Hence, the PCA has been adopted to fuse the 41 featurs into several representations in a low dimension.

The inputs of the PCA are the feature space of the KDD 99 training data, $F_{41\times5000}$, where 5000 is the sample number and 41 is the feature number of each sample.

The original feature space F was firstly transformed in a linear space Y, and the cumulative percent of each eigenvector was also calculated. Then, the 85% criteria was adopted to check the first several eigenvectors, and select the first p (p<41) components in Y as the extracted principal components. Thus the original feature space F was projected to a low space to get new feature space $P_{p\times5000}$.

The new feature space $P_{p\times5000}$ is treated as the input of the ANNs. The details of the improved GA optimization are given as follows: (1) for the BP NN, the improved GA is used to optimize the neuron number of the hidden layer and the weight matrix connecting the input layer and hidden layer; (2) for the PNN, the improved GA is used to optimize the neuron number of the hidden layer and the center parameters of the Gaussian functions; (3) for the RBF NN, the improved GA is used to optimize the neuron number of the hidden layer and the weight matrix connecting the input layer and hidden layer; (4) for the FNN, the improved GA is used to optimize the coefficients of a_{ij}, b_{ij}, ω_{lj} and ω_{kl}.

The improved GA first encodes the coefficient values to form chromosomes, and then performs replication, crossover and mutation to evolve the chromosomes.

Lastly, use the optimal chromosome to represent network weight and membership function coefficients. In the GA searching processing, the fitness function plays an important role in the optimization result. To ensure the searching precision, the following fitness function was used:

$$F=\frac{1}{e(q)},\quad \text{and} e(q)=\frac{1}{2}\sum_{p}\sum_{k}(z_k-T_k)^2, \tag{10}$$

where, $q(q = 1,\cdots, N)$ is the chromosome number, p is training sample number, T_k is desired output, and z_k is the real output of the ANN.

The GA optimization processing was continued until the fitness value of the strings came out to a very high value. The proposed network intrusion detection processes are given as follows:

Step 1: Pre-treat the original network intrusion data to standardized data format.

Step 2: Extract distinct features from the input network intrusion data in the form of principal components (PCs) by PCA.

Step 3: Train the multi-ANNS using the PCs, optimize the ANN structures by improved GA, and determine the network intrusion detection result according to each ANN model output.

Step 4: Test the performance of the proposed network intrusion detection model, and provide the test result as the base for a valid network intrusion management decision. A flow chart of the proposed network intrusion detection method is illustrated in Fig. 5.

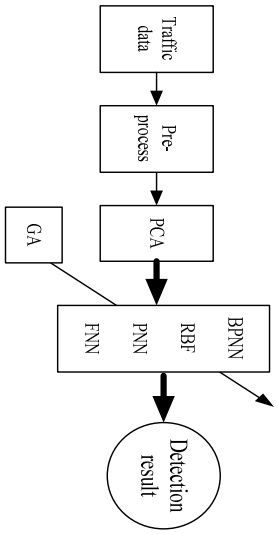

Figure 5. The network intrusion detection system based on PCA-GA-ANNs.

IV. Experimental Analysis

In order to validate the performance of the proposed algorithm, the intrusion experiments were carried out in real practice application in this paper. The experiment environment is shows in Fig. 6. It consists of a Linux server, a Windows server, the web link, a Linux host and two Windows hosts. We have adopted the experimental method that used in the KDD 99 collection by MIT. The only difference to the KDD 99 experiment is that we just simulate the DDoS intrusion. The recorded DDoS data describes 30 main attribute of the test network connection, including duration, service type, the bytes issued from source to destination, the bytes from destination to source, etc. In the DDoS detection, 5000 normal samples and 5000 DDoS samples were investigated.

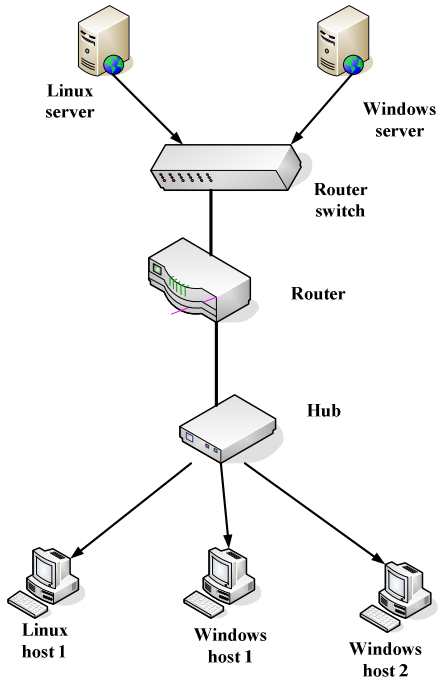

Figure 6. The structure of the intrusion detection experiment.

In experiments, PCA was adopted to reduce the 30 dimension of the original data to 2, 6 and 12 principal components, respectively. The contributions of different numbers of principal component are shown in Fig. 7. It can be seen from Fig. 6 that most of the information contained in the original data can be presented by the PCs, and when use 12 PC litter information is lost. However, the feature number may play some role in the intrusion detection result. A proper number will produce the best performance. Hence, in the pattern recognition, we discuss the performance of different PCs for the intrusion detection.

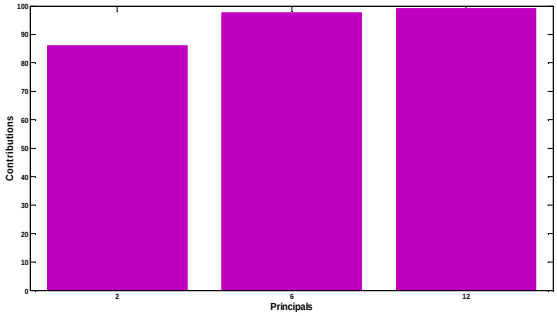

Figure 7. The contribution rate in different number principal components.

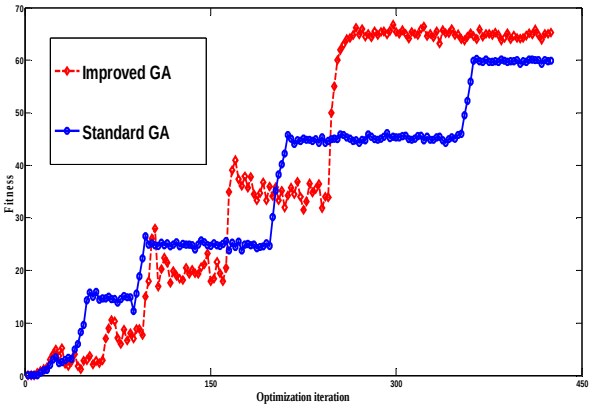

Figure 8. The performance for BPNN optimization using improved GA and standard GA: PCs=6.

The improved GA-ANNs are employed to identify the DDoS. The input feature vector of the ANNs is 2, 6 and 12 principal components, respectively. In the GA optimization, the population size is 300, the crossover probability is 0.95, and the mutation probability is 0.01. The GA optimization procedure is illustrated in Figs. 8-11. Fig. 12 shows the training results of different ANNs. In the optimization procedure, the input features of the ANNs select 6 PCs, and the performance of the improved GA has been compared with the standard GA. Form the evolution performance of the improved GA and standard GA, one can note that the improved GA has faster convergence speed and better fitness value, which is benefited from the energy entropy based annealing selection process.

Hence, after the GA optimization, the structures of the ANNs are better than before, and the intrusion detection abilities could be enhanced greatly. This is the advantages of the proposed intrusion detection method against the existing ANN based approaches. The intrusion detection performance is discussed below.

The intrusion detection performance of the proposed model and the standard GA optimized models is compared using 6 PCs in Table 1. The comparison results show that the proposed method for intrusion detection is more effective than the standard GA optimized models. By the improved individual search processing, the local minimum is avoided and thus the intrusion detection error is decreased by 1.56%. One can note that the improved individual search processing plays an effective role in the improvement of the intrusion detection.

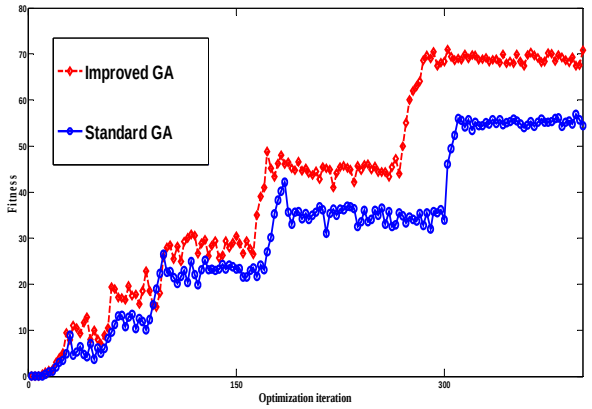

Figure 9. The performance for RBF optimization using improved GA and standard GA: PCs=6.

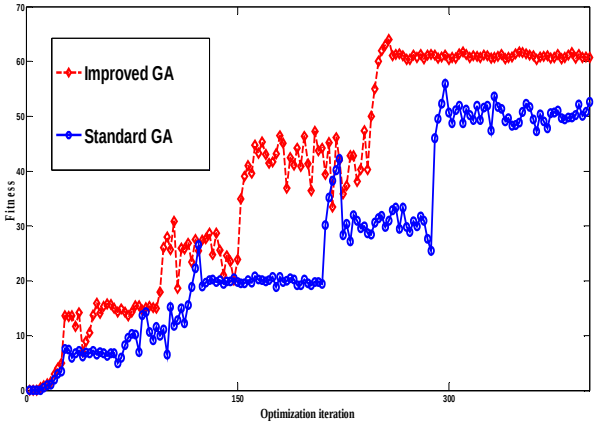

Figure 10. The performance for PNN optimization using improved GA and standard GA: PCs=6.

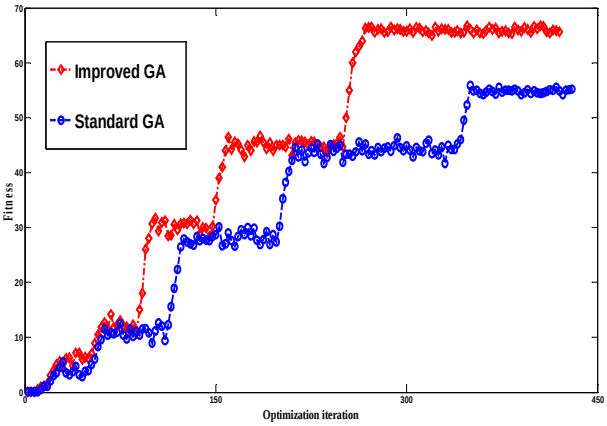

Figure 11. The performance for FNN optimization using improved GA and standard GA: PCs=6.

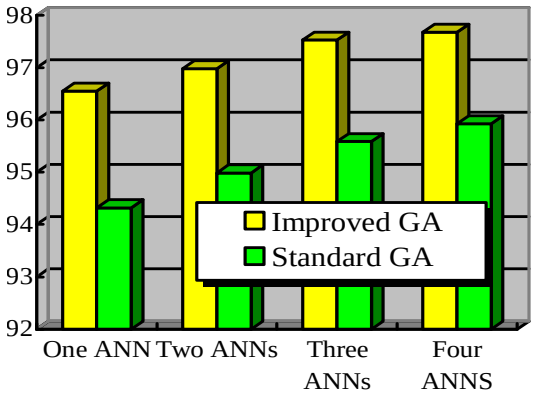

Figure 12. Comparison of the training performance using different number of ANNs for the intrusion detection: PCs=6.

Table 1. The intrusion detection performance.

Optimization method	Prediction performance
Improved GA	97.68%
Standard GA	95.92%

Table 2. The comparative results of the integrated ANN model and independent ANN models.

Optimization method	Intrusion detection error (%)				
	Hybrid ANNs	BPNN	RBF	PNN	FNN
Improved GA	0.46	1.21	1.26	1.34	0.78
Standard GA	1.33	1.85	1.78	1.63	1.66

The intrusion detection performance of the integrated ANN model and independent ANN models is compared in Table 2. It can be seen from Table 2 that by the integrated processing, the intrusion detection error is decreased by 0.32% or better. Hence, the hybrid intelligent model can provide more efficient prediction rate for the intrusion detection than the separated used of ANNs. One can also note that the GA optimization plays an important role in the improvement of the intrusion detection.

The intrusion detection performance of the use of PCA feature selection and without the PCA selection is compared in Table 3. It can be seen from Table 3 that by the PCA processing, the distinct features are obtained and thus the intrusion detection error is decreased by 3.0% or better. Hence, it can be seen that the PCA feature selection can improve the intrusion detection rate efficiently.

Table 3. The comparative results of the integrated model and independent models.

Input features	Prediction performance
2	96.67%
6	97.68%
12	96.33%
30	93.33%

The intrusion detection performance of the integrated ANN model and independent ANN models is compared using and not using the PCA selection in Table 4. It can be seen from Table 4 that by the integrated ANNs and the PCA selection processing, the intrusion detection error is decreased by 0.32% or better. Hence, the hybrid intelligent model with PCA selection can provide more efficient prediction rate for the intrusion detection.

Table 4. The comparative results of the integrated ANN model and independent ANN models.

Input features	Intrusion detection error (%)				
	Hybrid ANNs	BPNN	RBF	PNN	FNN
2	0.52	1.31	1.25	1.29	0.82
6	0.46	1.21	1.26	1.34	0.78
12	0.53	1.27	1.36	1.31	0.88
30	0.87	1.41	1.53	1.48	1.03

Hence, from the analysis results in Tables 1-4, it can be seen that the proposed combination of the multi-ANNs and PCA-GA algorithm can provide satisfactory intrusion detection performance, and its efficiency is superior to the independent ANN models with standard GA optimization or without PCA or others. So the proposed intrusion detection method can be used in industrial practice.

V. CONCLUSIONS

Intelligent method has been widely used in intrusion detection, especially for the fuzzy logic and ANN. However, reasonable structural parameters of the intelligent model play an important role in satisfactory detection performance. Therefore, this paper proposed a new intrusion detection method based on improved GA-PCA and multi-ANNs. The innovation is that the new method uses the energy entropy based selection method to ensure the diversity of the generations of the GA, and hence the optimization of the multi-ANNs' structures could be enhanced when compared with standard GA. In addition, the PCA feature selection can enhance the intrusion detection significantly. The real practice data was applied to the validation of the proposed approach. The analysis results verify the effectiveness of this method. The intrusion detection rate and false alarm have been improved when compared with standard GA based approaches, and hence the proposed method has application importance.

ACKNOWLEDGMENT

This work was supported by the Natural Science Foundation of Henan Educational Committee (2011A520013), and the Backbone Teachers Foundation of Henan Educational Committee (2011GGJS-129)

REFERENCES

[1] X. Zhao, R. Jing and M. Gu: Adaptive intrusion detection algorithm based on rough sets, *J T singhua Univ (Sci & Tech)*, Vo l. 48, pp. 1165-1168, 2008.

[2] Gu Yue-sheng, Ye Meng-tao and Gan Yong, Web Services Security Based on XML Signature and XML Encryption, *Journal of Networks*, Vol. 5,No. 9, pp. 1092-1097, 2010.

[3] Z. Li, X. Yan, C. Yuan, J. Zhao and Z. Peng: Fault detection and diagnosis of the gearbox in marine propulsion system based on bispectrum analysis and artificial neural networks, *Journal of Marine Science and Application*, Vol. 10, pp. 17-24, 2011.

[4] Xie Zhiqiang. Support vector machines based on genetic algorithm for network intrusion prediction, *Journal of Computer Simulation*, Vol. 27, pp. 110-113, 2010.

[5] L. Qiao, X. Peng and Y. Ma. GA-SVM-Based feature subset selection algorithm, *Journal of Electronic Measurement and Instrument*, Vol. 20, pp. 1-5, 2006.

[6] W. Xiong and C. Wang: Hybrid feature transformation based on modified particle swarm optimization and support vector machine, *Journal of Beijing University of Posts and Telecommunications*, Vol. 32, pp. 24-28, 2009.

[7] Yuesheng Gu, Yancui Li, Jiucheng Xu and Yanpei Liu, Novel Model Based on Wavelet Transform and Ga-fuzzy Neural Network Applied to Short Time Traffic Flow

Predicition, *Information Technology Journal*, Vol. 10, No.11, pp. 2105-2111, 2011.
[8] Li Z. and Yan X.: Application of independent component analysis and manifold learning in fault diagnosis for VSC-HVDC systems. *Hsi-An Chiao Tung Ta Hsueh*, vol. 45, pp. 46–51, 2011.
[9] Yuesheng Gu, Yanpei Liu and Jiucheng Xu, Improved Hybrid Intelligent Method for Urban Road Traffic Flow Forecasting based on Chaos-PSO Optimization, *International Journal of Advancements in Computing Technology*, Vol. 3, No. 7, pp. 282-290, 2011.
[10] Chang wook Ahn and R. Ramakrishna. A genetic algorithm for shortest path routing problem and the sizing of populations, *IEEE Transactions on Evolutionary Computation*, Vol. 6, pp. 566-579, 2002.
[11] Z. Li, X. Yan, C. Yuan, Z. Peng, and L. Li. Virtual Prototype and Experimental Research on Gear Multi-fault Diagnosis Using Wavelet-Autoregressive Model and Principal Component Analysis Method, *Mechanical Systems and Signal Processing*, Vol. 25, pp. 2589-2607, 2011.
[12] Xiang Fu and Zheng Zhengjian. *Research on complex electronic equipment fault location based on improved Genetic Algorithm*, In proceeding of 2010 International Conference on Computer Engineering and Technology, Vol. 1, pp. 1454-1457, 2010.
[13] Zhang Yi, Yang Xiuxia. A fast genetie algorithm based on energy-entropy, *Systems Engineering Theory and Practice*, Vol. 25, pp. 123-128, 2005.
[14] Huang Zhongyu, Yu Zhiqiang, Li Zhixiong and Geng, Yuancheng. A fault diagnosis method of rolling bearing through wear particle and vibration analyses, *Applied Mechanics and Materials*, Vol. 26-28, pp. 676-681, 2010.
[15] Russell, S. and P. Norvig. *Artificial Intelligence: A Modern Approach*. 2nd Edn. Prentice Hall, Inc, 2003.
[16] Kohonen, T.. *Self-Organizing Maps.* Springler-Verlag, Berlin, 1997.
[17] Sin, Y.L., W.L. Low and P.Y. Wong. Learning fingerprints for a database intrusion detection system. Proc. 7th Eur. Symp. *Research in Computer Security*, Zurich, Switzerland, 2002, pp: 264-280.
[18] Lee, S.C. and D.V. Heinbuch. Training a neural network-based intrusion detector to recognize novel attacks. *IEEE Trans. Systems, Man and Cybernetics Part A: Systems and Humans*, Vol. 31, pp. 294-299, 2001.
[19] Zhou, T., X. Liao and Y. Chen. A novel symmetric cryptography based on chaotic signal generator and a clipped neural network. Advances in Neural Networks, Intl. Symp. Neural Networks Proc., Part II. *Lecture Notes in Computer Science*, Vol. 3174, pp. 639-644, 2004.
[20] Nong, Y., S. Vilbert and Q. Chen. Computer intrusion detection through EWMA for auto correlated and uncorrelated data. *IEEE Trans. Reliability*, Vol. 52, pp. 75-82, 2003.
[21] D.F. Specht. Probabilistic neural networks. *Neural Networks*, Vol. 3, No. 1, pp. 109-118, 1990.
[22] P. Venkatesan and S. Anitha, Application of a radial basis function neural network for diagnosis of diabetes mellitus, *Current Science*, Vol. 91, No. 9, pp 1195-1199, 2006.

Yuesheng Gu, birth 1973, male, associate professor of Henan institute of science and technology. His current research area is computer network technology and Artificial Intelligence.

Yongchang Shi, birth 1971, male, associate professor of Pingdingshan University. His current research area is computer application technology.

Jianping Wang, birth 1981, male, M.S degree. His current research area is computer network technology and robot system.