Research on optimal allocation of protective resources of power network under malicious attacks

Jingyi Xiong*, Benwei Hou and Xiuli Du

Faculty of Urban Construction, Beijing University of Technology, Beijing, 100124, China

*Corresponding author’s e-mail: xjy_081696@163.com

Abstract: With the increase of global malicious activities, it is particularly necessary to optimize the allocation of limited urban protective resources and protect power network from malicious attacks. There is plenty of research on evaluating the risks of malicious attacks on electricity network, however, conventional risk-based approach does not take strategic adjustment of malicious into account, nor can it determine the optimal allocation of global protective resources. In this paper, an optimal allocation of protective resources based on game theory was proposed, which combined game theory with risk assessment, taking full account of strategic interaction between defender and attacker. IEEE 30-bus network was taken as an example to verify the applicability and reliability of the method, so as to confirm the advantages of the method in determining the global optimal allocation of protective resources.

1. Introduction

In recent years, with the development of economy and society, urban power network expands continuously, leading to increasingly complex electricity network in all kinds that reveals considerably vulnerable under external attacks and disturbances, threatened by growing malicious attacks. Due to the inherent connectivity among the nodes of modern urban power network, in case of a key node is hit, it will break the structure and vitiate functions of the whole network. Recently, malicious attacks remain unabated and grow rampantly, leading to increasing risks of malicious attacks on urban electricity network. The issue of defensing power network from malicious attacks becomes a hotspot in the field of engineering[1].

It is necessary to invest protective resources to protect power network. Protective resources refer to funds, materials and other consumables invested to protect power network from malicious attacks[2]. Nevertheless, protective resources of individual cities are limited due to numerous nodes of urban electricity network, therefore, an effective solution of protective resource allocation is crucial. Different from natural disasters, protective resource allocation under malicious attacks has to take account of strategic game between attacker and defender. Attacker refers to malicious and defender refers to authorities such as enterprise management or government of power network[3]. Defender shall predict attacker’s strategy according to the network status and intelligence information, and carries out effective protective measures. Likewise, attacker will adjust the strategy after learning the information of protective measures[4][5]. During the process of the game between the attack and defense, attacker aims to make great threat to power network, while defender focuses on reducing risks upon power network.
Therefore, the game purpose for both sides is to find the optimal strategy that is the most beneficial to each side respectively.

In general, the issue of optimal allocation of protective resources focuses on the value of target. Conventional protective resource allocation methods include key-point allocation, proportional allocation and uniform allocation that distribute resources from different perspectives[2]. However, these conventional methods of protective resource allocation do not take account of the impact of attacker’s strategy adjustment and strategic interaction between the attack and defense. In reality, attacker is likely to collect the information of the target in advance and predicts the strategy of resource allocation of defender, achieving the purpose of causing the great risk to electricity supply by adjusting the strategy. Therefore, conventional methods of resource allocation cannot effectively cope with the issue of strategic game between the attack and defense. Using methods based on game theory to the protective resource allocation in urban power network is preferable to practical requirements.

Although it is crucial to allocate protective resources of urban power network in a reasonable way, the research on the effective allocation of protective resources of urban power network is at the beginning that most of existing studies focus on vulnerability assessment and risk assessment of power network in all kinds under the threat of malicious attacks[6][7]. For example, Peng et al. analyzed the current situation of urban power network under threat of malicious attacks[7]. McMasters studied vulnerability identification and vulnerability assessment of the power network under malicious attacks according to the topological features of power network system[8]. These studies have established a complete vulnerability assessment model and risk assessment model of power network under malicious attacks, which laid a theoretical foundation for the study of protective resource allocation in power network.

In this paper, by combining the game model with the features of power network, an optimal allocation method of protective resources in the scenario of malicious attack was proposed. By this method, game theory was applied to urban power network for studying the allocation of protective resources of power network. IEEE 30-bus network was taken as an example to carry out a case study that takes network features of power flow into account, an allocation model of protective resources was established, so as to provide more reasonable and practical decision-making guidance for the allocation of protective resources in power network.

2. The game theory method of power network protective resource allocation

2.1. An overview of game theory methods
In general, the game model has four basic elements – decision maker, strategy set of both sides of decision-making, benefit, and information[10]. As for the issue of protective resource allocation, the decision makers are attacker (malicious) and defender (government or enterprise management) who are usually considered rational and smart[11][12]. The strategy set of each side is the set of action strategies derived from decision-making, the benefit is expected profit that the decision makers get from their respective specific action strategies. Finally, the information refers to the information obtained by each side for decision making. Effective information is conducive to making the optimal decision for decision makers.

As for the issue of allocation of protective resources of urban power network, the attacker will determine the attack strategy according to value evaluation of individual targets in power network, at the same time, the defender will predict the most likely attack strategy and allocate protective resources to the prioritized targets[13][14]. The attacker will get less benefits by attacking targets with more protective resources allocated. Therefore, the attacker may adjust strategy and switch to other targets from those with enough protective resources. In the end, the result of game of both sides will reach an equilibrium points, that is, “Nash equilibrium”, where both sides cannot get more benefits by changing their strategies, respectively. In other words, both sides shall adopt the optimal strategy that is most beneficial at the equilibrium point[15].
2.2. Strategy set of attackers and defenders

In the process of game, the attacker attempts to choose a certain target to maximize expected benefit. In general, the attacker is considered to attack one target at a time\(^5\), hence the attack strategy can be expressed by the probability of the target being attacked\(^6\). For a power network with \(n\) targets, the attacker’s attack strategy can be expressed as:

\[
A = (a_1, a_2, \cdots, a_n)
\]

\[\text{St: } 0 \leq a_1, a_2, \cdots, a_n \leq 1 \quad \forall i \in [1,n]
\]

\[a_1 + a_2 + \cdots + a_n = 1
\]

Where, \(A\) is the attack strategy, \(a_i\) is the probability of attack on target \(i\) in the power network. Increased value of \(a_i\) represents that under the attack, target \(i\) is more prone to be attacked. If the attack action is bound to occur, then the sum of probabilities of attack on each target is equal to 1 (see equation (3)).

According to equation (1) to equation (3), the set of attack strategies of the attacker \(S_A\) can be expressed as:

\[S_A = \{A \in \mathbb{R}^n; \text{ for } i=1,\cdots,n,0 \leq a_i \leq 1, \sum_{i=1}^{n} a_i = 1\}
\]

To deal with potential threat of attack and minimize the risk of being hit, the strategy of the defender can be expressed by the amount of protective resources allocated to each target. For a power network with \(n\) targets, the defense strategy adopted can be expressed as:

\[
D = (d_1, d_2, \cdots, d_n)
\]

\[\text{St: } 0 \leq d_1, d_2, \cdots, d_n \leq 1 \quad \forall i \in [1,n]
\]

\[d_1 + d_2 + \cdots + d_n \leq b
\]

Where, \(D\) is the defender’s defense strategy, \(d_i\) is the amount of protective resources allocated to target \(i\) in the power network, and \(b\) is the total amount of protective resources. As protective resources are limited, the defender needs to control the input of protective resources at a reasonable level, so that the total amount of protective resources cannot exceed \(b\) (see equation (7)).

According to equation (5) to equation (7), the set of defense strategies of the defender \(S_D\) can be expressed as:

\[S_D = \{D \in \mathbb{R}^n; 0 \leq d_i \leq b, \text{ for } i=1,\cdots,n, \sum_{i=1}^{n} d_i \leq b\}
\]

2.3. Payoff of attackers and defenders

The benefit is the outcome of each side at the end of the game\(^7\). In this study, the benefit of the attacker is defined as the risk arising from the attack on the power network. Therefore, the benefit resulting from the attack on the power network can be expressed as:

\[
U_a = \sum_{i=1}^{n} a_i \times p_i(d_i) \times G_i \quad i = 1,2,\cdots,n
\]

Where \(U_a\) is the benefit of attack strategy, \(a_i\) is the probability of attack on target \(i\) in the power network, \(p_i(d_i)\) is the vulnerability of target \(i\) that presents the probability of target \(i\) being successfully destroyed\(^8\)[9], \(G_i\) is the value of target \(i\) defined by the attacker.

In the static game, the benefit of the attacker increases the risk of the target, while the benefit reduces the risk of the target, that is, the attacker’s gains mean the defender’s losses. Therefore, the sum of gains and losses of both sides of the game is equal to \(G\). The total benefit of the defender \(U_d\) can be expressed as:

\[
U_d = -U_a = -\sum_{i=1}^{n} a_i \times p_i(d_i) \times G_i
\]
2.4 Nash equilibrium

In the game, the attacker will choose an appropriate attack target according to the attack strategy to maximize the risk of the power network. The function of expected benefit generated from attack on the power network can be expressed as:

$$\max_{a_i \in S_A} U_a = \max_{a_i \in S_A} \sum_{i=1}^{n} a_i \times p_i (d_i) \times G_i$$

(11)

Accordingly, the defender will minimize the risk of the power network by allocating limited protective resources. The function of expected benefit of the defender can be expressed as:

$$\max_{d_i \in S_D} U_d = \max_{d_i \in S_D} (-U_a) = \min_{d_i \in S_D} \sum_{i=1}^{n} a_i \times p_i (d_i) \times G_i$$

(12)

In the static game, the players act simultaneously and the two decision makers have no information of each other’s strategies. At the equilibrium point, the defender cannot further reduce the risk of the power network by changing the defense strategy, and vice versa.

When the equilibrium point is reached, the attack strategy and the defense strategy can be expressed as $A = (a_1', a_2', \ldots, a_n')$ and $D = (d_1', d_2', \ldots, d_n')$, respectively. Therefore, based on the minimax theory, the Nash equilibrium is valid for the two equations as:

$$\sum_{i=1}^{n} a'_i \times p_i (d'_i) \times G_i \geq \sum_{i=1}^{n} a_i \times p_i (d_i) \times G_i \quad (a_i \in S_A)$$

(13)

$$\sum_{i=1}^{n} a'_i \times p_i (d'_i) \times G_i \leq \sum_{i=1}^{n} a'_i \times p_i (d'_i) \times G_i \quad (d_i \in S_D)$$

(14)

3. Case study

According to the evaluation framework and method of optimal allocation of protective resources of power network under malicious attacks based on game theory in this paper, IEEE 30-bus network is taken as a case to calculate the optimal allocation strategy of protective resources of the power network under malicious attacks, so as to provide guidance for determining the optimal allocation of protective resources of urban power network under malicious attacks.

3.1 Power network topology and asset analysis

In reality, the line target of power network represents the transmission line, and the point target represents power plant, substation and load node. In urban power network, power plant converts the primary energy of nature into electricity, and substation transforms voltage, accepts and distributes electricity to load nodes through transmission line for end users. In the case study, IEEE 30-bus network is a local simplified network of North American Power Systems Interconnection, a standard system used in the power industry, which can simulate urban power network to a certain extent. The topological model of IEEE 30-bus network is shown in figure 1. In the model, there are six generator nodes (G1, G2, G3, G4, G5, G6) in the network that can be used as power plants in the city. There are four variable-ratio transformer branches that can be used as substations in the city (S1, S2, S3, S4). In addition, the system has 24 load nodes.
The power generator parameters of IEEE 30-bus network are shown in table 1, and transformer branch parameters are shown in table 2.

Table 1. Basic information of generator.

| Site number | Reference voltage(KV) | Maximum voltage(p.u.) | Minimum voltage(p.u.) | Generator capacity(MVA) |
|-------------|-----------------------|-----------------------|-----------------------|------------------------|
| G1          | 135                   | 1.05                  | 0.95                  | 100                    |
| G2          | 135                   | 1.05                  | 0.95                  | 100                    |
| G3          | 135                   | 1.05                  | 0.95                  | 180                    |
| G4          | 135                   | 1.05                  | 0.95                  | 250                    |
| G5          | 135                   | 1.05                  | 0.95                  | 100                    |
| G6          | 135                   | 1.1                   | 0.95                  | 100                    |

Table 2. Basic information of transformer branch.

| Site number | Branch reactance (p.u.) | Branch capacity (MVA) | Branch strain ratio |
|-------------|------------------------|-----------------------|---------------------|
| S1          | 0.21                   | 65                    | 1.01                |
| S2          | 0.56                   | 32                    | 0.96                |
| S3          | 0.26                   | 65                    | 1.01                |
| S4          | 0.40                   | 65                    | 0.98                |

3.2 The comprehensive value evaluation method of the site

The comprehensive value of different targets in the network can be calculated from two aspects – target value and system value. Target value refers to the value of its internal equipment and functions, while system value refers to the important role of the target in the network system. System value can be evaluated based on network connectivity index. Target value is evaluated through multi-attribute decision making by analytic hierarchy process (AHP)[23].

The value evaluation of the target system is related to the influence of the target on the network connectivity. It is necessary to not only take account of the connectivity of topology, but also the system features of power network. In this study, EPI (effective performance index) is adopted to characterize network connectivity. EPI is defined as the average reciprocal of the shortest distance between targets, which used to measure the average transmission efficiency between targets. As for the transmission of power network needs to conform to the physical characteristics of power flow along any path, with EPI, the shortest distance is replaced by the electrical distance. In the process of transmission, the active
power is actually consumed electricity, while the reactive power is electric power required to establish the magnetic field by components such as inductors and capacitors but is not consumed, therefore, merely the active power is analyzed\cite{22}. The unique power flow distribution solution is obtained through power flow calculation given network architecture, load demand and unit output, that is, the magnitude of power through each line. Therefore, $EPI$ can be expressed as:

$$EPI = \min \left( \frac{1}{N_g N_l} \sum_{g=1}^{N_g} \sum_{l=1}^{N_l} \frac{P_{Dl}}{|Z_{eqgl}|} \right)$$

(15)

Where $\min \left( P_{Dl}, P_{Gl} \right)$ is the minor value between active power of power plant node $g$ and active power of load node $l$, representing the maximum power that can be transmitted between the “generation – load” node pairs, which is the numerical solution of the equivalent impedance between the “generation – load” node pairs, that is, the electrical distance.

$$Z_{eqgl}$$ is equal to the voltage difference between the node pairs when the unit current flows from generation node $g$ to load node $l$. $Z_{eqgl}$ between “generation – load” node pairs can be expressed as:

$$Z_{eqgl} = \left| \frac{U_{g} - U_{l}}{I} \right| = \left| \frac{Z_{gg} - Z_{fl}}{I} \right| = \left| \frac{Z_{gg} + Z_{fl} - 2Z_{gl}}{I} \right|$$

(16)

In the equation, $Z_{gg}$ and $Z_{fl}$ are the self-impedance of nodes $g$ and $l$, respectively. $Z_{gl}$ is the mutual impedance between node pairs $(g,l)$.

Set the network connectivity as $EPI_0$ at the intact initial state of power network. When the target $j$ of power network is destroyed, the unit is removed, and connectivity $EPI_i$ is calculated after the network is stabilized. Finally, the variation (i.e. consequence) $\Delta EPI_i$ of the network connectivity is obtained as:

$$\Delta EPI_i = EPI_0 - EPI_i$$

(17)

After normalization, for connectivity-biased attackers, the equation for evaluating $V_i^1$, the value of target $i$, is as:

$$V_i^1 = \Delta EPI_i \left( \sum_{i=1}^{10} \Delta EPI_i \right)^{-1}$$

(18)

In the evaluation of target value, due to the nature and characteristics of power plant target, its influencing factors are active power ($P_g$), generator capacity ($m_{base}$) and the maximum reactive power ($Q_{max}$); due to the nature and characteristics of substation target, its influencing factors are the targeted branch reactance ($x$) and allowable capacity of long-distance, short-distance and emergency transmission branches ($rateA$, $rateB$ and $rateC$). Impact factor is expressed as $C_i$, and standardized impact factor is expressed as $r_i$.

Before making a decision, it is necessary to remove the influence of physical dimensions of impact factors on the decision-making results. The types of impact factors are benefit type, cost type, fixed type, deviation type, interval type, and deviation interval type. As for benefit type, the greater the impact factor value, the better the decision result; on the contrary, for cost type, the smaller the impact factor value, the better the decision result. Fixed type makes a better result if the value of impact factor is closer to a certain value, while deviation type gets a better result if the value of impact factor deviates far from a certain value. Interval type will have a better decision result for the value of impact factor falls into a certain interval, while deviation interval type makes a better result for the value of impact factor deviates far from a certain interval.

In this study, active power ($P_g$), generator capacity ($m_{base}$), maximum reactive power ($Q_{max}$), and allowable capacity for long-distance, short-distance and emergency-distance transmission branches ($rateA$, $rateB$ and $rateC$) are all benefit type indicators, which are standardized using the following
The impact factor branch reactance ($x$) is a cost type index that is standardized using the following equation:

$$r_i = \frac{C_i}{\max C_i}$$  \hspace{1cm} (19)

When making a decision, the impact factors of power plant and substation targets are compared in pair, and the consistency test is carried out, thus the corresponding impact factor weights of power plant and substation targets are obtained, respectively. In order to ensure good consistency of the scale of comparison matrix, a 9/9–9/1 is adopted in this study. Scale evaluation is shown in Table 3, in which 9/2, 9/4, 9/6, 9/8 is between two adjacent scales. A comparison matrix is constructed, and consistency ratio CR is calculated which is acceptable for CR < 0.1. Corresponding weights of impact factors calculated by AHP method are shown in Table 4.

Table 3. Scale evaluation form of comparison matrix.

| Scale method | Equally important | A little important | Obviously important | Highly important | Extremely important |
|--------------|------------------|--------------------|---------------------|-----------------|--------------------|
| 9/9–9/1      | 1                | 1.286              | 1.8                 | 3               | 9                  |

In power network, regardless of irresistible loss during the transmission, the total amount of power transmission is fixed, and the proportion of electricity of each type is the reciprocal of the number of targets of each type, respectively. In this study, only targets of power plant and substation are taken into account. In AHP, when the number of impact factors ≤ 2, the comparison matrix has consistency that can calculate weights of impact factors without consistency test. The weights of power plant and substation targets are 0.4 and 0.6, respectively.

Table 4 Weight of impact factors in AHP.

| Impact factors of power plant | The weight | Impact factors of substations | The weight |
|-------------------------------|-----------|-------------------------------|-----------|
| Pg                            | 0.1509    | x                             | 0.2727    |
| mbase                         | 0.2042    | rateA                         | 0.2424    |
| Qmax                          | 0.6449    | rateB                         | 0.2424    |
|                               |           | rateC                         | 0.2424    |

According to the calculated weights of target sites, the value of each target is calculated. The value of each target of power plant $V'_{gi}$ can be calculated by equation as:

$$V'_{gi} = 0.4 \times (0.1509 \times r_{pg} + 0.2042 \times r_{mbase} + 0.6449 \times r_{Qmax})$$  \hspace{1cm} (21)

The value of each target of substation $V'_{si}$ can be calculated by equation as:

$$V'_{si} = 0.6 \times (0.2727 \times r_x + 0.2424 \times r_{rateA} + 0.2424 \times r_{rateC})$$  \hspace{1cm} (22)

Substitute target values calculated from equation (21) and equation (22), so the comprehensive value can be expressed as:

$$V_j = \omega_1 \times V'_j + \omega_2 \times V'_i$$  \hspace{1cm} (23)

Where $\omega_1$ and $\omega_2$ are weight ratio of system value and target value, respectively, which are taken as 0.5 in this study. This means that in IEEE 30-bus network, the value of important target and the value of system are equally important to the attacker.
According to the calculated comprehensive value of each target from Equation (25), the target value assessment by the comprehensive value preferred attacker is shown in figure 2.

![Figure 2. The target value assessment from the perspective of the comprehensive value preferred attacker](image)

### 3.3 Build the game theory model

In order to construct an optimal allocation model of protective resources based on the game theory model, it is necessary to choose reasonable target vulnerability. The vulnerability is defined as a non-linear continuous function, such as exponential form, ratio form and segmented ratio form. The ratio form is adopted in this case, although it will cause calculation deviation, it greatly simplifies the calculation and facilitates the analysis. The target vulnerability is defined as:

$$ P_i(d_i) = \frac{1}{1 + \beta_i d_i} $$

Where $P_i(d_i)$ is the vulnerability of target $i$ with $d_i$ units of protective resources allocated in power network, $\beta_i$ is defense factor of defense efficiency per unit protection resources, which can be determined by security management perception and experience/expert knowledge\(^\text{[24]}\). It is worth mentioning that due to the confidentiality of defense factor, fictitious data is adopted for defense factor, as shown in table 5. Although the fictitious data may be different from real data, it still meets the needs of case study.

| Site number | Defense factor | Site number | Defense factor |
|-------------|----------------|-------------|----------------|
| G1          | 0.045          | G6          | 0.038          |
| G2          | 0.025          | S1          | 0.03           |
| G3          | 0.035          | S2          | 0.031          |
| G4          | 0.042          | S3          | 0.032          |
| G5          | 0.028          | S4          | 0.04           |

### 3.4 Optimal attack and defense strategy in complete information game

In order to facilitate to compare the distribution of protective resources of each target, in this paper, the total amount of protective resources is set as 500 units to study optimal allocation of protective resources based on game model. Strategy sets are established for both attack and defense sides according to Equation (4) and Equation (8), and the optimal strategy combination is derived from game theory model, that is, Nash equilibrium strategy. The attack and defense strategy combinations are shown in figure 3.
In section 3.2, the comprehensive value evaluation is analyzed, where G1, G6 and G2 have higher comprehensive values of 0.169, 0.135 and 0.115, respectively. Figure 3 shows that in the game model, the defender allocates more protective resources to G2, G1, G6 and S1, which are 84 units, 79 units, 69 units and 68 units, respectively. G3, G4 and S2 are allocated with less protective resources, which are 25 units, 19 units and 13 units. Accordingly, in terms of attack probability of targets, G2, G1 and G6 have a higher probability of being attacked, which are 0.154, 0.126 and 0.119, respectively. Whereas G3, S2 and G4 have a lower probability of being attacked, which are 0.068, 0.058 and 0.054. Therefore, when the attacker attacks a target site, the allocation of protective resources largely depends on the value of the target from perspective of the attacker. It shows that under the game circumstance, the attacker may think that the target with higher value has the priority to obtain more protective resources.

Using game theory method to optimize the allocation of protective resources significantly reduces the risk of being attacked in case of each target site under effective protective measures, as shown in Figure 4.

Figure 3 Optimal strategy combinations under the complete information game scenarios. (b = 500 units)

Figure 4 shows that the initial risk of G1, G6 and S3 is higher, which is 0.169, 0.135 and 0.112, respectively. Under the optimal allocation of protective resources proposed in this paper, the risk of each target site is significantly reduced, the risk of G1 decreases to 0.005, the risk of G6 decreases to 0.004, and the risk of S3 decreases to 0.004. Therefore, the optimal allocation of protective resources based on game theory can greatly reduce the risk value of each site, which is of guiding significance for studying protective resource allocation.

Figure 4 Risk values of each site under optimal allocation of protective resources
4. Conclusions
In reality, urban power network is often threatened by potential attackers. In this study, a game theory method is proposed to optimize the allocation of limited protective resources to reduce the attack risks of key sites in urban power network being hit by malicious attacks. IEEE 30-bus network is taken as an example to carry out the experimental study in order to verify the applicability and reliability of the method. The conclusions drawn are as follows:

1) Combining the game theory and risk assessment, this method is different from conventional methods. It takes full account of strategic interaction between the attacker and the defender.

2) By implementing the game model, this method can access to Nash equilibrium. Nash equilibrium refers to a circumstance where the strategy of both sides is the worst for the opponent, and vice versa. Therefore, using this method, the defender can identify the most unfavorable attack scenarios and find the optimal global defense strategy.

References
[1] Li G.H.(2014) Spatial and Temporal Evolution and Risk Analysis of Global Malicious Attack. Doctor Dissertation, University of Science and Technology of China.
[2] Zhao X.D., Cai H, Chen Z.L. (2016) Assessing urban lifeline systems immediately after seismic disaster based on emergency resilience. Structure and Infrastructure Engineering, 12(12): 1-16.
[3] Cox Jr., L.A. (2009) Game theory and risk analysis. Risk Anal. 29 (8): 1062-1068.
[4] Anton S.I., Gordon H, Daniela L,Bruce K.(2015) Organ Transplantation: An Introduction to Game Theory. Transplantation, 99(7).
[5] Berleur J., Hercheui M.D., Hilty L.M. ed. (2007) What Kind of Information Society? Governance, Virtuality, Surveillance, Sustainability, Resilience. Berlin: Springer-Verlag 328: 363–372.
[6] Pitilakis K, Argyroudis S, Martin C, Alexoudi M, Monge O.(2006) Earthquake risk assessment of lifelines. Bulletin of Earthquake Engineering,4(4):365-390.
[7] Peng D.K., Zhan B, Sun A.J., Liu F, Kui Q. (2010) Risk Analysis of National Electric Power Infrastructure Suffering from Terrorism Attack. Power and Energy Engineering Conference (APPEEC), Asia-Pacific,2010.
[8] McMasters AW, Mustin TM.(1970) Optimal interdiction of a supply network. Naval Research Logistics,17:261–8.
[9] Bier V , Oliveros S , Samuelson L . (2007) Choosing what to protect: strategic defensive allocation against an unknown attacker. J Public Econ Theory,9(4):563–87 .
[10] Cox Jr., L.A.,(2009). Game theory and risk analysis. Risk Anal. 29 (8):1062-1068.
[11] Bier, V.M., Lin, S.W.(2013). Should the model for risk-informed regulation be game theory rather than decision theory? Risk Anal. 33 (2):281-291.
[12] Bier, V.M., Aziaiez, M.N.(2009). Game Theoretic Risk Analysis of Security Threats .Springer, New York.
[13] Chkhartishvili, A.G. (2003). Bayes–nash equilibrium: infinite-depth point information structures. Automation and Remote Control, 64(12):1922-1927.
[14] Cartwright E. ,Wooders M. (2009). On purification of equilibrium in bayesian games and expost nash equilibrium. International Journal of Game Theory, 38(1): pp.127-136.
[15] Myerson, R.B.(2013). Game Theory. Harvard university press, London
[16] Ouyang M, Liu H, Mao Z.J.(2009) A methodological approach to analyze vulnerability of interdependent infrastructures. Simulation Modelling Practice and Theory, 17(5): pp.113-127.
[17] Neumann J.V ., Oskar M.(1944) "Theory of Games and Economic Behavior." princeton university press princeton 26.1-2:131-141.
[18] Powell R.(2007) Defending against Malicious Attacks with Limited Resources. The American Political Science Review, 101(03): 527-541.
[19] Hausken K, Bier V.M. (2011). Defending against multiple different attackers. Eur J Oper Res;211(2):370–84 .
[20] Baykal-Gursoy, M., Duan, Z., Poor, H.V., Garnaev, A., (2014). Infrastructure security games. Eur. J. Oper. Res. 239 (2): 469-478

[21] Gallardo A, Lowther D.A.(2000) Some aspects of niching genetic algorithms applied to electromagnetic device optimization. Ieee T Magn 36:1076-9.

[22] Glover, J. D.(1987) Power Systems Analysis and Design. PWS Publishing Co.

[23] Saaty T.L.(1980)The analytic hierarchy process: Planning, priority setting, resource Allocation. McGraw-Hill, NY, USA[M]/ The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation.

[24] Electric power survey and design enterprise safety production standards and standards for compliance rating.(2014) China electric power press.Beijing.