Modbus Communication Behavior Modeling and SVM Intrusion Detection Method

Wenli Shang1,2  
1Shenyang Institute of Automation Chinese Academy of Science  
2Key Laboratory of Networked Control Systems of Chinese Academy of Sciences  
Shenyang 110016, China  
024-23970389  
shangwl@sia.cn

Junrong Cui1,2,3  
1Faculty of Automation and Electrical Engineering Shenyang Ligong University  
2Key Laboratory of Networked Control Systems of Chinese Academy of Sciences  
3Shenyang Institute of Automation Chinese Academy of Science  
Shenyang 110159, China  
024-23970561  
cuijunrong@sia.cn

Ming Wan1,2, Panfeng An1,2,3, Peng Zeng1,2  
1Shenyang Institute of Automation Chinese Academy of Science  
2Key Laboratory of Networked Control Systems of Chinese Academy of Sciences  
3Shenyang Institute of Automation Chinese Academy of Science  
Shenyang 110016, China  
024-23970395  
wanming@sia.cn  
anpanfeng@sia.cn  
zp@sia.cn

ABSTRACT  
The security and typical attack behavior of Modbus/TCP industrial network communication protocol are analyzed. The data feature of traffic flow is extracted through the operation mode of the depth analysis abnormal behavior, and the intrusion detection method based on the support vector machine (SVM) is designed. The method analyzes the data characteristics of abnormal communication behavior, and constructs the feature input structure and detection system based on SVM algorithm by using the direct behavior feature selection and abnormal behavior pattern feature construction. The experimental results show that the method can effectively improve the detection rate of abnormal behavior, and enhance the safety protection function of industrial network.

CCS Concepts  
• Security and privacy→Intrusion/anomaly detection and malware mitigation →Intrusion detection systems

Keywords  
Industrial control network; intrusion detection; Modbus/TCP; feature extraction; SVM

1. INTRODUCTION  
Under the wave of “made in China 2025”, although the industrialization, the fusion and development of the network and information technology make the industrial control system connectivity degree is higher, but which is associated with worse information security problems [1,2]. Industrial control system has a lot of information security risks. One of the important reasons is that the “information island” of the industrial control system is not considered the information security and the lack of a corresponding security mechanism [3].

Different from the traditional complex communication, industrial control systems are often repeated to perform a series of process operation. That is to say, the control communication and data interaction of the industrial control network have the characteristics of "limited behavior" and "limited state". Therefore, according to the industrial control system of the characteristics of the communication can be summed up the exploratory research thought for anomaly detection methods: Changes in industrial communication behavior as a starting point, through artificial intelligence, mathematical statistics and other research methods, learn the industrial control network communication interaction rules and behavior mode, to provide the theoretical model for intrusion detection method design.

Intrusion detection is a kind of active defense technology. Intrusion detection can monitor and analyze communication behavior and intercept the intrusion before it can be harmful. It is a supplement to the function of the firewall[4]. According to the complexity of the industrial network system, based on the protection technology of security defense architecture and rules to match the detection can play an important role in the protection [5], but it cannot detect the basic features of the normal behavior of the attack. Intrusion detection system can detect the abnormal attack behavior by analyzing the characteristics of the communication behavior.

At present, the study of industrial network intrusion detection technology has obtained the certain research results. The main methods are K - NN classification data mining algorithm based on statistical learning [6], abnormal behavior detection method based on model parameters [7], the detection method based on industrial network traffic [8, 9] and the support vector machine (SVM) anomaly detection method based on machine learning [10, 11]. For Modbus protocol is widely used in industrial control system, the Modbus/TCP network security methods are mainly based on deterministic finite automata (DFA) modeling method of intrusion detection, intrusion detection method based on signature way and traffic detection method based on SVM [12-14]. Support vector machine (SVM) is a structural risk minimization algorithm of machine learning, can solve the small sample, nonlinear, high dimension classification problem, have the advantage of strong generalization ability.

Currently, the main aim of using SVM industrial network intrusion detection is to attack the abnormal behavior detection and classification, the related research is mainly concentrated in the kernel function of SVM model selection, parameter optimization and algorithm structure. In the application of SVM model in different fields, the method of data feature extraction is very different. There is no certain way of guidance. Different
industrial network intrusion detection system is the detection of abnormal behavior of network traffic analysis and data processing, study communication data feature extraction based on abnormal behavior will not only help to establish the SVM intrusion detection system model, data processing for other algorithms of intrusion detection system also has important significance.

In this paper, the depth analysis of the network security of Modbus/TCP industrial system is carried out. Through Modbus / TCP industrial system of typical attack behavior analysis depth analysis of abnormal behavior mode of operation, and analysis of network traffic changes, and then puts forward the data extraction method of SVM intrusion detection system, establish the communication behavior detection model.

2. MODBUS/TCP SECURITY ANALYSIS

Modbus/TCP is widely used in petroleum, chemical, electric power, energy and other fields of open industrial network communication protocol [15]. Modbus/TCP is the Modbus message transfer service on the TCP/IP, using a typical master-slave communication structure. Intrusion detection method based on SVM is the use of data to establish communication behavior anomaly detection model, and data feature reflect the abnormal behavior and the normal operation mode difference, combined with support vector machine (SVM) can deal with the high dimension, nonlinear, small sample data classification model and improve the detection rate of industrial control network attack behavior. Communication system is first and foremost a client sends a communication request, server receives a request message, function code, check data address and data threshold and according to the function code to perform the requested operation and send a response message to the client. If an error is detected in the communication data validation or execution operation, an exception response is sent to the client [16-17]. The communication structure of Modbus/TCP is shown in Figure 1.

![Figure 1. Communication structure of Modbus/TCP](image)

Because the Modbus/TCP protocol is based on Ethernet TCP/IP industrial communication protocol, which makes the industrial control system vulnerable to the traditional TCP/IP network attacks. At the same time Modbus is the most simple industrial communication protocol, the fundamental security problem lies in the lack of authentication, authorization and encryption mechanism. Firewall technology based on rule blocking can play a certain role in the security flaw of traditional network communication, but it cannot effectively detect and intercept the attack behavior of the application layer protocol data. This kind of attack behavior is similar to the basic feature of normal behavior communication, and it is difficult to realize the effective protection against the system with the traditional network defense technology. Abnormal attack behavior is the operation of the purpose of attack damage, its behavior patterns and normal behavior have a certain difference. Extraction method based on the characteristic of abnormal behavior pattern, not only from the attacking methods and ways to analysis the abnormal operation mode, also combining with the system of protection objectives and requirements, and according to the existing system vulnerabilities and safety risk, analyses the operating mode of behavior, to extract the detection characteristics of communication behavior, and improve the data characteristics of abnormal behavior detection of robustness. Therefore, it is very important to fully exploit the communication behavior characteristics and to establish the protection system of intrusion detection system.

The research shows that the intrusion detection system based on Modbus/TCP network is an effective way to improve the performance of security defense. The detection performance of intrusion detection system is determined by its working principle and application environment, thus establishing the correct rate of intrusion detection systems need to combine the actual application environment. We need to extract the communication behavior characteristics which can effectively reflect the problem of system security, and establish an intrusion detection model based on the extracted feature data to improve the interception of the Modbus/TCP industrial network attack behavior[18]. To evaluate the security rate of a dynamic system, an appropriate model that considers various aspects and factors, and which likewise mimics the attacker’s choice of exploits, should be set up [19]. Depth analysis of communication behavior model and resolve of network data communication features is not only beneficial to establish an intrusion detection system, and provide reference value to rule learning control method, and it also can further improve the industrial control system security protection technology to enhance the system security performance.

3. TCP MODBUS FEATURE EXTRACTION METHOD BASED ON ABNORMAL BEHAVIOR

3.1 Communication Behavior Analysis of Abnormal Attack

The attack on the Modbus / TCP industrial network is mainly through the loopholes in the system, using Modbus Protocol specification of malicious attacks to achieve the key data access, modification and destruction of the master station and the field equipment, control of the main station or field equipment to produce network communication path of denial of service, etc. Attack of the operator may be hackers from the Internet, may also be from enterprise network of internal staff. The main ways of attack are master station, field equipment and network communication path. Common attack actions are listening, interference, modification and forgery [20].

Exception attack is a serious threat to the operation of industrial control system. Unlike the traditional network systems, industrial control systems have high requirements for the availability of equipment, real-time and controllability. The likelihood for an attacker to carry out certain exploit on certain machine and the chance of success [21]. Once the attack will have an immeasurable life, property damage. Modbus/TCP attacks can include three levels: confidentiality, integrity, and availability. The confidentiality attacks mainly read data from field device, network traffic and information; Integrity attacks mainly insert the wrong data, configuration and cheat the main or field devices; availability attack mainly cut off communication connection, resulting in main station and field equipment cannot to lose the main function, restart or shutdown, which the most serious attacks may as control main station and field equipment.
Extract the abnormal behavior characteristics of intrusion detection is mainly divided into two aspects, the first is parses the communication flow of meaning and function to extract revealed the characters of abnormal behavior, the other is to analyze the abnormal behavior operation mode to extract the characteristic quantity which is easy to cause the abnormal operation. The feature extraction method based on abnormal behavior is mainly characterized by feature selection and feature construction, the actual Modbus/TCP industrial network traffic flow is shown in Figure 2.

### 3.2 Feature Selection of Communication Behavior

Intrusion detection system is based on the characteristics of the input to identify, in order to detect the abnormal attack behavior. Network traffic data is embodied communication behavior. Commonly used data feature selection method has two kinds, one is to directly extract part of the communication data, and processing data to get the input characteristics of the intrusion detection system. The other is much choose communication data, for data dimension reduction, compression to gain input features.

According to the communication flow chart shows, the network communication data contains IP address, port number, Modbus length, function code and other data features. A feature selection method based on abnormal behavior is according to abnormal behavior patterns, read Characteristics of the data from the network traffic, such as an attacker on the system of malicious attacks is the implementation of the corresponding operation through the function code, choose the function code for characteristic x1; For the Modbus protocol network communication, choose the identifier as a character x2, to prevent malicious attacks change the protocol; for the source and destination IP address can reveal the subject of malicious attacks, so choose two IP address as the characters x3 and x4; an attacker using Modbus protocol attacks, may produce Modbus packet malformation, the length of the data can reveal the changes, select the length as the data input characteristics of x5; attack when accessing a device data may show that the attack characteristic of the unknown data address, so choose a data address as characteristic quantity x6; Based on the analysis of the abnormal behavior of the communication mode, the method chose 12 input characteristics of intrusion detection system, the selected features based on the abnormal behavior are shown in Table 1.

| Feature | Feature description | Attribute |
|---------|---------------------|-----------|
| x1      | function code       | choice    |
| x2      | protocol identifier | choice    |
| x3      | source IP address   | choice    |
| x4      | destination IP address | choice     |
| x5      | length              | choice    |
| x6      | data address        | choice    |
| x7      | IP packet header length | choice   |

### 3.3 The Characteristic Structure of Communication Behavior

However, data characteristics in a single application of traffic to the operation of the abnormal behavior patterns reflect the shortcomings. For example, an attacker could use the function code to access device data information, under the normal behavior, master station may also be from station equipment data access in order to realize information collection, thus application function code data feature is can't reflect the abnormal patterns of behavior.

The feature construction method based on the abnormal behavior is mainly based on the Modbus/TCP attack mode, which can resolve the characteristics of the network traffic data, so as to construct the related behavior characteristics. Such as function code scanning attack, an attacker using loopholes in the system invaded the host system, query the network system function code used by Modbus message sending, When an attack occurs, the query of the unknown function code is easy to go wrong and the response of the function code is abnormal, so the x13 is used as the characteristic quantity of the abnormal number of the function code. In 20 seconds, happened five 01 function code exception response can determine the communication operation is aggression.

In order to obtain the abnormal behavior of the device information, the attack operation may read the device information for several times. This behavior does not conform to the normal operation mode of the system, so the number of times of the equipment information can be constructed x15, so that the system can detect the abnormal behavior. According to the attack pattern of abnormal behavior, the time length and the connection frequency attribute of communication data are constructed, which will affect the real system's intrusion detection. For example, the relatively long time and the number of connections can improve the detection efficiency of hidden attacks, but the real time will be reduced. The communication time is used to extract the data characteristics of abnormal behavior patterns, and the specific parameter selection should be based on the characteristics of the protocol operation and the communication behavior. In this method, the 8 characteristic variables are constructed by analyzing

Figure 2 Modbus/TCP industrial network traffic map

| Feature | Feature description | Attribute |
|---------|---------------------|-----------|
| x8      | source port         | choice    |
| x9      | unit identifier     | choice    |
| x10     | destination port    | choice    |
| x11     | transaction identifier | choice  |
| x12     | data quantity       | choice    |
the characteristic changes of the abnormal behavior, and the structural features based on the abnormal behavior are shown in Table 2.

### Table 2. The structure characteristic quantity based on the abnormal behavior

| Feature | Feature description | Attribute |
|---------|---------------------|-----------|
| x13     | 20 second function code | structure |
| x14     | 30 second data address abnormal code number | structure |
| x15     | 20 connected reading equipment identification number | structure |
| x16     | whether the illegal data exception code | structure |
| x17     | 20 times the number of connections to the same device | structure |
| x18     | 20 times the number of abnormal code in the same equipment | structure |
| x19     | 10 read function code number | structure |
| x20     | 10 connected write function code number | structure |

### 4. SVM INTRUSION DETECTION MODEL

Intrusion detection system is to design a classifier, which can distinguish the normal and abnormal data from the data flow, so as to realize the detection of the attack behavior. Commonly used classification method has the decision tree and naive Bayesian method, neural network and support vector machines, decision tree with time series data needs to be more preprocessing, classification error rate with the category number increases rapidly increase, the naive Bayesian method need to know a priori probability existed problem such as fitting and generalization ability. According to the complexity of the environment of industrial control system, the intrusion detection model based on SVM is to transform the industrial network communication data into the system input feature, and get the decision function of the network communication behavior. SVM kernel function can be non-linear mapping input data, while overcoming the curse of dimensionality of data, using a method to maximize the spacing so that the algorithm avoids local minima and over-fitting problem, which makes the SVM intrusion detection suitable for application of Modbus / TCP industrial network system.

In this paper, by using the nonlinear largest soft margin SVM dual algorithm, through the most optimal solution to obtain communication behavior of discriminant function, design intrusion detection model. Concrete steps are as follows:

**Step1** extraction of network traffic data, through the data feature selection and construction methods, access to the SVM model of the input characteristics.

**Step2** select the appropriate kernel function \( K(x, z) \) and the appropriate parameters of \( C, \) structure and solve the optimization problem:

\[
\min_{\alpha} \frac{1}{2} \sum_{i=1}^{N} \sum_{j=1}^{N} \alpha_i \alpha_j y_i y_j K(x_i, x_j) - \sum_{i=1}^{N} \alpha_i \]

\[
\text{s.t} \quad \sum_{i=1}^{N} \alpha_i y_i = 0, \quad 0 \leq \alpha_i \leq C, \quad i = 1, 2, \ldots, N
\]

Get the optimal solution

\[
\alpha^* = (\alpha_1^*, \alpha_2^*, \ldots, \alpha_N^*)^T
\]

**Step3** Choose a characteristic component of \( \alpha^* \) as \( 0 \leq \alpha_i^* \leq C \), calculation

\[
b^* = y_j - \sum_{i=1}^{N} \alpha_i^* y_i K(x_i, x_j)
\]

**Step4** structure decision function:

\[
f(x) = \text{sign}\left( \sum_{i=1}^{N} \alpha_i^* y_i K(x_i, x_j) + b^* \right)
\]

**Step5** according to the characteristics of the decision function and the input data, the classification of the communication behavior of SVM is calculated.

In traditional SVM intrusion detection application, mainly studies the choice of kernel function, parameter optimization, improved algorithm structure in order to improve the detection efficiency of the algorithm, this paper combines the advantages of the special nature of industrial network environment and support vector machine algorithm, Mainly studied the SVM intrusion detection based on abnormal behavior feature extraction and modeling method. In the actual establishment of model learning algorithm structure and parameters of the application, Intrusion detection system based on abnormal behavior patterns can extract the data features which reflect the difference of communication behavior, so as to improve the detection efficiency of abnormal attack behavior. Data feature structure is the input of intrusion detection system, which plays a key role in the performance of communication behavior. Through this method to extract features and a process framework of SVM intrusion detection model is shown in Figure 3.

![Figure 3. Flow chart of SVM intrusion detection model](image-url)
5. NUMERICAL ANALYSIS

In view of the intrusion detection system feature extraction modeling and intrusion detection methods proposed in this paper, the control system simulation environment of Modbus/TCP communication is set up. The system simulation in the production of chemical reactor control flow, the M340 PLC as controller, the reactor temperature, liquid level and flow rate for acquisition and control, with the Modbus/TCP protocol in network communication, real-time display the reactor control parameters change.

According to the design requirements of the intrusion detection system, the simulation experiment uses the master station which is attacked by the attack to send malicious attack code to the controller PLC, which makes the control system running fault of the reactor. The experimental design simulation Modbus/TCP attack operation behavior has read the key data from the station equipment, try to obtain the system operation, rewrite the control parameters and other illegal operation. Communication behavior of operations collect temperature, liquid level, flow and other parameters according to the protocol function code and the corresponding control. Simulation experiment design of external attack and internal attacks, external attacks due to the lack of understanding of the actual system, easy to produce the basic function code, data address, the amount of data, and other errors. Attacks from the simulated internal staff are more subtle in the operation, which requires the operation of the frequency and the number of connections to get abnormal behavior information.

At the same time, according to abnormal behavior mode selection of intrusion detection data characteristics, the Wireshark capture the actual network traffic, extract SVM model selection and construction of 20 feature quantity x, the feature data extraction, obtained 1000 samples of the training data set which + 1 and - 1 two types of sample 500 each. 400 samples were obtained as intrusion detection test data sets, in which +1 and -1 two kinds of samples of each of the 200. The test samples are divided into two kinds, the first is to extract the 400 test data set detection classification, and then add and training data in the unknown abnormal attack samples for testing classification experiment. The prediction results of the two test data samples are shown in Figure 4 and Figure 5.

![Figure 4. Comparison of the results of test data set](image)

![Figure 5. The result of test set with unknown abnormal data](image)

According to the simulation results, the intrusion detection system for the training data set the correct classification rate reached 99.7%, the classification of the test set accuracy rate is 98.25%. Indicating the communications traffic feature extraction based on abnormal behavior, can fully reveal the communication behavior model. This model has better classification ability of communication behavior to add a new type of unknown attack data samples. The classification accuracy was 97.5%, which was found from the abnormal samples of the results. The model to the unknown abnormal data also has a good classification ability and the actual feature extraction is starting from the perspective of a behavior pattern, at the same time, this feature may also reflect other types of abnormal behavior patterns.

In order to compare feature extraction method based on abnormal behavior, the experiment only according to the communication flow directly select the feature data and The correct classification rate of the detection model is 86.7%, and the classification rate of the test data is 87.25%, indicating that based on abnormal behavior of feature selection and construction method can effectively improve the classification ability of SVM intrusion detection. The simulation results are shown in Table 3.

| Table 3. Experimental results |
|-------------------------------|
| Abnormal behavior modeling | Direct feature modeling |
| Training set data | 99.7% | 86.7% |
| Test set data | 98.25% | 87.25% |
| Add unknown exception data | 97.5% | / |

6. CONCLUSION

This article in view of the Modus/TCP industrial network security problem of intrusion detection is firstly analyzed the security of network system, by parsing the Modbus/TCP network communication behavior mode of operation, abnormal intrusion detection of feature extraction method is proposed, and the SVM intrusion detection model is established. In this method, the data characteristics of communication behavior are selected and constructed in the view of the reflection of the network traffic flow and the security defense. Finally, the experimental simulation environment is built to capture the communication data flow, the training model of intrusion detection and simulation experiment.
On the basis of the data feature and the training detection model of abnormal behavior, this paper adds the unknown abnormal behavior and the direct selection of the data samples, establishes the SVM detection model. Through the comparative analysis, the performance of the method is proposed, which fully shows that the modeling method of feature extraction based on abnormal behavior can improve the detection performance of abnormal attack behavior. The method of feature extraction based on abnormal behavior will be affected by the diversity of abnormal behavior and the detection rate is not high, which is the need for further research and improvement. At the same time, it is also effective to improve the accuracy of intrusion detection model in the aspects of reducing dimension, compressing process and improving SVM model.

7. ACKNOWLEDGMENTS

The authors would also like to acknowledge the helpful comments and suggestions of the industry control system security software group. Their efforts are greatly appreciated. This work is supported by Beijing Finance refers to a [2015] 1170. The name of this project is "the development and verification platform supported by Beijing Finance refers to a [2015] 1170. The name of this project is "the development and verification platform construction of industrial information security key standards for intelligent manufacturing".

8. REFERENCES

[1] K. Yim, A. Castiglione, J. H. Yi, et al. 2015. Cyber threats to industrial control systems. Proceedings of the 7th ACM CCS International Workshop on Managing Insider Security Threats (Colorado, USA, Oct. 2015), 79-81.

[2] M. Cheminod, L. Durante, A. Valenzano. 2013. Review of security issues in industrial networks. IEEE Transactions on Industrial Informatics, 2013, 9(1):277-293.

[3] Y. Yang, K. Mclaughlin, S. Sezer, et al. 2014. Multiattribute SCADA-specific intrusion detection system for power networks. IEEE Transactions on Power Delivery, 2014, 29(3):1092-1102.

[4] Alireza Osareh, Bita Shadgar. 2008. Intrusion detection in computer networks based on machine learning algorithms[J]. International Journal of Computer Science and Network Security, 2008,11(8):15-23.

[5] Hamed Okhravi, David M. Nicol. 2009. Application of trusted network technology to industrial control networks[J]. International Journal of Critical Infrastructure Protection, 2009(2):84-94.

[6] Pedro Silva. 2014. On the Use of K-NN in Intrusion Detection for Industrial Control Systems[D]. Ireland Galway: national university of Ireland Galway, 2014.

[7] Y. L. Mo, R. Chabukswar, B. Sinopoli. 2013. Detecting integrity attacks on SCADA systems. IEEE Transactions on Control Systems Technology, 2013, 22(4):1396 - 1407.

[8] M. Wei, K. Kim. 2012. Intrusion detection scheme using traffic prediction for wireless industrial networks. Journal of Communications and Networks, 2012, 14(3): 310-318.

[9] M. Wan, W. L. Shang, P. Zeng. 2015. Anomaly detection approach based on function code traffic by using CUSUM algorithm. Proceedings of 2015 4th National Conference on Electrical, Electronics and Computer EngineeringXi an, China, Dec. 2015),1506-1511.

[10] L. A. Maglaras, J. M. Jiang. 2014. OCSVM model combined with k-means recursive clustering for intrusion detection in SCADA systems. Proceedings of 2014 10th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness,(Rhodes, Greece, Aug. 2014), 133-134.

[11] A. Anoop, M. S. Sreela. 2013. New genetic algorithm based intrusion detection system for SCADA. International Journal of Electronics Communication and Computer Engineering, 2013, 2(2):171-175.

[12] Niv Goldenberg, Avishai Wool. 2013. Accurate modeling of Modbus/TCP for intrusion detection in SCADA Systems[J]. International Journal of Critical Infrastructure Protection, 2013 (2):63-75.

[13] DIAZ J J 2011. Using SNORT for intrusion detection in Modbus TCP/IP communications [EB/OL]. 2011. DOI= http://www.giac.org/paper/gcia/7218/snort-intrusion-detection-modbus-tcp-ip-communications/124438

[14] SHANG Wenli, ZHANG Shengshan, WAN Ming. 2013. Modbus/TCP communication anomaly detection based on PSO-SVM[C]/Proceedings of 2013 the 3rd International Conference on Communication and Network Security, London UK:. Trans Tech Publications, 2013,1745-1753.

[15] Thomas H, Morris, Bryan A, Jones, Rayford B. 2013. Deterministic Intrusion Detection Rules for MODBUS Protocols[C]. Hawaii: 2013 46th Hawaii International Conference on System Sciences, 2013, 1773 - 1781.

[16] GB/T 19582.1-2008, Modbus industrial automation network specification - Part 1: Modbus application protocol [S].

[17] GB/T 19582.3-2008, Modbus industrial automation network specification - Part 3: Modbus protocol implementation guide over TCP/IP [S].

[18] Srilatha Chebrolu, Ajith Abraham, Johnson P. Thomas. 2004. Feature deduction and ensemble design of intrusion detection systems[J]. Computers & Security, 2004,24(4):295-307.

[19] Huang, H., Zhang, S., Ou, X., Prakash, A., and Sakallah, K.2011. Distilling critical attack graph surface iteratively through minimum-cost sat solving.Proceedings of the 27th Annual Computer Security Applications Conference,2011, 31-40.

[20] Peter Huitsing, Rodrigo Chandia, Mauricio Papa, et al. 2008. Attack taxonomies for the Modbus protocols[J]. International Journal of Critical Infrastructure Protection, 2008,37-34.

[21] Zhao, F., Huang, H., Jin, H., and Zhang, Q. 2011.A hybrid ranking approach to estimate vulnerability for dynamic attacks. Computers & Mathematics with Applications, 2011, 4308-4321.