ISSN 2616-5767 Vol.5, Issue 8: 1-5, DOI: 10.25236/AJETS.2022.050801

Dynamic Monitoring Method of Abnormal Intrusion of Distribution Terminals for Power Internet of Things

Gao Jie

University of Science and Technology, Anshan, Liaoning, China
jxhx3231547272@163.com

Abstract: *At this stage, the security protection system of power IOT distribution terminals lacks effective anomaly intrusion detection methods, and the distribution terminals of power IOT have the characteristics of large number and wide range, which plays an important role in maintaining the normal operation of power IOT. Once the distribution terminal encounters illegal intrusion, it can lead to the damage of the important infrastructure of the distribution terminal of the power Internet of things, and pose a great security threat to the stable operation of the power Internet of things. This paper analyzes the content of building the network flow order of distribution terminals for the power Internet of things. From the aspects of basic attribute selection, data processing, building the network flow order, attribute classification, abnormal feature extraction, and realizing abnormal monitoring, it deeply discusses the abnormal intrusion dynamic monitoring method of the network flow order for the power Internet of things, in order to accurately monitor the abnormal intrusion dynamic data and enhance the abnormal intrusion dynamic monitoring effect, Improve the level of abnormal intrusion dynamic monitoring technology, and effectively ensure the safe and stable operation of power distribution terminals of the Internet of things.*

Keywords: *Power Internet of things; Power distribution terminal; Abnormal intrusion; Dynamic monitoring*

1. Introduction

The security of power IOT distribution terminal is related to the normal and stable operation of power IOT. At present, the protection system of power IOT distribution terminal is relatively weak, and it is often subject to abnormal intrusion [1]. However, traditional monitoring methods are difficult to accurately monitor abnormal intrusion dynamics, and can not eliminate abnormal intrusion hidden dangers in time, resulting in damage to some power IOT distribution terminal equipment, which seriously affects the normal operation of power IOT distribution terminals [2]. To realize the dynamic monitoring of abnormal intrusion of power distribution terminals, we first need to select the basic attributes of network traffic, summarize the integrated data to form a complete network flow order, and then carry out attribute classification, abnormal feature extraction, white list matching. If the data in the order can operate stably, it is normal data. If the data outside the data is regarded as abnormal problem data, we can judge whether there is abnormal intrusion, Finally, abnormal intrusion dynamic monitoring is realized. This monitoring method helps to improve the dynamic monitoring technology of abnormal intrusion of power distribution terminals, accurately monitor the dynamic data of abnormal intrusion, timely deal with the hidden dangers of power distribution terminals, improve the security and defense capability of power IOT power distribution terminals, and ensure the safe and stable operation of power IOT power distribution terminals [3].

2. Construction of distribution terminal network flow order for the power Internet of things

The content of the distribution terminal network flow order for the power Internet of Things includes: IP address, traffic type, packet size, packet time slot and packet direction. According to the constructed network flow order, the problems existing in the IoT terminal are judged, and then the next attribute classification is carried out until the final dynamic abnormality monitoring. The schematic diagram of the specific network flow order is shown in Figure 1.

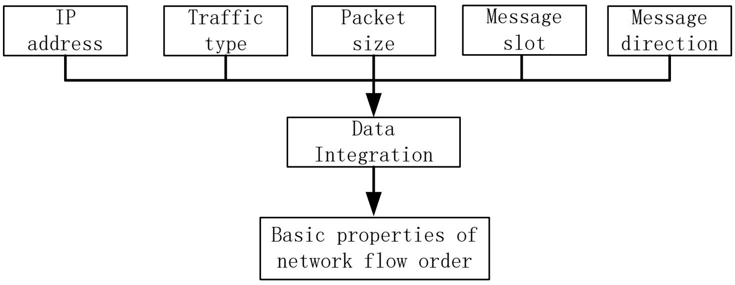

Figure 1: Schematic diagram of the selection of basic attributes of network flow order

Figure 1 is a schematic diagram of the selection of the basic attributes of network flow order. IP address refers to the source address and destination address, traffic type refers to the protocol type of the message, message size refers to the total length of the message, message slot refers to the difference between the time stamps of the two adjacent messages, and message direction refers to the device receiving or sending. According to the collected IP address, traffic type, message size, message slot, message direction and other data information, these data information are analyzed and integrated, so as to form the basic attribute selection of distribution terminal network flow order for the power Internet of things.

3. Network flow order abnormal intrusion dynamic monitoring

To realize the dynamic monitoring of abnormal intrusion of network flow order for the power Internet of things, we can select the basic attributes of network traffic, summarize the data, and then build the network flow order, and then carry out attribute classification, abnormal feature extraction, white list matching, and finally realize abnormal monitoring.

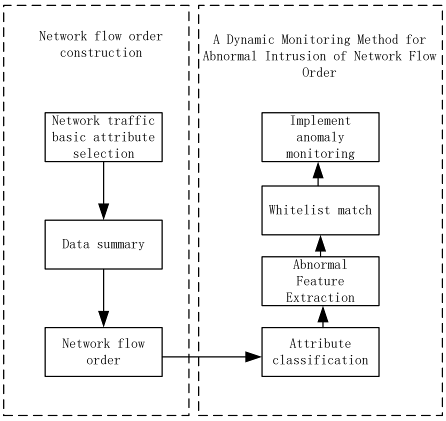
Network flow order construction
A Dynamic Monitoring Method for Abnormal Intrusion of Network Flow Order
Network traffic basic attribute selection
Data summary
Network flow order
Implement anomaly monitoring
Whitelist match
Abnormal Feature Extraction
Attribute classification

Figure 2: Dynamic monitoring method for abnormal intrusion of network flow order for power Internet of Things

Figure 2 shows the dynamic monitoring method of abnormal intrusion of network flow order for the power Internet of things. In the selection of the basic attributes of the established network flow order, the integrated data is summarized to form a complete network flow order. If the data in the order can operate stably, it is normal data, and the data outside the data is regarded as abnormal problem data, so as to judge whether there is abnormal intrusion.

3.1. Data summary

To realize the abnormal intrusion dynamic detection of network flow order for the power Internet of things, we must first extract the data information in the network flow order, collect and summarize it, and analyze and process the huge data. Because the power Internet of things mostly belongs to intranet communication, in the process of information processing, the last eight bits of the IP address are taken, and the message slot is obtained by subtracting the time of the previous adjacent message from the current message time. The receiving direction of the message is represented by A, and the sending direction is represented by B, and then each data information is summarized and processed through the voting algorithm. In order to further realize the data processing process, it is necessary to define the triplet set formula, as shown in the following formula (1):

$$A=\left(S,P,V\right) \tag{1}$$

In the formula, A refers to the network flow order vector, S refers to the total amount of data to be processed, P refers to the data attribute composition in the network flow order, and V refers to the specific value of the attribute composition in the network flow order. After the above steps, the data collection in the network flow order is realized, the useful and important content is selected from all the data, the processing of the basic attribute data is completed, the complete network flow order is constructed, and the attribute classification in the next step is done. Prepare.

3.2. Attribute classification

In order to maintain the stability of power distribution terminals in the Internet of things, it is necessary to classify the attributes of abnormal intrusion dynamic monitoring.

A two-step algorithm is used in clustering. First, the dynamic monitoring in the returned results are clustered, and the results of this clustering are used as the centroid of the initial clustering to further cluster the rest of the dynamic monitoring.

The cosine between the feature vectors of dynamic monitoring is used as the similarity of vectors, that is, the similarity between m and n of dynamic monitoring is defined, as follows (2):

$$SM_{m,n}=\frac{v_m v_n}{\left|v_m\right|\times\left|v_n\right|} \tag{2}$$

Set the threshold value $\partial_{\min}$, and dynamically monitor m and n for any two items in the first several dynamic monitoring items. If $SM_{m,n}>\partial_{\min}$, then classify the two dynamic monitoring items m and n into one category, and iteratively calculate the centroid of several initial clusters; set Threshold $\partial_{\max}$, calculate the similarity between the rest of the dynamic monitoring and the centroid, if the maximum similarity is greater than $\partial_{\max}$, classify it as a class with the largest similarity, otherwise, take it as a new centroid, and then continue to carry out the rest of the dynamic monitoring Clustering, this clustering algorithm provides the necessary prerequisites for good attribute classification, and then further completes the attribute classification according to the clustering results, which provides a classification basis for extracting abnormal features.

3.3. Abnormal feature extraction

The white list of network flow order is established according to the set of characteristic words. During the dynamic monitoring of abnormal intrusion of network flow order, the data information is compared with the set in the white list. If it does not appear in the set, it is determined as abnormal intrusion.

The feature to be extracted in this paper is the data based on the weight and bias term of the coding part. The specific process is as follows:

(1) Given tagged data, learn features

Input samples according to the data processing results, the input samples are labeled, ie (input, label). Then, based on the deviation between the output obtained after autoencoder learning and the label, the parameters of the previous layers are changed until convergence.

(2) Activation function

The activation function of the hidden layer of the neural network is generally a nonlinear function in order to learn a more complex objective function. In this paper, the Sigmoid activation function is used, and the expression of the Sigmoid function is as follows (3):

$$f\left(z\right)=\frac{1}{1+e^{-z}} \tag{3}$$

In the formula, $f\left(z\right)$ refers to the objective function, e refers to the eigenvalue of the fitting function, and z refers to the gradient. This is a non-linear transformation where the function takes values in the interval [0,1]. It can fit the function better, but because the derivative of the sigmoid function is small, the gradient update speed in the backpropagation algorithm is slower. More importantly, because the two-layer function value of this function is close to zero, the gradient is likely to disappear as the number of layers is superimposed and the gradient is updated accordingly. If the activation function disappears, there will be an abnormal invasion situation. Abnormal feature extraction is completed.

3.4. Implement abnormal monitoring

The anomaly monitoring process relies on the sequence of the above steps to realize the unloading of computing tasks and data sinking brought by the anomaly monitoring process, which is conducive to improving the real-time performance of anomaly monitoring and reducing the bandwidth pressure of the backbone link connected to the cloud platform. If there is an anomaly in the original data, the generated error fluctuates greatly compared with the conventional error. The anomaly monitoring method proposed by the design method mainly uses the error fluctuation. At time t, the square error between the original sampling data and the restored value is defined as equation (4).

$$\varepsilon=\left\|g_{\theta'}\left(f_{\theta}\left(\overline{x}^{(t)}\right)\right)-\overline{x}^{(t)}\right\|_2^2 \tag{4}$$

In the formula, $\overline{x}^{(t)}$ is the original sampled data after normalization at time t, and $g_{\theta'}\left(f_{\theta}\left(\overline{x}^{(t)}\right)\right)$ is the data after encoding and decoding. According to the above content, the algorithm steps to realize abnormal monitoring can be summarized as follows:

(1) Calculate the Sigmoid activation function on the data. With the stacking of layers and the subsequent update of the gradient, the gradient is likely to disappear. During the process of activating the function, if the gradient disappears, there will be abnormal invasion and abnormal feature extraction. Completed to represent the impact of different scales on the data.

(2) Calculate the square error of the extracted data. If the square error value exceeds the preset threshold, it is determined that there is an anomaly in the sampling data at that time, and the original data and the anomaly warning are uploaded to the cloud platform for subsequent processing. If the square error value is lower than the threshold, the encoded data will be uploaded to the cloud platform, and the data will be decoded and restored on the cloud platform, so as to reduce the amount of data uploaded.

Through the above algorithm steps, the dynamic monitoring of abnormal intrusion of network flow order is realized, and a complete network flow order is formed. If the data in the order can operate stably, it is normal data, and the data outside the data is regarded as abnormal problem data, so as to judge whether there is abnormal intrusion. The dynamic monitoring method of abnormal intrusion of network flow order for the Internet of things is established.

4. Conclusion

To realize the abnormal intrusion dynamic monitoring of network flow order for the power Internet of things, we can select the basic attributes of network traffic, summarize the data, and then build the network flow order, and then carry out attribute classification, abnormal feature extraction, white list matching, use a safer algorithm to normalize the data, and finally realize the abnormal intrusion dynamic monitoring. Through this monitoring method, it helps to improve the abnormal intrusion dynamic monitoring technology of the power Internet of things distribution terminal, accurately monitor the abnormal intrusion dynamic data, timely deal with the hidden dangers of the distribution terminal, help to improve the defense system of the power Internet of things distribution terminal, maintain the basic equipment of the power Internet of things distribution terminal, and effectively ensure the safe and stable operation of the power Internet of things distribution terminal [4].

References

[1] Lu Lining, Zhu Weiguang. Application of electric Internet of things technology in power equipment online monitoring [J]. Information Technology, 2021(07):155-159.

[2] Zhu Yue, Gao Yuan, Liu Qiang et al. The Frame of Distribution Terminal Common Information Model Facing Power Distribution IoT [J].Distribution & Utilization, 2021, 38(07):51-57.

[3] Jiang Fan, Sun Guoqi, Du Jinbao et al. Power Internet of things terminal security protection system based on EDR technology and machine learning [J]. Network Security Technology & Application, 2021(01):126-128.

[4] Lu Wenshuai, Li Mengnan, Liang Jiaqian. On-line NBIoT Sensing Terminal for Smart City Transmission Line Monitoring [J]. Journal of China Academy of Electronics and Information Technology, 2019, 14(04):412-415+422.