American Journal of Networks and Communications
2016; 5(5): 115-120
http://www.sciencepublishinggroup.com/j/ajnc
doi: 10.11648/j.ajnc.20160505.15
ISSN: 2326-893X (Print); ISSN: 2326-8964 (Online)

An Improved Routing Method for Electric Power Communication Networks

Fan Bing[1, *], Wang Yujie[2]

[1]State Key Laboratory of Alternate Electrical Power System with Renewable Energy Sources (North China Electric Power University), Beijing, China

[2]School of Electrical & Electronic Engineering, North China Electric Power University, Beijing, China

Email address:

bbqice@163.com (Fan Bing), jessie950415@sina.cn (Wang Yujie)

[*]Corresponding author

To cite this article:

Fan Bing, Wang Yujie. An Improved Routing Method for Electric Power Communication Networks. *American Journal of Networks and Communications.* Vol. 5, No. 5, 2016, pp. 115-120. doi: 10.11648/j.ajnc.20160505.15

Received: September 26, 2016; **Accepted**: October 12, 2016; **Published**: October 19, 2016

Abstract: An improved routing method to reduce the risk of electric power communication networks (EPCN), called low risk routing method (LRRM), is proposed based on the fact that different types of traffic with different service importance levels in EPCN. In order to calculate the vulnerability of EPCN under artificial attacks, deliberate attack and betweenness first attack models are created. Based on the attack models, a routing model considering service importance distribution, edge betweenness distribution and path length is presented. Taking into account both network risk and service delay requirements, optimized routing is calculated using Dijkstra algorithm and chaotic clonal genetic algorithm (CCGA). Under different artificial attacks, the vulnerability of an EPCN applying LRRM and Shortest Path First method (SPFM) are compared by numerical simulation. The results show that LRRM can effectively reduce the network risk.

Keywords: Electric Power Communication Networks, Network Vulnerability, Routing Method, Attack Model, Genetic Algorithm

1. Introduction

Electric power communication networks (EPCN), which is called the central neural system of smart grid [1], is the important support network to guarantee the steady running of smart grid. Research on the reliability, vulnerability and risk of EPCN is of great significance [2, 3].

From different perspectives, network risk is studied based on different metrics. Focusing on the business aspect, a risk-aware design and management of resilient networks is proposed in [4], which measured network risk by Value-of-Risk, the maximum penalty to a single service or a whole network with a given confidence interval, due to SLA violation, and presented five risk mitigation strategies considering different trade-offs between budget for risk mitigation and Value-of-Risk. In addition to considering penalty defined in SLA, literature [5] characterized network risk by the product of the penalty per unit time and the probability of network-element failures caused by disasters, and proposed a heuristic algorithm based on finding shortest paths by transforming the penalty, probability of link failures, and free wavelength number into link cost.

Path availability is also a common network risk metric. In order to find the maximum available path under multiple link failures, a series of algorithms are proposed in [6] based on shared risk link groups (SRLGs), which transforms a link belonging to multiple SRLGs into multiple links each belonging to one SRLG and finds a shortest path covered by a SRLG set with the maximum availability using polynomial algorithms or heuristic algorithms.

Optimizing routing is an effective method to reduce network risk without changing the topology, so the low risk routing problem has been researched by many scholars in different network layers. In the physical layer, a risk-aware routing method in optical mesh networks was proposed [7], which characterizes the quality of a network's optical-layer routing by SLA violation risk instead of statistical path availability and transforms the risk into the failure arrival rate of reference links for calculating the low-risk paths by

Dijkstra algorithm. In the transport layer, a minimum delay routing algorithm in heavy traffic network is presented [8] to balance traffic load on links and minimize network risk. In the network layer, a dynamic risk-aware routing for OSPF resilient networks is proposed in [9], which takes advantage of existing failure prediction technologies to anticipate failures and prompt traffic flow to avoid the failures by assigning a high weight to the links related to these failures. Network availability and routing oscillations using this routing mechanism are estimated based on an analytical model, and the results show that the gain is proportional to the ratio of correctly identified failures to the number of all predictions. All of the above algorithms are studied for common networks other than EPCN. In the electric power communication field, the authors of [10] and [11] studied the service importance of traffic in EPCN and proposed some routing optimization algorithms. In [10], service average risk degree and service risk balancing degree are used as reliability evaluation indexes of NSGA II [12] to optimize routing. In [11], node and link risk degree is computed and the path is selected using min-max strategy. Only equipment natural failures are taken into account in [10] and [11] but artificial attacks are not considered.

Finding a path that considers many risk factors is a multi-constrained routing problem. Genetic algorithms (GA) are widely used in solving the problem but the uncertainty of GA is a defect which leads many authors into using the average of multiple running results to illustrate the superiority of the algorithms [13-16]. However, the uncertainty can't be accepted in the traffic routing of EPCN.

In this paper, network risk under artificial attack is considered. First, two artificial attack modes and the calculation method of network vulnerability are presented. Second, a comprehensive risk routing model is created associated with the attack modes. Then, a hybrid routing method is proposed which considers both network risk and service delay requirements of different types of traffic in EPCN. Last, the performance simulation and analysis of our routing method is given and the results show that the method can improve the EPCN defense ability against artificial attacks and can output a certain optimized routing to reduce network risk.

2. Attack Modes

Assets, threats and vulnerability are the essential elements of security risk, so the research on threat modes and network vulnerability is necessary before studying routing risk. Treat modes include artificial attacks and natural failures, and artificial attacks are considered in this paper.

2.1. Network Vulnerability

The main loss of an EPCN under artificial attacks is the interrupted traffic of which the effect on electrical production is measured by service importance [17]. Service importance can be used to describe the degree of impact on network users due to the interruption of data streams with different service levels in EPCN. For example, a service for a real-time production data stream in EPCN is more important than a service for a non-real-time office data stream. In this paper, the EPCN vulnerability is denoted by the service importance of the lost traffic.

Although the most destructive attack is based on the distribution of different traffic, it is difficult for attackers to capture the accurate traffic distribution information. So attackers usually use network topology information, which is relatively easy to obtain, to destroy a network. Only edge attack is considered in this paper because the failure probability of the nodes in EPCN is very small due to the fact that all the nodes have standby units.

A network is denoted by a triple (G,H,W), where $G=(V,E)$ is the network topology of which V is the node set and E is the undirected edge set, H is the routing method, W is the traffic distribution. The relation between the edge set and the path set is described by the matrix $A=[a_{nm}]_{N\times M}$, where $N=|E|$, $M=\binom{|V|}{2}$ and $|\bullet|$ is the cardinality of a set. In A, the row vectors are related to the edges of E and the column vectors are related to the source-destination node pairs (SDNPs) of the network. When the path between the m-th SDNP include the n-th edge e_n, $a_{nm}=1$ and otherwise $a_{nm}=0$. Let w_m, which is the sum of the service importance of all traffic between the m-th SDNP, be the weight of the mth column vector and the service importance on edge e_n is

$$I(e_n)=\sum_{m=1}^{M} w_m a_{nm} \tag{1}$$

The network vulnerability is defined as

$$V(x)=\frac{\sum_{m=1}^{M} w_m q_m}{\sum_{m=1}^{M} w_m}, \tag{2}$$

where q_m is the m-th element of vector Q and $Q=e_1\vee e_2\vee\cdots\vee e_x$, where e_x is the x-th element of an attacked subset corresponding to an attack mode, sign $\vee$ denotes OR operation.

2.2. Betweenness First Attack Mode

Edge betweenness indicates the number of shortest paths between all node pairs that pass through an edge [18], which is defined as

$$b_e=\sum_{i\neq j\in V}\frac{n_{ij}(e)}{n_{ij}}, e\in E, \tag{3}$$

where $n_{ij}(e)$ denotes the number of the shortest path passing by edge e between node i and node j, and n_{ij} denotes the total number of the shortest path between node i and node j.

The edges with big edge betweenness have higher possibility of carrying much service importance than other edges with small edge betweenness, and these edges with big

edge betweenness will be attacked first. When the edges in E are sorted in descending order according to the betweenness, the attacked subset is constituted by the first x edges to which the row vectors e_1, e_2, ⋯, e_x in A are related. The network vulnerability under betweenness first attack can be computed by Equation 2

2.3. Deliberate Attack Mode

If the attacker captures not only the network topology but also the node property information of a network, the edges in edge subset E_d, which are connected to the provincial dispatching and control center node, are attacked first with high probability because the traffic in EPCNs mostly flow into or out of the provincial dispatching and control center node. If the elements in E_d are sorted in descending order according to $I(e_n)$, where n=1,2,…,N_d, and $N_d = |E_d|$, the attacked subset consists of the first x edges. The network vulnerability under deliberate attack can be computed by Equation 2.

3. Low Risk Routing Method

3.1. Comprehensive Routing Risk Model

3.1.1. Risk Under Betweenness First Attack

The network loss under betweenness first attack is the traffic with different service importance levels, so the risk of edge e_n is defined as

$$R(e_n) = B(e_n) \times I(e_n), \tag{4}$$

where $B(e_n)$ is the betweenness of edge e_n. Equation 4 takes into account the probability of edge e_n being attacked and the loss after edge e_n being attacked. When $B(e_n)$ and $I(e_n)$ are both large, $R(e_n)$ is very large, which means that edge e_n is in favor with attackers and the loss caused by the failure of e_n is much. On the other hand, if $B(e_n)$ is large but $I(e_n)$ is small, $R(e_n)$ will not be very large, which means that although edge e_n is in favor with attackers, the loss caused by the failure of e_n is little. If $B(e_n)$ is small but $I(e_n)$ is large, $R(e_n)$ will not be very large too because the loss caused by the failure of e_n is much but edge e_n is not in favor with attackers.

The network risk under betweenness first attack can be characterized by the distribution of $R(e_n)$. If $R(e_n)$ concentrates upon a few edges, these edges are likely to be attacked and the network loss is so much, but if $R(e_n)$ is uniform on every edge, i.e. an edge either has large $B(e_n)$ and small $I(e_n)$ or has large $I(e_n)$ and small $B(e_n)$, the network risk will be low.

In the information field, for a ε-ary source, the information entropy is given by

$$\theta = -\sum_{j=1}^{\varepsilon} \mu_j \log_2 \mu_j, \ 0 \le \theta \le \log_2 \varepsilon, \tag{5}$$

where $\sum \mu_e = 1$, and when $\mu_j = \frac{1}{\varepsilon}$ the entropy $\theta = \theta_{\max} = \log_2 \varepsilon$ [19]. If μ_j represents a certain distribution or denotes the proportion of the j-th part of an entirety, the more uniform the distribution, the larger the entropy value. This conclusion has been applied to assessing and optimizing portfolio risk [20, 21]. In this paper, this conclusion is used to measure the equilibrium degree of the distribution of $R(e_n)$.

The network risk under betweenness first attack is defined as

$$f_T = 1 - \theta_R, f_T \in (0,1), \tag{6}$$

where

$$\theta_R = \frac{-\sum_{e \in E} (\overline{I(e_n)} \cdot \log_2 \overline{I(e_n)})}{\log_2(|E|)}, \theta_R \in (0,1) \tag{7}$$

and

$$\overline{I(e_n)} = \frac{I(e_n)}{\sum_{i=1}^{N} I(e_i)}. \tag{8}$$

The smaller the f_T, the lower the network risk.

3.1.2. Risk Under Deliberate Attack

Under deliberate attack, if the service importance of all traffic is focused on a few edges in E_d and the edges are attacked, the loss of the network is huge. Therefore, the network risk is determined by the distribution of service importance on the edges in E_d, and the network risk is defined as

$$f_D = \sqrt{\frac{1}{N_d - 1} \sum_{e_n \in E_d} [I'(e_n) - \overline{I'(e_n)}]^2}, f_D \in (0,1), \tag{9}$$

where

$$I'(e_n) = \frac{I(e_n)}{\max_{e_n \in E} I(e_n)}, \tag{10}$$

and

$$\overline{I'(e_n)} = \frac{1}{N_d} \sum_{e_n \in E_d} I'(e_n) \tag{11}$$

The The smaller the f_D, the lower the network risk.

3.1.3. Risk of Path Length

If only the above two attacks are considered, the path calculated by the routing method may be relatively long to minimize the risk. Long path increases the delay and decreases the transmission quality of traffic. The path length of an important traffic should be as short as possible to reduce both the delay and the risk of being attacked. For lowering the network risk, relatively unimportant traffic should bypass the edges with high betweenness value or those carrying many or highly important traffic. Therefore, the more important the traffic is, the shorter the path should be. The risk of path length is defined as

$$f_L = \frac{l(p_0) I_0}{\sum_{b \in B} l(p_b) I_b + l(p_0) I_0}, f_L \in (0,1), \tag{12}$$

where $l(p)$ is the length of path p, B is the set of the existing traffic, I_b and p_b are the importance and the path of traffic b respectively, $b \in B$, I_0 and p_0 are the importance and the path of the new traffic respectively.

The smaller the f_L, the lower the network risk.

3.1.4. Comprehensive Routing Risk

Taking into account the above three risks, the comprehensive routing risk is defined as

$$f = \alpha f_T + \beta f_D + \gamma f_L, \ f \in (0,1), \tag{13}$$

where $\alpha + \beta + \gamma = 1$, and the value of α, β and γ can be distributed according to the network situation or the decision makers.

3.2. Hybrid Routing Method

In order to output a certain optimized result, the path of a new service requirement with minimum comprehensive risk is calculated by CCGA [22]. CCGA is a chaotic clonal genetic algorithm which applies chaotic search into the crossover and mutation operators of traditional GA to accelerate the global convergence and ensure the stability of the optimizing process and results. The detail procedure of CCGA is presented in [22], so we don't repeat here.

Some traffic in EPCN is very important to electric power system and the service requirements of the traffic are very sensitive to time delay, so the paths of these service requirements can't be computed by CCGA. In order to meet both time delay and network risk requirements, a hybrid routing method called LRRM is proposed. This method first computes the paths of those delay-sensitive service requirements of very important traffic by Dijkstra algorithm, and then computes other paths by CCGA looking the traffic assigned paths as the network background traffic. In CCGA, Equation 13 is the fitness function.

4. Simulation and Analysis

4.1. Background and Parameters

The background network is described by a triple (G,H,W), where G=(V,E) is the network topology (shown in Figure 1) with 14 nodes and 16 edges, H is the routing method including two cases—LRRM and SPFM, W is the traffic distribution.

This network is derived from a real provincial backbone network, where node 1 is the provincial dispatching and control center node, node 2, node5 and node 7 are sink nodes, the numbers on the edges denote the distance between nodes.

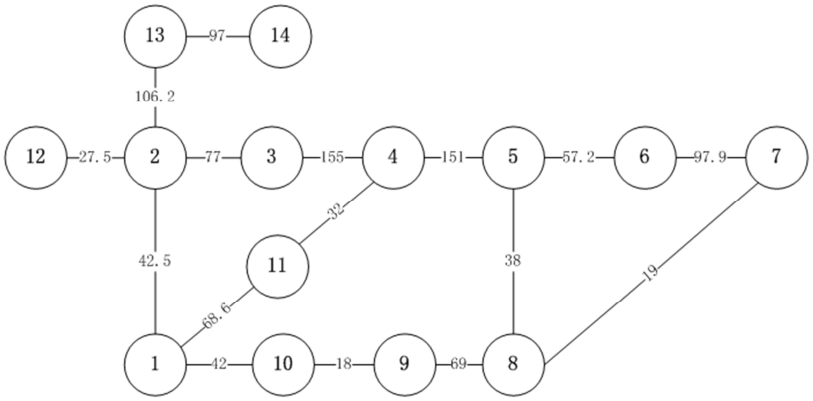

Figure 1. *Topology of an electric power communication network.*

Referring to [17], there are 5 types of traffic, whose service importance value vector is (0.99,0.94,0.62,0.29,0.13), in the network, and the traffic distribution is shown in Table 1.

Table 1. *Traffic distribution in network.*

SDNP	type×number	Normalized w_m
(1,2)	II×5+III×20+IV×5+V×10	0.117
(1,3)	II×3+III×12+IV×3+V×6	0.070
(1,4)	II×2+III×8+IV×2+V×4	0.047
(1,5)	II×5+III×20+IV×5+V×10	0.117
(1,6)	II×2+III×8+IV×2+V×4	0.047
(1,7)	II×6+III×24+IV×6+V×12	0.140
(1,8)	II×3+III×12+IV×3+V×6	0.070
(1,9)	II×2+III×8+IV×2+V×4	0.047
(1,10)	II×2+III×8+IV×2+V×4	0.047
(1,11)	II×2+III×8+IV×2+V×4	0.047
(1,12)	II×3+III×4+IV×1+V×2	0.035
(1,13)	II×4+III×8+IV×6+V×5	0.066
(2,3),(2,12),(3,4),(4,5), (4,11),(5,6),(5,8),(6,7), (7,8),(8,9),(9,10)	I×1+V×2	0.007
(13,14)	II×3+III×12+IV×3+V×6	0.070

In LRRM, the paths of class I and II traffic are calculated by Dijkstra algorithm first, and the paths of class III to V traffic are calculated by CCGA. The parameters of CCGA are assigned as follows: the population size N=10, the iterations G=5, the elite proportional coefficient λ=0.2, the crossover proportional coefficient μ=0.6, the chaotic equation is Logistic one [23], and the fitness function is Equation 13 where $a=\beta=\gamma=1/3$, which means that the weights of the three types of network risk mentioned in the comprehensive routing risk model is equal to each other.

In LRRM, the paths of class I and II traffic are calculated by Dijkstra algorithm first, and the paths of class III to V traffic are calculated by CCGA. The parameters of CCGA are assigned as follows: the population size N=10, the iterations G=5, the elite proportional coefficient λ=0.2, the crossover proportional coefficient μ=0.6, the chaotic equation is Logistic one [23], and the fitness function is Equation 13 where $a=\beta=\gamma=1/3$, which means that the weights of the three types of network risk mentioned in the comprehensive routing risk model is equal to each other.

4.2. Simulation Results and Analysis

The vulnerability curves of the network under betweenness first attack are shown in Figure 2, where bottom axis x denotes the number of attacked edges, left axis $V(x)$ denotes the network vulnerability when x edges are attacked. When x=1 (the edge with the biggest betweenness is attacked), the two curves overlap, but when x=2, the network vulnerability corresponding to SPFM rises rapidly to 75.53% from 28.77%, while the network vulnerability corresponding to LRRM only rises to 66.77%. From x=3 to x=5, the vulnerability of LRRM is about 9% lower than the vulnerability of SPFM. In EPCN, the edge with the biggest betweenness may not carry the most service importance because most traffic is centralized rather than randomly distributed. Therefore, although the two curves overlap at x=1, the vulnerability of LRRM is lower than the vulnerability of SPFM from x=2. When x=7, the tow curves overlap again because most of the services are interrupted and $V(x)$=87.25%, which means there is no space and no significance to optimize the network.

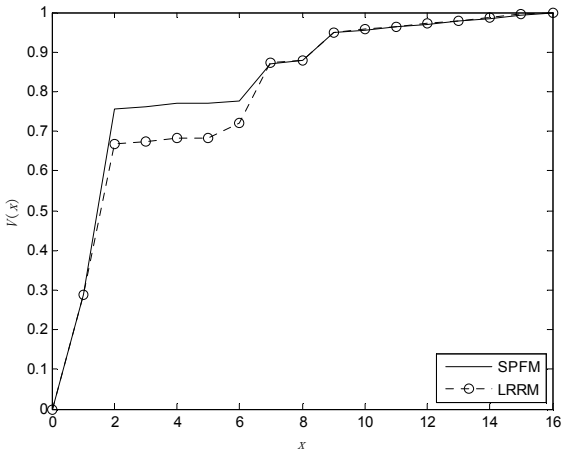

Figure 2. *The network vulnerability under betweenness first attack.*

The vulnerability curves under deliberate attack are shown in Figure 3. In the network, there are three edges in set E_d. When x=1, the vulnerability $V(x)$ of SPFM is 46.76%, while the vulnerability of LRRM only is 38%. When x=2, the vulnerability $V(x)$ of SPFM and LRRM are 75.53% and 66.77% respectively, which shows LRRM is significantly superior to SPFM.

In the comprehensive routing model, the risk of path length f_L is proposed to shorten service paths and improve the network performance of defending random attack. In order to observe the network vulnerability under random attack (one random edge will be removed in one attack), we obtained the vulnerability curves after 50 times of simulation as shown in Figure 4. The fluctuation range, mean value and standard deviation of the curve of LRRM is [0.6%, 34.06%], 0.137 and 0.104 respectively, while the fluctuation range, mean value and standard deviation of the curve of SPFM is [0.7%, 46.76%], 0.146 and 0.164 respectively, which shows that the performance of defending random attack of LRRM is superior to SPFM.

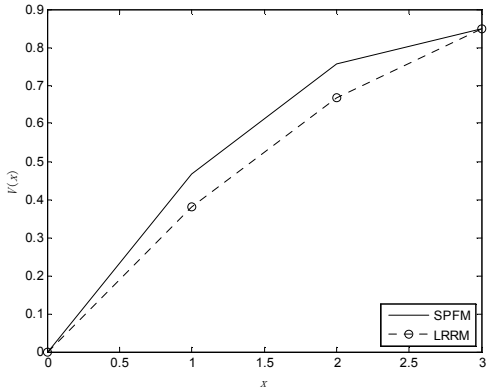

Figure 3. *The network vulnerability under deliberate attack.*

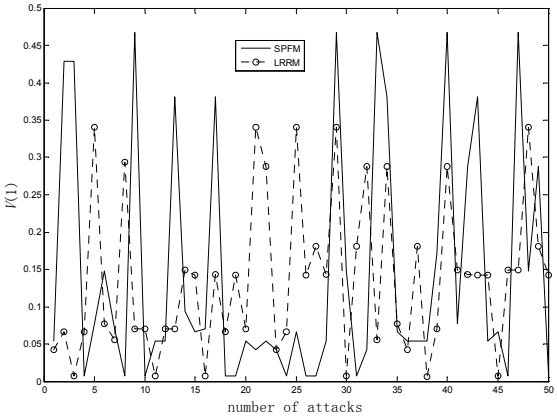

Figure 4. *The network vulnerability V(1) when random one edge is attacked.*

5. Conclusion

Considering the three basic risk factors of asset, threat and vulnerability, a comprehensive routing risk model for electric power communication networks is created. The model takes

into account artificial network attack modes, service importance distribution on network edges, and delay requirements of traffic. After that, a low risk routing method called LRRM is proposed, which first computes the paths of delay-sensitive services using Dijkstra algorithm and then computes other paths using the comprehensive routing risk model and CCGA. The LRRM can minimize the network comprehensive risk and meet the delay requirements of those very important services in electric power communication networks. CCGA can insure the determinacy of the output of LRRM due to the introduction of chaotic research instead of stochastic strategies based on probability in traditional GA. Compared with Shortest Path First method, the simulation results show the superiority of LRRM under betweenness first attack, deliberate attack and random attack modes.

Acknowledgements

This work is supported by the National Natural Science Foundation of China (Grant No. 51677065)， the National High Technology Research and Development Program of China (Grant No. 2014AA01A701), Beijing Natural Science Foundation of China (Grant No. 4142049), and the Fundamental Research Funds for the Central Universities of China (Grant No.2016MS05).

References

[1] X. Deng, X. Wang and X. Chen et al., "Reliability of power telecom network based on the efficient energy model," Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), vol. 24(3), 2012, pp. 378–382.

[2] C. H. Hauser, D. E. Bakken and A. Bose, "A failure to communicatepp. next generation communication requirements, technologies, and architecture for the electric power grid," IEEE Power & Energy Magazine, vol. 3(2), 2005, pp. 47–55.

[3] X. Zhaoxia, G. Manimaran and V. Vittal, "An information architecture for future power systems and its reliability analysis," IEEE Transactions on Power Systems, vol. 17(3), 2002, pp. 857–863.

[4] P. Chołda, "Risk-aware design and management of resilient networks," The 9th International Conference on Availability, Reliability and Security (ARES), pp. 468–475, September, 2014.

[5] F. Dikbiyik, M. Tornatore and B. Mukherjee, "Minimizing the risk from disaster failures in optical backbone networks," Journal of Lightwave Technology, vol. 32(18), 2014, pp. 3175–3183.

[6] S. Yuan and B. Wang, "Highly available path routing in mesh networks under multiple link failures," IEEE Transactions on Reliability, vol. 60(4), 2011, pp. 823–832.

[7] X. Ming, M. Tornatore and C. U. Martel et al., "Risk–aware provisioning for optical WDM mesh networks," IEEE/ACM Transactions on Networking, vol. 19(3), 2011, pp. 921–931.

[8] S. W. Jeon, K. Jung and H. Chang, "Fully distributed algorithms for minimum delay routing under heavy traffic," IEEE Transactions on Mobile Computing, vol. 13(5), 2014, pp. 1048–1060.

[9] B. Vidalenc, L. Noirie and L. Ciavaglia et al., "Dynamic risk–aware routing for OSFP networks," The 13th IFIP/IEEE International Symposium on Integrated Network Management (IM2013), pp. 226–234, May, 2013.

[10] W. Cai, H. Yang, and F. Xiong et al., "An optimized service routing allocation method for electric power communication network considering reliability," Power System Technology, vol. 37(12), 2013, pp. 3541–3545.

[11] Q. Zeng, X. Qiu, and S. Guo et al., "Risk balancing based routing mechanism for power communications service," Journal of Electronics & Information Technology, vol. 35(6), 2013, pp. 1318–1324.

[12] K. Deb, A. Pratap and S. Agarwal et al., "A fast and elitist multiobjective genetic algorithm: NSGA–II," IEEE Transactions on Evolutionary Computation, vol. 6(2), 2002, pp. 182–197.

[13] P. Wright, M. C. Parker and A. Lord, "Minimum- and maximum-entropy routing and spectrum assignment for flexgrid elastic optical networking," IEEE/OSA Journal of Optical Communications and Networking, vol. 7(1), 2015, pp. A66–A72.

[14] S. C. Huang, M. K. Jiau and C. H. Lin, "Optimization of the carpool service problem via a fuzzy-controlled genetic algorithm," IEEE Transactions on Fuzzy Systems, vol. 23(5), 2015, pp. 1698–1712.

[15] Z. Cai, L. Zheng, and S. Zhu, "Chaotic immune optimization based resource allocation in cognitive radio network," Acta Phys. Sin., vol. 61(11), 2012, pp. 118801.

[16] H. Yetgin, K. T. K. Cheung, L. Hanzo, "Multi–objective routing optimization using evolutionary algorithms," 2012 IEEE Wireless Communications and Networking Conference (WCNC), pp. 3030–3034, April, 2012.

[17] B. Fan, L. Tang, "Vulnerability analysis of power communication network," Proceedings of CSEE, vol. 34(7), 2014, pp. 1191–1197.

[18] M. Igor, B. Mario and K. Ljupco, "Vulnerability of complex networks," Communications in Nonlinear Science and Numerical Simulation, vol. 16, 2011, pp. 341–349.

[19] L. Hanzo, R. Maunder and J. Wang et al., "Near-capacity variable-length coding: regular and exit-chart-aided irregular designs," Wiley-IEEE Press, 2011, pp. 36–37.

[20] J. Ou, "Theory of portfolio and risk based on incremental entropy," The Journal of Risk Finance, vol. 6(1), 2005, pp. 31–39.

[21] Y. Jiang, S. He and X. Li, "A maximum entropy model for large-scale portfolio optimization," International Conference on Risk Management & Engineering Management 2008, pp. 610–615, Nov, 2008.

[22] B. Fan, Y. Zeng and L. Tang, "Chaotic clonal genetic algorithm for routing optimization," Advanced Materials Research, vol. 1046, 2014, pp. 371–374.

[23] S. Fang, E. Zou and J. Xin et al., "New chaos genetic algorithm applied in multi–constrained QoS routing," Application Research of Computers, vol. 29(8), 2012, pp. 3078–3080.