Journal of Information Security, 2023, 14, 39-51
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

User Station Security Protection Method Based on Random Domain Name Detection and Active Defense

Hongyan Yin[1], Xiaokang Ren[2*], Jinyu Liu[3], Shuo Zhang[2], Wenkun Liu[4]

[1]School of Information Engineering, University of Shenyang, Shenyang, China
[2]Shenyang Institute of Computing Technology, Chinese Academy of Sciences, Shenyang, China
[3]Shenyang Institute of Computing Technology Co. Ltd., CAS, Chinese Academy of Sciences, Shenyang, China
[4]Turpan Electric Power Supply Company, State Grid Xinjiang Electric Power Company Limited, Turpan, China
Email: *renxiaokang19@mails.ucas.ac.cn

How to cite this paper: Yin, H.Y., Ren, X.K., Liu, J.Y., Zhang, S. and Liu, W.K. (2023) User Station Security Protection Method Based on Random Domain Name Detection and Active Defense. *Journal of Information Security*, **14**, 39-51.
https://doi.org/10.4236/jis.2023.141004

Received: December 19, 2022
Accepted: January 26, 2023
Published: January 29, 2023

Abstract

The power monitoring system is the most important production management system in the power industry. As an important part of the power monitoring system, the user station that lacks grid binding will become an important target of network attacks. In order to perceive the network attack events on the user station side in time, a method combining real-time detection and active defense of random domain names on the user station side was proposed. Capsule network (CapsNet) combined with long short-term memory network (LSTM) was used to classify the domain names extracted from the traffic data. When a random domain name is detected, it sent instructions to routers and switched to update their security policies through the remote terminal protocol (Telnet), or shut down the service interfaces of routers and switched to block network attacks. The experimental results showed that the use of CapsNet combined with LSTM classification algorithm can achieve 99.16% accuracy and 98% recall rate in random domain name detection. Through the Telnet protocol, routers and switches can be linked to make active defense without interrupting services.

Keywords

User Station, Random Domain Name Detection, Capsule Network, Active Defense, Long Short Term Memory

1. Introduction

The power monitoring system is facing informationization, digitalization and intelligent reform. The high integration of information system and physical system brings the development mode of "power-information-business", and also brings new challenges to the security of the power monitoring system [1]. Due to the weak safety protection awareness of the user stations, its safety protection ability mainly depends on special security equipment. And most of the security personnel in the user stations are mainly operation and maintenance personnel, lacking professional safety protection skills. At present, security attacks and vulnerabilities affecting the energy industry appear frequently. A large number of modern malicious codes, such as ransomware and worm virus targeting the energy industry, mostly use random domain names to communicate with Command and Control Server (C&C) in order to avoid the scrutiny of security personnel. This communication mode can effectively resist domain name blacklist blocking and attribute code detection. These problems make the user station of the power monitoring system in a great security risk, and the network attack events against the user station can even spread from the user station to the master station and other user stations through the dispatching data network, thus posing a huge security threat to the entire power monitoring system. In order to solve the security protection problem of user stations, abnormal behaviors by detecting network traffic has become a mainstream method [2] [3] [4] [5] [6]. However, the massive heterogeneous terminals in power system bring great difficulties to the detection and analysis of traffic data. How to effectively detect the security risks faced by power monitoring system is a problem many researchers are thinking about [7] [8] [9].

In order to effectively detect the security risks faced by user stations in power monitoring system, this paper takes random domain name as the research object, and proposes a method combining random domain name detection and active defense technology to improve the security protection ability of user stations. The method proposed in this paper combines Capsule Network (CapsNet) and Long Short Term Memory (LSTM) to detect random domain names, and uses active defense technology to prevent malicious resolution behavior of random domain names. The experimental results show that the proposed reconstruction network based on the integration of CapsNet and LSTM has a significant improvement in the accuracy of random domain name detection, reaching 99.16%. And the active defense technology can effectively defend against malicious domain name resolution behavior.

2. Literature Review

At present, machine learning and deep learning are the mainstream methods to detect random domain names. Machine learning requires manual extraction of domain name character features. The detection effect is relatively poor for deep learning, but it is highly interpretable. Deep learning does not need to manually extract features and has good detection effect. It is the most widely used method in the domain name detection field.

Because random domain name is generated by random domain name generation algorithm, it is easy to cause statistical difference between random domain name and normal domain name. Therefore, traditional machine learning methods can effectively detect random domain names from the perspective of domain names themselves [10] [11] [12] [13]. Guo Xiangmin *et al.* took the Domain name generated by the Domain Generation Algorithm (DGA) as the identification object, and performed clustering analysis on malicious domain names based on implicit Markov model, so as to realize DGA domain name determination [14]. Zhang Yang *et al.* proposed a malicious domain name detection method based on multiple attribute features. This method extracts more fine-grained features in lexical features and then uses random forest algorithm to detect random domain names [15]. Yu Guangxi *et al.* designed a domain name detection system, which first used random forest to classify and analyze domain names, and then used clustering and set analysis methods to further detect suspected malicious domain names to reduce the false detection rate of the system [16]. Although machine learning has achieved satisfactory results in random domain name detection, traditional machine learning methods need to manually extract a large number of domain name features, and cannot extract the relationship between domain name characters. The detection effect depends on the quality of feature engineering, so the detection efficiency and detection accuracy are low.

DGA domain name classification detection based on deep learning has become a mainstream solution from the perspective of natural language processing [17]. Woodbridge *et al.* [18] designed a LSTM model specifically for malicious domain names to realize real-time prediction of malicious domain names without context information and manual feature extraction [19]. Chen *et al.* proposed a random domain name detection model based on Gate Recurrent Unit (GRU). The domain name vector features are automatically learned by GRU, and finally the classification is calculated by neural network [20]. Chen Lihuang *et al.* introduced attention mechanism on the basis of GRU recurrent neural network to strengthen some high randomness features in domain names [21]. Zhang Bin *et al.* proposed a domain name detection model based on the Convolutional Neural Network (CNN) and LSTM. The model detects malicious domain names by extracting sequence features of different length character combinations in the domain name string. At the same time, the attention mechanism is introduced to assign a small weight to the output features at the position of the filled characters, reduce the interference of the filled characters on feature extraction, and enhance the ability to extract features of long-distance sequences [22]. Extracting the combined features of domain name string based on CNN and using LSTM to fully mine the character context information in domain name string can achieve a higher detection accuracy than simply using LSTM, GRU or CNN. However, CNN has great limitations in identifying spatial relationship features, and the pooling operation of CNN will lose a lot of valuable information. Based on this, this paper proposes a domain name detection model combining CapsNet [23] and LSTM fusion. The model realizes the security protection of user station by detecting random domain name and combining with active defense technology.

3. Research Methodology

In order to ensure the invisibility and security of the communication process with C & C server, a large number of modern malicious codes such as ransomware and worms virus use DGA to establish communication with C & C server. In order to hide the real malicious domain names, malicious code can create up to thousands of fake domains at a time. In order to effectively detect random domain names in user stations, this paper proposes a domain name detection model that integrates CapsNet and LSTM to detect random domain names. The model structure diagram is shown in Figure 1. The model is divided into input layer, feature extraction layer and output layer. At the same time, the model combines the active defense technology to defend against malicious domain name resolution.

The random domain name in the data set used by the random domain name detection model in this paper is the random domain name actually generated by 26 malicious samples, and the normal domain name is the top 1 million domain names of Alex website. In this paper, the detection of domain names is only for the subdomain of the domain name, such as google.com whose subdomain is google.

3.1. Input Layer

In order for the neural network to process domain name data, it is necessary to first convert the domain name into a vector. In this paper, we first count all the characters that appear in the data set to form a dictionary, and then assign a

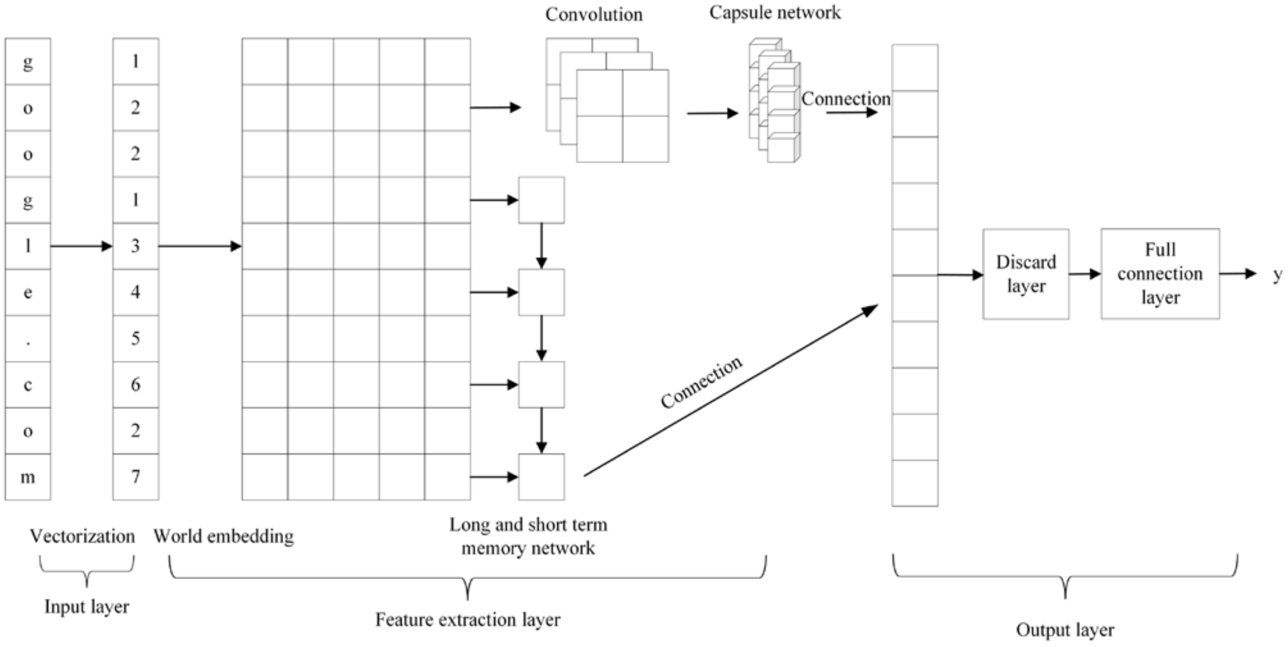

Figure 1. Structural diagram of CapsNet + LSTM model.

unique index to all the characters in the dictionary. Any domain name $D(c_1, c_2, c_3, \cdots, c_L)$ is represented by a vector with the length of *L*. *L* is the length of the longest domain name in the dataset, and the value of *L* in this dataset is 63. The value in *D* is the index value of the character $c_i\,(i = 1, 2, 3, \cdots, L)$ in the dictionary.

3.2. Feature Extraction Layer

Feature extraction layer uses deep learning network to extract character combination and sequence features of domain name. This layer is composed of word embedding layer, CapsNet and LSTM.

This paper uses word embedding to transform domain name into vector, which has the advantages of low dimension and computable semantics compared with one-hot representation and matrix representation [24]. The vectorized domain name is transformed into a vector sequence $(w_1, w_2, w_3, \cdots, w_L)$, $w_i \in \mathbb{R}^d$ by the word embedding layer. *d* is the vector dimension of the embedded layer. In this paper, *d* is 128, which can retain enough context information.

Capsule network emphasizes the encoding of image features' spatial relationship [25]. CapsNet is used to extract the spatial characteristics of domain name strings. The domain name vector is input into CspsNet. CapsNet first extracts the n-gram syntax information in the domain name string using one-dimensional convolution. One-dimensional convolution is extracted by the convolution kernel *ω*, $\omega \in \mathbb{R}^{k \times d}$ of size *k*, $k \in \{2, 3, 5\}$, and the convolution operation uses the 0 filling method. Convolutional feature extraction includes two steps, convolution calculation and convolution kernel movement. The convolution calculation uses the convolution kernel of size *k* to translate on the sequence vector, and executes the convolution calculation for *k* input sequences each time. The calculation formula is shown in Equations (1)-(2).

$$x_i = \oplus\left(w_{i:i+k-1}\right) \tag{1}$$

$$c_i = g\left(x_i \cdot u + b\right) \tag{2}$$

$x_i, u \in \mathbb{R}^{k \times d}$. $\oplus$ represents vector splicing, u is weight matrix and b is bias quantity. The convolution calculation makes the inner product operation between the weight matrix and the splicing vector b. After the bias *b* is added, the output is processed by the nonlinear function *g*, here the nonlinear function *g* uses the ReLU function. The convolution kernel moves on the sequence vector with a step of 1 each time. The convolution operation forms three 63 × 64 two-dimensional tensors. Three two-dimensional tensors are spliced to form a 63 × 192. CapsNet uses dynamic routing to replace pooled operations on the input 63 × 192 tensors for feature extraction, final output 64 × 128. The dynamic routing process is shown in Table 1. u_1, u_2 are input vectors, and c_1^r, c_2^r are dynamically updated parameters.

The value of T is 3, and the weighted sum of u^1, u^2 plus c_1^r, c_2^r respectively gives s^r. a^r is obtained through the Squash function, and a^r is dotted

Table 1. Dynamic routing process.

```
$b_1^0 = 0, b_2^0 = 0$
For $r = 1$ to $T$ do
    $c_1^r, c_2^r = \text{softmax}\left(b_1^{r-1}, b_2^{r-1}\right)$
    $s^r = c_1^r u^1 + c_2^r u^2$
    $a^r = Squash\left(s^r\right)$
    $b_i^r = b_i^{r-1} + a^r \bullet u^i$
```

product with u^i ($i = 1, 2$) to get b_i^r. Loop T ($T = 3$) times to get the final updated parameters c_1^r, c_2^r, and complete the dynamic routing.

LSTM is an improved time cycle neural network, which is suitable for processing sequential data [26] [27]. The LSTM layer is used to extract the single character sequence features of the domain name string. The domain name vector sequence through the word embedding layer is spliced into a single vector $e = \oplus\left(w_{1:L}\right), e \in \mathbb{R}^{L\times d}$ and input into the LSTM network.

3.3. Output Layer

Finally, this paper spliced the output of CapsNet and LSTM into the full connection layer for classification. Sigmoid function was used as the classification function, binary cross entropy was used as the loss function, and Adam optimizer was used to minimize the loss function. The output result is recorded as y, where $y \in [0,1]$. The calculation equation of loss function is

$$L\left(\hat{y}, y\right) = -\frac{\sum_i^N \left[\hat{y}_i \log \hat{y}_i + \left(1 - y_i\right)\log\left(1 - \hat{y}_i\right)\right]}{N} \tag{3}$$

where $\hat{y}$ is the prediction probability obtained by Sigmoid function, y is the actual target value, DGA domain name value is 1, and normal domain name value is 0.

At the same time, in order to verify the actual effect of CapsNet, we also used LSTM model to detect random domain names. The LSTM model structure is shown in **Figure 2**. Compared with the CapsNet plus LSTM model structure, the convolution operation and capsule neural network are removed in LSTM. After vectorization and word embedding, only LSTM is used to extract domain name features, and then the detection results are output after passing through the output layer. The detectable results will compare with the results of CapsNet + LSTM model to verify the actual contribution of CapsNet to the model in part four.

4. Research Results

4.1. Data Source and Data Preprocessing

The data set used in this experiment consists of normal domain names and random

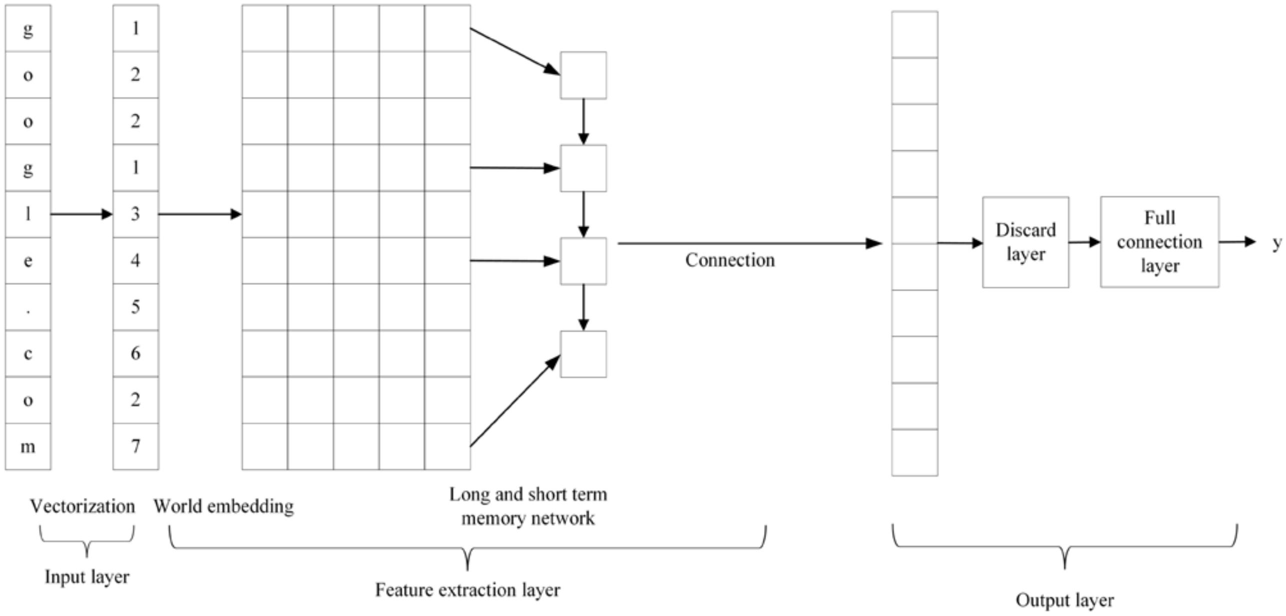

Figure 2. Structural diagram of LSTM model.

domain names. Among them, the random domain names are 1 million randomly generated domain names from 26 malicious samples, and the category mark is 1; The normal domain names come from the top 700,000 domains on Alex's website, and the category is marked as 0. This paper first counts all the unique characters in the domain name to form a dictionary, uses the dictionary to vectorize the domain name, and the domain name vector passes through the word embedding layer in Keras to form a 63 × 128 tensor as the input of the neural network. 80% of the data set in this paper is for training and 20% for testing.

4.2. Model Parameter Setting

The proposed model is divided into input layer, feature extraction layer and output layer. The input layer selects a sequential structure to connect the neurons in the neural network in a sequential manner. The feature extraction layer first uses the embedding layer to embed words at the character level, and the embedding dimension d is 128. Then three convolution kernels of size k and $k \in \{2,3,5\}$ are used for convolution operation, and the number of neurons is set to 64. Then the capsule network is used for feature extraction. The number of capsule networks is set to 64, the number of routes is set to 3, and the output dimension is 128. At the same time, a LSTM network is paralleled at the feature extraction layer to extract the context information of characters in the domain name string. The number of neurons is set to 64. To prevent LSTM from overfitting, set the discard layer and the discard rate to 0.5. Batch_size and epochs are set to 128 and 10 respectively during the training.

4.3. Model Evaluation Criteria

There are four kinds of test statistics results in the test set, as shown in Table 2.

Table 2. Statistical results of domain name test.

	Random domain name	**Normal domain name**	
Random domain name	TP	FP	TP + FP
Normal domain name	FN	TN	FN + TN
	TP + FN	FP + TN	

TP (True Positive): the actual number of samples of random domain names determined to be random domain names; FP (False Positive): the number of samples that are actually normal domain names and are determined to be random domain names; TN (True Negative): the actual number of samples of normal domain names determined to be normal domain names; FN (False Negative): the actual number of samples of random domain names that are determined to be legal domain names.

In traditional machine learning and deep learning classification tasks, accuracy, precision, recall and F1 value are most often used to measure the classification effect of the model.

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{TN} + \text{FN}}$$

$$\text{F1-Score} = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

Among them, the accuracy rate reflects the reliability of the model discrimination results; Recall rate reflects the missing report of the model; The F1 score reflects the comprehensive performance of the model. The larger the F1 score, the better the model performance.

4.4. Model Evaluation

In order to evaluate the effect of the fusion of CapsNet and LSTM domain name detection model proposed in this paper, CNN model, LSTM model, and CNN + LSTM model are compared with it. The traditional machine learning classification method K-Nearest Neighbor (KNN), Logical Regression (LR), Decision Tree (DT) and other models are used for reference.

As can be seen from Table 3, the classification model based on deep learning has better performance than the classification method based on traditional machine learning. The CNN detection model can extract n-gram syntactic information of domain name through convolution operation, but a deeper convolutional network needs to be designed to extract longer distance syntactic information to improve accuracy. LSTM detection model can extract the sequence features of domain name strings. The F1-Score of LSTM is 1 percentage point higher than that of CNN, and the accuracy is 1 percentage point higher. It shows that the accuracy can be improved by extracting the sequence features of domain name strings. Compared with the CNN model and LSTM model, the accuracy of the CNN and LSTM fusion model is improved by one percentage point and two percentage points respectively. At the same time, by comparing CapsNet + LSTM and LSTM, it is found that the recall rate, accuracy rate and precision rate of CapsNet + LSTM are respectively 1, 2 and 3 percentage points higher than that of LSTM alone.

In order to more intuitively measure the classification performance of different models, this paper gives receiver operating characteristic (ROC) curves of different models, as shown in Figure 3. The closer the area under the ROC curve (AUC) is to 1, the higher the authenticity of the detection model.

According to Table 3 and Figure 2, the detection model of CapsNet combined with LSTM proposed in this paper has the highest detection accuracy of 99%. It shows that using dynamic routing of capsule network to replace pooling operation of CNN can effectively reduce information loss and achieve higher

Table 3. Comparison of model detection performance.

Model	Recall (%)	Precision (%)	Accuracy (%)	F1-Score
Caps-LSTM	98	98	99	0.98
CNN	95	96	96	0.97
LSTM	97	96	96	0.98
CNN-LSTM	98	97	98	0.98
LR	92	90	89	0.91
KNN	95	93	92	0.94
DT	92	91	90	0.92

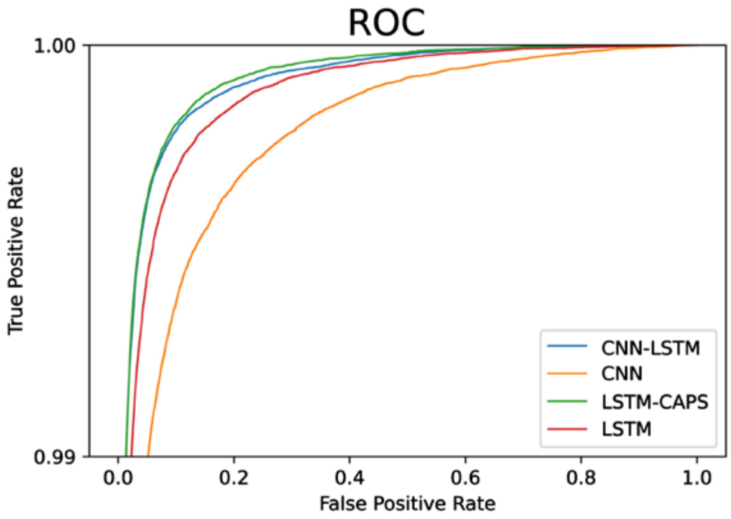

Figure 3. ROC curve comparison chart (color printing).

accuracy. At the same time, the AUC area of the model proposed in this paper reaches 0.999, which has the highest detection authenticity.

4.5. Active Defense

The active defense module is used to make active defense according to the resolution results of random domain names when the random domain name detection module detects random domain names, so as to prevent further spread of network attacks. The random domain name detection model extracts domain names in DNS traffic successively and filters them using whitelists. Then the random domain name detection model classifies domain names. If the detection model determines that the domain name is random, the IP address corresponding to the domain name is extracted. Then the active defense module updates the access control list (ACL) of the switch through the Telnet protocol according to the IP address, and prevents the connection with the IP address. If the domain name is determined to be a normal domain name, continue to analyze the next domain name. The active defense process is shown in Figure 4.

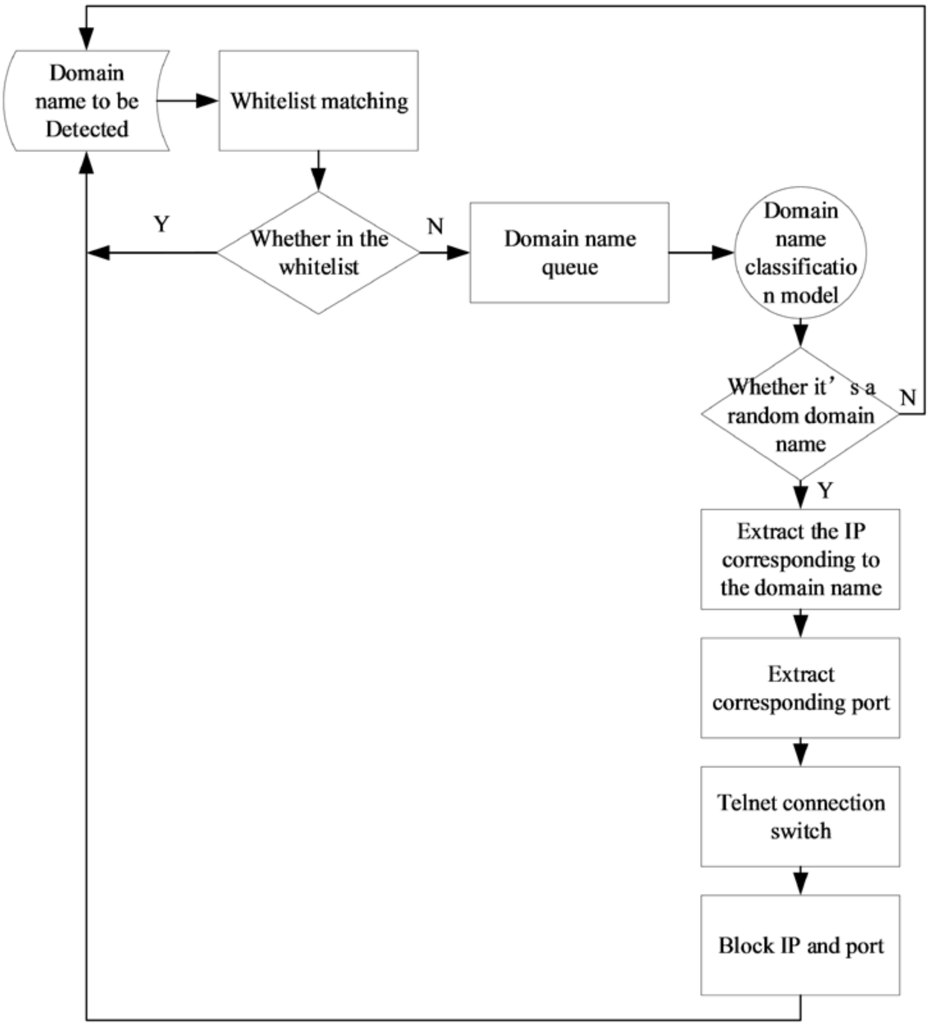
Domain name to be Detected
Whitelist matching
Y
Whether in the whitelist
N
Domain name queue
Domain name classificatio n model
Whether it' s a random domain name
N
Y
Extract the IP corresponding to the domain name
Extract corresponding port
Telnet connection switch
Block IP and port

Figure 4. Flowchart of active defense.

5. Conclusions

This paper proposes a security protection method for user station of power monitoring system, which combines random domain name detection and active defense technology. The method proposed in this paper can detect random domain names from the DNS traffic of the user stations, and then use the active defense technology to block malicious connections according to the resolution results of random domain names. In the random domain name detection phase, the detection model proposed in this paper first vectorizes domain names and then classifies them. Active defense extracts the Internet Protocol (IP) address corresponding to the domain name according to the results of random domain name detection and blocks the malicious connection of the corresponding IP address. Finally, the method proposed in this paper is verified by DNS traffic data of user station. The experimental results show that the CapsNet + LSTM model successfully detects 304 random domain names in DNS traffic for 30 consecutive days. The ACL of the two switches is updated successfully to prevent two malicious connections, and the detection effect is the best. The simple LSTM model only detected 268 random domains, the second most effective. In the best case, only 158 random domain names can be detected using machine learning methods. Through the actual verification, CapsNet + LSTM model can meet the actual use requirements.

The method proposed in this paper can solve the security protection problem by random domain name detection and active defense technology without interrupting the service of the user station. Compared with the existing user station protection schemes, this method has the following advantages: 1) In view of the security protection status of user stations, a protection idea based on the combination of random domain name detection and active defense is proposed; 2) When random domain name resolution behavior is found in the user station, active defense measures can be taken to prevent malicious connections without interrupting the service. The main work in the future is to: further improve the accuracy of existing detection engines; further shorten the training time of random domain name detection model.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Zhang, L. (2020) Analysis of Network Security Threat Traceability Technology of Power Monitoring System. *Telecom Power Technology*, **37**, 3.

[2] Du, H.L., Kong, P.H., Jin, X.Q. and Huang, Y.Q. (2021) Traffic Anomaly Detection of Power Communication Networks Based on Deep Learning. *Zhejiang Electric Power*, **40**, 117-123.

[3] Liu, D., Jiang, Z.W., Zhu, Y.W., *et al.* (2022) Network Traffic Anomaly Detection of Power Monitoring System Based on LDSAD. *Zhejiang Electric Power*, **41**, 87-92.

[4] Yang, H., Liu, Y.S., Liu, G.H. and Zhou, F.Y. (2020) Safety Monitoring Technology of Power Grid Industrial Control System Based on Abnormal Detection of Network Traffic. *Electronic Technology & Software Engineering*, **22**, 259-260.

[5] Li, Y.C. (2019) Research on Anomaly Detection Technology of Power Industrial Control Network Traffic Based on Machine Learning. Thesis, Shanghai Jiao Tong University, Shanghai.

[6] Liu, Y.L., Meng, L.Y. and Ding, Y.F. (2018) Application and Algorithm Improvement of Abnormal Traffic Detection in Smart Grid Industrial Control System. *Computer Systems & Applications*, **27**, 173-178.

[7] Liu, B., Li, L., Liu, J.N., *et al.* (2021) Analysis of Weak Links in Network Security of Power Monitoring System in New Energy Fields. *Electric Engineering*, **18**, 78-80.

[8] Jin, X.Q., Su, D., Mao, N.P., *et al.* (2019) Research on Active Monitoring and Early Warning Technology for New Energy Station. *Zhejiang Electric Power*, **38**, 106-112.

[9] Gunduz, M.Z. and Das, R. (2020) Cyber-Security on Smart Grid: Threats and Potential Solutions. *Computer Networks*, **169**, Article ID: 107094. https://doi.org/10.1016/j.comnet.2019.107094

[10] Yadav, S., Reddy, A.K.K. and Reddy, A.L.N. (2010) Detecting Algorithmically Generated Malicious Domain Names. *Proceedings of the* 10*th ACM SIGCOMM Conference on Internet Measurement*, Melbourne, 1-30 November 2010, 48-61. https://doi.org/10.1145/1879141.1879148

[11] Schiavoni, S., Maggi, F. and Cavallaro, L. (2014) Phoenix: DGA-Based Botnet Tracking and Intelligence. In: *International Conference on Detection of Intrusions and Malware*, *and Vulnerability Assessment*, Springer, Cham, 192-211. https://doi.org/10.1007/978-3-319-08509-8_11

[12] Zhang, W.W., Gong, J., Liu, Q., *et al.* (2016) Lightweight Domain Name Detection Algorithm Based on Morpheme Features. *Journal of Software*, **27**, 2348-2364.

[13] Truong, D.T. and Cheng, G. (2016) Detecting Domain-Flux Botnet Based on DNS Traffic Features in Managed Network. *Security and Communication Networks*, **9**, 2338-2347. https://doi.org/10.1002/sec.1495

[14] Guo, X.M., Liang, G.J. and Xia, L.L. (2021) Domain-Flux Malicious Domain Name Detection and Analysis Based on HMM. *Netinfo Security*, **21**, 1-8.

[15] Zhang, Y., Liu, T.W., Sha, H.Z. and Shi, J.Q. (2016) Malicious Domain Detection Based on Multiple-Dimensional Features. *Journal of Computer Applications*, **36**, 941-944+984.

[16] Yu, G.X., Zhang, Y., Cui, H.J., *et al.* (2020) Design and Implementation of A DGA Domain Name Detection System by Machine Learning. *Journal of Cyber Security*, **5**, 35-47.

[17] Liu, Y., Zhao, K., Ge, L.-S. and Liu, H. (2019) A Fast DGA Domain Detection Algorithm Based on Deep Learning. *Journal of Shandong University* (*Natural Science*), **54**, 106-112.

[18] Woodbridge, J., Anderson, H.S. and Ahuja, A. (2016) Predicting Domain Generation Algorithms with Long Short-Term Memory Networks.

[19] Wu, J. (2021) Research on Detection Technology of Malicious Domain Name Based on Deep Learning. Thesis, People's Public Security University of China, Beijing.

[20] Chen, L.G., Zhang, Y.D., Geng, G.G. and Yan, Z.W. (2018) Detection of Random Generated Names Using Recurrent Neural Network with Gated Recurrent Unit. *Computer Systems & Applications*, **27**, 198-202.

[21] Chen, L.H., Cheng, H. and Fang, Y.Q. (2019) Detecting Domain Generation Algo-

rithm Based on Attention Mechanism. *Journal of East China University of Science and Technology*, **45**, 478-485.

[22] Zhang, B. and Liao, R.J. (2021) Malicious Domain Name Detection Model Based on CNN and LSTM. *Journal of Electronics & Information Technology*, **43**, 2944-2951.

[23] Sabour, S., Frosst, N. and Hinton, G.E. (2017) Dynamic Routing between Capsules. *Proceedings of the* 31*st International Conference on Neural Information Processing Systems*, Long Beach, 4-9 December 2017, 3859-3869.

[24] Yu, Z. (2016) The Study and Application of Text Embeddings with Deep Learning Technique. Thesis, East China Normal University, Shanghai.

[25] Liu, L.S., Tong, M.L. and Wu, D.L. (2021) SA-CapsNet: Self-Attention Capsule Network. *Application Research of Computers*, **38**, 3005-3008.

[26] Deng, H.W. and Li, X.W. (2022) Abnormal Network Flow Identification and Detection Based on Deep Learning. *Computer Systems & Applications*.

[27] Yang, Z.F., Chang, J., Xu, Y., *et al*. (2022) VPN Encrypted Traffic Identification for Joint Capsule and Bidirectional LSTM Networks. *Computer Engineering and Applications*.