Research on Network Traffic Anomaly Detection of Source-Network-Load Industrial Control System Based on GRU-OCSVM

Xuesong Huo, Kehe Wu, Weiwei Miao, Liming Wang, Hui He, Dawei Su

1 State Grid Jiangsu Electric Power Co., Ltd. Power Dispatching Control Center, Nanjing 210000, China.
2 School of Control and Computer Engineering, North China Electric Power University, Beijing 102206, China.
3 Information and Communication Branch of State Grid Jiangsu Electric Power Co., Ltd., Nanjing 210019, China.

*Corresponding author e-mail: 754573146@qq.com

Abstract. With the large number of distributed generators and diverse loads connected to industrial control systems, there are more and more interactions among power supply, power grid and load. Any network link attack in the source network will affect the security of the industrial control system, resulting in economic loss of the industrial control system. Therefore, it is very important to study the network attacks against the source-network-load industrial control system. Aiming at the current insufficient situation of network traffic anomaly detection in the source-network-load industrial control system, this paper analysed the composition and flow characteristics of the source-network-load system, studied the scheme of network traffic anomaly detection of the source-network-load system, and proposed a network traffic anomaly detection algorithm based on GRU-OCSVM. The time characteristics of the traffic sequence were extracted by the GRU and input into OCSVM for traffic anomaly detection. Finally, the original network traffic of the source-network-load system was collected to construct anomaly detection data set for simulation experiment. The experimental results showed that the proposed method had high detection rate and low false positive rate, which can meet the needs of network traffic anomaly detection in the source-network-load system.

1. Introduction

With the rapid development of global energy Internet construction, ultra-high voltage power grid and distributed energy, new types of loads with double characteristics of "source" and "load" such as electric vehicles and controllable users are constantly emerging. The temporal and spatial distribution characteristics of power grid power flow are becoming increasingly complex. The importance and urgency of realizing interaction and cooperative control among power grid, power source and users are continuously increasing.

The essence of traffic anomaly detection problem is to find abnormal changes in traffic rules in the network. The traffic characteristics of network attacks are generally quite different from normal traffic types. The traffic detection algorithm detects attacks based on this principle. At present, network traffic...
anomaly detection mainly includes: methods based on statistical analysis, methods based on machine learning, and methods based on neural network.

In order to solve this problem, this paper analyzes the characteristics of the source network load control network traffic, analyzes the network protocol of the source network load control system, and proposes an anomaly detection method based on GRU - OCSVM to identify attack behavior and anomaly behavior, so as to improve the security protection level of the source network load control system.

2. Source Network Load Control System

Under the background of interaction between source network and load, the source network and load control system monitor and controls the power transmission and production operation of the source network and load system. It widely uses information network technology, and its networking and intelligence are getting higher and higher. At the same time, it also makes the system more vulnerable to attacks.

2.1. Analysis of Security Requirements for Source Network Load Control System

With the rapid increase of network attacks and security threats, network attacks against industrial control systems are also gradually increasing, and network security has become the top priority of security protection for power grid industrial control systems. Compared with the traditional industrial control system of power grid, the source network load system has the characteristics of "wider network, more interaction, newer technology and more extensive users", which has higher requirements for information security protection and also increases the difficulty of system security prevention.

When hackers break through the security protection of the system, attacks on the system will have serious consequences and affect the normal operation of the system. It is of great significance to improve the security level of the source network load control system to study the network traffic anomaly detection of the source network load control system and discover the attack behavior and anomaly behavior in time.

2.2. Feature Processing

When the data is input into the detection model, it is necessary to extract feature vectors and preprocess the collected data. Because a single data packet cannot reflect the current state of network traffic, it is necessary to analyze the data traffic for a period of time.

In this paper, the time window method is used to extract data feature attributes. During the construction of anomaly vectors, entropy values of each dimension in a time window are calculated. The change information of the dimension attribute can be obtained through entropy value.

Let the size of the time window be W, and move forward L (L < W) each time. As shown in fig. 1, let time window $T_{02}$ be $(t_0, t_2)$ and time window $T_1$ be $(t_1, t_3)$, where:

$$L = t_2 - t_1 = t_2 - t_0$$
$$W = t_2 - t_0 = t_3 - t_1$$

![Fig.1 Graphic of time window](image)

Let traffic flow\(p_1(T_1, T_2), p_2(T_1, T_2), \ldots, p_n(T_1, T_2)\) be traffic characteristic information on a time window, where there are n data packets, $T_i$ represents the characteristic attributes of the data packets. $T_i$ has $m_i$ possible values. If the number of packets with value j is $n_i$, the entropy of $T_i$ is:

$$H(T_i) = \sum_{j=1}^{m_i} \frac{n_i}{n} \ln \left( \frac{n_j}{n} \right)$$

In this paper, the entropy quantification of type identifier, transmission reason, source IP, destination IP, source port, destination port and protocol type is carried out on the time window respectively. In
abnormal flow, the entropy of these features may be quite different from that in normal state, providing basis for anomaly detection.

3. Algorithm Analysis

In order to improve the detection accuracy and reduce the detection false alarm rate, this paper proposes to use GRU-OCSVM to detect network traffic anomaly. The automatic encoder based on GRU extracts the features of the traffic feature sequence, and the extracted features are input to OCSVM for anomaly detection.

3.1. GRU Neural Network

Gated Recurrent Unit, GRU is a special kind of recurrent neural network (RNN), which can extract the time characteristics between network traffic data. GRU is an improved model of Long Short Term Memory, LSTM and is composed of Cho K. Compared with the traditional RNN, GRU avoids the problems of gradient disappearance and gradient explosion. Fig. 2 is a structural diagram of GRU. GRU realizes the calculation of update gate and reset gate, namely $z_t$ and $r_t$ in the figure. The update gate is used to control the degree to which the state information at the previous time is brought into the current state. The larger the value of the update gate, the more the state information at the previous time is brought in. The reset gate is used to control the degree to which the state information at the previous time is ignored. The smaller the value of the reset gate, the more is ignored.

The following expression can be used to indicate that GRU propagates forward.

$$r_t = \sigma(W_r x_t + U_r h_{t-1} + b_r)$$  \hspace{1cm} (4)

$$z_t = \sigma(W_z x_t + U_z h_{t-1} + b_z)$$  \hspace{1cm} (5)

$$\tilde{h}_t = g(W_h x_t + U_h (r_t \circ h_{t-1}) + b_h)$$  \hspace{1cm} (6)

$$h_t = (1 - z_t) h_{t-1} + z_t \tilde{h}_t$$  \hspace{1cm} (7)

Fig.2 Structure of GRU

Wherein $r_t$, $z_t$, $\tilde{h}_t$ and $h_t$ respectively represent reset gate state, update gate state, update activation of time $t$ and hidden activation of time $t$ $W, U, B$ represent the weight of input, weight and deviation of hidden cells. $\sigma$ means Sigmoid function, $g$ means ReLu function.

In order to extract the most useful information from the traffic feature sequence and reduce the feature dimension of the data, this paper uses an automatic encoder to analyze and process the traffic feature data. Automatic coding machine is an unsupervised learning method based on neural network, which is mainly used for centralized representation of learning input. These centralized representations can reflect most important and key information in the original data set.

In this model, $X = (x_1, x_2, ..., x_n)$ is an n-dimensional random variable, and the main goal of the automatic encoder is to minimize the reconstruction error, that is, the original input and output are as equal as possible.

The automatic encoder first passes the input $x$ through the encoder to generate an intermediate vector $C$, and then uses $C$ as the input of the decoder to obtain the output $\hat{X}$ through the decoder. As shown in the figure.
Since the goal of the automatic encoder is to make the input $x$ and output $\tilde{x}$ as close as possible, we use cross entropy to measure the difference between $x$ and $\tilde{x}$.

$$
\text{loss} = \sum_{i=1}^{n} -[x_i \cdot \log \tilde{x}_i + (1 - x_i) \cdot \log(1 - \tilde{x}_i)]
$$

The smaller the value of loss, the closer the sum of $x$ is.

### 3.2. Single Class Support Vector Machines

Different from support vector machine (SVM), single-class support vector machine (OCSVM) only needs one class of samples to train anomaly detection model, which is an unsupervised anomaly detection method. It can be used to solve some cases where only one class of samples can be used to train classifiers. The idea of standard SVM is to construct a generalized optimal classification surface, making the two types and two types of data points of the training data set be located on both sides of the classifier as far as possible, and making the interval between the two types of data points as close as possible. OCSVM assumes that the coordinate origin is an abnormal sample, and constructs an optimal hyperplane in the feature space to realize the maximum interval between the data target and the coordinate origin. The task of OCSVM classification is to find a function $f(x)$, if the value of $f(x)$ is positive, data $x$ is considered normal; if the value of $f(x)$ is negative, data $x$ is considered abnormal.

One-class support vector machine solves the following quadratic programming problem:

$$
\min_{\xi \in \mathbb{R}^l, \rho \in \mathbb{R}} \frac{1}{2} \||\omega||^2 + \frac{1}{\nu} \sum_{i=1}^{l} \xi_i - \rho
$$

s.t. $f(x_i) = \phi(x_i)\omega - \rho \geq -\xi_i, \ \xi_i \geq 0$

Where $x_i$ is the sample in the original space, $l$ is the number of training samples, $\phi$ is the mapping from the original space to the feature space, $\omega$ and $\rho$ are the normal vector and compensation of the required hyperplane in the feature space respectively, the adjustable parameter $\nu \in (0,1)$ is the upper bound for controlling the proportion of erroneous samples in the total number of samples, and the relaxation variable $\xi_i$ is the degree to which some training samples are misclassified.

The selection of kernel function has an important influence on the accuracy of OCSVM detection. Literature has proved that radial kernel function has better accuracy in detection. In this paper, radial kernel function $K(x, y) = e^{-|x-y|^2/(2\sigma^2)}$ and adjustable parameter $\nu$ are selected to solve the following optimization problem and $\alpha^* = (\alpha_1^*, ..., \alpha_l^*)$:
\[
\min_{\alpha} \frac{1}{2} \sum_{i=1}^{l} \sum_{j=1}^{l} \alpha_i \alpha_j K(x_i, x_j)
\]
\[\text{s.t. } 0 \leq \alpha_i \leq \frac{1}{\nu_l}, \quad i = 1, \ldots, l
\]
\[\sum_{i=1}^{l} \alpha_i = 1
\]

Select \(\alpha^*\) which satisfies \(0 < \alpha^* < \frac{1}{\nu_l}\), and calculate \(\rho = \sum_{i}^{l} \alpha_i^* K(x_i, x_j)\), where \(\alpha\) satisfying \(0 < \alpha^* < \frac{1}{\nu_l}\) \(\alpha^*\) is the support vector.

The integration decision function \(f(x) = \sum_{i}^{N_{sv}} \alpha_i^* K(x_i, x) - \rho\), if \(f(x) > 0\), then return +1, meaning the data is normal data, \(f(x) < 0\), then return -1, meaning the data is abnormal data. \(N_{sv}\) is the number of support vectors.

3.3. Model Building

This paper designs a GRU-OCSVM detection model. Its structure is shown in the figure.

![Fig. 4 Structure of detection model](image)

The model consists of an automatic encoder based on GRU and an OCSVM classification model. The automatic encoder extracts the time features in the traffic sequence and reduces the dimension of the feature vectors, thus improving the efficiency of OCSVM in data processing.

In the data input stage, in order to eliminate dimensional differences between different dimensions of the data, the data in the training data are standardized by using the Min-max method. The range of standardization is \([0, 1]\). The expression is as follows:

\[
y = \frac{x - x_{\text{min}}}{x_{\text{max}} - x_{\text{min}}}
\]

4. Experimental Results and Analysis

4.1. Feature Extraction and Analysis of Automatic Coding Machine Based on GRU

In this experiment, we first analyze the training results of automatic encoder based on GRU.

The running environment of the experiment is windows 10 operating system and 8G memory hardware environment, and the algorithm model is built based on tensorflow. The experimental data collected the network traffic of Jiangsu Huashen 110KV substation. After screening and data processing, a total of 2,000 characteristic samples were obtained, of which 1,500 were selected as training samples and the remaining 500 as test samples. Input the sample sequence into the automatic coding machine for training, and extract the key features of the sample sequence.

As can be seen from fig. 5, with the increase of iteration times, the training error gradually decreases, and after eight iterations, the reconstruction error begins to stabilize.

As can be seen from fig. 6, with the increase of iteration times, the training error gradually decreases, and after eight iterations, the reconstruction error begins to stabilize.
As can be seen from fig. 6, when the number of iterations reaches seven, it starts to converge rapidly. as the number of iterations increases, the accuracy becomes more and more stable. From the above, it can be found that the training results are basically stable in a small number of iterations, and the effect is getting better and better with the increase of iterations.

4.2. Abnormal Sample Generation
OCSVM trains the normal flow model through normal samples. In order to verify the performance of the trained normal flow model, it is necessary to generate abnormal flow data for model verification.

The normal flow in this paper is collected from 110kv substation, and the abnormal flow selects abnormal samples from common data set. The normal sample and abnormal sample are combined into a new data set for model detection, i.e. test set.

The common data set used for abnormal data extraction in this paper is CICIDS2017. CICIDS2017 data set is a public data set of Canadian Network Security Institute (CIC) of New burns Wake University (UNB). This data set includes 3.1 million flow records. The data set collected the flow data for the 5 days starting from July 3, 2017, and 81 features were extracted from it. The data set consists of marked network flow groups, including complete data packets in PCAP format, corresponding marked data flow files, and CSV files that can be used for machine learning and depth learning purposes. As a classic intrusion detection data set, KDD99 data set can no longer meet the needs of current traffic anomaly detection. CICIDS2017 dataset contains normal traffic and the latest common attack traffic, including DoS, DDoS, port scanning, botnet, infiltration, etc.

4.3. The Experimental Evaluation
In order to evaluate the performance of the model, this paper compares the model with PCA-OCSVM and simple OCSVM models. Verify on 3 test sets respectively.

|                  | OCSVM | PCA-OCSVM | GRU-OCSVM |
|------------------|-------|-----------|-----------|
| Detection rate (%) | 97.00 | 96.67     | 98.33     |
| False alarm rate (%) | 1.59  | 1.63      | 1.25      |
From the above results, it can be seen that the method described in this paper has higher detection flow and lower false alarm rate, and the detection capability has been greatly improved.

5. Conclusion
In view of the lack of network traffic anomaly detection system in the current source network load control system, this paper studies the network traffic anomaly detection in the source network load control system. According to the characteristics of the source network load control system protocol, an unsupervised network traffic anomaly detection method based on GRU-OCSVM is proposed. Experimental results show that the detection rate and false alarm rate of this method are greatly improved compared with the traditional OCSVM network traffic anomaly detection method. It can more accurately identify abnormal behaviors in traffic and reduce the false alarm rate of the system.

Acknowledgments
This work was supported by the Science and Technology Project of the State Grid Corporation of China under Grant 5210021800U.

References
[1] Yao Jianguo, Yang Shengchun, Wang Ke, et al. Concept and research framework of smart grid "source - network - load" interactive operation control [J]. Power system automation, 2012, 36 ( 21 ): 1 - 6 + 12.
[2] Hou Zhongyuan, Jianghan Hong, Rui Wanzhi, Liu Liang. Probabilistic Principal Component Analysis Method for Industrial Network Traffic Anomaly Detection [J]. Journal of Xi ’an Jiaotong University, 2012,46 ( 02 ): 70 - 75.
[3] Zheng Liming, Zou Peng, Jia Yan, Han Weihong. Research on the Extraction and Training Methods of Classifiers in Network Traffic Anomaly Detection [J]. Chinese journal of computers, 2012, 35 ( 04 ): 719 - 729 + 827.
[4] Xia Fei, Bao Lishan, Wang Jijun, Zhuang Ling, Li Hucheng. Introduction to Communication Networking Scheme of Source Network - Holland Friendly Interactive System [J]. Jiangsu Electric Engineering, 2016, 35 ( 06 ): 65 - 69.
[5] Liu Yali, Meng Lingyu, Ding Yunfeng. Application and algorithm improvement of flow anomaly detection in power grid industrial control system [J]. Computer system application, 2018, 27 ( 03 ): 173 - 178.
[6] Lin li, Shang Wenli, Yao Jun, Zhao Jianming, Ceng Peng. Review on the Application of Single - class Support Vector Machines in Intrusion Detection of Industrial Control Systems [J]. Computer Application Research, 2016,33 ( 01 ): 7 - 11.
[7] Lin li, Shang Wenli, Yao Jun, Wan Ming, Ceng Peng. Intrusion Detection Algorithm for Industrial Control System PCA-OCSVM [J]. Computer Engineering and Design, 2016, 37 ( 11 ): 2928 - 2933.
[8] Cho K, Van Merrienboer B, Gulcehre C, et al. Learning Phrase Representations using RNN Encoder-Decoder for Statistical Machine Translation[J]. Eprint Arxiv, 2014.