2015 5th International Conference on Information Science and Technology (ICIST)
April 24–26, 2015, Changsha, Hunan, China

# Vulnerability Analysis of Smart Grid Based on Complex Network Theory

Xisong Dong, Timo R. Nyberg, Pekka Hämäläinen, Gang Xiong, Yuan Liu, and Jiachen Hou

*Abstract*—**Smart grid has been widely acknowledged around the world. The rapid development of complex network theory provides a new perception into the research of smart grid. Based on the latest progress in the field of complex network theory, smart grid can be treated as small world networks. This paper examines the tolerance of smart grid against attacks to analyze its vulnerability, and proposes a technique to study the relationship between the electric betweenness and the reliability of smart grid. Based on these researches, the specific concept of vulnerability investigation to indicate smart grid is clarified. Furthermore, the proposed method will be investigated by an IEEE test system in contrast with the result from actual concept in power grid to indicate its effectiveness.**

## I. Introduction

The electrical grid stands tall as a marvel of the centuries, with high level of reliability and the capability to deliver omnipresent electricity to the world. The grid is a highly complex network with millions miles lines; and any damage will cause serious problems, so the vulnerability topic concerning this grid would be a critical research topic. Accompanying with the Smart Grid Dynasty, a focal point for this topic will be highly discussed. [1]

This topic has anyhow brought some interesting new challenges in the power arena: As facilities around the world have updated major power grid infrastructure over the past several years, grid protection has become a critical priority. Power securities are designed to protect the electrical grid from attacks by internal and external threaten, as well as strengthening its resilience against inadvertent threats such as equipment failures and user errors. The frequent occurrence damages have attached researchers both in the fields of engineering and science. Finding the intrinsic component of the vulnerability as well as the way to prevent them has become the very point of representational basic requirements and brought practical meanings. [2]

In recent years, the complex network theory is increasingly being exploited to tackle some sorts of complex issues, which presents a new point of view which is profitable for us to investigate the complexity of smart grid. For an extensive review on complex networks we refer to, specimens of utilization include infrastructures for electricity generation, transmission and distribution, water supply, transportation systems, financial and security services. The most applications of complex network concepts to power systems are aimed at understanding the behavior of power grids both in case of accidental failures and of malicious attacks. [3] However, the study of failures from the nodes of topological view is equally important as finding a way to assess the vulnerability of the network. Particularly, the small-world effects have been found in the actual power grid; [4] however, how the small-world effects will promote the smart grid's development have not been specially studied yet. [5]

This paper aims at the relationship between small-world effects and a feasible research method for smart grid, in which the characteristics of complex networks and small-world networks are reexamined, the smart grid is analyzed, and the vulnerability of the smart grid is studied. The rest of its context is organized as follows: Section II introduces the smart grid. Section III presents the reexamination of complex network and small-world networks as well. Section IV implements the electric betweenness and vulnerability assessment on the smart grid model. Conclusions are drawn in Section V.

## II. Smart Grid

Smart Grid is basically overlaying the physical power system with an information system which links a variety of equipments and assets together with sensors to form a service platform. It allows the utility and consumers to monitor and adjust electricity use. The management of operation will be more intelligent and scientific. In comparison with traditional grid, smart grid includes integrated communication systems, advanced sensing, metering, measurement infrastructure, complete decision support and human interfaces. [6] The different between smart grid and today's power grid can be seen from the figure 1. From the figure, we can see the smart grid is more complex than existing grid. And smart grid has more users and multi-forms generators. Resources and services that were separately managed will be integrated and re-bundled to address traditional problems in new ways;

This work was supported in part by the Natural Science Foundation of China (61233001, 71232006); Finnish TEKES's project "SoMa2020: Social Manufacturing" (2015-2017); and Chinese Nanjing's Talents Project (Gang Xiong).

X. S. Dong is with the Key Laboratory of Complex System Intelligent Science, Institute of Automation, Chinese Academy of Sciences, Beijing, 100190, CHINA (e-mail: xisong.dong@ia.ac.cn).

T. R. Nyberg is with the Department of Industrial Engineering and Management, Aalto University, FI-00076 Aalto, FINLAND (e-mail: timo.nyberg@aalto.fi).

P. Hämäläinen is with the Tekla Corporations, Metsänpojankuja, FI-02130 Espoo, FINLAND (e-mail: Pekka.Hamalainen@tekla.com).

G. Xiong is with the Cloud Computing Center, Chinese Academy of Sciences, Dongguan, CHINA (corresponding author to provide phone: +861082544787; e-mail: gang.xiong@ casc.ac.cn).

Y. Liu is with the Nanjing Smart Energy Information Technology Co., LTD. Nanjing, CHINA (e-mail: liuyuan@casc.ac.cn).

J. C. Hou is with the Beijing Engineering Research Center of Intelligent Systems and Technology, Institute of Automation, Chinese Academy of Sciences, Beijing, 100190, CHINA (e-mail: hou.jiachen@gmail.com).

978-1-4799-7489-4/15/$31.00 ©2015 IEEE

adapt the system to tackle new challenges; and discover new benefits that have transmission potential. Smart Grid is a major upgrade to the existing utility system with a more complex configuration that includes power parks, new technologies, and other associated information networks.

In spite of the smart grid has some intelligent advantages which will make up traditional grid's some vulnerability problems; but the grid's structure will be more sophisticated and variable, the grid will face more damages and attacks, the grid's vulnerability risks will be still exist even increasing.

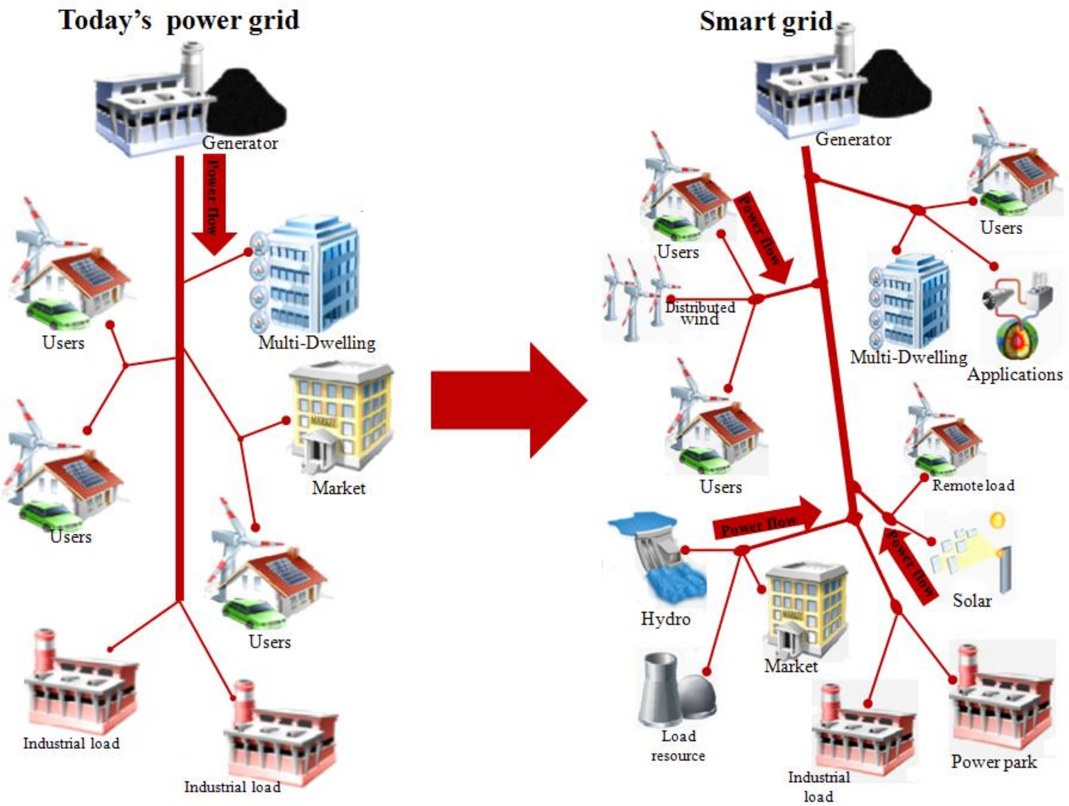

Figure 1 Smart Grid Change From the Existing Power Grid

The drivers for Smart Grid's security research can be concluded into circumstances, safety and power quality. There still remain challenges that how to improve the efficiency of power grid's construction; how to ensure the security and reliability of power grid's operation; how to decrease the vulnerability risks; how to improve the power grid management. [7]

## I. Complex Network Theory

Recent researches have presented a point of view that the structures of power grid are in frames of complex systems and small-world networks. Based on the complex network theory, the models of components in the smart grid are illustrated in this section. How the complex network theory promotes the smart grid's development is worth following up.

### *A. Topology Parameters*

For a universal graph G with n nodes and *k* links, the characteristic parameters of this graph are as follows:

The characteristic path length *L* is defined as the average over the network of the minimum path length between two nodes, given by:

$$L = \frac{1}{N(N-1)} \sum_{i,j\in G, i\neq j} d_{ij..} \qquad (1)$$

The shortest path length $d_{ij}$ is defined as the number of edges along the shortest path between node *i* and *j*.

(1) The clustering coefficient *C* gives a measure of the average closeness between nodes in G. It is defined as:

$$C = \frac{1}{N} \sum_{i\in G} C_i$$

(2)

Where

$$L = \frac{\text{number of edges in } G_i}{k_i(k_i-1)/2} \qquad (3)$$

$k_i$ is the number of neighboring nodes of node $i$, $k_i(k_i-1)$ is the possible maximum links among node i and its neighboring nodes, $C_i$ is the ratio between the number of links and the possible maximum links in the sub graph $G_i$.

(2) Line betweenness $B_L$ is defined as the times of being

passed through by the shortest paths between nodes in G.

(3) Giant component size $S$ is defined as the number of nodes in the biggest connected sub graph. [8]

### B. Complex Network Models

Most of the complex systems in the world can be described in the form of complex networks. At the primary stage of complex network research, the connection topology was assumed to be completely regular, but regular net model is not sufficient to describe the networks in the real world. In 1959, Erdōs and Rényi put forward the concept of random network that greatly promoted the network research. [9] Watts and Strogatz proposed the Small-World network model in 1998. [10] In 1999, Barabási and Albert revealed the Scale-Free characteristic. [11] These advances overcome the shortage of random networks and revealed many characteristics of complex networks.

### C. The Impact of Remote Connection On Small World Network

Primary research has proposed that some smart grids have the characteristic of small world network, i.e. having relative big clustering coefficient and relative small characteristic length path. WS model uses random rewiring procedure, as shown in Figure 2, to generate small world network. [12] This paper presents a regular ring lattice that has 20 nodes; each connects to its four nearest neighbors. Take *P* as the ratio of random rewiring lines number versus all lines amount. Then for *0=P* the original ring is unchanged; as *P* increases the network becomes increasingly disordered until for *1=P* all lines are rewired randomly. The small world phenomenon exists in intermediate region *0<P<1*. From the angle of the formation mechanism of small world network, the rewiring procedure brings in a few remote connections that greatly decrease the characteristic path length. The existence of some remote connections makes the grid system keep a relative small electric distance between generator nodes and load nodes. The breakdown of those remote connections will increase the characteristic path length, decrease the transfer capacity of smart grid, cause partial power shortage and ultimately destroy the power system stability. As a result these remote connections have important influence on power system stability. If we can identify these remote connections, then the vulnerable lines in the smart grids can be identified. [13]

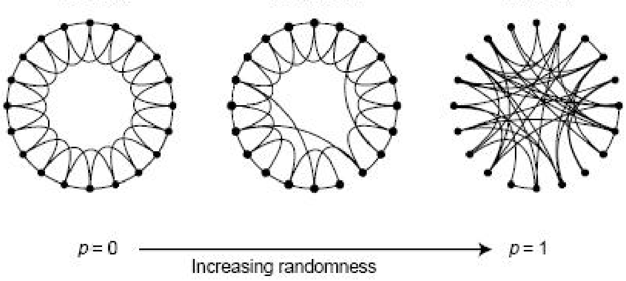

Figure 2 Small World Network (from Ref. [13])

### D. Electric Betweeness

Electric betweenness is illustrated in the following formula ：

$$eBt(m,n)=\sum_{i\in G,j\in L}\sqrt{W_iW_j}\left|I^y(m,n)\right| \tag{4}$$

Where $eBt(m,n)$ is electric betweenness of Line $(m,n)$ ; $(i,j)$ is for a “plant-load” pairs; $W_i$ and $W_j$ are weighted coefficients of generator $i$ and load $j$ ; $G$ and $L$ are sets of generators and loads, respectively.

Electric betweenness makes a quantification of the used-ratio of each line by each “plant-load” pair in the power system effectively with consideration of different generation capabilities and operating modes; the contribution of each line for power transmitting. As based on electric equations, it is more reasonable for power system than weighted betweenness based on the shortest path.

In order to reduce the amount of calculation, the formula could be simplified. Setting a system of $N+1$ node and defining the last node as reference node. Then the deflation admittance matrix is $Y(N*N)$ . Given the additive unit between node $i$ and reference nodes in pouring current element $e^i$ . The electric current of circuit branch $(m,n)$ is showing below.

$$I^y(m,n)=(U^i(m)-U^j(n))y_{mn} \tag{5}$$

Where $U^i$ the vector quantity is composed by voltage of each node, viz, contented $YU^i=e^i$Y. $U^i(m)$ and $U^j(n)$ are the components in node $m$ and $n$ . $y_{mn}$ is admittance of circuit branch $(m,n)$ . According to the electric theory, $U^{ij}=U^i-U^j$ .The current on line $(m,n)$ caused by $e^{ij}$ is just a linear summation of both the currents caused by $e^i$ and $e^j$ respectively, which can improve the calculation efficiency in the formula much obviously. Videlicet, we can get the formula $e^{ij}=e^i-e^i$ . In the mean time, according to the linear circuit’s additives, it can also be gotten:

$$I^{ij}(m,n)=I^i(m,n)-I^j(m,n) \tag{6}$$

Thus, we can get electric betweenness. [14]

## II. Case Studies of Vulnerability Identification of Smart Grid

In this section, the reliability of the smart grid is assessed by identifying its vulnerability suffer random failures and targeted attacks to its high betweenness nodes.

### A. Chain Attack Based On Electric Betweenness

In order to test the electric betweenness’s status in power system, three different attack modes were used to launch chain attack. To prove high betweenness circuits suffer attacks is very fragile. The modes are shown below:

*1) Static attacks*

Range the circuit by level of electric betweenness, letting every line failures in big to small sequence.

*2) Dynamic attacks*

Similar to static attack, but recalculate the rest of circuit's betweenness after each attacks.

*3) Random attacks*

Initially, the network is subject to random attacks where the links are removed randomly. A total of ten such links are removed one after the other and the efficiency of the network is calculated after every attack. It is expected that the system will be robust to such attacks. [15]

Suppose inactive circuit no longer recovered after each attack, and recalculate immediately system variety of connectedness level and maximum power transfer capability after end. To analyze the affection of inactive circuit affect the system. In large-scale power grid, net topology change minuteness each time, we can use compensation method to heighten the effect.

### *B. Case Studies*

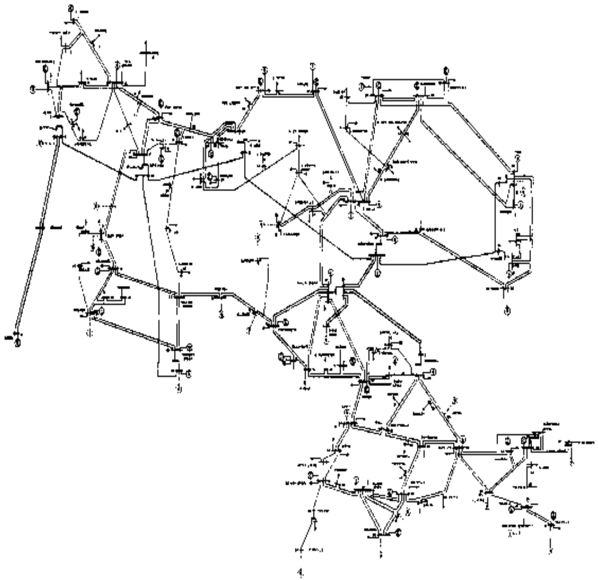

Figure 3 The Figure of IEEE 118 Bus System

Examples are shown using the IEEE 118-Bus test system (54-generator, 186-line and 91-load) obtained from the website contain static network, generation, and load parameters. [16]

The experiment has been developed and studied by the use of *Matlab*. Typical dynamic parameters were used where required for dynamic generator and load models.

Step-by-step can be summarized as follows：

*a) Read relevant input data.*

*b) Establish the power system model with Simulink in Matlab and generate a connection adjacency matrix.*

*c) Calculate topology parameters equations (1)-(3).*

*d) Calculate circuit branch with equations (4)-(5).*

*e) Compute electric betweenness with equation (6).*

*f) Calculate the shortest electric path according to conjunction.*

*g) Find out the shortest electric path.*

*h) Use step d to process the shortest electric path to get the line betweenness of each line.*

*i) Revise line betweenness and sort the betweenness list.*

*j) Calculate the line betweenness based on the new betweenness index.*

*k) Classify the lines with high betweenness as the vulnerable lines.*

*l) Calculate and compare the efficiency of the network for different types of attacks to verify the results.*

The IEEE 118 bus system is modeled with the above principles and a graph with 118 nodes. The vulnerable lines in IEEE 118 bus system are attacked by the above method. Those lines with betweenness weight higher than 15000 is classified as vulnerable lines and 51 vulnerable lines are found. The betweenness weight of the top vulnerable lines is listed in Table.

TABLE I.

VULNERABLE LINES FOR IEEE 118 BUS SYSTEM

| Line No. | Betweenness weight | Vulnerable rank |
|---|---|---|
| $L_{64-65}$ | 31200 | 1 |
| $L_{38-65}$ | 27300 | 2 |
| $L_{30-38}$ | 22340 | 3 |
| $L_{68-81}$ | 18640 | 4 |
| $L_{80-81}$ | 16510 | 5 |

If a generator is out of step, except those directly connected to the breaking point, this line is considered vulnerable. By online verification field simulation time, 5 out of 51 lines have been certified as the most vulnerable lines, all lines with betweenness weight lower than 15000 are verified as strong lines.

The result is shown in Table I, in which represents the top vulnerable lines in the whole system. From the result, $L_{64-65}$ with high betweenness weight is the most vulnerable part in the system, once it down, this part will cause the whole system chain reaction damaged.

The common feature is that these lines are all at risk in the corridor. The results have been verified by calculating the sensitivity of the network to random and dynamic and static attacks. In figure 4, the blue line means random attacks. The green line represents static attacks. The red line expresses dynamic attacks.

It should be noted that the system is very robust against random attacks. Considering that, under dynamic and static attacks, where lines are removed with a high betweenness weight, the performance of the network decreases drastically to about 20% and 40% after the attacks on the 118 bus IEEE systems respectively. If the identification of vulnerable lines, not only lines in the load, but also the location of the grid lines must all be considered.

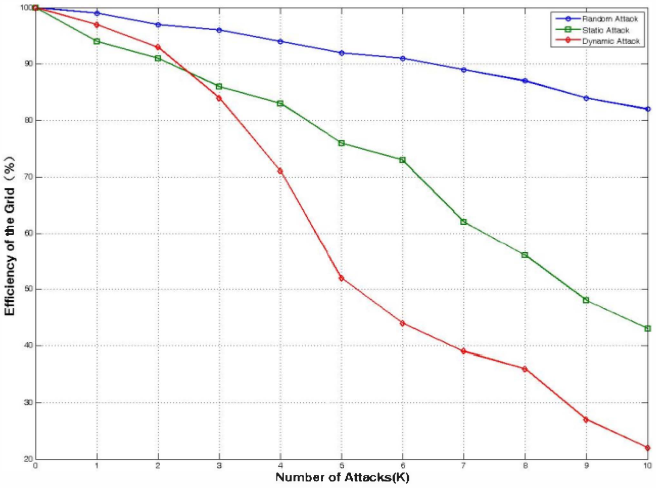

Figure 4 The Effect of Attacks on the Efficiency of IEEE 118 Bus System

The above results demonstrate the smart grid's vulnerability under attacks concerning two elements:

*1) Node type*

On the one hand, contact nodes with high betweenness ensure the grid's connectedness; on the other hand, add fuel to the fire of fault's spread. Smart grid's fault scope can extend terrifically owing to these nodes and cause the grid's breakdown at last.

*2) Structural property*

In small-world network, long range contact is majority shortest paths' only way to pass through. When the node with highest betweenness under attack, the long range will be damaged causing chain reaction, result in redistribution of the shortest paths and setback of the grid's negotiability.

In brief, when the nodes suffer strongest calculated attack, the small-world network will resist worse destruction than random attack's damage. In order to update the whole grid's reliability, especially the grid with small-world characteristic, must strengthen nodes' protection and safeguard which closely associates to network structure. As a result, get avoid of these nodes' fault chain reactions and decrease massive chain reactions' occur probability.

According to the topological properties of the smart grid, the characteristics of small world networks will be much higher and safer. Since the nodes with the highest degree are not necessarily the nodes with the highest betweenness, the influence of these failures in the reliability of the smart grid is smaller than nodes with highest betweenness. Grid's topology structures have important influence to the networks' vulnerability; high betweenness paths and high betweenness nodes have important influence to the system's vulnerability, but relatively high betweenness node is more important. Therefore, in order to increase the whole gird's reliability, the key parts especially high betweenness nodes must be enhanced to avoid these parts' fault chain reaction, and then decrease massive accidents occurrence probability.

## III. CONCLUSION

Based on the latest progress in the field of complex network, electric betweenness weight is proposed as vulnerability weight in this paper. The simulation results verify that the electric betweenness can be used to identify the most vulnerable lines, and also can understand the critical lines due to its special position in the network. A more detailed analysis will achieve better results. Further investigation of the network must strive to improve performance and weaknesses of the system. This idea can also be extended to other domains of smart grid research.

## REFERENCES

[1] The Department of Energy, "What the smart grid means to you and the people you serve," 2009.

[2] M Rahnamay-Naeini, Z Y Wang, N Ghani, A Mammoli, M M Hayat. Stochastic Analysis of Cascading-Failure Dynamics in Power Grids, IEEE Transactions on Power Systems, 2014, 29(6): 1767- 1779.

[3] Y F Guo, R Duan, J Cao, S Li, Power Grid Vulnerability Identifying Based on Complex Network Theory, 2nd International Conference on Instrumentation, Measurement, Computer, Communication and Control, 2012: 474- 477

[4] L Fu, W J Huang, S Xiao, Y Li, S F Guo, Vulnerability Assessment for Power Grid Based on Small-world Topological Model, Asia-Pacific Power and Energy Engineering Conference, 2010: 1-4.

[5] J S A Carneiro, L Ferrarini. Reliability Analysis of Power System Based on Generalized Stochastic Petri Nets, 10th International Conference on Probabilistic Methods Applied to Power Systems, 2008: 1- 6.

[6] Y X Yu, Technical Composition of Smart Grid and its Implementation Sequence, Southern Power System Technology, 2009, Page(s): 1-5

[7] J J Lu, D Xie, Q Ai, Research on smart grid in China, Transmission & Distribution Conference & Exposition: Asia and Pacific, 2009: 1-4.

[8] X Zhu, W M Zhang, B Yu, W G Gong, Identification of vulnerable lines in power grid based on complex network theory, International Conference on Mechatronic Science, Electric Engineering and Computer, 2011: 118- 121.

[9] P Erdos, A Renyi, On the evolution of random graphs , Publications of the Mathematical Institute of the Hungarian Academy of Sciences, 1960,5: 17-61.

[10] D J Watts, S H Strogatz, Collective dynamics of 'small-world' networks, Nature, 1998: 440-442.

[11] A L Barabási, R Albert, Emergence of scaling in random networks, Science, 1999, 286(5439): 509-12

[12] C X Liu, Q Xu, Z Chen, C LBak, Vulnerability evaluation of power system integrated with large-scale distributed generation based on complex network theory, 47th International Universities Power Engineering Conference, 2012: 1- 5

[13] D J Watts, Small Worlds: The Dynamics of Networks between Order and Randomness, Princeton University Press, 1999, pp.11-40.

[14] L Xu, X L Wang, X F Wang, Equivalent Admittance Small-World Model for Power System II. Electric Betweenness and Vulnerable Line Identification, Power and Energy Engineering Conference, 2009, pp.1-4.

[15] S Z Xu, H Zhou, C X Li, X M Yang, Vulnerability Assessment of Power Grid Based on Complex Network Theory, Asia-Pacific Power and Energy Engineering Conference, 2009: 1- 4

[16] http://www.ee.washington.edu/research/pstca/pf118/pg_tca118bus.htm