IOP Conference Series: Earth and Environmental Science

PAPER • OPEN ACCESS

Defensive resource allocation for cyber-physical systems in global energy interconnection

To cite this article: Xiaodong Chu *et al* 2019 *IOP Conf. Ser.: Earth Environ. Sci.* **227** 042002

View the article online for updates and enhancements.

IOP | ebooks™

Bringing you innovative digital publishing with leading voices to create your essential collection of books in STEM research.

Start exploring the collection - download the first chapter of every title for free.

This content was downloaded from IP address 49.83.23.59 on 23/09/2019 at 03:03

Defensive resource allocation for cyber-physical systems in global energy interconnection

Xiaodong Chu[1, 3], Yu Yi[1], Maosen Tang[1], Haoyi Huang[1] and Lei Zhang[2]

[1] School of Electrical Engineering, Shandong University, Jinan, China;
[2] Electric Power Research Institute of State Grid Shandong Electric Power Company, Jinan, China.

[3] E-mail: chuxd@sdu.edu.cn

Abstract. Due to close coupling between physical and information systems, an unexpected attack on the node of the information system will result in great operational risk of global energy interconnection. A defensive resource allocation strategy for cyber-physical systems is proposed. Various risk factors of information systems are quantitatively evaluated in this paper. An optimal defensive resource allocation model is built to strengthen the security and stability of the cyber-physical systems, which accounts for nodal vulnerability and nodal risk degree. Simulations results of a test power system and its corresponding communication networks verify the effectiveness of the proposed allocation strategy.

1. Introduction

As the concept of global energy interconnection being put forward in electrical industry, more operational state and information of power system must be transmitted through the long distance telecommunication line [1-2]. Any failure of the communication node will result in data incomplete, seriously, the structure of the network will change due to cascading failure when the key nodes are attacked [3-4]. The risk factors for communication node will greatly reduce the stability and reliability of power system operation in a coupling cyber-physical system.

There are numerous works to effectively measure the risk status of the information system against various types of attack. The removal strategies [4] based on the degrees and betweenness centralities often have a great effect on the vulnerability of the complex networks because the network structures will be changed as the vital nodes or edges being removed [6]. Therefore, it's vital to study the reconstruction of the network after a failure happen. A simple “one-to-one" interdependence model was considered in [7] to build interdependent networks under cascade of failures. In [8], the author suggested that high-betweenness nodes should be planned as autonomous nodes, in order to have the best resiliency in an interdependent network.

In order to assure the safety of the network under attack, literature [9] studied the steady-state effect of a failure in a cyber-physical system. The influence of active small clusters appearing after an attack on the whole network performance is studied in [10]. The degree weighting models in [11-12] are used to find out the key nodes in networks, and the results show that the best defensive status of nodes are their capable of maintaining the highest priority protective degree when the defensive resources for them are limited. However, the biggest shortage is that the existing models for the assessment of nodal vulnerability neither the linear ones nor exponential ones are difficult to reflect the features in actual systems due to the marginal effect and ‘trailing’ phenomenon.

Content from this work may be used under the terms of the Creative Commons Attribution 3.0 licence. Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.
Published under licence by IOP Publishing Ltd

In this paper, the importance of node is firstly assessed by means of graph theory and then the quantitative evaluation of risk factors is built based on nodal importance and the theory of probability. To reduce the risk level of the cyber-physical network, an optimal allocation model for defensive resources taking nodal vulnerability and nodal risk degree into account is proposed to maximize the usage of the limited defensive resources in the network and strengthen the security and stability of the cyber-physical systems.

2. Quantitative evaluation of risk factors

2.1. Nodal importance

Since the communication network carries the real-time information and dispatch command of the power system, the safety of the key nodes in communication network will directly affect the security and stability of the cyber-physical system. Referring to complex network graph theory, this section puts forward the method of quantitative evaluation for nodal importance in communication system considering nodal degree and closeness.

The communication network can be expressed as a simple diagram $G(I,A)$. $I=(i_1,i_2,...,i_N)$ is a collection of node; *N* is the number of communication nodes; $A=(a_{ij})_{N\times N}$ is an symmetric adjacency matrix where $a_{ij}=1$ represents there is a connection between node *i* and node *j* while $a_{ij}=0$ represents disjunction between two nodes. The nodal degree k_i which describe the number of adjacent nodes connecting to node *i* can be expressed as:

$$k_i=\sum_{i=1}^{N}a_{ij} \tag{1}$$

The degree index evaluates the ability of node *i* to establish a direct contact with the neighbor nodes, however, it cannot show the detail information of connection between two nodes. Therefore, the sum of the nodal degree k_i and its neighbor nodal degree k_j is used to depict the connectivity of each node in the realistic network, which can be expressed as:

$$f_i=k_i+\sum_{j\in B_i}k_j \tag{2}$$

Nodal closeness shows the indirect influence of one node on the others in the network, which means the difficulty of the path that one node to reach others. Hence, the nodal closeness is introduced to analyze the impact of node location in the network on the speed of information transmission. In the network with *N* nodes, the sum of the distances that a node reaching all the other nodes is not less than *N*-1. Therefore, nodal closeness m_i is normalized as:

$$m_i=\frac{N-1}{\sum_{j=1}^{N}d_{ij}} \tag{3}$$

In equation (3), d_{ij} represents the shortest path from node *i* to node *j*. The ability of transferring information is preferable with a higher value of m_i on each node. In fact, the information generated on the central node will be transmitted through the entire network in the shortest time. Hence, the nodal importance consists of the degree and closeness index can reflect not only the connection between two nodes, but also the locations of the node in the network, which is writing as:

$$o_i=\frac{f_i}{\sqrt{\sum_{j=1}^{N}f_j^2}}+\frac{m_i}{\sqrt{\sum_{j=1}^{N}m_j^2}} \tag{4}$$

2.2. *Three types of risk factors*

Due to the coupling characteristic of cyber-physical, the attack in communication network will increase the risk of power system significantly. Therefore, it is vital to predict the probability that nodes will fail against different attack events. In this paper, we take man-made attack, equipment damages and natural hazards into account as kinds of risk factors.

Generally, the attackers destroy one or more communication nodes in the network, which results in the data incomplete when they are uploaded to the scheduling center. A "smart" attacker usually has the ability to master the topology of the entire information network and attempt to cause the most serious damage at the smallest possible cost. Therefore, nodes with greater importance are more vulnerable to be attacked so that the probability that each node will fail under man-made attack can be expressed as:

$$P_{Evevt-ma}^{i}=\frac{o_i}{\sum_{j}o_j} \tag{5}$$

Communication equipment are often exposed to a complex and volatile external environment and experience sudden temperature change, electromagnetic interference and a lot of dust pollution, which will increase the uncertainty of measurement. In this paper, the probability of the failure on each node with equipment damages can be considered to follow the Poisson distribution, writing as:

$$P_{Event-ed}^{i}=(1-e^{-\lambda_i})e^{-\sum_{j\neq i}\lambda_i} \tag{6}$$

where λ_i is the average accident rate of the equipment in the examined time. The probability of fault on each equipment is independent and only one equipment is breakdown while the others work normally in each accident.

To model simply, the probability that nodes fail against natural hazards are consistent in each area and they are depend on the severity of the disasters. Assuming that communication network is divided into *n* regions, the probability is writing as:

$$P_{Event-nh}^{i}=1/n \tag{7}$$

3. Defensive resources optimal allocation model for cyber-physical network

3.1. *Nodal vulnerability analysis*

The vulnerability of the network involves the probability that a defensive resource will fail under attack, which is mainly affected by the amount of available defensive resources. If there are more defenders available, the system will have more defensive measures to take and then much survivable the network will be, and vice versa.

The proposed linear [11] and exponential model [12] can depict the relationship between defensive resources and the vulnerability of their connecting nodes, however, they cannot accurately reflect the practical problem. For instance, the linear model cannot solve the marginal effect of the decreasing rate of vulnerability with the increase of available resources. For another, the exponential model has a serious 'trailing' phenomenon. Only when the available resources reach infinity, there is no risk of vulnerability in the network, which is seriously inconsistent with the actual situation. Therefore, to overcome the shortage of the above models, the power function is used in this paper to show the relation between the vulnerability of nodes and availability of defensive resources corresponding to them, which follows as:

$$v_i=(1-\frac{x_i}{\max X_i})^2 \tag{8}$$

In Equation (8), v_i is the vulnerability of node *i* in information network; x_i is the number of available defensive resources on node *i*, which are abstracted from defensive strategies; $\max X_i$ is the maximal requisite defensive resources to achieve the highest security level on node *i*, which is determined by the number of available resources on each node or in each sub-region. The power function model can not only effectively characterize the decreasing trend of the network vulnerability as the defensive resources increases allocation but also feature the upper limitation of allocation for the defenders.

3.2. Nodal risk assessment

The probabilistic risk analysis (PRA) [14] is a combination of the qualitative and quantitative method, which is an important mathematical tool for quantitative risk assessment of complex systems. PRA utilizes the probabilistic model to differentiate the risk extent of network caused by various factors, which is helpful to find out the weak links in the systems and enhance the safety of the systems. PRA is mainly divided into the following parts as: find the most vital risk factors, propose the possible distribution of risk factors, put forward and discuss the acceptable risk decisions. Based on the theory of PRA, a nodal risk assessment model is proposed to quantize risk factors as:

$$r_i = p_i v_i c_i \tag{9}$$

where r_i is the expect loss when node *i* fail, which represents the risk degree of node *i*. p_i is the probability that node *i* affected by risk factors. v_i is the vulnerability of node *i* calculated via equation (8), which represents the defensive ability of node *i*. c_i is the maximum load-shedding in electricity network when communication node *i* fail, which features the coupling relationship of cyber-physical systems. The calculating method of c_i can be seen in our formal work in [14].

3.3. Optimal configuration model for defensive resources

Due to the coupling characteristic of the cyber-physical system, after communication equipment being damaged, the electricity system will cut load demand because of the cascading failure. Hence, the optimal allocation model for defensive resources is established in this paper to minimize network risk utilizing limited defenders. The risk of man-made attack, communication quality and natural disaster on systems are indicated by different weights. The mathematical model of optimal allocation for defensive resources is as follows:

$$\min R = \sum_{i=1}^{n} p_i v_i c_i = \sum_{i=1}^{n} p_i c_i (1 - \frac{x_i}{\max X_i})^2 \tag{10}$$

$$s.t. \qquad 0 \le x_i \le \max X_i \tag{11}$$

$$\sum_{i=1}^{n} x_i \le B \tag{12}$$

In the objective function, *R* is the risk level of the entire network. *n* is the number of communication nodes. *B* is the maximum available defensive resources on node *i*, which should be limited within $\sum_{i=1}^{n} \max X_i \le B$. The probability p_i of node *i* consider the risk factors including man-made attacks, equipment damages and natural hazards, which are defined as $p^i_{event,ma}$, $p^i_{event,ed}$ and $p^i_{event,nh}$ respectively.

4. Simulation results

4.1. Test system

New England 39-node power network is used as the physical system [6], which can be represented as two topologies of communication network named random topology and binary topology with Pajek. In

Figure 1 which is a random topology of communication network, node 1-39 is corresponding to the same number of node in power network respectively while node 40 is a dispatch center (DC). The information are directly transmitted to CDC. In Figure 2 which is a binary topology communication network, node 1-39 is corresponding to the same number of node in power network respectively and node 40 is a central dispatch center (CDC) while node 41-50 represent the regional dispatch center (RDC) and node 51 is a standby dispatch center (SDC). The information is firstly centralized on RDC and then transmitted to CDC. RDCs are the relay nodes of their regions, for instance, RDC1 is a data collecting point of node 19, 20, 33 and 34.

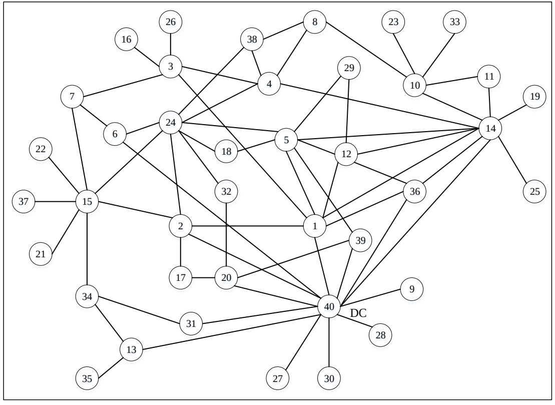

Figure 1. Random topology.

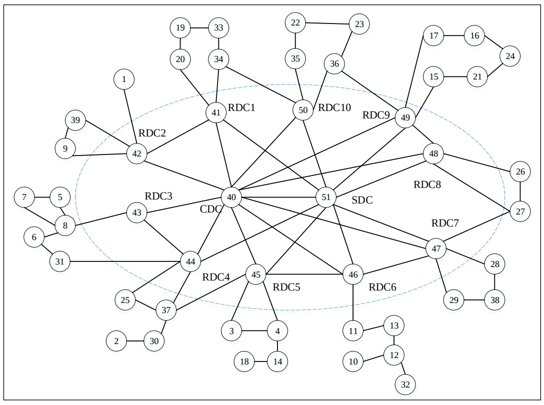

Figure 2. Binary topology.

The number of nodes that need to strengthen the defensive ability are 39 for random topology while that for binary topology are 49. For both network topologies, the maximum defensive resources required for each node to be a best security level are 20 under man-made attacks and equipment damage. When considering natural hazards, two types of communication network are divided into 10 regions and the defensive resources required for each region to achieve the best security level are 60. The total amount of defensive resources are set as B = 200, 300, 400 and 500 in each simulation. The value of B is related to the total number of available network resources in actual projects. In this paper, we make some simple assumptions for B. Besides, it is a non-linear programming problem to find the optimal solution for the model proposed in 3.3, which is solved by the fmincon toolbox in MATLAB.

4.2. *Resource allocation with different risk factors*

The results of defensive resources allocation against man-made attacks in two network topologies are shown in Figure 3 and Figure 4. There are most defensive resources acquired at node 14 in random topology and at node 49 in binary topology because the probability that these nodes will fail under man-made attacks in their topologies are the highest among all nodes, up to 0.05 and 0.04 respectively. Therefore, the higher risk degree of nodes are, the more defenders they will need. With the total amount of defensive resources decreasing, the defensive resources allocated at each node reduce and some of are close to 0.

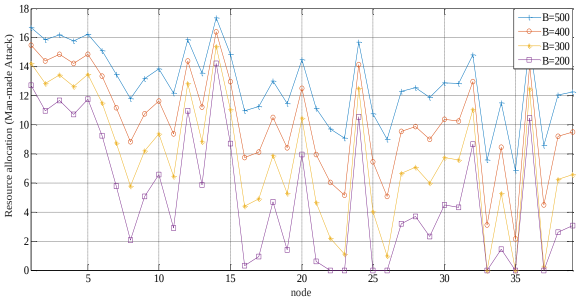

Figure 3. Man-made attack in random topology.

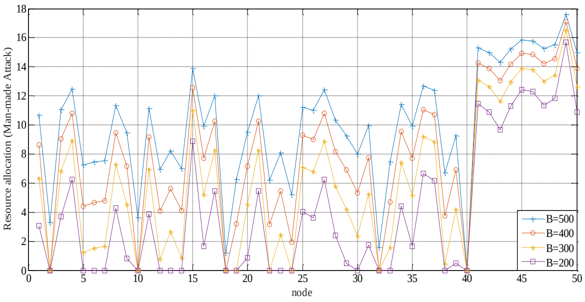

Figure 4. Man-made attack in binary topology.

The risk degree with the factor of equipment damage are determined by the installed time and number of usage of the devices. In Figure 5 and Figure 6, there are some nodes without the requirement of defensive resources no matter how much the total number of the defensive resources are.

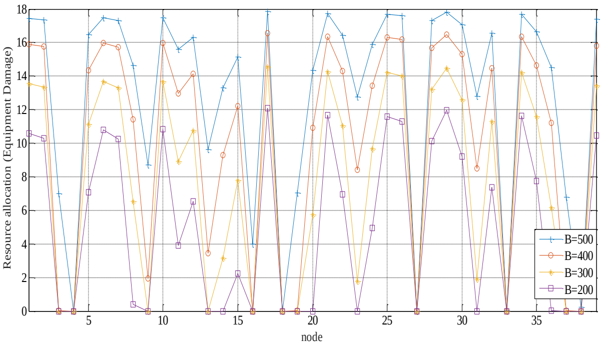

Figure 5. Equipment damage in random topology

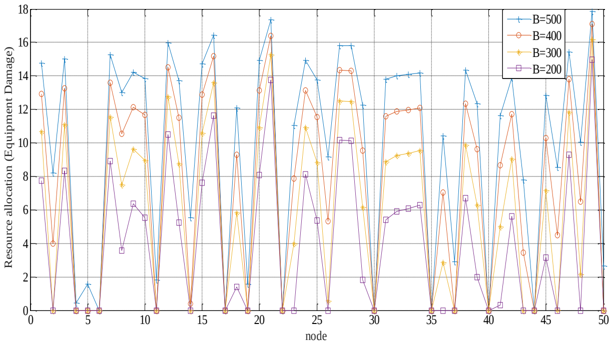

Figure 6. Equipment damage in binary topology.

The results of defensive resources allocation against natural hazards in two network topologies are depicted in Figure 7 and Figure 8. Taking the case of B=500 as an example, region 2 and 9 in random topology and region 4, 5 and 9 in binary topology are allocated more defensive resources, which are more than 50 in two topologies. Therefore, the defensive resources such as lightning, waterproofing, fire prevention should be firstly deployed in these regions. In addition, as the total amount of defense resources decreases, the peak and valley differences of the curve become larger.

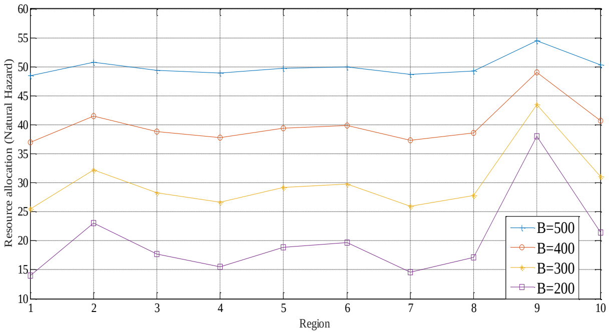

Figure 7. Natural Hazard in random topology.

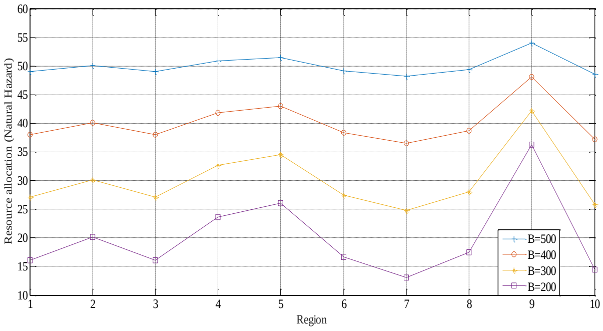

Figure 8. Natural Hazard in binary topology.

5. Conclusions

Firstly, the importance of nodes and the risk degree of nodes against communication network including man-made attack, equipment damage and natural hazards are assessed through the graph theory and probability basis. Secondly, an optimal configuration model for defensive resources is proposed to rationally distribute the defenders in the network and reduce the risk level of the entire cyber-physical network. Finally, simulations results of New England 39-node power network and its corresponding communication networks demonstrate the effectiveness of the modelling.

Acknowledgment

This work was financially supported by Science and Technology Project of State Grid Corporation of China (SGSDDK00KJJS1600061).

References

[1] Liu Z Y 2015 Global energy internet *China Electric Power Press*

[2] Jacobson M Z and Delucchi M A 2011 Providing all global energy with wind, water, and solar power, Part I: Technologies, energy resources, quantities and areas of infrastructure, and materials *Energy Policy* **39** 1154-69

[3] Pastor-Satorras R, Castellano C, Van Mieghem P and Vespignani A 2015 Epidemic processes in complex networks *Reviews of Modern Physics* **87** 925

[4] Jalili M and Perc M 2017 Information cascades in complex networks *Journal of Complex Networks* **5** 665-693

[5] Holme P, Kim B J, Yoon C N and Han S K 2002 Attack vulnerability of complex networks *Physical Review E* **65** 056109

[6] Lü L, Chen D, Ren X L, Zhang Q M, Zhang Y C and Zhou T 2016 Vital nodes identification in complex networks *Physics Reports* **650** 1-63

[7] Buldyrev S V, Parshani R, Paul G, Stanley H E and Havlin S 2010 Catastrophic cascade of failures in interdependent networks *Nature* **464** 1025-28

[8] Schneider C M, Yazdani N, Araújo N A, Havlin S and Herrmann H J 2013 Towards designing robust coupled networks *Scientific Reports* **3** 1969

[9] Behfarnia A and Eslami A 2017 A Error correction coding meets cyber-physical systems: message-passing analysis of self-healing interdependent networks *IEEE Transactions on Communications* **65** 2753-68

[10] Huang Z, Wang C, Nayak A and Stojmenovic I 2015 Small cluster in cyber physical systems: Network topology, interdependence and cascading failures *IEEE Transactions on Parallel and Distributed Systems* **26** 2340-51

[11] Al Mannai W I and Lewis T 2007 Minimizing network risk with application to critical infrastructure protection *Journal of Information Warfare* **6** 52-68

[12] Al Mannai W I and Lewis T G 2008 A general defender-attacker risk model for networks *The Journal of Risk Finance* **9** 244-261

[13] Uwe J 2002 Probabilistic Risk Analysis: Foundations and Methods *Journal of the American Statistical Association* **97** 925

[14] Chu X D, Tang M S, Huang H Y and Zhang L 2017 A security assessment scheme for interdependent cyber-physical power systems *2017 8th IEEE International Conference on Software Engineering and Service Science* 816-819