An abnormal traffic detection method in smart substations based on coupling field extraction and DBSCAN

Jianwei Tian[1,4], *Zongchao* Yu[2,*], *Li* Liu[3], *Weidong* Wu[3], *Hongyu* Zhu[1,4], and *Xuan* Liu[2]

[1]State Grid Hunan Electric Power Company Limited Information and Communication Company, Changsha, China
[2]College of Electrical and Information Engineering, Hunan University, Changsha, China
[3]State Grid Hunan Electric Power Co., Ltd., Changsha, China
[4]Hunan Key Laboratory of Ubiquitous Power Internet of Things, Changsha, China

Abstract. Smart Substation becomes more vulnerable to cyber attacks due to the high integration of information technologies, so it is essential to detect intrusion behaviour by abnormal traffic analysis in smart substations. Although there have been many detection methods for abnormal traffic, the existing ones all focus on the format check of a single field of the industrial transmission protocol, and ignore the deep coupling relationships among multiple protocol fields, which lead to more or less false detections and missed detections. To overcome this problem and further improve the detection accuracy, in this paper, we propose an abnormal traffic detection method based on the coupling field extraction and the density-based spatial clustering of applications with noise (DBSCAN). By using correlation analysis to extract the coupling fields of the protocol fields and using DBSCAN to remove the noise in the coupling fields, the deep coupling relationship between the coupling fields can be mined by the piecewise linear function fitting method, and used to detect abnormal traffic. The simulation results on 10,000 frames traffic prove that the proposed detection method can effectively identify the abnormal traffic.
Keywords. Abnormal traffic detection; Coupling fields; DBSCAN; Piecewise linear function fitting; IEC 60870-5-104.

1 Introduction

With the continuous coupling of communication networks and power systems, traditional power grids are rapidly transforming into cyber-physical power systems (CPPS)[1]-[2]. In the modern smart grid, the electricity supply network plays the role of transmitting electric energy, and the communication networks are responsible for transmitting control signals and so on. On the one hand, the power system has become more flexible because of the integration of communication technologies. On the other hand, since the communication network will transmit many important data of the power system, how to ensure the security of the data transmitted in the communication network has also become a

* Corresponding author: zongchaoyu@hnu.edu.cn

huge challenge. In other words, it is very necessary to accurately detect abnormal traffic in the power system.

The smart substation is the core node of the smart grid. The accuracy of the data transmitted through the smart substation directly affects the safe and stable operation of the power grid. At present, the communication protocol between a smart substation and the control center is the International Electro technical Commission (IEC) 60870-5-104 (recorded as IEC-104), which is more likely to be attacked due to the lack of the corresponding encryption and authentication mechanism in the data transmission process [3]-[4]. Therefore, it is necessary to develop the corresponding anomaly traffic detection for the IEC-104 protocol to improve the security level of the power system, which also falls the scope of this paper.

Considering the frequent occurrences of cyber events in recent years, several abnormal traffic detection methods have been proposed to mitigate the risk of cyber attacks. In ref.[5], a method based on the principal component analysis (PCA) was proposed to detect the modified data by separating the power flow variability into regular and irregular subspaces. And a Kullback-Leibler distance (KLD) detection method was proposed in ref. [6]. The authors in [7] proposed an abnormal data detection method to explore the spatial and temporal inconsistency between normal data and abnormal data by using discrete wavelet transform and deep neural network. Besides, some detection methods based on machine learning have also been studied. In ref.[8], an abnormal traffic detection method based on Particle Swarm Optimization (PSO) optimal Elman neural network was proposed. And a deep learning based long short term memory method was proposed to detect the abnormal traffic in [9]. More works about traffic detection can be found in [10]-[13].

However, most of the above detection methods focus on the general statistical characteristics of the traffic in substations, and only consider the format check of a single field of the IEC 104 protocol. The coupling relationships between the protocol fields are ignored. Even the machine learning method has been used for traffic detection, the detection rules of protocol fields cannot be well set up, leading to missed detections or false detections with a high probability.

To overcome the shortcomings of the existing detection methods, we in this paper propose an abnormal traffic detection method based on the coupling field extraction and DBSCAN. First, the coupling fields are automatically extracted by using correlation analysis. Then, the DBSCAN method is used to remove the noise points in the coupling fields. Finally, the deep relationships between the coupling fields are mined by using piecewise linear function fitting, which are used to detect the abnormal traffic.

2 The IEC 60870-5-104 protocol

The functionality of the IEC-104 mainly relies on the TCP/IP, which inevitably introduces many network security problems into the smart substation. So, it is necessary to carry out abnormal detection on the traffic data of the IEC-104 protocol. First, we analyze the protocol structure of the IEC-104. The application layer of the IEC-104 protocol consists of a basic communication unit, named as Application Protocol Data Unit (APDU), and APDU can be further divided into Application Protocol Control Information (APCI) and Application Service Data Unit (ASDU)[14]. The detailed structure of the IEC-104 is illustrated in Figure 1.

As shown in Figure 1, the IEC-104 protocol defines the start character (68H) and the maximum length specification of APDU (max.253) and control fields. By defining different values of control fields, the IEC-104 protocol formulates three corresponding APCI frame formats, which are *I*-format, *S*-format, and *U*-format, respectively.

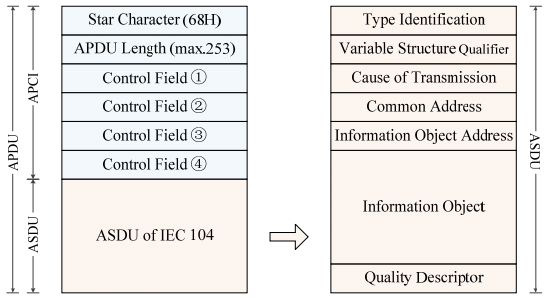

Fig. 1. The structure of IEC 60870-5-104.

In practice, the definition of each field of an ASDU customized by the IEC 104 used by a smart substation are as follows: The field of type identification (TI) represents the byte length of the data in information object; The field of variable structure qualifier (VSQ) represents the number of the data in information object; And the cause of transmission (CT) represents the command type corresponding to the frame message, such as sudden upload (03), activation (06), activation confirmation (07), response to the general call (20) and so on. The meaning of the other fields in the ASDU is straightforward and will not be explained.

However, the IEC-104 protocol lacks any encryption measures, which makes it vulnerable to cyber attacks, such as DDoS attacks, false data injection attacks, man-in-the-middle attacks and so on. Therefore, it is necessary to carry out anomaly detection on the data transmitted by the IEC-104 protocol.

3 The detection method based on coupling field extraction and DBSCAN

In this section, we proposed an abnormal traffic detection method based on coupling field extraction and DBSCAN for smart substations (take the IEC-104 protocol as an example in this paper). As mentioned in section I, the existing abnormal traffic detection methods are partly based on the payload transmitted in the protocol, and partly on the statistical characteristics of the traffic, which both ignore some inherent features contained in each frame of traffic itself. However, if the data in the traffic is slightly tampered with, the detection methods based on the above two principles will not be able to detect such attacks. To overcome the disadvantages of the existing detection methods and discover the internal relationships among protocol fields, a coupling field extraction method is proposed to perform the correlation analysis. Then, the DBSCAN clustering algorithm is used to further reduce the noise in the data of the coupling field.

3.1 The method of coupling field extraction

Since the master station stores a large amount of traffic data, it provides a basis for correlation analysis among protocol fields. By using correlation analysis, we can know the degree of correlation between two or more protocol fields, that is, when one field changes, the other field also changes. This phenomenon is more obvious in the protocol traffic of the smart substation. If the correlation between some fields is very prominent, they are defined as the coupling fields. Furthermore, the correlation of coupling fields is used to verify each protocol field to achieve the purpose of abnormal traffic detection.

Pearson correlation coefficient is currently one of the most commonly used correlation analysis methods, but it can only be applied to continuous data, and there are discrete data

in the IEC 104 protocol, so this paper adopts the Spearman correlation coefficient method. In addition, to further improve the reliability of the correlation analysis, the Kendall correlation coefficient method is also employed to further improve the reliability of the correlation analysis for increasing the accuracy of the abnormal traffic detection.

I: Spearman correlation coefficient.

Assuming that the dataset of two random protocol fields are **X**, **Y**, and the number of two datasets both are *N*. First, we sort **X** and **Y** (ascending or descending at the same time), and get two new datasets **x**, **y**. And x_i and y_i represent the *i*-th element in **x** and **y**, respectively. Then, we can calculate the Spearman correlation coefficient by using the following equation:

$$\rho = 1 - \frac{6\sum_{i=1}^{N}(x_i - y_i)^2}{N(N^2-1)} \tag{1}$$

where ρ is the value of Spearman correlation coefficient.

II: Kendall correlation coefficient.

Assuming that the dataset of two random protocol fields are **X**, **Y**, and the number of two datasets both are *N*. And X_i and Y_i represent the *i*-th element in **X** and **Y**, respectively. And if $(X_i < X_j) \wedge (Y_i < Y_j)$ or $(X_i > X_j) \wedge (Y_i > Y_j)$, we denote them as consistency; if $(X_i < X_j) \wedge (Y_i > Y_j)$ or $(X_i > X_j) \wedge (Y_i < Y_j)$, we denote them as inconsistency; if $(X_i = X_j) \wedge (Y_i = Y_j)$, we denote them as equivalent. Then, we can calculate the Kendall correlation coefficient by using the following equation:

$$\tau = \frac{A - B}{\sqrt{(M_3 - M_1)(M_3 - M_2)}} \tag{2}$$

$$\begin{cases} M_1 = \sum_{i=1}^{S} \frac{1}{2} U_i(U_i - 1) \\ M_2 = \sum_{i=1}^{T} \frac{1}{2} V_i(V_i - 1) \\ M_3 = \frac{1}{2} N(N-1) \end{cases} \tag{3}$$

where τ is the value of the Kendall correlation coefficient. *A* represents the number of elements in **X** and **Y** that meet the consistency, and *B* represents the number of elements in **X** and **Y** that meet the inconsistency. And S and T are the number of equivalent sets in **X** and **Y**, U_i and V_i represent the number of elements in each equivalent set of **X** and **Y**.

3.2 The DBSCAN clustering algorithm

DBSCAN is a typical density-based clustering method which has been proved to have the advantage of finding noise points which represent the extreme scenarios of coupling fields. This clustering model contains two important parameters: *Eps* (the threshold of the neighborhood distance) and *MinPts* (the minimum number of samples in the neighborhood), which can be recorded as ϵ and M. DBSCAN can automatically classify data according to the density of data, and find the noise points that are considered as extreme scenarios.

As shown in Figure 2, the core idea of DBSCAN is to start with one point, if the point is a core point, then expand the cluster of this point according to the density-reachable rule, and filter out all the core points, border points and noise points based on those rules in [15]. By using the DBSCAN method, we can find and reduce the noise points in the data of coupling fields. And the selection of the two parameters of DBSCAN (ϵ and M) will be given in the case study. Moreover, the above coupling field extraction and DBSCAN method are the basis of the abnormal traffic detection, the corresponding detection methods are still needed to make reasonable use of the features obtained by the two parts, which will be discussed in the next section.

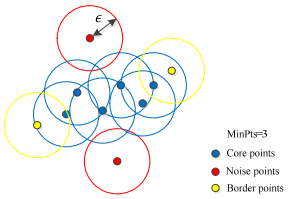

Fig. 2. The schematic diagram of the DBSCAN clustering method.

3.3 The abnormal traffic detection method

As mentioned above, after the processing of the coupling field extraction and abnormal coupling field elimination, a detection model is needed to measure the numerical relationship between coupled fields.

The whole process of the proposed abnormal traffic detection method is illustrated in Figure 3, and the detailed steps are summarized as follows:

Step-1: Collect historical traffic data and parse out the value corresponding to each protocol field.

Step-2: Calculate the correlation coefficient matrix of all protocol fields by using the Spearman correlation coefficient method and the Kendall correlation coefficient method. Define two protocol fields with a correlation coefficient not less than 0.6 as a coupling field, and extract all coupling fields according to the correlation coefficient matrix.

Step-3: Determine the noise points of the coupled fields of discrete data by using the DBSCAN method. It is worth noting that the DBSCAN clustering algorithm is only for the coupled fields of discrete data.

Step-4: Aiming at the coupled fields of continuous data, this paper uses piecewise linear function fitting to realize the mining of numerical relationships. Next, we will explain in detail how the piecewise nonlinear function fitting is achieved.

1) Piecewise: Assuming that the extracted coupling fields after DBSCAN are coupling fields **A**, **B** and **C**. The data in coupling fields **A** and **B** are continuous, and the data in coupling field **C** is discrete. Therefore, for each coupling field element C_i in **C**, a function fitting $B = f(A)$ of its corresponding coupling fields A_i and B_i in **A** and **B** needs to be made. This process is defined as piecewise fitting in this paper.

2) Normal coupling field: As mentioned above, we need to perform function fitting for each coupling field element C_i in **C**. And if the C_i can correspond to a series of coupled data $(A_i, B_i), (A_{i+1}, B_{i+1}), \dots, (A_{i+n}, B_{i+n})$ in **A** and **B**, we can easily fit the corresponding function. This process is defined as normal coupling field fitting in this paper, and the linear function fitting method based on the least square method is as follows:

$$B_i = \hat{\beta}_0 + \hat{\beta}_1 A_i + e_i \tag{4}$$

$$e_i = B_i - \hat{\beta}_0 - \hat{\beta}_1 A_i \tag{5}$$

where e_i is the fitting error of sample (A_i, B_i). And $\hat{\beta}_0$ and $\hat{\beta}_1$ are the constant coefficients of the fitting function.

Generally, the purpose of the least squares method is to minimize the squared loss function value corresponding to the fitting function, where the squared loss function Q is calculated as follows:

$$Q = \sum_{i=1}^{n} (B_i - \hat{\beta}_0 - \hat{\beta}_1 A_i)^2 \tag{6}$$

By performing the function fitting on the normal coupling field data, one can get the values of e_i, $\hat{\beta}_0$ and $\hat{\beta}_1$, which will be used in the subsequent abnormal traffic detection.

3) Special coupling field: If the C_i only correspond to a set of coupled data (A_i, B_i) in **A** and **B**, it is difficult for us to determine a unique set of the corresponding function. This process is defined as special coupling field fitting in this paper.

In order to reduce the appearance of more different piecewise functions, we first use the function coefficients obtained by the normal coupling fields fitting to verify whether the special coupling fields can be satisfied. If yes, one uses the corresponding function coefficient; if not, the linear fitting method is used above to refit for obtaining the corresponding function coefficient.

Step-5: Extract the corresponding coupling field of the real-time traffic, and determine whether the coupling field is the noise points selected by the DBSCAN clustering algorithm. If yes, record it as the abnormal traffic; if not, go to step-6.

Step-6: Calculate the error according to the corresponding piecewise function coefficient. If the error of the real-time traffic exceeds the corresponding value e_i, record it as the abnormal traffic; otherwise, record it as the normal traffic.

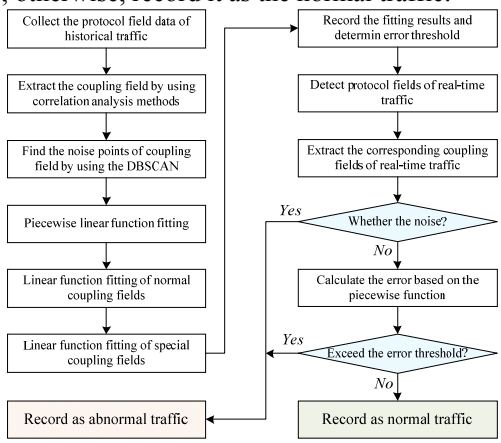

Fig. 3. The process of the proposed abnormal traffic detection method.

Based on the above proposed abnormal traffic detection method, we can detect abnormal traffic that cannot be detected by the conventional methods, even if the protocol data has been slightly tampered with. Unlike the existing methods that only perform abnormal detection on the general statistics of network traffic, the proposed method investigates the coupling relationships between protocol field data. By doing so, the proposed method can further reduce, and improve the detection accuracy of abnormal traffic by reducing the rate of missed detection.

4 Case study

In this section, we use 100,000 frames of traffic data (IEC-104) from a substation in a province of China to test the proposed abnormal traffic detection. Simulations are carried out on a 3.9GHz personal computer with 8GB of RAM.

4.1 The result of coupling field extraction

First, we need to extract all the protocol fields of the IEC-104 protocol. A total of 10 protocol fields have been extracted in this paper. APDU length (**AL**) represents the length

of APDU; Data type (**DT**) and data byte length (**DB**) are obtained from the type identification field, and DT represents the type of data in the information object, **DB** is the byte length of data in the information object; Variable structure qualifier (**VSQ**) represents the number of the data in the information object; And cause of transmission (**CT**) represents the command type corresponding to the frame message; And the five protocol fields in the quality descriptor of the information object, namely **BL**, **SB**, **NT**, **IV** and **SPI**, and the detailed explanation can be found in paper [16].

In order to speed up the correlation analysis, we divide the 100,000 frames of traffic data into 10 groups. Then, the corresponding correlation coefficient matrices are calculated respectively, and finally calculate the average value of the 10 correlation coefficient matrices as the overall correlation coefficient matrix. And the correlation coefficient matrices of Spearman and Kendall are listed in Table I.

In Table I, the upper triangle part is the result of the correlation coefficient matrix determined by Spearman method, and the lower triangle part is the result of the correlation coefficient matrix determined by Kendall method. Based on Table I, we can see that the results of the Kendall and Spearman methods are roughly the same, which can verify the correctness of the correlation results. And note that the correlation coefficients of protocol fields **BL**, **SB**, and **IV** are all '-', the reason is that the data of these three protocol fields are constant. Besides, it can be observed that the protocol fields **AL** and **VSQ** are related; and the protocol fields **DT** and **DB, DT** and **CT** are related, and the protocol fields **DB** and **CT** are also related. Therefore, we can get the coupling fields in the IEC-104 protocol, which are listed in Table II.

And in coupling field 1, the data of **AL** and **VSQ** are continuous data. In coupling field 2, the data of **DT**, **DB**, and **CT** are discrete data. In order to verify the effectiveness of the proposed abnormal traffic detection method based on the coupling field, the above coupling fields in the 20 frames of normal traffic are modified for evaluating the accuracy rate of the proposed method.

Table 1. The results of correlation coefficient matrices.

ρ	AL	DT	DB	VSQ	CT	BL	SB	NT	IV	SPI
AL	1	0.07	-0.08	**0.94**	0.17	-	-	-	0.03	-0.05
DT	0.11	1	**-0.98**	0.37	**0.86**	-	-	-	0.14	0.47
DB	-0.11	**-0.99**	1	-0.38	**-0.85**	-	-	-	-0.14	-0.47
VSQ	**0.93**	0.31	-0.31	1	0.43	-	-	-	0.06	0.18
CT	0.17	**0.88**	**-0.87**	0.35	1	-	-	-	0.12	0.41
BL	-	-	-	-	-	-	-	-	-	-
SB	-	-	-	-	-	-	-	-	-	-
NT	-	-	-	-	-	-	-	-	-	-
IV	0.02	0.16	-0.16	0.05	0.14	-	-	-	1	0
SPI	0.00	0.36	-0.36	0.11	0.32	-	-	-	0	1

Table 2. The Results of Coupling Fields.

Coupling field 1	Coupling field 2
{AL, VSQ}	{DT, DB, CT}

4.2 The result of DBSCAN

Considering the speed of the DBSCAN clustering, we first preprocess 10 groups of traffic data. We only extract all non-repeated protocol field traffic data, and filtered out massive amounts of completely consistent protocol data. After the preprocessing, we get 516 sets of protocol data.

Then, as mentioned in section III.C, DBSCAN clustering algorithm is used to eliminate the noise data in the discrete coupled field (coupling field 2 in this paper). After the optimal

selection of multiple sets of parameters ϵ and M, the clustering algorithm has the best performance when ϵ =1 and M =4, so the parameters ϵ and M are set as 1 and 4.

The results of the DBSCAN method are shown in Figure 4. And the size of the point reflects the number of occurrences in the total 100,000 frames of the traffic data, and the points with a small number of occurrences are screened out and recorded as noise points. According to Figure 4, it can be seen that there are 2 noise points, and the corresponding values of {**DT**, **DB**, **CT**} are {100, 1, 3} and {200, 1, 5}. The remaining normal coupling fields will be used in the piecewise linear function fitting, and their corresponding values of {**DT**, **DB**, **CT**} will also be given.

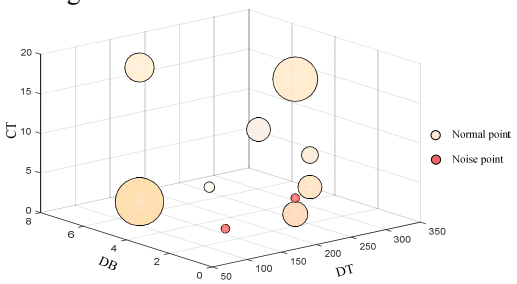

Fig. 4. The process of the proposed abnormal traffic detection method.

4.3 The result of linear function fitting

Based on the results of normal coupling fields determined by the DBSCAN, we extract the coupling field {**AL**, **VSQ**} corresponding to each coupling field {**DT**, **DB**, **CT**}, and use the least squares method to fit the linear function between protocol fields **AL** and **VSQ**. In order to reduce the influence of abnormal traffic on the function fitting results, we use iterative fitting and verification methods to obtain the final fitting function. For each coupling field of {**DT**, **DB**, **CT**}, we first perform function fitting on the corresponding coupling field {**AL**, **VSQ**}, calculate the average error of the fitting result, and delete the data larger than the average error in the coupling field {**AL**, **VSQ**} until that no data is deleted or the average error is less than 1, then stop the iteration and record the final fitting function. And the general formula of the fitting function is $AT = k_1 * VSQ + k_2 + e$, the results of linear function fitting are listed in Table III.

Table 3. The results of linear function fitting.

{DT,DB,CT}	k_1	k_2	e
{100, 5, 3}	8	10	0
{100, 5, 20}	5	13	0
{200, 1, 3}	4	10	0
{200, 5, 3}	11	10	0
{200, 1, 20} {222, 1, 6} {222, 1, 7} {222, 1, 10}	1	13	0
{333, 7, 6} {333, 7, 7}	7	13	0

In Table III, we can see that there are a total of 10 coupling fields of {**DT**, **DB**, **CT**}, and the corresponding coupling fields {**AL**, **VSQ**} are fitted to 6 different linear functions. Due to the numerical relationship between the protocol fields of the IEC-104 traffic data in the substation, the values of e obtained by the fitting function are all 0.

4.4 The result of abnormal traffic detection

In this section, we will use the proposed abnormal traffic detection method and the original DBSCAN method to detect the abnormal behavior of the 100,000 frames of traffic data. And the detection results of the proposed method based on the fitting functions and DBSCAN method are listed in Tables IV and V, respectively.

It can be seen from Table IV that the proposed method accurately detect 20 frames of abnormal traffic, among which, the coupling field {**AL**, **VSQ**} of the 18 frames of abnormal traffic data (black font) cannot satisfy the corresponding fitting function, and the coupling field {**DT**, **DB**, **CT**} of the other 2 frames (red font) cannot match the normal points determined by DBSCAN.

On the other hand, it can be seen from Table V that the original DBSCAN method cannot successfully detect all abnormal traffic. And the original DBSCAN method detects a total of 6 frames of abnormal traffic, but 4 frames (black font) are false detections. Therefore, we can see that the detection accuracy of the proposed detection method is 100%, while the accuracy of the original DBSCAN detection method is only 10%. The results indicate that the proposed method can effectively utilize the deep coupling relationships in the protocol field to detect abnormal traffic, so as to overcome the disadvantage of the existing detection method that does not consider the protocol field.

Table 4. The detection results of the proposed method.

{DT,DB,CT}{AL,VSQ}	{DT,DB,CT}{AL,VSQ}	{DT,DB,CT}{AL,VSQ}
{100,5,3}{186,20}	{200,5,3}{162,14}	{100,5,20}{193,38}
{100,5,3}{17,1}	{100,5,20}{196,36}	{222,1,10}{18,1}
{222,1,6}{16,1}	{333,7,6}{20,2}	{100,5,3}{40,3}
{222,1,7}{14,2}	{333,7,7}{22,1}	{100,5,3}{58,7}
{200,1,20}{83,72}	{100,5,3}{202,25}	{200,1,5}{14,1}
{200,1,3}{12,1}	{100,5,3}{180,9}	{100,1,3}{138,16}
{200,5,3}{252,21}	{100,5,3}{114,25}	

Table 5. The detection results of original DBSCAN method.

{DT,DB,CT}{AL,VSQ}	{DT,DB,CT}{AL,VSQ}	{DT,DB,CT}{AL,VSQ}
{200,5,3}{252,22}	{200,5,3}{164,14}	{200,5,3}{252,21}
{200,5,3}{252,22}	{200,5,3}{164,14}	{200,5,3}{162,14}

5 Conclusions

In this paper, we propose an abnormal traffic detection method based on coupling field extraction and DBSCAN for smart substations. The coupling fields are identified by correlation analysis, and the DBSCAN method is used to remove the noise points in the coupling fields. Finally, the deep relationships between the coupling fields are mined by using piecewise linear function fitting, which are used to detect the abnormal traffic. By performing the coupling field extraction and piecewise linear function fitting on 10,000 frames of traffic data, the corresponding simulation results prove that the proposed method can accurately detect the abnormality of the protocol fields of the IEC 104 protocol. In the future, we will study the logical relationship between the frames to enhance the performance of the abnormal detection of traffic data in smart substations.

Acknowledgment

This work was supported by the 2020 industrial Internet innovation and development project - smart energy Internet security situation awareness platform project.

References

1. R. He, H. Xie, J. Deng, T. Feng, L. L. Lai and M. Shahidehpour, "Reliability Modeling and Assessment of Cyber Space in Cyber-Physical Power Systems," IEEE Trans. Smart Grid, **11**, 5, (2020)
2. W. Liu, Q. Gong, H. Han, Z. Wang and L. Wang, "Reliability Modeling and Evaluation of Active Cyber Physical Distribution System," IEEE Trans. Power Syst., **33**, 6, (2018)
3. Telecontrol Equipment and Systems—Part 5-104: Transmission Protocols—Network Access for IEC 60870-5-101 Using Standard Transport Profiles, IEC Standard 60870, (2006)
4. G. Han, B. Xu and J. Suonan, "IEC 61850-Based Feeder Terminal Unit Modeling and Mapping to IEC 60870-5-104," IEEE Trans. Power Del., **27**, 4, (2012)
5. J. Valenzuela, J. Wang and N. Bissinger, "Real-time intrusion detection in power system operations," IEEE Trans. Power Syst., **28**, 2, (2013)
6. G. Chaojun, P. Jirutitijaroen and M. Motani, "Detecting False Data Injection Attacks in AC State Estimation," IEEE Trans. Smart Grid, **6**, 5, (2015)
7. J. J. Q. Yu, Y. Hou and V. O. K. Li, "Online False Data Injection Attack Detection With Wavelet Transform and Deep Neural Networks," IEEE Trans. Industrial Informatics, **14**, 7, (2018)
8. W. Guoli, "Traffic Prediction and Attack Detection Approach Based on PSO Optimized Elman Neural Network," 2019 11th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), Qiqihar, China, 2019.
9. M. S. Elsayed, N. -A. Le-Khac, S. Dev and A. D. Jurcut, "Detecting Abnormal Traffic in Large-Scale Networks," 2020 International Symposium on Networks, Computers and Communications (ISNCC), Montreal, QC, Canada, 2020.
10. U. K. Premaratne, J. Samarabandu, T. S. Sidhu, R. Beresh and J. Tan, "An Intrusion Detection System for IEC61850 Automated Substations," IEEE Trans. Power Del., **25**, 4, (2010)
11. Y. Yang, K. McLaughlin, S. Sezer, Y. B. Yuan and W. Huang, "Stateful intrusion detection for IEC 60870-5-104 SCADA security," 2014 IEEE PES General Meeting | Conference & Exposition, National Harbor, MD, USA, 2014.
12. Y. Yang, H. Xu, L. Gao, Y. Yuan, K. McLaughlin and S. Sezer, "Multidimensional Intrusion Detection System for IEC 61850-Based SCADA Networks," IEEE Trans. Power Del., **32**, 2, (2017)
13. B. Dong and X. Wang, "Comparison Deep Learning Method to Traditional Methods Using for Network Intrusion Detection," 2016 8th IEEE International Conference on Communication Software and Networks (ICCSN), Beijing, China, 2016.
14. Y. Yang, K. McLaughlin, T. Littler, S. Sezer, B. Pranggono and H. F. Wang, "Intrusion Detection System for IEC 60870-5-104 based SCADA networks," 2013 IEEE Power & Energy Society General Meeting, Vancouver, BC, Canada, 2013.
15. W. Lai, M. Zhou, F. Hu, K. Bian and Q. Song, "A New DBSCAN Parameters Determination Method Based on Improved MVO," IEEE Access, **7**, 2019.
16. P. Musil and P. Mlynek, "Overview of Communication Scenarios for IEC 60870-5-104 Substation Model," 2020 21st International Scientific Conference on Electric Power Engineering (EPE), Prague, Czech Republic, 2020.