A method of eliminating false alarm based on deep learning

P Wei, Z Zhang, B Chen
National Digital Switching System Engineering & Technological Research Center, Zhengzhou, China
willerise@163.com

Abstract: Alarm data in intrusion detection system is mixed with a large amount of false alarm data, which brings great interference for network managers to analyze attack behavior. For a large deal of false alarm data in intrusion detection, this paper proposed an DBN construction method based on genetic operator improving the particle swarm, and used this DBN as a false alarm elimination classifier in IDS, firstly, using the improved particle swarm algorithm to search for the candidate network structure of DBN based on the fitness evaluation criteria, considering the candidate network structure with the optimal fitness as the final DBN network structure, secondly, using this DBN for false alarm elimination in intrusion detection. The experimental results showed that the average elimination rate of the proposed method is 5.54% and 2.9% higher than that of the SOM and KNN algorithms respectively, and the average misuse rate is 3.99% and 1.22% lower than that of the SOM and KNN algorithms respectively.

1. Introduction
The false alarm in intrusion detection refers to the misjudgment of normal data as abnormal data, which deeply affects the analysis of attack events by network managers. How to eliminate false alarm has become the focus of current research [1]. Deep belief network (DBN) is a classic deep learning model [2]. It is very suitable for classification or prediction [3]. It is also suitable for the analysis of massive data and widely used in text detection and image recognition. In this paper, DBN is applied to intrusion detection false alarm elimination to improve the efficiency of intrusion detection system.

2. Background and related works
According to the research on false alarm in intrusion detection, false alarm elimination method has three types: associated behaviors-based method, eliminates false alarm through the analysis of many associated behaviors triggered by intrusion behaviors; statistics-based method, according to the common features of false alarm, forms rules and characteristics that can distinguish false alarm based on false alarm and normal alarm; environmental information screening-based method, executes the secondary screening according to different network environment.

In order to reduce false alarm of network intrusion detection system(NIDS), document [4] proposed a post-processing filtering method based on the statistical characteristics of alarm data. Experiment proves that this method works well. Document [5] proposed a method of eliminating false alarm using condition for random fields. In order to obtain reasonable recommendation data for the corresponding feature window and perform false alarm elimination, it is necessary to perform repeated experiments on single and multiple alarm features. However, the above method only has a good effect in eliminating false alarm for small sample data, and has no obvious effect on the elimination of false alarm for massive network data. According to the problem of intrusion detection false alarm...
elimination of massive network data, this paper applies the DBN model to intrusion detection. The method can improve the efficiency of the intrusion detection system. DBN structure is shown in Figure 1.

As shown in Figure 1, DBN is composed of RBM and BP neural network. Among them, RBM is a two-layer neural network, including input layer and output layer, and BP neural network which can classify the data is a neural network with error back propagation.

3. Applying deep learning to false alarm elimination

3.1. Process of false alarm elimination in intrusion detection

According to a large amount of alarm data in IDS, this paper uses the DBN to eliminate the false alarm data. The false alarm elimination process includes the construction of false alarm data set, elimination of false alarm, and evaluation effects [6], as shown in Figure 2.

1) Construction of false alarm data set: KDD CUP99 is the standard data in the field of intrusion detection [7], which is used as the original data. Support vector machine (SVM) algorithm is used to classify the attack data and normal data in intrusion detection. The classified attack data is used as alarm data, in which normal alarm and false alarm are marked in the alarm data.

2) Elimination of false alarm: KNN algorithm, SOM algorithm and the improved particle swarm optimizing DBN model are used to process the false alarm data set. The purpose is to classify true alarm and false alarm data, eliminate false alarm, and improve intrusion detection efficiently.

3) Evaluation effect: this paper defines evaluation indicators, such as elimination rate and misuse rate, to evaluate the false positive elimination effect and evaluate the performance of various aspects of the adopted algorithm.

3.2. GPSO-DBN-Algorithm-based false alarm elimination method

Particle swarm optimization algorithm is an evolutionary algorithm that can be used to solve many
engineering problems. Each particle has its own position and moving speed, using pbest to record the optimal position of the particle history, using gbest to record the optimal position of the particle group history. The performance of the particle is evaluated by the fitness criterion [8]. The particle velocity and position are updated according to the following equations (1) and (2):

\[ v_{step}^{i+1} = vstep_i + c_1 * r_{d_1} * (pbest_i - x_i^t) + c_2 * r_{d_2} * (gbest_i - x_i^t) \] (1)

\[ x_{id}^{t+1} = x_{id}^t + v_{step}^{i+1} \] (2)

Where \( t \) means the \( t^{th} \) iteration, \( d \) is the \( d^{th} \) dimension of the search space, \( r_{d_1} \) and \( r_{d_2} \) are two random numbers uniformly distributed between \([0,1]\). \( c_1 \) and \( c_2 \) are two acceleration weights. \( w \) is an inertia weight.

In this paper, DBN network structure includes the depth of DBN and the number of nodes at each layer. The number of input layer and output layer nodes is fixed. The document [9] indicates that DBN which has four hidden layers has great performance, and set the number of DBN’s hidden layer as 4. We only need to determine the number of hidden layer’s nodes per layer. In this paper, genetic operators are used to improve the particle swarm optimization (GPSO) to optimize the DBN network structure. The number of nodes in each hidden layer corresponds to each dimension of the particle. The integer-type particle swarm generated in a random manner is used as the initial network structure. Particle group \( swarm = [x_1, x_2, \ldots, x_{numh_1}, \ldots, x_{numh_n}] \) , whose velocity matrix is \( svstep = [vstep_1, vstep_2, \ldots, vstep_{numh_1}, \ldots, vstep_{numh_n}] \) . The \( i^{th} \) particle position is \( x_i = [num(h_1), num(h_2), \ldots, num(h_d), \ldots, num(h_n)] \), and the \( i^{th} \) particle position speed is \( v_{step_i} = [v_{s_1}, v_{s_2}, \ldots, v_{s_{numh_1}}, \ldots, v_{s_{numh_n}}] \) . Where \( v_{s_id} \) means speed component, and \( num(h_{id}) \) is position component which means the number of nodes in the \( d^{th} \) layer of the DBN’s hidden layer. The process of particle swarm optimizing DBN network structure is shown in Algorithm.

Algorithm: Pseudo-code of GPSO

begin
Initialization parameters: particle swarm’s weight \( w \) and acceleration weights \( c_1 \), \( c_2 \), particle’s maximum speed \( v_{max} \) and minimum speed \( v_{min} \), DBN hidden layer’s maximum width \( s_{max} \) and minimum width \( s_{min} \), the maximum number of iterations \( maxiter \), the number of DBN’s hidden layers \( n \), the number of iterations \( iter \), particle swarm’s size \( nswar \);
Initialization matrices: particle swarm \( swarm \), particle swarm’s velocity \( svstep \), initialize \( pbest \) to \( swarm \), calculate \( pbest \)’s Fitness \( fpbest \), initialize \( gbest \) as optimal fitness particle in \( swarm \), calculate \( gbest \)’s Fitness \( fgbest \);
while iter is not reached maxiter do
for \( i=1 \) to \( nswar \) do
Update the \( f_{swarm} \) of particle \( i \);
end for
for \( i=1 \) to \( nswar \) do
Update the \( pbest \) and \( fpbest \);
end for
Perform crossover operation on the \( swarm \);
Update the \( gbest \) and \( fgbest \);
Perform mutation operation on the \( swarm \);
for \( i=1 \) to \( nswar \) do
Update velocity of particle \( i \);
Update position of particle \( i \);
end for
iter=iter+1;
end while
Consider globally optimized particle \( gbest \) as the final network structure of DBN;
end
The **Fitness** in Algorithm is defined as formula (3).

\[
Fitness(x_i) = (1 - b - c) * (1 - ER) + b * \frac{\sum_{d=1}^{n} num(h_d)}{n * smax} + c * MR
\]

Where \( b, c \in [0,1] \) is corresponding weight parameter, \( n \) is the number of DBN’s hidden layers, setting as 4 \([9]\), \( smax \) is the maximum node number of hidden layer, \( \sum_{d=1}^{n} num(h_d) \), \( \sum_{d=1}^{n} x \) is the total node number of DBN’s hidden layers, the elimination rate ER and the misuse rate MR can be obtained after the DBN model processing the false alarm elimination data set.

4. **Experiments and results**

4.1. **KDD CUP99 data set**

The KDD CUP99 data set is a classical data set in the field of network security \([10]\). The entire data set includes 7 million network connection records, of which the training set and the test set are 3:1. In this paper, the KDD CUP99 sample data set selected is shown in Table 1:

| Abnormal sample size | Normal sample size | Total sample size |
|----------------------|--------------------|------------------|
| Probe | DoS | U2R | R2L | 7251 | 15021 |
| 1823 | 5323 | 51 | 573 |

4.2. **Data preprocessing**

The original data set for this article uses the KDD CUP99 data set. By referring to the accuracy, false alarm rate, and misuse rate in intrusion detection \([11]\), this paper defines the elimination rate and misuse rate: elimination rate (ER) indicates the proportion of detected false alarms to actual false alarms, which can describe the degree to which the algorithm can distinguish false alarm; misuse rate (MR) indicates the proportion of true alarms detected as false alarms to actual normal alarms, which can describe the error rate of the algorithm.

The input layer of the deep belief network must input floating-point numbers ranging from 0 to 1. Preprocessing data has two stages, the digitization of features and the normalization of digital features \([12]\). The digitization of features uses a new coding mapping method to map non-numerical features to ordered numbers. The normalization of digital features is to eliminate the effect of each feature dimension and to normalize the training set and test set data. According to the following conversion formula (4), the values of each column in the preliminary processed data set are normalized in the range [0, 1].

\[
Y = \frac{Y_{original} - Y_{min}}{Y_{max} - Y_{min}}
\]

\( Y_{original} \) means \( y^{th} \) feature column original value, \( Y_{min} \) is the minimum value of \( Y_{original} \), \( Y_{max} \) is the maximum value of \( Y_{original} \).

4.3. **Experimental results**

In the experiment, using SVM algorithm to detect the pre-processed KDD CUP99 data, normal alarm is manually annotated. The false alarm elimination data set is shown in Table 2 below.

| True alarm sample size | False positive sample size | Total number of alarm samples |
|------------------------|---------------------------|------------------------------|
| 7381                   | 152                       | 7533                         |
The experiment uses DBN, SOM algorithm and KNN algorithm to eliminate false alarm based on the false alarm elimination data set in the same experimental conditions. We perform ten experiments respectively, to compare the misuse rate and elimination rate. The experimental results is shown as Table 3.

| The k\textsuperscript{th} experiment | Elimination rate(%) | Misuse rate(%) |
|--------------------------------------|---------------------|----------------|
|                                      | DBN | SOM | KNN | DBN | SOM | KNN |
| k=1                                  | 74.21 | 63.62 | 71.31 | 5.13 | 7.28 | 6.35 |
| k=2                                  | 74.21 | 67.21 | 71.31 | 5.13 | 12.36 | 6.35 |
| k=3                                  | 74.21 | 73.72 | 71.31 | 5.13 | 10.71 | 6.35 |
| k=4                                  | 74.21 | 68.12 | 71.31 | 5.13 | 9.29  | 6.35 |
| k=5                                  | 74.21 | 62.13 | 71.31 | 5.13 | 8.14  | 6.35 |
| k=6                                  | 74.21 | 71.28 | 71.31 | 5.13 | 7.17  | 6.35 |
| k=7                                  | 74.21 | 72.36 | 71.31 | 5.13 | 15.41 | 6.35 |
| k=8                                  | 74.21 | 66.22 | 71.31 | 5.13 | 6.23  | 6.35 |
| k=9                                  | 74.21 | 78.22 | 71.31 | 5.13 | 8.31  | 6.35 |
| k=10                                 | 74.21 | 63.82 | 71.31 | 5.13 | 6.34  | 6.35 |
| Average                              | 74.21 | 68.67 | 71.31 | 5.13 | 9.1240 | 6.35 |

Figure 3. Comparison of elimination rate of the three algorithms

Clustering algorithm SOM has dependence on the selection of the initial value, and the parameter setting of the algorithm will also affect the running result, therefore, the result of the multiple running algorithm is not the same. the multiple running results of KNN and DBN are stable. We can select ten times running result of the algorithm and take the average to compare the three algorithms. It is easy to see that in terms of elimination rate, the results of the DBN model and the KNN algorithm are relatively stable, the result of the SOM algorithm fluctuates the most, the average of the DBN model results is the highest which is 2.9% higher than the KNN average result and 5.54% higher than the SOM average result. In the misuse rate, the average rate of false alarm elimination of DBN is 1.22% lower than that of KNN algorithm and 3.794% lower than that of SOM algorithm. The experimental results show that the DBN model is applied to the intrusion detection false alarm elimination, and it is more feasible to identify false alarm than KNN and SOM algorithms.
5. Conclusion and future work

Aiming at a large number of false alarms in intrusion detection, this paper proposes a DBN construction method based on genetic algorithm improving the particle swarm, and uses the DBN to eliminate false alarm in IDS: firstly, take advantage of the improved particle swarm algorithm to optimize the DBN network structure, secondly, optimize the network structure with optimal classification performance, lastly, use the corresponding DBN classifier for false alarm elimination in intrusion detection. Experimental results show that compared with the clustering algorithms SOM and KNN algorithms, this method can effectively improve the elimination rate and reduce the misuse rate. In order to further improve the elimination rate of intrusion detection, the next step is to improve the algorithm of this paper to build a better DBN network structure and improve the classification performance of the DBN model.

References
[1] Jiao J L, Jin D H, Zhou M N. Dominant Alarm Research and Implementation Based on Static Defect Detection[J]. CIMNS, 2017.
[2] Tan Q, Huang W, Li Q. An intrusion detection method based on DBN in ad hoc networks[C]// International Conference on Wireless Communication and Sensor Network. 2016:477-485.
[3] Sun Y, Gemmek K F, Cranen B, et al.. Using a DBN to Integrate Sparse Classification and GMM-Based ASR[J]. Proceedings of Interspeecch, 2010:2098-2101.
[4] Spathoulas G P, Katsikas S K. Reducing false positives in intrusion detection systems[J]. Computers & Security, 2010, 29(1): 35-44.
[5] Nurbu L, Xie N, Chen F, et al. A method of filtering out false positives based on conditional random fields[J]. Chinese Scientific Papers, 2012, 7(10): 757-761.
[6] Xie N N. Application of Machine Learning Method in Intrusion Detection[D]. Jilin University, 2015.
[7] Wu J, Zhang W, Ma Y. DATA ANALYSIS AND STUDY ON KDDCUP99 DATA SET[J]. Computer Applications & Software, 2014.
[8] Yapici H, Cetinkaya N. An Improved Particle Swarm Optimization Algorithm Using Eagle Strategy for Power Loss Minimization[J]. Mathematical Problems in Engineering, 2017, 401-403(5):550-556.
[9] Gao N, Gao L, Gao Q, et al. An Intrusion Detection Model Based on Deep Belief Networks[C]// Second International Conference on Advanced Cloud and Big Data. IEEE Computer Society, 2014: 247-252.
[10] Huang Y, Chen X. Research on intrusion detection technology[J]. Journal of Shenyang Electric Power Institute, 2004.
[11] Tanasa D, Trousse B. Advanced Data Preprocessing for Intersites Web Usage Mining[J]. Intelligent Systems IEEE, 2014, 19(2):59-65.
[12] Wang H, Yang H, Xu Z, et al. A Clustering Algorithm Use SOM and K-Means in Intrusion Detection[C]// International Conference on E-Business and E-Government. IEEE, 2010:1281-1284.