Acta Technica *62* (2017), No. 5B, 1039–1048

The identification about the role of components in the energy internet information security risk

Guohuan Wang[2], Zhimin Cai[1], Min Li[1], Shi Yu[1]

Abstract. The topological structure of the energy Internet is complex and often changes, which bring the difficulties to identify and evaluate the security risk. In order to recognize the situation of security risk about the whole energy Internet efficiently when the topological structure changes, it is necessary to understand the role of each component in the network security, but most of the studies took the target network as a whole to evaluate its security risk. In this study, a novel method to identify the role of each component in energy Internet security is proposed. The relationship of components in the network is described and formulized. Applying the security value formula of each component, the security value formula of the whole system is expressed. By simulation experiment, the security value of the network is explored when the menace probability of the component in the network changes. Further, the roles of the different components in the whole network security are obtained. Results demonstrate that each component has different impact on the system information security and the degree of the impact changes from 0% to 11%. The method can help the network administrators to find the key components that need take more notice. This research provides a good way to evaluate dynamic network security.

Key words. Energy Internet, Security Risk, Security Evaluation, Topological Component.

1. Introduction

With the “Third Industrial Revolution” published by the American writer Rifkin as the mark, the concept of energy Internet began to rise. On Sept. 26th, 2015, President Xi Jinping gave a speech at the United Nations Development Summit titled "To Seek the Common Sustainable Development, and Become Win-win Cooperation Partners" in which he announced to the world: China proposes to explore the construction of global energy Internet, and promotes to meet the global demand for electricity by a clean and green way. As the world’s largest power grid enterprise, State Grid Corporation of China has carried on positive exploration and practice,

[1]Workshop 1 - State Grid Jiangxi Information & Telecommunication Branch, Nanchang, China
[2]Corresponding author: Guohuan Wang

and has ranked among the top in the world in terms of building up the global energy Internet[1].

The construction of energy Internet cannot run smoothly without the information technology support. Energy Internet provides users with open and convenient communication and interaction ways, and at the same time, it may leave chances for the malicious attackers to use more diverse ways to attack energy Internet[2,3]. While improving the degree of interconnection and interoperability in energy network, the far-ranging interconnected characteristics also spread to wider scope impact for the malicious attacks and bring serious harm more easily than ever. Under the energy Internet environment, the information system which supports the six core links of the smart power grids will surely face more diversified information security risks and the situation of information security threat has become increasingly serious. Information security risk evaluation is the basis work and important step for information safety guarantee, which confirms the anticipated loss when the computer system and network suffers destroy or gets out of resources. It evaluates threat and vulnerabilities in network and measures risk quantity. The risk evaluation runs through every stage of information system, including plan stage, design stage, implement stage, maintenance stage and abandon stage.

The energy Internet is featured by the complex network structure, the diversified trend of Internet users and the constant change of the network structure. During the safety management of the energy Internet, it is more difficult to identify the risks in it. As the traditional static security risk identification methods are no longer applicable, in the assessment of the energy Internet information security risks, the dynamic changes of the system should be considered, and the dynamic evaluation method should be adopted for qualitative and quantitative safety analysis of the system [4].

2. State of the art

Information security evaluation must be based on some technology methods and evaluation model. The evaluation method should be chosen according to the practical condition because evaluation method determines each step of evaluation process and the evaluation result. The traditional evaluation methods are divided by three types: quantitative method, qualitative method and the combination method between quantitative method and qualitative method [5]. The quantitative method applies quantity index to assess network risk. The classic quantitative analysis method may include factor analysis, time series model, cluster analysis, regression model, and decision tree model etc. The qualitative method depends on the experience, technical ability and knowledge of the evaluation experts and this method can provide more comprehensive risk analysis. However this method has strong subjectivity and need set stricter standards on experts, which is the weakness of this method. The typical qualitative methods include history comparison, logical analysis, factors analysis, Delphi method etc. The third method is the combination of quantitative method and qualitative method, which absorbs the advantage of above two methods. This method has been applied to risk evaluation of complex information system

widely. The Analytic Hierarchy Process(AHP) method is very popular which was suggested by Saaty professor in Pittsburgh university[6].

The above traditional evaluation methods has important situation in network risk evaluation field, and also accumulate many research results. However most of the traditional methods put their focus on once evaluation and form one result. They have not taken into consideration about the dynamic change of network. For the energy Internet, the network is very complex, and it can change with time and safe factors variance. The variation of the network structure and safe factor may change the security features of whole system. Moreover the topological structure of energy Internet shift as the form of flexibility and by random way which could cause dynamic process about its security features.

Yu et al. [7] presented an approach based on colorful Petri network which can realize post-processing and correlation analysis for alert. The approach increases the ability to analyze network data. Sommestad et al. [8]constructed the security risk analysis models based on probability relational models. This method makes it possible to describe the relationship of object's attributes. Based on the service-dependency graph, Shameli-Sendi [9]assessed the dependency cost about resource dependencies and the number of users. They also analyze the attack cost by service dependence graph. Ghasemigol et al. [10]designed a forecasting method that can predict threat from attack more precisely with environment change applying dependency graph.

Santos et al.introduced a framework for enforcing risk-based policy based on XACML. Applying this framework, they evaluated the risk in the cloud by an ontology-based risk evaluation method. But this method has not considered the condition when the components of the network change which usually happen in the cloud environment.

Most of the previous studies laid on their stress on the whole network, which means they researched the risk evaluation of the whole network. For energy Internet, the topological structure is more complex and would change frequently. So the network manager must grasp the role of each component or some components in the network security risk management so that they can take more notice about the key components. This paper focused on the relationship of each component in the network for evaluating security risk. The paper concluded the relationship of each component in the network, and expressed the relationship by security value formula. Applying simulation experiments, the paper got the dynamic security value of the whole network with time change and explored the role of each component.

3. Topological Structure of the Energy Internet

The energy Internet is featured by the complex network structure, the diversified trend of Internet users and the constant change of the network structure. During the safety management of the energy Internet, it is more difficult to identify the risks in it. As the traditional static security risk identification methods are no longer applicable, in the assessment of the energy Internet information security risks, the dynamic changes of the system should be considered, and the dynamic evaluation

method should be adopted for qualitative and quantitative safety analysis of the system. The former literature proposed a dynamic evaluation model applicable to the mobile self-organizing network. This paper makes use of the model method for risk assessment of the local energy Internet. It also tests the impact of the structure change upon the risks of the whole system.

4. Component-based topological structure of the network

Component refers to the software system or hardware device with specific functions or a set of access interface in the information system. Components can become the constituent part of the larger components through combination; they can also be divided into even smaller components. In the information network, each network device can be considered as a component. This paper studies the large-scale energy Internet with slightly larger components, and it refers to a specific system.

The component-based topological structure consists of access paths between components. Access path refers to the request and response relationship existing between the components and an orderly access sequence will form in the system topological structure. These sequence set is called access path, hereinafter referred to as the path.

This paper extracts a part of an actual energy Internet, and its topological structure is shown in Fig.1. The part is abstracted to become the component-based topological structure. Its security risks are analyzed and evaluated in the paper. Fig. 2 shows the component-based topological structure studied here, with $C_i$representing the component i.

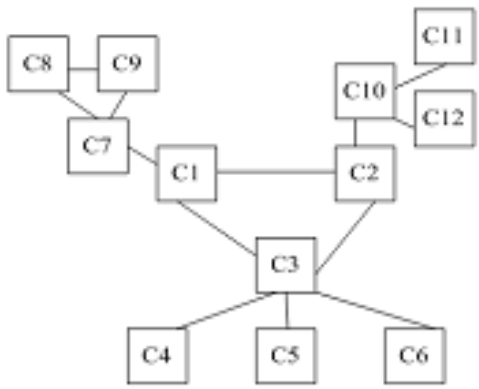

Fig. 1. the topological structure of network instance

4.1. The relationship of the components

Three types of relationships exist between the components, including independent, collaborative and special relationships.

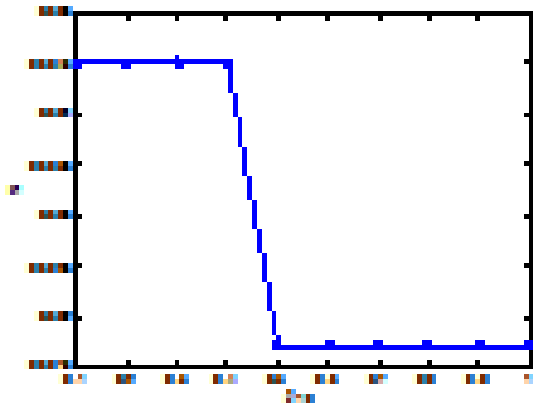

Fig. 2. the component-based topological structure

(1) Independent relationship refers to that no access path bP_i exists between the components C_i andC_j, namely the function of the component C_i is independent of the component C_j and does not need the latter's participation or collaboration. Thus, their security properties change will not affect each other.

(2) Collaborative relationship refers to that at least one path P_i exists between the components C_i andC_j, and collaborative relationship exists between them. They need to cooperate with each other in the real functions, and their security properties are also related to each other.

(3) Special relationship refers to that at least one path P_i exists between the components C_i andC_j. But unlike the collaborative relationship, the function of component C_i is independent of the component C_j and does not need the latter's participation or collaboration. In most cases, their security properties change will not affect each other. But in some cases, some harm will use pathP_i to launch attack and at this moment the two components' security attributes will influence each other.

The topological structure of this paper is analyzed according to these several relationships to determine the relationships between the components. Among them, $C1, C2, C3$ are collaboratively related, $C4, C5, C6$ are independent relationship, $C7, C8, C9$ are collaboratively related, $C10, C11, C12$ are also collaboratively related.

5. Security Risks Assessment of the System

5.1. Security value assessment of each component

Before the assessment of the security value in the entire network, it is necessary to determine the security value of each component. There are many ways to measure the security of the individual component. This paper adopts the classical assessment

method based on probability. Two aspects of risks should be considered in the assessment method: one is the vulnerability, anti-attack ability and possible damage that exist in the component. Vulnerability is expressed by insecurity rate α $\alpha \in [0, 1]$. The greater value αhas, the higher vulnerability the component will have, and the lower its security degree will be. The other is to consider the risk probability $\beta$of the component. The greater value βhas, the greater the probability that the component will be under attack. In addition, the security value of the component will change with the change of the running time. In conclusion, the security value formula of the componentC_i is as follows:

$$S_i(t) = 1 - (1 - e^{-\alpha_i t})\beta_i \tag{1}$$

In the formula (1), t signifies running time $\alpha_i$signifies the insecurity probability of the component i and β_i signifies the risk probability of the component i.

The insecurity probability and risk probability of each component are obtained in this paper according to a given network evaluation report, as is shown in Table 1. The formula (1) can be used to calculate the security value of each component.

Table 1. The insecurity probability and risk probability of each component

Component	Insecurity probabilityα	Menace probabilityβ	Component	Insecurity probabilityα	Menace probabilityβ
C1	0.1	0.3	C7	0.4	0.4
C2	0.1	0.4	C8	0.4	0.4
C3	0.1	0.4	C9	0.4	0.4
C4	0.3	0.5	C10	0.3	0.6
C5	0.3	0.5	C11	0.5	0.5
C6	0.3	0.5	C12	0.6	0.3

5.2. Security value assessment of component-based network

Based on the analysis given in the section 3 and by referring to Fig. 2, the composition relationship between the components can be expressed as

$$T = (C7\Delta C8\Delta C9)\,|\{(C1\Delta C2\Delta C3)\Upsilon(C4\Upsilon C5\Upsilon C6)\}\,|(C10\Upsilon C11\Upsilon C12) \tag{2}$$

In formula (2), Δrepresents triangle combination structure of components, Υrepresents star combination structure, and $|$ represents serial combination structure.

The security value formula of each component can be obtained from the composition analysis:

$C1, C2, C3$ are triangle combination and collaboratively related, so the security value of the three components can be expressed as:

$$S_{1,2,3} = \min(S_1, S_2, S_3) \tag{3}$$

$C4, C5, C6$ are star combination and independent relationship, so the security value of the three components can be expressed as:

$$S_{4,5,6} = S(1) - \prod_{1}^{n}(S(1) - S(\phi_i)),\ n = 4, 5, 6 \tag{4}$$

$C7, C8, C9$ are triangle combination and collaboratively related, so the security value of the three components can be expressed as:

$$S_{7,8,9} = \min(S_7, S_8, S_9) \tag{5}$$

$C10, C11, C12$ are star combination and also collaboratively related, so the security value of the three components can be expressed as:

$$S_{10,11,12} = \max(S_{10}, S_{11}, S_{12}) \tag{6}$$

At the same time, the combination of $C1, C2, C3$ and $C4, C5, C6$ is star structure and the relationship is special, so their security value can be expressed as:

$$S_{1,2,3,4,5,6} = \varepsilon \times \max(S_{1,2,3}, S_4, S_5, S_6) \tag{7}$$

ε is weight coefficient, which is decided by the degree of vulnerability and threat probability.

The above six components and $C7, C8, C9$ are collaborative relationship and star combination, so their security value is :

$$S_{1-9} = S_{1,2,3,4,5,6,7,8,9} = \max(S_{7,8,9}, S_{1,2,3,4,5,6}) \tag{8}$$

And $C10, C11, C12$ and the above nine components are special relationship and serial combination, so the security value of the system can be expressed as:

$$S = \varepsilon \times \max(S_{1-9}, S_{10,11,12}) \tag{9}$$

On the basis of formula (1)$\sim$(9), we can calculate the security value of the system by computer simulation. Considering the different time effect, the experiments were done under the different period.

5.3. The role analysis of each component in the network security value

During further analysis and experiment about the network security value formula, it is found that different components have different influence upon the network security values of the whole network. Therefore the simulation experiment is carried out by changing the threat probability of each component. The changes of the security value in the whole network are respectively given in Figures 3(a)(b) when the threat probability of components $C7$, and $C10$ changes. It is found that the threat probability of component $C1$ has no effect on the network security value, while the threat probability changes of components $C7$ and $C10$ have different degrees of influence on

network security value. In the daily management of the network, attention should be paid to the impact of these components upon system security, and supervision and management work should be strengthened.

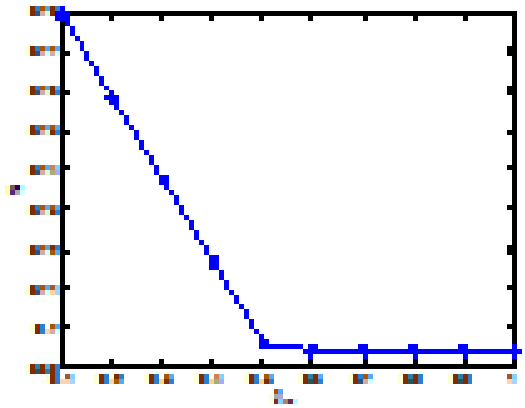

Fig. 3. security value with the threat probability varying

6. Conclusions

It is difficult to identify and control the security risk for the energy Internet on account of its complex structure. To identify security risk in the energy Internet more accurately and efficiently, a novel method based on network component analysis was developed to provide the security values variance with the component security menace change. A case study about a complex practical network was analysed by this method.

This study about security risk evaluation can help the network administrators recognize the critical components in the network in advance, so as to make countermeasures to enhance the overall safety performance of the network.

References

[1] R. Felix, D. Pravin, A. Varaiya: *Smart grids with intelligent periphery: an architecture for the energy Internet.* Engineering *4* (2015), No. 1, 436–446.

[2] T. Rintam, A. Siddiqui, A. Salo: *Does renewable energy generation decrease the volatility of electricity prices? an analysis of denmark and Germany.* Energy economics *1* (2017), No. 62.

[3] Y. E. Yizhi, C. Academe: *Technology research and application for energy Internet.* Electrical & energy management technology *1* (2016), No. 22, 234–245.

[4] M. Dacier, F. Kargl, H. Knig: *Network attack detection and defense: securing industrial control systems for critical infrastructures.* Dagstuhl reports *1* (2014), No. 4, 62–79.

[5] L. Zhang, J. Peng, Y. Du: *Information security risk assessment survey.* Journal of tsinghua university *10* (2012), No. 52, 1364–1369.

[6] T. L. Saaty: *How to make a decision: the analytic hierarchy process.* European journal of operational research *1* (1990) 9–26.

[7] D. Yu, D. Frincke: *Improving the quality of alerts and predicting intruder's next goal with Hidden Colored Petri-Net.* Computer networks the international journal of computer & telecommunications networking *3* (2006), No. 51, 632–654.

[8] T. Sommestad, M. Ekstedt, P. Johnson: *A probabilistic relational model for security risk analysis.* Computers & security *6* (2011), No. 29, 659–679.

[9] A. Shameli-Sendi, M. Cheriet, A. Hamou-Lhadj: *Taxonomy of intrusion risk assessment and response system.* Computers & security *3* (2014), No. 45, 1–16.

[10] M. Ghasemigol, A. Ghaemi-Bafghi, H. Takabi: *A comprehensive approach for network attack forecasting.* Computers & security *3*, (2016), No. 58, 83–105.

Received November 16, 2017