

# Detection technology for underlying intrusion of large embedded network

Lai Yimei

ChengDu Polytechnic, Sichuan Chengdu 610000

**Keywords:** rough set theory; neural network; Attribute Reduction; intrusion detection;

**Abstract.** The underlying intrusion accurate detection of large embedded network is studied. For the problem that low accuracy of underlying intrusion detection for the large embedded network, an underlying intrusion detection method for the large embedded network based on field rough set theory and BP neural network algorithm is proposed. Firstly, the concept of field is introduced on the basis of rough set theory to reduce the loss of information, field rough set theory is utilized to simplify data, the simplified data set are regarded as the input data of BP neural network, so as to simplify the structure of BP neural network, while reducing the training time of a sample, and improve the classification accuracy of BP neural network. The simulation results in Matlab show that the proposed algorithm for intrusion detection can achieve shorter training time for samples, while the false alarm rate of the invasion has been improved to meet the underlying intrusion detection needs of a large embedded network.

## 1 Introduction

With the continuous development and popularity of network technology, the large-scale embedded network has penetrated into many aspects of people's production and life, and plays an irreplaceable role [1]. Therefore, large embedded network security has also been paid a great deal of attention. Which leads to underlying intrusion detection technology for a large embedded network becomes the core issue in network areas requiring to be researched [2]. The underlying intrusion detection of large embedded network is through certain means to detect potential threats that may exist in large embedded networks, mainly by viewing real-time data acquired in logs related to the system to get some important information of the computer itself, so as to analyze the health of large embedded networks [3]. Before large-scale embedded network has been effected by an external attack, the underlying intrusion detection is able to conduct a comprehensive investigation for potentially dangerous invasion procedures through initiative attack, in a timely manner to filter out risk factors of possible and potential security risks, which is a necessary complement for current firewall [4-6]. The underlying intrusion detection for large embedded network can achieve the following functions: (1) monitor the specific actions of the user operation, scan, analyze and extract of anomalies and abnormal data occurred in the system timely; (2) Once intrusion or abnormal behavior found, effective detection means is adopted to detect timely, isolate and alert.

## 2 Underlying intrusion detection system design for RS BP large embedded network

### 2.1 The establishment of rough set BP neural network model

Firstly, underlying data of large-scale embedded network is acquired by data receiver, and pretreatment, like format conversion are conducted to the data, then the data is transmitted into the database after preprocessing, the database will transfer all the data to the rough set module, through the rough set module discrete the data afterwards, as well as attribute reduction and other operations, so as to reduce the number of bits of data, at the same time remove some redundant data to simplify data sets. Training is done for desired output error value, the obtained threshold and weight are saved, the collection composed of the desired input and output data is transferred to the database, which provides a solution for the deficiency that the results obtained by BP neural network is not easily understood. Real-time detector receives processed data from the rough set, based on the rules

to determine whether the data is underlying invasion data of large-scale embedded network, if it is, the alarm will be notified to employ appropriate measures for intrusion.

## 2.2 The establishment of BP neural network

BP neural network algorithm is one of the algorithms with wide applications in computer smart recognition. BP neural network is a two-way reversible tradition, in the forward propagation, from the input layer to pass through each hidden operational layer, the number of operation layers is determined by the accuracy of the algorithm, and finally get to the output layer. If the results obtained at output layer by calculating is not fully consistent with the expected results, the reverse operation can be started, and the parameter weights used in calculating can be constantly adjusted to ensure accuracy, until more accurate results are achieved. The block diagram of the three-BP neural network is as shown in the following figure.

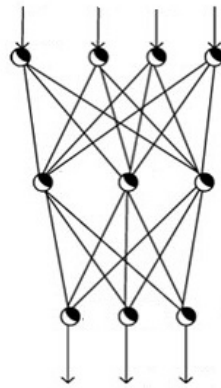


Figure 1 A three-layer BP neural network structure

BP neural network algorithm has localized gradient descent, the function with it involved in operations is easily to reach saturation, so that the algorithm has two features: a flat curved surface and is easy to fall into local minimum point, these two points are in line with underlying intrusion detection requirements of large embedded network, so the introduction of this algorithm in underlying intrusion detection of a large embedded network, can significantly enhance the accuracy of detection.

## 2.3 achievement of BP neural network Rough Sets intrusion detection

BP neural network rough sets intrusion detection has two main steps, the first is to pre-processing the collected data, and the second is the attribute reduction.

### 1) Data preprocessing

To begin with, underlying data of large-scale embedded network is acquired by the data receiver, and pretreatment like data format conversion is conducted for the data, discrete attributes is numbered with natural numbers, a local discrete algorithm based on decision tree is regarded as discrete algorithm, continuous attributes need to be normalized to reduce the effects of different amounts of the properties on the prediction results.

### 2) Attribute Reduction

In the underlying data decision-making table of a large embedded network, not every attribute is just as important, because some of the attributes are redundant, which will generate a lot of useless rules, it is necessary to delete irrelevant or unimportant data knowledge, under the premise that classification ability of knowledge base is kept same. The basic principles of data reduction algorithm based on rough set is to seek and sequence the importance of attributes, in order to produce more concise rules, the reduction of information knowledge is necessary to be achieved. By considering, the minimum reduction of computer attributes set is a relatively difficult problem, heuristic approximation algorithms must be used to shorten the training time, so as to obtain an optimal solution. Therefore, with the genetic algorithms to find a more favorable initialization parameter to process global optimum search can produce better attribute reduction in a shorter time.

### 3) Extraction and filtration of Rules

The generated rule set of reduction attribute set *RED* is calculated as follows: for each sample data in simplified information system, a conjunctive term of rules formed for the antecedent

of each condition attribute "attribute - value" , a conjunctive term also formed for the seccedent, and then decision rule sets is available. However, all the generated rule sets have a lot of redundant rules, or repeated rules, for such situations, filtering treatment is necessary for all rules:

①  $\alpha \rightarrow \beta_1$  and  $\alpha \rightarrow \beta_2$  are the two rules with repeated conditions, according to the situation of the training set to remove the data set of low reliability;

② If  $\alpha \rightarrow \beta_1$  and  $\alpha \rightarrow \beta_2$ ,  $\alpha_1 \cup \alpha_2$ ,  $\alpha_2 \rightarrow \beta$  are redundant rules, it need to be removed.

### 3. Experimental results and analysis

In order to evaluate the effectiveness of the underlying proposed intrusion detection method for large embedded network based on field rough set theory and BP neural network algorithm, a single experiment need to be conducted. During the experiment, the experiment needs to be programmed with JAVA language.

During the experiment, with different algorithms to process underlying intrusion detection experiments for large embedded network, assuming that data is determined as the invasion, it will be timely warning, otherwise, not warning. Experiments conducted with different algorithms, the comparison results of the false alarm rate obtained in the experiments can be described by the following figure:

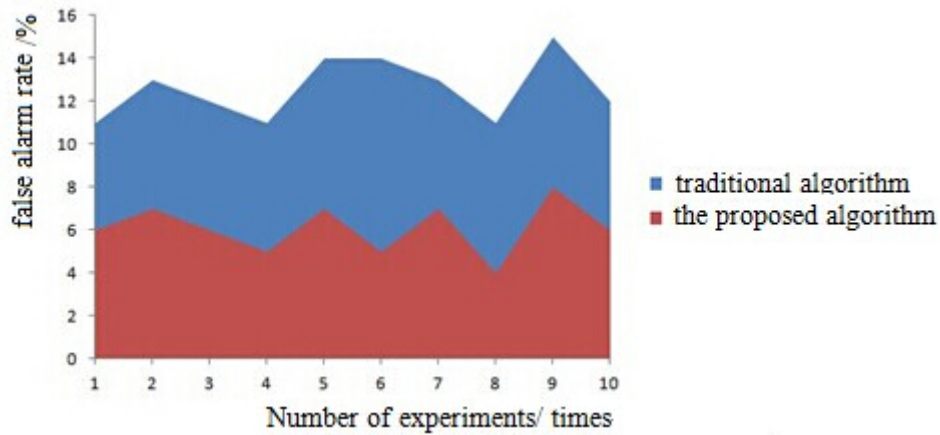


Figure 2 Comparison of false alarm rate of different algorithms

According to the above figure, it can be known that the false alarm rate of using the proposed algorithm to detect the underlying network intrusion of large-scale embedded, is lower than the traditional algorithm.

The relevant data in the above mentioned experiments process are analyzed to obtain Table 1 described below:

**Table 1 Experimental data tables of different algorithms**

Number of experiments	false alarm rate of traditional algorithm (%)	false alarm rate of the proposed algorithm (%)
1	11	6
2	13	7
3	12	6
4	11	5
5	14	7
6	14	5
7	13	7
8	11	4
9	15	8
10	12	6

According to the above figure, it can be known that the false alarm rate of using the proposed

algorithm to detect the underlying network intrusion of large-scale embedded, is lower than the traditional algorithm, demonstrating the superiority of the proposed algorithm.

#### 4. Conclusion

On the basis of the advantages of field rough set and BP neural network algorithms, an underlying intrusion detection method for the large embedded network based on field rough set theory and BP neural network algorithm is proposed. Firstly, the concept of field is introduced on the basis of rough set theory to reduce the loss of information, field rough set theory is utilized to simplify data, the simplified data set are regarded as the input data of BP neural network. The simulation results in Matlab show that the proposed algorithm for intrusion detection can achieve shorter training time for samples, compared with the traditional underlying intrusion detection system model of large embedded network, it possess lower false alarm rate of the invasion.

#### References

- [1] D. Subhadrabandhu, F. Anjum, and S. Sarkar. On optimal placement of intrusion detection modules in sensor networks[C]. Proceedings of the First International Conference on Broadband Networks, 2004: 690-699.
- [2] Anjum F, Subhadrabandhu D, Sarkar S, et al. On Optimal Placement of Intrusion Detection Modules in Sensor Networks[C]. 1st International Conference on Broadband Networks. Washington: IEEE Press, 2004: 433–439.
- [3] Everthon Silva Fonseca, Rodrigo Capobianco Guido, Paulo Rogério Scalassara, Carlos Dias Maciel, José Carlos Pereira. Wavelet time-frequency analysis and least squares support vector machines for the identification of voice disorders [J]. Computers in Biology and Medicine, 2007, 37(4): 571-578.
- [4] Wang Hui. Research on Network Intrusion Detection System Based on Danger Theory [J]. Computer simulation, 2010, 27(6):159-190.
- [5] Wang Tao, Gong Huili. Application of Support Vector Machine in the Intrusion Detection System [J]. Control & management, 2006, 22(12):89-91.
- [6] Li Fayin, Hu Yupu, Li Gang. An Efficient Identity-Based Signcryption Scheme [J]. Chinese journal of computers, 2006, 29(9): 1641-1647.