A New Method for Intrusion Detection using Manifold Learning Algorithm

Guoping Hou[1], Xuan Ma[1], Yuelei Zhang[2]
[1]Chongqing Electric Power College, No.9 Wulongmiao, Jiulongpo District, Chongqing 400053, China
Tel: 86-23-68501490
[2]Unit 94270 of PLA, No.19 Hangkong Road, Jinan 250117, China
Tel: 86-521-86710091
Corresponding author, e-mail: houguoping1982@163.com[1], zyl3836@163.com[2]

Abstract

Computer and network security has received and will still receive much attention. Any unexpected intrusion will damage the network. It is therefore imperative to detect the network intrusion to ensure the normal operation of the internet. There are many studies in the intrusion detection and intrusion patter recognition. The artificial neural network (ANN) has proven to be powerful for the intrusion detection. However, very little work has discussed the optimization of the input intrusion features for the ANN. Generally, the intrusion features contain a certain number of useless features, which is useless for the intrusion detection. Large dimensions of the feature data will also affect the intrusion detection performance of the ANN. In order to improve the ANN performance, a new approach for network intrusion detection based on nonlinear feature dimension reduction and ANN is proposed in this work. The manifold learning algorithm was used to reduce the intrusion feature vector. Then an ANN classifier was employed to identify the intrusion. The efficiency of the proposed method was evaluated with the real intrusion data. The test result shows that the proposed approach has good intrusion detection performance.

Keywords: *intrusion detection, nonlinear feature reduction, artificial neural network, manifold learning*

1. Introduction

Great advances have been made in the field of communication and computer technology in recent years. The internet now is indispensible for people’s life. However, due to complex operation environment, the network suffers from various offensives and violations. It is therefore imperative to detect the network intrusion to ensure the normal operation of the intnet. The intrusion detection research has hence received extensive attentions [1].

Intrusion detection is crucial for computer security and defense. Terrible intrusion may damage the internet for weeks [2]. To realize effective intrusion detection, many advanced technologies have been proposed, including the artificial neural network (ANN) [3], rough sets [1], and support vector machine (SVM) [4] etc. Among them, ANN is the most promising method [5]. ANN has the ability to find the nonlinear connection between the Intrusion features and the Intrusion patterns, and has been widely used in the Intrusion detection. However, ANN detection performance is mainly determined by its structural parameters, especially by the input feature vector of the intrusion data. Although the principal component analysis (PCA) and its derivative algorithms have been proved to be a useful tool for feature reduction and extraction to improve the network attack detection accuracy, their main limitation lies in their ability is to capture the nonlinear properties of the original data [6-8]. The same problems are also found in other linear methods [7], including multi-dimensional scaling (MDS) and linear discriminate analysis (LDA). Fortunately, the manifold learning algorithms provide a new means to deal with the nonlinear dimensionality reduction problems. The Isomap [6] and locally linear embedding (LLE) [7] etc., are able to deal with the underlying nonlinear behavior of the data. Compared with the linear methods, the purpose of manifold learning is to project the original high-dimensional data into a lower dimensional feature space by preserving the local topology of the original data [9-10]. Thus, the intrinsic structure of the data of interest can be extracted effectively.

Received June 25, 2013; Revised July 28, 2013; Accepted August 15, 2013

The advantage of the Isomap and LLE in the intrusion detection is the identification of underlying nonlinear manifold. However, in the identification of nonlinear manifold the Isomap and LLE mainly use the neighborhood graphs, which sometimes may fail to ensure the connectedness of the constructed neighborhood graphs. In order to improve the robustness of the neighborhood graphs of the manifold learning algrithm to enhance the intrusion detection, this work presents a new method based on the improved LLE. An adaptive scheme is proposed to build suitable neighborhood graphs. By doing so, it is reasonable to reduce the original feature space and find the distinct nonlinear characteristics about the intrusion data. Then, an ANN classifier is employed to recognize the intrusion patterns. By implementing the intrusion detection experiments, the analysis results show that the feature reduction is very essential in the intrusion detection because the original feature space have many redundant features to influence the intrusion identification. Eliminate these redundancies can enhance the intrusion detection. In addition, the comparision of the improved LLE and the original LLE has been done. The comparision result shows that the improved LLE with adaptive scheme outperforms the original LLE in the intrusion detection.

2. Research Method

2.1. The Improved LLE

Here in we propose an adaptive scheme to build suitable neighborhood graphs. The details are expressed below.

Given a nonlinear high-dimensional dataset $S = [\mathbf{s}_1 \quad \mathbf{s}_2 \quad \cdots \quad \mathbf{s}_l] \in R^p$, where *l* is the total sample number and *p* the dimensionality of each sample, the objective of LLE is to reconstruct a nonlinear mapping to project *S* into a reduced manifold space $S_r = [\mathbf{s}_{r1} \quad \mathbf{s}_{r2} \quad \cdots \quad \mathbf{s}_{rl}] \in R^q$ (*q*<<*p*). The improved LLE algorithm is described as following.

Step 1: Compute *k* neighbours of every sample.

Step 2: Identify the neighborhood graph and finds the points out of the connected graph.

Step 3: Increase *k* if exist unconnected points. Otherwise, go to step 5

Step 4: Compute new *k* nearest neighbors.

Step 5: Compute the local reconstruction weight matrix *W* by minimizing the following cost function:

$$\min \varepsilon(W) = \sum_{i=1}^{l} \left| \sum_{j=1}^{k} w_j^i (s_i - s_{ij}) \right|^2 \tag{1}$$

Where w_j^i is the weight values. If s_i and s_j are not neighbours, $w_j^i = 0$ and $\sum_{j=1}^{k} w_j^i = 1$.

Step 6: Map the original dataset into the embedded coordinates. Compute the reconstructed *q*-dimensional manifold space S_r by minimizing the following constraint:

$$\min \varepsilon(S_r) = \sum_{i=1}^{l} \left| s_{ri} - \sum_{j=1}^{k} w_j^i s_{rij} \right|^2 \tag{2}$$

Where s_{ri} is the projection vector of s_i in the embedded coordinates, and s_{rij} are the neighbours of s_{ij}. Equation (2) can be rewritten as:

$$\min \varepsilon(S_r) = \sum_{i=1}^{l} \sum_{j=1}^{k} m_j^i s_{ri}^T s_{rj} = tr(S_r M S_r^T)\,, \tag{3}$$

Where the cost matrix *M* can be expressed as:

$$M = (I_{l\times l} - W)^T (I_{l\times l} - W)\,. \tag{4}$$

Hence, the minimization of (4) can be reduced to an eigenvalue problem, and S_r could be determined by the *q* smallest nonzero eigenvectors of *M*.

2.2. The Backpropagation 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 [8-13]. One of the most commonly used supervised ANN model is BPNN. The BPNN uses one of the well-known algorithms, backpropagation learning algorithm [13]. The structure of BPNN is arranged into different layers: input layer, middle layer and output layer. The workflow of the BPNN can be expressed as follows [8-13]:

(1) The input layer propagates a particular input vector’s components to each node in the middle layer.

(2) The middle layer nodes compute output values, which become inputs to the nodes of the output layer.

(3) The output layer nodes compute the network output for the particular input vector.

The forward pass produces an output vector for a given input vector based on the current state of the network weights. Since the network weights are initialized to random values, it is unlikely that reasonable outputs will result before training. Although the weights can be adjusted to reduce the error by propagating the output error backward through the network, the training may suffer from the local minimum. Thus, the improved LLE feature reduction is an efficient compensation to the training process of the ANN.

2.3. The Proposed Intrusion Detection Method

In this paper the improved LLE-ANN are used for the network intrusion detection. 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 manifold by improved LLE.

Step 3: Train the BPNN using the new features, 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 diagram block of the proposed network intrusion detection method is illustrated in Figure 1.

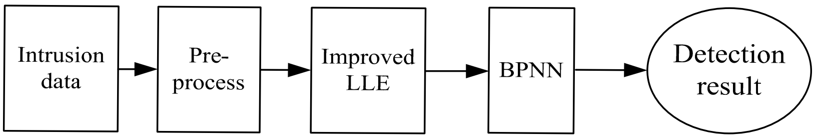

Figure 1. The Network Intrusion Detection based on the Improved LLE and ANN

2.4. Experiments

In order to evaluate the performance of the proposed computer intrusion method, experiment tests have been implemented in this work. Figure 2 shows the experiment principle. A mini computer network has been established to conduct the experiments. The computer network is composed of a linux server, a windows server, the web link, two linux host and four windows hosts. Some manual attacks have been simulated and tested using this experimental system.

In this work, the Denial of Service (DoS), Remote to Local (R2L), User to Root (U2R) and Probe or Scan (PoS) are introduced into the experiment system to validate the new detection method. Forty-one features are monitored and recorded for every intrusion. These features include the bytes issued from source to destination, the bytes from destination to source, duration, teardrop, neptune, etc. There are 5,000 samples for each intrusion type and the total samples are 20,000.

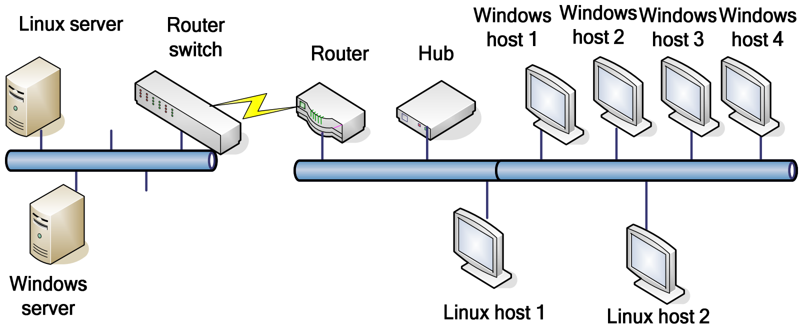

Figure 2. The Principle of the Experiment Tests

3. Results and Analysis

In experiments, LLE was adopted to reduce the 41 dimension of the original data to 2 and 3 dimensions, respectively. Figure 3 shows the feature reduction result of the improved LLE with 2 dimensions, and Figure 4 shows the feature reduction result of the improved LLE with 3 dimensions. It can be seen from Figure 3 and Figure 4 that after feature reduction there are obvious bounderies between different intrusion type besides some overlaps. Hence, the feature reduction can efficiently eliminte the useless features in the original feature vector and extract the most distinguished information for the intrusion detection. Moreover, it can provide a virtual 3D presentation of the intrusion feature space using 3 dimensions in the feature reduction.

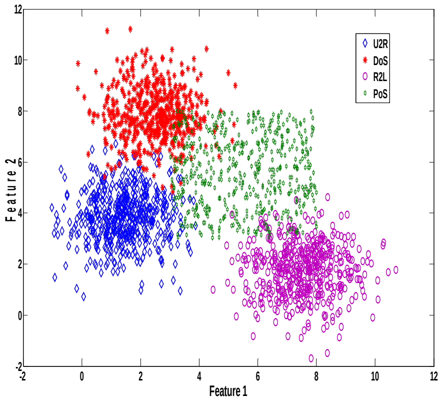

Figure 3. Feature reduction result of the Improved LLE with 2 Dimensions

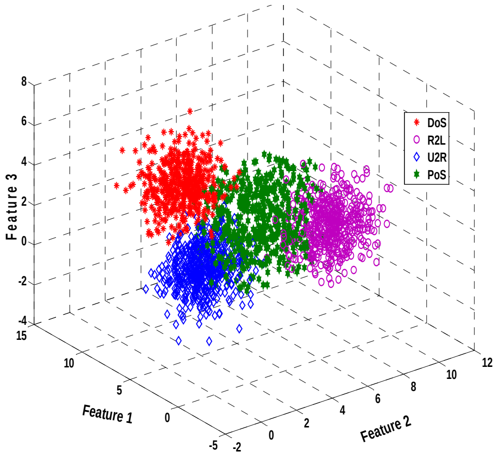

Figure 4. Feature Reduction Result of the Improved LLE with 3 Dimensions

In the intrusion recognition, 3, 000 samples of each intrusion type was used for train the ANN, and the reminders were used for testing. Table 1 lists the intrusion detection results using the proposed method. Here in the detection rate and false positive rate were used to evaluate the ntrusion detection performance. The detection rate means the hits of correct samples to the total samples and the false positive rate is defined as the misclassifications.

Table 1. The Performance of the ANN Detection

Feature reduction method	KPCA-PSO-SVM	
	Detection rate (%)	False positive rate (%)
None	81.6	13.8
LLE with 2 dimensions	90.2	6.4
LLE with 2 dimensions	90.6	6.8
Improved LLE with 2 dimensions	93.8	6.6
Improved LLE with 3 dimensions	94.4	6.4

The intrusion detection performance of the use of LLE feature selection and without the LLE selection is compared in Table 1. It can be seen from Table 1 that by the LLE processing, the distinct features are obtained and thus the intrusion detection rate is enhanced by 8.6% or better and the false positive rate is decreased at least by 7.4%. Hence, it can be seen that the LLE feature selection can improve the intrusion detection rate efficiently. It also can be noticed that the improved LLE increases the detection rate by 3.6% or better than the LLE.

4. Conclusion

Intelligent method has been widely used in intrusion detection, especially for the ANN based methods. However, reasonable input feature vector of the ANN model plays a criticle role in desired detection performance. Therefore, this paper proposed a new intrusion detection method based on the improved LLE and BPNN. The innovation of this work is that the new method uses the improved LLE algorithm to reduce the dimensions of the input features of the BPNN to eliminate useless information. The real practice data was applied to the validation of the proposed approach. The analysis results verify the effectiveness of this method.

References

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

[2] Sin Y, Low W, Wong P. *Learning fingerprints for a database intrusion detection system*. Proc. 7th Eur. Symp. Research in Computer Security. Zurich. 2002; 7: 264-280.

[3] Li Z, Yan X, Yuan C, Zhao J, Peng Z. 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*. 2011; 10: 17-24.

[4] Li Z, Yan X, Yuan C, Peng Z. Intelligent fault diagnosis method for marine diesel engines using instantaneous angular speed. *Journal of Mechanical Science and Technology*. 2012; 26(8): 2413–2423.

[5] Lee S, Heinbuch D. Training a neural network-based intrusion detector to recognize novel attacks. *IEEE Trans. Systems, Man and Cybernetics Part A: Systems and Humans*. 2001; 31: 294-299.

[6] Tenenbaum J, Silva V, Langford J. A global geometric framework for nonlinear dimensionality reduction. *Science*. 2000; 290: 2319–2323.

[7] Roweis S, Saul L. Nonlinear dimensionality reduction by locally linear embedding. *Science*. 2000; 290: 2323-2326.

[8] Belkin M, Niyogi P. Laplacian eigenmaps for dimensionality reduction and data representation. Neural Comput. 2003; 15: 1373-1396.

[9] Jiang Q, Jia M, Hu J, Xu F. Machinery fault diagnosis using supervised manifold learning. *Mech. Syst. Signal Proces*. 2009; 23: 2301–2311.

[10] Li Z, Yan X, Tain Z, Yuan C, Peng Z. Blind vibration component separation and nonlinear feature extraction applied to the nonstationary vibration signals for the gearbox multi-fault diagnosis. *Measurement*. 2013; 46: 259–271.

[11] Zhu S, Hu *B.* Hybrid feature selection based on improved GA for the intrusion detection system. *TELKOMNIKA*. 2012; 11(4): 1725–1730.

[12] Chen X, Li F, Wang L.Fault-tolerant method for detecting coverage holes of wireless sensor networks. *TELKOMNIKA*. 2012; 10(4): 876–882.