Electric Grid Vulnerability Assessment under Attack-Defense Scenario Based on Game Theory

Zhou Jian, Libao Shi
National Key Laboratory of Power System in Shenzhen,
Graduate School at Shenzhen
Tsinghua University, Shenzhen, China
shilb@sz.tsinghua.edu.cn

Liangzhong Yao
China Electric Power Research Institute
Beijing 100192, China
yaoliangzhong@epri.sgcc.com.cn

Bazargan Masoud
ALSTOM Grid Research &Technology Centre
Stafford, ST17 4LX, United Kingdom

***Abstract*—In recent years, how to effectively assess the electric grid vulnerability in protecting against a malicious attack becomes one of the most challenging cutting-edge issues to be solved in power systems. This paper presents a framework to analyze the vulnerability of electric grid under different attack-defense scenarios based on the knowledge of game theory. Pure strategy and mixed strategy Nash Equilibrium corresponding to the attack-defense contest can be obtained by solving the payoff matrix under different pre-defined attack-defense scenarios. Based on the Nash Equilibrium, the vulnerability rankings of power grid components can be obtained and the vulnerability assessment can be conducted as well as the allocation plan of defense fund.**

***Index Terms*--electric grid vulnerability; game theory; Nash equilibrium; assessment framework; defense fund allocation**

I. INTRODUCTION

Electric grid is one of the most important infrastructures of a country and is critical for the functioning of a society and its economy. The rapid development of modern power system along with the increasing of load demand all over the world since the 21st century has made the electric grid more stressed and vulnerable. From the United States and Canada blackouts happened in 2003, to the India blackout recently, the cascading failures of power system impel people to focus on power system vulnerability assessment issue further. To make power system more resilient to disruptions, electrical engineers and scientists evaluate the failure probability of components in the power system and place more surveillance, protection, and backups to those which have larger probability to fail and have more serious failure impacts according to security criteria. Those criteria, like the famous n-1 criterion [1] and high risk n-k contingency identification [2], are used to defense electric grid against random accidents or acts of nature.

However, with terrorism issues appear more severe around the world, electric grid may become the attack object of terrorists, which are considered as fully intelligent and strategic attackers. They tend to choose those targets with low failure probability so that they have less protection, but whose malfunction can cause huge impacts. Accordingly under the scenario of deliberate attacks, the traditional electric grid vulnerability assessment methods may no longer stand. In this situation, terrorists have limited resources and allocate those resources on different components of electric grid to launch malicious attack so they can reach their maximum expectations. Meanwhile, the power system operators try their bests to protect against the potential attacks. The acts of both the terrorists and the operators will affect the final results. Thereupon, the interaction between them becomes a game, which can be analyzed by game theory [3].

J. Salmeron et al. [4] firstly proposed a bilevel model to analyze the vulnerability of power system by setting the maximum damage plan for the terrorist. Later, J. M. Arroyo et al. [5] improved the bilevel model as a single level model, and further converted to a single linear programming model [6]. J. M. Arroyo et al. [7] summarized the bilevel programming vulnerability assessment method. A. J. Holmgren et al. [8] firstly introduced the knowledge of game theory into finding defense plan against attack for electric grid by solving zero-sum game's pure strategy Nash Equilibrium and found that there is no dominant defense strategy. Guo Chen et al. [9] focused on dynamic game of complete information and explored reliable strategies. Natalia Romero et al. [10] proposed a three-level optimization model in the case of dynamic game of complete information. Ettore Bompard et al. [11] simulated an attack and defense situation, in which the attacker and the defender can only choose one or two transmission lines to allocate their resources, and solved the mixed strategy Nash Equilibrium. Most of existing references that apply knowledge of game theory are confined to certain game situation which is either the type of game or the strategies players can choose.

In this paper, a much more generalized framework for electric grid vulnerability assessment using game theory is presented. It is applicable in different types of game and on different kinds of players. Furthermore, the proposed framework can be extended quite easily according to various situations that are not discussed in this paper.

This work was supported in part by the National Basic Research Program of China, 973 program (2013CB228203), the Research Project of Science and Technology from Shenzhen Development and Innovation Committee (ZDSY20120619141142918).

978-1-4799-2522-3/13/$31.00 ©2013 IEEE

The rest of this paper is organized as follows. Section Ⅱ describes the mathematical game model of the attack and defense situation in electric grid. Section Ⅲ discusses the strategies of electric attacker and defender in different games, which show the optimal allocation plan of defense funds. The method to assess the electric grid vulnerability under attack-defense scenario is given in Section Ⅳ, while the numerical examples are presented in Section Ⅴ. The conclusion remarks are drawn in Section Ⅵ.

II. ATTACK-DEFENSE MODEL

This section will describe the mathematical game model of the attack and defense situation in electric grid. The model presented in this section is inspired and improved from [8] and [9]. The attacker and the defender in the improved model both have enough flexibility to allocate their resources which are much more real and can reflect electric grid components' true vulnerability.

In this paper, we treat the interaction between the attacker and the defender of the electric grid as a game, in which both players tend to choose the best strategy to gain maximum payoff.

A. Strategy

Consider an electric grid with N components, which include generators, transmission lines, transformers, etc.

The terrorist, who is named as attacker, has limited resources which might be weapons, manpower resources, techniques, etc. Here, we denote the amount of resources of attacker as parameter A. The attacker has a set of strategies defined as $\mathbf{I_a}$ which has K_a elements:

$$\mathbf{I_a} = \{\mathbf{S_{a,1}}, \mathbf{S_{a,2}}, ..., \mathbf{S_{a,K_a}}\} \tag{1}$$

Each of the elements in $\mathbf{I_a}$ is a strategy which the attacker can select to allocate his resources:

$$\mathbf{S_{a,j}} = (a_{1,j}, a_{2,j}, ..., a_{N,j}), \tag{2}$$

where j=(1,2,...,K_a) and $a_{i,j}$ stands for the amount of resources that the attacker invests on components i (i=1,2,…,N) in strategy j:

$$\sum_{i=1}^{N} a_{i,j} = A \tag{3}$$

The power system operator, who is named as defender, has limited resources as well which include monitors, policemen, backups, etc. Here we denote the resources of operator as parameter D. The defender has a set of strategies defined as $\mathbf{I_d}$ which has K_d elements:

$$\mathbf{I_d} = \{\mathbf{S_{d,1}}, \mathbf{S_{d,2}}, ..., \mathbf{S_{d,K_d}}\} \tag{4}$$

Each of the elements in $\mathbf{I_d}$ is a strategy which the defender can select to allocate his resources:

$$\mathbf{S_{d,j}} = (d_{1,j}, d_{2,j}, ..., d_{N,j}), \tag{5}$$

where j=(1,2,...,K_a) and $d_{i,j}$ stands for the amount of resources that the defender invests on components i (i=1,2,…,N) in strategy j:

$$\sum_{i=1}^{N} d_{i,j} = D \tag{6}$$

The allocation strategies of attacker and defender affect the failure probability of component i, which is defined as p_i. The more attacker invests resources on component i, the more likely the component i is going to stop working, while on the other hand the defender's investment on component i decreases the failure probability:

$$p_i = f(a_i, d_i), \tag{7}$$

where function f varies in different attack-defense scenarios.

B. Payoff

After one game, every player in the game gets their payoff, which is decided by the strategies of all the players took.

In the case of electric grid attack and defense, the payoff of the attacker varies with different types of terrorists. There are attackers whose purpose is to maximize the expected loss U. There are also attackers who want to maximize the probability that the expected loss U goes beyond a threshold u_{min}, so their payoff is $P(U>u_{min})$, etc. [8]. The defenders can have different goals as well. For instance, they may want the expected loss of load U to be as little as possible, or the fastest process of recovery, etc. They have various payoffs accordingly.

When an electric grid is attacked, it may collapse with different consequences involving loss of load, social panic and disorder, destruction of infrastructures, economic losses, etc. In this paper, we consider the loss of load after attack as the consequence. Attacker can regard the loss of load as his payoff while the payoff of the defender is the negative loss of load. In this situation, their interaction forms a zero-sum game.

1) *Minimum Loss of Load:* When the components of the electric grid fail due to malicious attack, it may cause the loss of load. We apply dc power flow model to calculate the loss of load. The objective is to minimize the total losses of load, which is described as parameter *mLS(t)*, and solved by the linear optimization function *linprog* in MATLAB™.

2) *Recovery Time:* After attack, it takes time, which is defined as T_i, for the malfunctioned component i to recover. The longer it takes, the bigger the total losses the electric grid will have to bear. The minimum loss of load *mLS(t)* changes from time to time as the components starting to fix. We define the total losses of load in an electric grid as parameter y, then we have:

$$y = \int_{0}^{\max(T_i)} mLS(t) \cdot dt \tag{8}$$

3) *Expected Loss:* Since the failure of a component after a malicious attack is a probability event, the loss of load

should be stochastic as well. Here, we define parameter U as the expected loss. If only one component is attacked, say component No. 1, and then we have:

$$U = p_1 y_1 , \tag{9}$$

where y_1 stands for the total losses of load after component No. 1 is attacked and destroyed. If there were two of the components, say component No. 1 and No. 2, and then:

$$U' = p_1 p_2 y_{12} + p_1 (1 - p_2) y_1 + (1 - p_1) p_2 y_2 , \tag{10}$$

where y_{12} stands for the total losses of load after component No. 1 is attacked and destroyed.

When more than 2 components were attacked, we can get the expected loss U in the same way [8].

III. Vulnerability Assessment

In this section, we will discuss how to assess the vulnerability of electric grid under attack-defense circumstance.

A. Scenario Setting

The first step of vulnerability assessment is to set the attack-defense scenario, which involves resources A and D, set of strategies $\mathbf{I_a}$ and $\mathbf{I_d}$, information, order, payoffs, etc. Then we get the payoff matrix between the attacker and the defender.

B. Payoff Matrix

After the setting of attack-defense scenario, we can calculate the payoffs under different combinations of $\mathbf{S_{a,i}}$ and $\mathbf{S_{d,j}}$ and get the payoff matrix, defined as parameter $\boldsymbol{Z}$.

C. Nash Equilibrium

By solving the payoff matrix $\boldsymbol{Z}$, we can get the mixed strategy Nash Equilibrium (including Pure Nash Equilibrium) of the game:

$$\begin{cases} \mathbf{sp_a^m} = \{sp_{a,1}^m, sp_{a,2}^m, ..., sp_{a,K_a}^m\} \\ \sum_{i=1}^{K_a} sp_{a,i}^m = 1 \\ 0 \le sp_{a,i}^m \le 1 \end{cases}, \tag{11}$$

$$\begin{cases} \mathbf{sp_d^m} = \{sp_{d,1}^m, sp_{d,2}^m, ..., sp_{d,K_d}^m\} \\ \sum_{i=1}^{K_d} sp_{d,i}^m = 1 \\ 0 \le sp_{d,i}^m \le 1 \end{cases}, \tag{12}$$

where $sp_{a,i}^m$ stands for the probability that attacker may use strategy $\mathbf{S_{a,i}}$ on the Nash Equilibrium point m, and $sp_{d,i}^m$ stands for the probability that defender may use strategy $\mathbf{S_{d,i}}$ on the Nash Equilibrium point m.

There may exist more than one Nash Equilibrium point (m=1, 2, 3, ... , H) and they should all be taken into account during analysis.

D. Vulnerability Assessment

We define the concept of vulnerability of electric grid as follows: the more resources the attacker and the defender invest on, the more vulnerable the component is. Since the mixed Nash Equilibrium involves probability, here we use weighted average method to calculate the total investment.

1) *Game of incomplete information:* In the game of incomplete information, for example the defender is not clear about how many resources the attacker has, so unlike game of complete information there exists a set of possible game scenarios $\mathbf{G}$ for the defender. If the defender wants to assess the vulnerability of components and deploys defending strategies, he will have to take all the possible game senarios into account.

Consider one game scenario g ($g \in \mathbf{G}$), For component i, we define its total attacking investment as follows:

$$F_a^{i,g} = \frac{\sum_{m=1}^{H} \sum_{n=1}^{K_a} sp_{a,n}^m \cdot a_{i,n}}{H}, \tag{13}$$

where H stands for the number of Nash Equilibrium point and K_a stands for the number of strategies the attacker can take. In the same way, we define its total defending investment in one game g as follows:

$$F_d^{i,g} = \frac{\sum_{m=1}^{H} \sum_{n=1}^{K_d} sp_{d,n}^m \cdot d_{i,n}}{H} \tag{14}$$

According to the definition of vulnerability in this paper, the next step is to consider both the attacking investment and the defending investment together. Because the investments of attacker and defender may not have comparability, the only thing we care is their rankings. We define function R as the ranking function when the larger number, the lower the ranking, thus the smaller the indicator, the higher vulnerable component is. We define the vulnerability indicator of component i in game of incomplete information as:

$$V^i = R \sum_{g \in \mathbf{G}} \left[R(R(F_a^{i,g}) + R(F_d^{i,g})) \right], \tag{15}$$

and the smaller V^i is, the more likely component i is to become the target of attacker and need more defending. Based on sort sequence of V^i, we can obtain the vulnerability ranking of components.

2) *Game of complete information:* In the case of complete information, $\mathbf{G}$ only has a single element and (15) can be rewritten as:

$$V^i = R(R(F_a^i) + R(F_d^i)) \tag{16}$$

3) *Game of different orders:* Order means the sequence that the attacker or the defender settles their strategy. Either the defender settles his strategy first and then the attacker settles his strategy correspondingly, which is studied in [9], or they settle their strategies at the same time. If the attacker takes the first move then it makes no sense for the defender to decide his strategy, since the electric grid would be destroyed

already. Game of both orders can be analyzed by the framework proposed in this paper.

The flow chart of proposed vulnerability assessment framework is shown in Fig. 1.

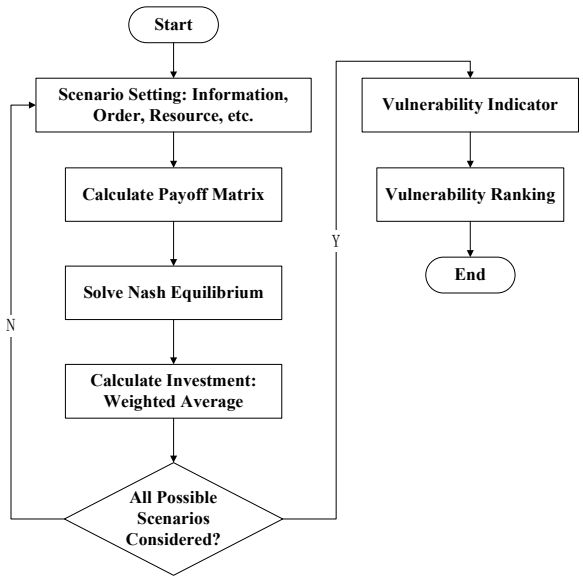

Figure 1. Flow chart of vulnerability assessment framework

IV. APPLICATION EXAMPLE

For simplicity, we choose a small electric grid as shown in Fig. 2 with 5 generators and 6 transmission lines for case studies.

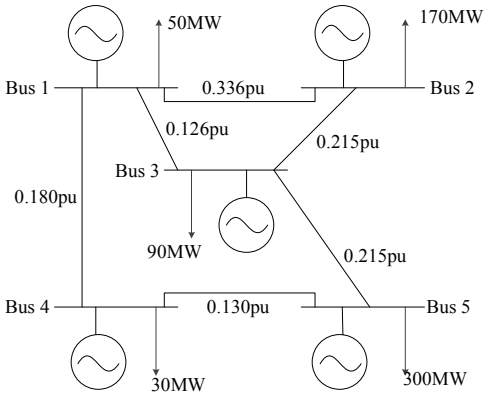

Figure 2. Single line diagram of test system

The corresponding parameters are given in Table Ⅰ.

TABLE Ⅰ. PARAMETERS OF TEST SYSTEM

Generator Capacity(MW)	0~150
Transmission Line Thermal Capacity Limits(MW)	100

The scenario settings are as follows, which is inspired and improved from [9]:

1) *Target:* For simplicity, the attacker will only attack the transmission lines. Accordingly the defender only has to defend transmission lines.

2) *Resources:* Both attacker and defender have resources called 'unit'，but the unit of attacker and the unit of defender can represent different types of resources. To ensure that the Nash Equilibrium exists, the allocation of resources is discrete, and the smallest investment is 1 unit.

3) *Failure Probability:* Consider the marginal decrease of investment, we define the failure probability of every transmission line as follows:

$$p_i = \frac{a_i}{c_1 + a_i} \cdot \frac{1}{c_2 + d_i}, \tag{17}$$

and for simplicity, we set c_1=c_2=1 during analysis.

4) *Recovery Time:* The recovery time T is equal to the number of transmission lines that are destroyed, and all the destroyed ones are repaired at the same time, i.e.：

$$y = mLS \cdot T \tag{18}$$

5) *Type of game:* The static game is considered during simulations.

6) *Payoff:* The attacker wants to maximize the loss of load while the defender wants to minimize it, which makes a zero-sum game.

According to the assessment framework mentioned in the previous section, we calculate the vulnerability indicator V^i of every transmission line under different game scenarios, i.e. different combinations of attack-defense resources. The result is shown in Fig.3, from which we can get the vulnerability assessment under different games of complete information. It can be seen that there are several crossover points, which indicates that the vulnerability indicator of a transmission line varies to different attack-defense scenarios.

Consider a type of incomplete game, in which the defender is not clear about how many resources the attacker has, but only knows the range. We hold defense resource unchanged, and let attack resource vary from 2 to 6, and at the same time, add the indicators together according to (15). The results are shown in Fig. 4. Fig. 4 is a guide for the operators about how to defense the electric grid when they are not sure how many resources the attackers have, which is called an incomplete information game. It should be noticed that lines in Fig. 4 are quite steady and do not go up and down like in Fig. 3, which can reflect the vulnerability ranking of transmission lines in multiple scenarios and gives us a more reliable ranking.

At last, we can add up every transmission line's vulnerability indicator in Fig. 4 and gain the overall ranking of vulnerability which is given in Table II. Although there is no completely dominant defense strategy, as discussed in [8], the proposed frame work still can conduct the assessment and obtain the vulnerability ranking of components as shown in Fig. 4 and Table II, which can be referred to when deploying defense strategies.

It should be noticed that in this paper, we just only consider the static game and the resources varying from 2 units to 6 units. Other types of game can be evaluated in the same framework easily via only changing the payoff matrix.

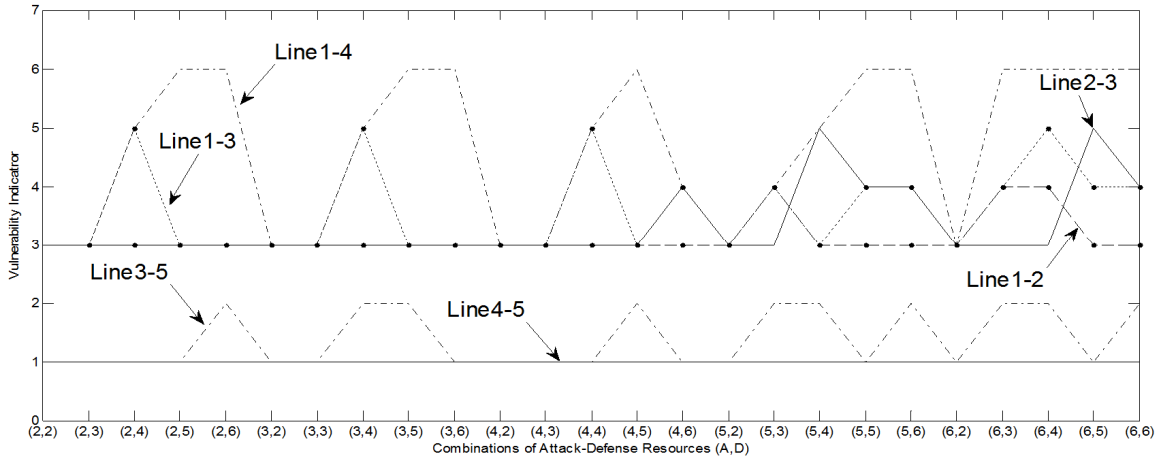

Figure 3. Vulnerability indicator under different combinations of attack-defense resources

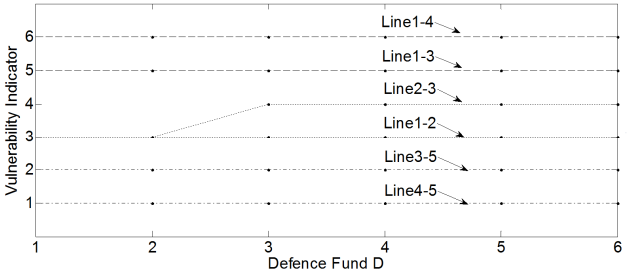

Figure 4. Vulnerability indicator under different defense resources when attack resources vary from 2 to 6

V. CONCLUSION

The vulnerability assessment has become one of the most important issues and topics to prevent the electric grid from cascading blackouts in recent years. This paper presents a generalized frame work to assess the vulnerability of electric grid under attack-defense scenario using the knowledge of game theory. The frame work can be used to calculate the vulnerability rankings of components in various types of game including game of complete information, incomplete information, etc., as shown in the application example. Although there is no completely dominant defense strategy as found in [8], the vulnerability rankings resulted from the frame work in this paper can give the operators of the power system a reference involving how to defend the electric grid against antagonistic attacks. Especially, it is very easy to extend the proposed framework for vulnerability assessment of electric grid according to different cases.

TABLE Ⅱ. OVERALL VULNERABILITY RANKING

Line	Overall Ranking
4-5	1
3-5	2
1-2	3
2-3	4
1-3	5
1-4	6

REFERENCES

[1] Hui Ren, Ian Dobson, Benjamin A. Carreras, "Long-term effect of the n-1 criterion on cascading line outages in an evolving power transmission Grid," *IEEE Trans. Power Systems*, vol. 23, pp. 1217-1225, Aug. 2008.

[2] Qiming Chen, James D. McCalley, "Identifying high risk n-k contingencies for online security assessment," *IEEE Trans. Power Systems*, vol. 20, pp. 823-834, May. 2008.

[3] Martin J. Osborne, Ariel Rubinstein, *A course in game theory*, The MIT Press, 1994.

[4] J. Salmeron, K. Wood, R. Baldick, " Analysis of electric grid security under terrorist threat," *IEEE Trans. Power Systems*, vol. 19, pp. 905-912, May. 2004.

[5] J. M. Arroyo, F. D. Galiana, "On the solution of the bilevel programming formulation of the terrorist threat problem," *IEEE Trans. Power Systems*, vol. 20, pp. 789-797, May. 2005.

[6] A. L. Motto, J. M. Arroyo, F. D. Galiana, "A mixed- integer LP procedure for the analysis of electric grid security under disruptive threat," *IEEE Trans. Power Systems*, vol. 20, pp. 1357-1365, Aug. 2005.

[7] J. M. Arroyo, "Bilevel programming applied to power system vulnerability analysis under multiple contingencies," *IET Generation, Transmission & Distribution*, vol. 4, pp. 178-190, 2010.

[8] A. J. Holmgren, E. Jenelius, J. Westin, "Evaluating strategies for defending electric power networks against antagonistic attacks. IEEE Transactions on Power Systems," *IEEE Trans. Power Systems*, vol. 22, pp. 76-84, Feb. 2007.

[9] Guo Chen, Zhao Yang Dong, David J. Hill, Yu Sheng Xue, " Exploring Reliable Strategies for Defending Power Systems Against Targeted Attacks," *IEEE Trans. Power Systems*, vol. 26, pp. 1000-1009, Aug. 2011.

[10] Natalia Romero, Ningxiong Xu, Linda K. Nozick, Ian Dobson, "Investment planning for electric power systems under terrorist threat," *IEEE Trans. Power Systems*, vol. 27, pp. 108-116, Feb. 2012.

[11] Ettore Bompard, Ciwei Gao, Roberto Napoli, Angela Russo, Marcelo Masera, Alberto Stefanini, " Risk Assessment of Malicious Attacks Against Power Systems," *IEEE Trans. Power Systems*, vol. 39, pp. 1074-1085, Sept. 2009.

[12] (2010) Gambit. [Online] Available: www.gambit-project.org.