Determining Defense Optimum Strategy of Power System against the Malicious Attacks using Nash Equilibrium based on Expected Energy not Served

Ali Marjanin and Soodabeh Soleymani

Department of Electrical Engineering, Science & Research Branch, Islamic Azad University, Tehran, Iran

Abstract:
The power system is one of the most important critical infrastructures in every country. Losing this critical network, even for a short time, causes the outbreak of some serious problems and impose the irreparable and destructive damages to the national security, economy, and the citizens' life. This matter causes the power system to be an attractive purpose for terrorist and malicious attacks. Therefore, attackers want to maximally damage the power system, and defenders want to minimize the losses to the system by determining an optimum defense strategy. This strategic behavior between the defenders and attackers has been modeled as a zero-sum game. In this paper, the presented model between the attackers and defenders has been developed based on the expected energy not served (EENS). This new decision-making standard based on EENS will result in better decision-making in comparison to the previous methods. Because some important parameters, including the powerplants features (Maximum Capacity, Derated Capacity States, Forced Outage Rates), and the load features and annual load graph have been considered in this paper unlike the previous papers. The other innovation of this paper is that the game equilibrium point and the best defense strategy have been obtained based on mixed strategy Nash Equilibrium (MSNE). Meanwhile, a new algorithm has been presented based on genetic algorithm for solving MSNE problem and obtaining the optimum strategy. The effect of recovery budget and the calculation of its optimum amount are studied at the end. The algorithm and method presented in this paper are tested by five-bus system, and the operation of the presented method has been proved.

Keywords
Expected energy not served, game theory, mixed strategy Nash equilibrium, power system security, malicious attack

1. Introduction

Since the demolition of power system causes weakening the economic and national security, it is an attractive and appropriate purpose for terrorist and enemy countries which are going to damage the economic, military, and political infrastructures. According to the report of U.S. department of energy, from 1980 to 1989, thirty nine attacks are accomplished every year to the U.S. energy equipment on average, most of which have been accomplished to the power system [1].

Although there is not any other formal report about the malicious attacks, according to the accomplished analyses, the rate of attacks has become more than the past [2]. These attacks can include so many economic effects. For example, in the blackout of November 4th, 2006 in Europe, the power imbalance in the network at western part of union for the coordination of transmission of electricity (UCTE) causes the severe frequency deviation, and the whole network was divided to three separate parts, so the electrification to 15 million home subscribers was disrupted in Europe [3]. On the other hand, the rest of the other critical infrastructures are highly dependent on the power system. For example, in the cross-country power outage of North East America in 2003, the water pressure was loosened because of the pumps' interruption; all of the trains, whose destination was New York, were stopped, mobile connections were disrupted, and the television system was interrupted[4].

These attacks can include the cyber-attacks, confusion, explosive bombs, etc. [5]. According to the importance of the issue, the countries do so many investments to defend the power system as the most important critical infrastructure. But, according to the limited defense budget and the broadness of the power system, this investment must be optimum. One of the first methods to consider the restriction of the security against a normal breakdown is N-1 method [6]. The usual methods, among N-1 or N-K method [7], do not consider the attacker as an intelligent person who can change his own behavior according to the defender's behavior. In [8], Salmeron has presented a bi-level model based on modern analytical methods to evaluate the power system's vulnerability. In that research, some solutions are presented by a new mathematical model and also DC-OPF, and using GAMS software to preserve the vital equipment of system including the transmission lines, transformers,

Manuscript received May 5, 2026
Manuscript revised May 20, 2026
https://doi.org/10.22937/IJCSNS.2026.26.5.8

and generators. In [9, 10], a more generalized model of Salmeron's research is presented. In this study, first, the bi-level model of problem is rectified and improved to a single model, and then it is converted by a single linear-programming model (SLPM) or a more flexible bi-level-programming problem. In [11], the problems of [9, 10] have been converted to a Mixed integer bi-level programming model [MIBP], and a new solution method has been presented. By studying [9-11], it can be observed that, by terrorists' entrance, the powerful power system is even vulnerable against the likely attacks. In current methods, the relation between the attackers and defenders is considered as a situation of decision-making; while considering the fact that there is an intellectual relation between the defenders and attackers, this relation can be modeled as a game. The game theory is used in the strategic situations including electronic market, transportation, and social problems, etc. [12-14].

In [15], by helping Tabu search along with an algorithm, embedded greedy algorithm is introduced in order to solve the problem of the best defense decision. In [16, 17], using the conditions of Karush-Kuhn-Tucker, the bi-level problem is first converted to a single optimization problem, and then the optimum defense strategy is obtained. In [18], first, the knowledge of game theory and its performance on finding the appropriate defense plans against attacks on the power network are introduced. In that research, the problem of seeking the appropriate strategy for defending the network is modeled by a kind of zero-sum game (ZSG), and is solved by solving pure strategy Nash equilibrium. In [17], two new algorithms are presented to obtain the confident strategies for two problems of common defense:

1. When the defenders have a specific budget, how do they devote this validity to apply their own safe strategy?
2. When the defenders want to limit their loss to a determined amount, how much validity do they need?

In the previous studies and models, the presented method is accomplished based on the load flow of system at the moment of attack, and the system features, including power-plants features (Maximum Capacity, Derated Capacity States, Forced Outage Rates), have not been considered, and the loads are assumed to be constant throughout the year[17,19]. This matter causes the defender not to be able to make decisions optimally. So, in this paper, EENS is used as the main index of decision-making for modeling the behavior of the defenders and the attackers. Meanwhile, the features of the generative and load units have been considered. The reliability probabilistic indexes, including EENS, are highly sensitive to the features of power-plants and loads. So, it can be concluded that it is essential to consider the features of power-plants and loads in the game modeling.

In this paper, first, the game between the defenders and attackers is modeled according to EENS index and their probabilistic behavior; then, the relation between attackers and defenders is modeled as a zero-sum game. Considering the mentioned game does not have Nash Equilibrium for the pure strategies, the game between attackers and defenders is modeled as a Mixed Strategy. In the next section, a new method based on Genetic Algorithm is presented to compute MSNE of the game. Then, the equilibrium point is compared in the state of considering and not considering EENS rate and the features of powerplants and loads. Finally, the defenders' behavior is analyzed according to the available budget, and it is studied how the defenders' behavior change through increasing the budget. Also, the effect of allocated budget for reducing the recovery time on the loss to system is studied. The proposed algorithm is simulated for a five-bus system, and the investment strategies are presented to optimally defend these networks.

2. Defender Attacker Modeling

Since the power system is one of the most sensitive infrastructures of every country, it is an attractive purpose for the terrorist attacks or the enemy countries. The reason is that disrupting these critical infrastructures will result in the irreparable economic and social losses to the system. One of the most important elements of power systems is power-plants; in this paper, determining an optimum defense strategy against the physical attacks to this equipment has been studied, and the presented method can be easily generalized to the other kinds of equipment. The power system's defender and attacker are the players who make some intelligent decisions, and these decision-makings are essentially related to each other. In other words, a player's behavior depends on its own decisions and also the rival's. therefore, this strategic relation between the defenders and the attackers is modeled as a game. In this game, the attacker plans to bring the maximum loss to the power system, and on the other hand, the defender tries to minimize this loss. It may include different cases:

- ✓ The loss due to the expected energy
- ✓ The loss caused to the equipment which is not usually significant compared to the first case;
- ✓ The losses with political and social targets
- ✓ The loss due to the repair costs

On the other hand, according to the broadness of power system, a specific budget is devoted to each defender to protect all system components including transmission lines, generators, substations, etc., which must be spent with an intelligent decision to protect and retrieve the power system. Therefore, first, the objective function, which the attacker is going to maximize and the defender to minimize it, should be found. A power system includes N elements (generators, transmission lines, substations, etc.) that each of them may be exposed to malicious attacks. Each of these elements, according to the devoted defense budget, has a degree of protection which can be defined by a parameter named successful protection probability; the more the rate of defense budget for element, the higher its successful protection probability will be. This parameter is shown for element i_{th} as$P_i(C_i)$. Where, C_i is the defense budget rate for element i_{th}, considering this parameter is the successful protection probability of the element, so:

$$0 \le p_i \le 1 \quad i = 1,2,...,N \tag{1}$$

$$p_i(c_i) = \frac{c_i}{c_i + h_i} \tag{2}$$

That:

$$h_i = \begin{cases} 2 & regional\ \ power\ \ gride \\ 3 & generator \\ 4 & power\ \ line \end{cases} \tag{3}$$

the form of the function (2) is selected mainly because it is the simplest function satisfying this condition that increasing the defense budget causes increasing the successful protection probability. Of course, there are many other reasonable functions such as the exponential form ($P_i(C_i) = 1 - e^{-\lambda_i C_i}$).
whereλ_i is a parameter.

Given that this function is suitably fitted to data, we believe that the results are fairly to this choice. the amounts of h_i are obtained according to the survey and the statistical analysis performed in the electric company of Khuzestan in Iran.

It should be noticed that the defender's budget is determined; this budget can be spent for defense of the elements, recovery, or purchasing of equipment to improve the reliability. Here, it is assumed that the total cost would be spent for recovery and protection [19]:

$$\sum_{i=1}^{N} c_i + c_{recovery} = c_{Total} \tag{4}$$

$$M = \binom{N}{2} = \frac{N!}{2!(N-2)!}$$

Where C_{Total} is the total cost of protection.
Considering there are N elements, the protection can be defined as a vector $(P_1, P_2, \ldots, P_N)$. The defender, in addition to increasing the defense probability of system, intends to restore the lost energy and damaged equipment at the shortest possible time. So, with some cost, the defender tries to decrease the recovery time, as follows [19]:

$$t_i = t_i^{base} \times f_i(recovery) \tag{5}$$

$$f_i(recovery) = \frac{k_i}{k_i + c_{recovery}}$$

$$q_j = p\ (the\ \ target\ \ j_{th}\ \ is\ \ attack \mid attack) \tag{6}$$

That:

$$k_i = \begin{cases} 200 & user \\ 300 & generator \\ 100 & power\ \ line \end{cases} \tag{7}$$

Where f_i(recovery) is a function of the cost rate to restore the system; therefore, the higher the budget, the lower the recovery time will be. On the other hand, the distribution or transmission and generation companies can do recovery according to the initial facilities during a determined time shown by t_{base}. Computing t_{bases} is different for various countries depending on the staff preparation, the equipment, and initial investment.

Meanwhile, the amount of this time is different for recovery of substation, transmission line, and transformer. Basic recovery time is one year for the severe losses to the Generator according to the questionnaires given to the staff of electric company in the state of Khuzestan in Iran. The functions of f_i (recovery) and p_i (c_i) are estimated, and it is not possible to obtain an exact experiential function for them.

The attackers can attack N targets including transmission lines, generators, transformers, and substations. The rate of these attacks may be changed; for example, the attacker can attack 1, 2, 3…, N elements. If Q is a set of targets, and M shows the number of them, so:

A: if the attackers attack one target, then:

$$Q = \{i_1, i_2, i_3, ..., i_N\} \quad \text{and} \quad M = N \tag{8}$$

B: if the attacker attack two targets, then:

$$Q = \{\{i_1, i_2\}, \{i_1, i_3\}, \{i_1, i_4\}, ..., \{i_1, i_N\}\} \tag{9}$$

$$\tag{10}$$

And it will be the same for n attacked targets as above, so, the number of targets will be as:

$$M = \binom{N}{n} = \frac{N!}{n!(N-n)!} \tag{11}$$

Now, the attacker can attack each of these targets with a probability, if q_j is defined as the probability of attack to the target j_{th}, so [19]:

$$\tag{12}$$

$$0 \le q_j \le 1 \qquad j=1,2,3,...,N \tag{13}$$

$$\sum_{j=1}^{N} q_j = 1 \tag{14}$$

3. Game Framework

In the previous modeling and studies, the modeling of the defender's loss and the attacker's profit has been accomplished based on the load flow at the moment of attack. The reliability indexes and system features have not been considered in any of the references that studied the behavior of the defenders and attackers to determine the appropriate strategy. For example, the load is assumed to be constant throughout the year, and or, FOR has not been considered for the powerplants. In this section, first, EENS and the reason of its importance for modeling of the behavior between attackers and defenders are explained, and then, the game modeling of defender and attacker is accomplished based on EENS.

3.1. EENS and the reason of its importance for modeling the game between the defender and the attacker

EENS index is the rate of expected energy which is not received by the network consumers because of the insufficient generative power of powerplants. So it can be an appropriate index for comparing the effects of attacks to each piece of the power system equipment. This means that the attacker tends to attack the powerplant that, by omitting it, the rate of EENS will be increased. On the other hand, the rate of EENS index is so sensitive to the parameters of generative units and the load features. In this section, first, the effect of system features on the reliability indexes has been obtained by Monte Carlo method. Considering Monte Carlo method can model more details of the system, it is more accurate than the other methods. To show the sensitivities, the numbers among 0 to 5 are used. The work process is as follows, when the index is not sensitive to the feature change in the system, number 1, and when it has the maximum sensitivity, number 5 will be considered. The rate of EENS sensitivity to the parameters of generative units is obtained by the simulation of an IEEE 5-buses system using Monte Carlo method as it is shown in table I.

As it is clear from the table I, the rate of EENS is highly sensitive to the amounts of MC, DCS, and FOR. So according to the definition of EENS, and considering the load curve, and also, the amount of MC, DCS, and FOR for the powerplants, a more accurate and optimum decision can be made in comparison with the decisions of the previous methods.

3.1.1. Modeling of the game of defenders and attackers based on EENS index and considering the features of load and powerplants

In the game between defenders and attackers, the attacker wants to increase the rate of system EENS after omitting the powerplants. However, the defender tries to minimize this loss using appropriate investment. So, first, the rate of EENS must be obtained according to the load curve and the features of powerplants (MC, FOR, DCS), and also, the limitation of the lines capacity.

To obtain EENS, first, the attacked powerplants must be omitted according to the algorithm of figure 1, and then, after accomplishing load flow in the system, and considering the limitation of lines capacity, the rate of EENS can be computed. As mentioned, the attackers intend to damage the power system to the maximum, while the defenders want to minimize this loss by defense costs. So there is no agreement between the attackers and defenders; the game can be defined as a two-player zero-sum one.

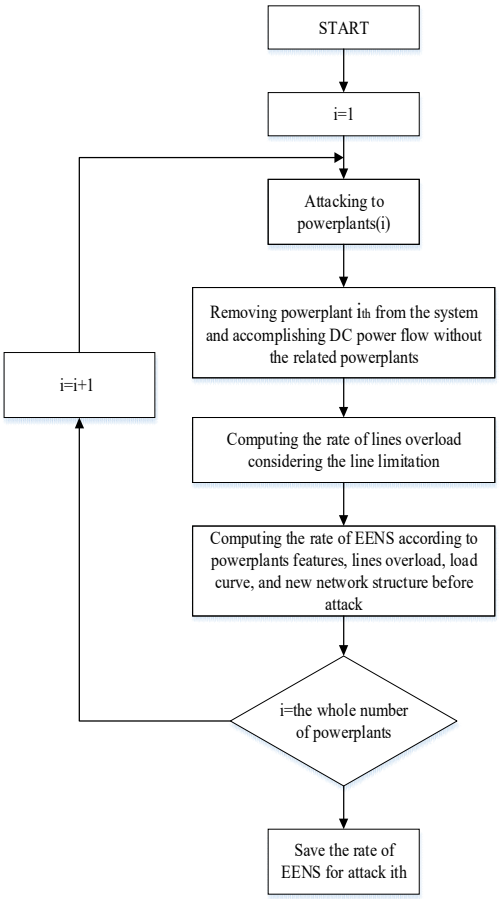

Fig.1.The algorithm of computing EENS after each attack

Considering the above, the competition between the attackers and defenders can be defined as follows:

$$x = \sum_{j=1}^{M} q_j w_j(c) \tag{15}$$

$$w_j(c) = (1 - p_j(c_j)) \times EENS_j \tag{16}$$

Where, $EENS_j$ is the expected energy not served because of attacking the generator i_{th}.

If the number of attacks is more than one, the above formula will be extended as follows:

$$\begin{aligned} w_j(c) &= (1 - p_{i_1}(c_{i_1}))...(1 - p_{i_n}(c_{i_n})) \times EENS\{i_1,...,i_n\}... \\ &+ (1 - p_{i_1}(c_{i_1}))...(1 - p_{i_{n-1}}(c_{i_{n-1}})) \times (p_{i_n}(c_{i_n})) \times EENS\{i_1,...,i_{n-1}\} + ... \\ &+ (1 - p_{i_2}(c_{i_2}))...(1 - p_{i_n}(c_{i_n})) \times (p_{i_1}(c_{i_1})) \times EENS\{i_2,...,i_n\} + \\ &... + (1 - p_{i_1}(c_{i_1})) \times (p_{i_2}(c_{i_2}))...(p_{i_n}(c_{i_n})) \times EENS\{i_1\} \end{aligned} \tag{17}$$

Now, the defenders intend to minimize the function X, and the attackers to maximize it:

$$\max_{q}\left[\min_{c}\sum_{j=1}^{M} w_j(c).q_j\right] \tag{18}$$

For an attack including one element, (19) is obtained as follows:

$$\max_{q}\left[\min_{c}\sum_{j=1}^{M}(1-p_j(c)).EENS_i.q_j\right] \tag{19}$$

And for each attack including (n) elements, (19) is obtained as follows:

$$\begin{aligned} w_j(c) = \max_{q}[\min_{c}(1-p_{i_1}(c_{i_1}))...(1-p_{i_n}(c_{i_n}))\times EENS\{i_1,...,i_n\}... \\ +(1-p_{i_1}(c_{i_1}))...(1-p_{i_{n-1}}(c_{i_{n-1}}))\times(p_{i_n}(c_{i_n}))EENS\{i_1,...,i_{n-1}\}+... \\ +(1-p_{i_2}(c_{i_2}))...(1-p_{i_n}(c_{i_n}))\times(p_{i_1}(c_{i_1}))\times EENS\{i_2,...,i_n\}+ \\ ...+(1-p_{i_1}(c_{i_1}))\times(p_{i_2}(c_{i_2}))...(p_{i_n}(c_{i_n}))\times EENS\{i_1\}] \end{aligned} \tag{20}$$

4. The Proposed Algorithm

In the proposed method in this paper, the relation between the attackers and defenders is modeled as a game, and considering the players play completely greedily, in order to solve this problem, MSNE is proposed. To find MSNE, a genetic algorithm is used. MSNE problem is one of the most complicated subjects in the optimization. In fact, finding Nash equilibrium point for the mixed strategy for the related game has been nonlinear and non-cooperative. So genetic algorithm is an appropriate solution to solve the problem. In this section, first, the genetic algorithm and MSNE are explained, and then an algorithm is presented for combining these two methods in order to solve the attackers – defenders problem.

4.1. Genetic Algorithm

The genetic algorithm is an optimization method which uses Darwin's principle of natural selection to find the optimum formula. In genetic algorithm, first, some answers are produced to solve the problem recognized as the initial population, and each answer is recognized as a chromosome. Then, the appropriate number of chromosome pairs are selected according to their fitness rate to be used at the later steps. The chromosome, with higher fitness number, may be selected at the production steps several times, and then cross-over with p (e) probability would be applied on the parents' chromosomes, and by composing them, new chromosomes will be produced.

Afterwards, the mutation with P (m) probability would be applied on the chromosome resulted by cross-over, and will provide a new way for new information by changing the number of chromosomes. Then fitness rate of new chromosomes are calculated in order to evaluate the children, and the new population is produced and evaluated. This process continues until the final condition of the algorithm is provided. In figure 2, the process of genetic algorithm is shown.

4.2. Nash equilibrium

Nash Equilibrium point has been defined by John Nash as a solution for two or N-players games. John Nash, by presenting this concept, tried to state that it is impossible to predict the result of a relation between several decision-makers without considering their being together. It is assumed that a player knows the strategies and pay-off of the other players, and he can obtain some pay-off just via his own choices and without directed imposition on the others'. Nash equilibrium can be defined as follows: Nash equilibrium is a point at which none of the players can earn more profit by changing their own strategy when the performance of the other players is fixed. In other words, x_i is a Nash equilibrium point, if for each of the players we have :

$$\begin{aligned} &\forall\, i : u_i(x_1^*, x_2^*,..., x_i^*,..., x_n^*) > \\ &u_i(x_1^*, x_2^*,..., x_{i\ 1}^*, x_i, x_{i+1}^*,..., x_n^*) \end{aligned} \tag{21}$$

Where x_i means that the player x_i is removed from the equilibrium point, and it will certainly lose. The aim of presenting this paper is to obtain a strategy in which, if each of the players (attackers and defenders) change his strategy, he will lose; and this is precisely the concept of Nash equilibrium point

In the games in which the players play completely greedily, the games don't have Nash equilibrium point for the pure strategy and the concept of mixed strategy Nash equilibrium (MSNE) will be defined for these games, which it has been completely explained in 4.2.1.

4.2.1) Mixed strategy Nash equilibrium

MSNE, in fact, follows the same mentioned Nash concepts, the difference is that the obtained equilibrium is defined for mixed strategy. In this situation, a probable factor has been determined for each of the allowable pure strategies, defined as a mixed strategy, and the game equilibrium is here named MSNE.

A mixed strategy profile in an N player game is $\alpha = (\alpha_{1,},..., \alpha_N)$ where $\alpha_i$is a vector of probabilities over the actions of player i(i = 1,..., N). Each element of α_i assigns a probability to the actions of one player i.

A mixed strategy profile $\alpha^* = (\alpha^*_1, ...,, \alpha^*_N)$ is a Nash equilibrium of a strategic game if for every i = 1,..., N. , if:

$\forall \alpha_i \in L_i: \quad u_i(\alpha^*) \geq ui(\alpha i, \alpha_{\neg i}^*)$
(22)

Considering that it is difficult to obtain MSNE, the problem can be first defined as follows:
A player's expected payoff to the mixed strategy profile, $\alpha = (\alpha_1,...,\alpha_N)$ is a weighted average of his expected payoffs when he plays his pure strategies. The weights are the probabilities assigned to each pure strategy:

$$u_i(\alpha) = \sum_{\alpha i \in Ai} \alpha_i(a_i).ui(ai, \alpha_{\neg} i)$$
(23)

Then, to obtain MSNE, the following proposition which makes it easy to compute MSNE has been used:

A mixed strategy profile $\alpha^* = (\alpha^*_1,...,\alpha^*_N)$ is an NE in a game with vN-M preferences in which each player has finitely many actions if and only if for every i = 1,...,N.

I) $U_i(a_i, \alpha^*_{\neg i}) =$ Constant $\forall a_i \in A_i$ and $\alpha^*_i(a_i) > 0$ this constant is $U_i(\alpha^*_i)$
(24)

II) $U_i(a_i, \alpha^*_{\neg i}) \leq U_i(\alpha^*_i) \quad \forall a_i \in A_i$ and $\alpha^*_i(a_i) = 0$ (25)

Therefore, a necessary and sufficient condition for a mixed strategy profile to be an NE is to make players indifferent over the pure strategies appearing in the mixed NE with positive probabilities. These pure strategies also should be at least as good as any other pure strategies (which are not part of the mixed NE).

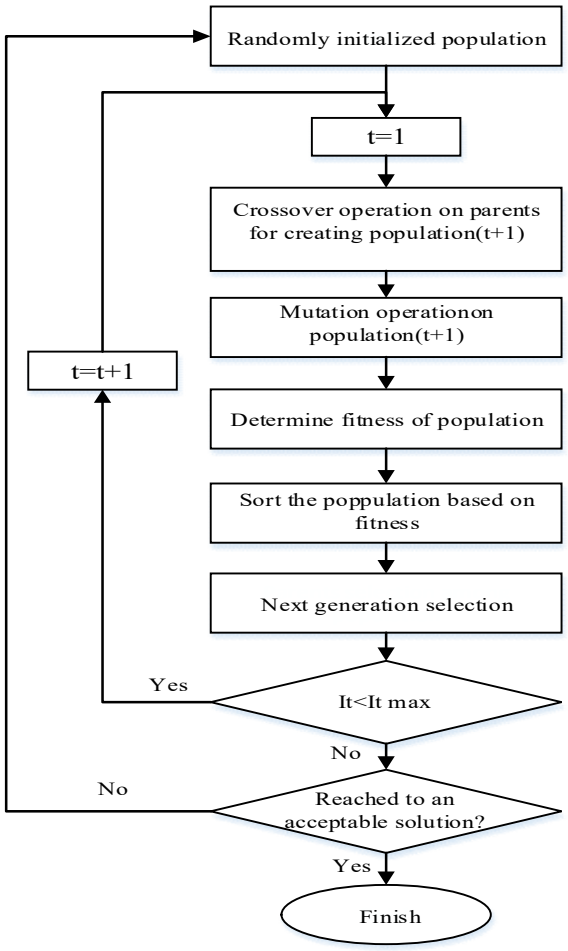

Fig. 2. The Structure of Genetic Algorithm

4.3. The Proposed Solution Method

As mentioned, the game between attackers and defenders of power system does not have Nash Equilibrium for the pure strategies, because the players act very greedily (which can be proved by solving the equation 23 for the game), and so the optimum solution for the above game will be a Mixed Strategy. In this game, also, each of two players determines its own strategy according to the opponent's action, and meanwhile, the power system structure and the budget rate of defenders and attackers also affect determining Mixed Strategy Nash Equilibrium. However, the game between defenders and attackers is a zero-sum one, and the rate of defender's expected payoff is equal to the negative one of the attacker. In this game, the attacker wants to maximize the loss to the system, while, the defender intends to minimize this loss by making an appropriate decision on investment planning.

According to the functions related to the rate of the lost power, the appropriate defense probability, and the recovery time defined in the previous section for defenders and attackers, the expected payoff related to the defender and attacker can be defined based on the equations 26 and 27.

$$u(qi) = \sum_{j=1}^{n+1} p_j (EENS_i.(1\neg\frac{c_i}{c_i+4}).t_i) \quad (26)$$

$$u(pi) = \sum_{j=1}^{n} q_j (EENS_i.(1\neg\frac{c_i}{c_i+4}).t_i) \quad (27)$$

Where, U (qi) is equal to the attacker's expected payoff, and U (pi) is equal to the defender's. The vector P is a probability vector for Mixed Strategy related to the defender; this means that it is the probability made by the defender for each of the lines or the cost of system recovery.

The rate of $EENS_i$ will be equal to the rate of the expected energy not served because of attacking the generator $i_{th,}$ and this rate is obtained from the algorithm of figure 1. In this game, first, the defender obtains his Mixed Strategy. There is a difference between this game and the usual mixed games, that is to say, the probability rate selected by the defender affects the amount of each game's expected payoff. The attacker's game probability is obtained based on the payoff determined by the defender's probabilities. To obtain Mixed Strategy, equations 25-26 are used, which is completely shown on algorithm in figure 3. As mentioned, the attacker intends to maximize the loss to the system, while the defender wants to minimize this loss. Since the game does not have Nash Equilibrium based on the pure strategies, it has a Mixed Strategy Nash Equilibrium, and the defenders and attackers will play based on the expected payoff obtained in part 1.

In this paper, to obtain Mixed Strategy Nash Equilibrium, a Genetic Algorithm is used, which is the first time that an intelligent algorithm is used to obtain MSNE. The proposed algorithm, in this paper, is shown in figure 3 to solve the problem of determining the defense optimum strategy.

As it can be seen in figure 3, in this algorithm, first, two separate populations are selected for P and q, which represent the mixed game for the defender and the attacker respectively; in these populations, each person is shown by Pi and qi, and their genes are also shown by P_{ij} and q_{ij}. The number of pi genes is equal to L, and the number of qi genes is equal to L, which l is the number of lines exposed to attack.

At first, the expected payoff of the attacker, which is dependent on P_{ij}, is obtained, and then the expected payoff amount of the defender is obtained according to formulas 21-26. In the next step, it will be checked by the algorithm whether the obtained strategy has necessary conditions for MSNE. These two conditions are:

First, The Rate of the expected payoffs in the rows, which represent the defender's utility in the game and considering that the result of the game for P in those rows is not zero, must be equal and more than the expected payoffs of the other rows.

Second, previous conditions must exist for the attacker, too. This algorithm will be repeated until MSNE is finally obtained.

5. Case Study

In this paper, the generators are just studied, while the generality of the issue and method is not reduced, and this proposed method can be generalized to the other items of equipment. Meanwhile, the rate of loss due to power insecurity has been assumed much higher than the damage to the equipment. In this paper, the studies are accomplished on a 5-bus system [19].

The assumed five-bus system is shown in figure 4. This system includes 5 buses and 6 transmission lines. The network of five bus system is shown in figure 4 considering power base of 100 MVA, voltage base of 138 KV, and capacity line of 100 MW. All generators produce power from zero to 150 MW.

In this paper, this system is used as the test system. The reactance of the lines is illustrated based on the power 100MVA and voltage 138KV as per-unit.

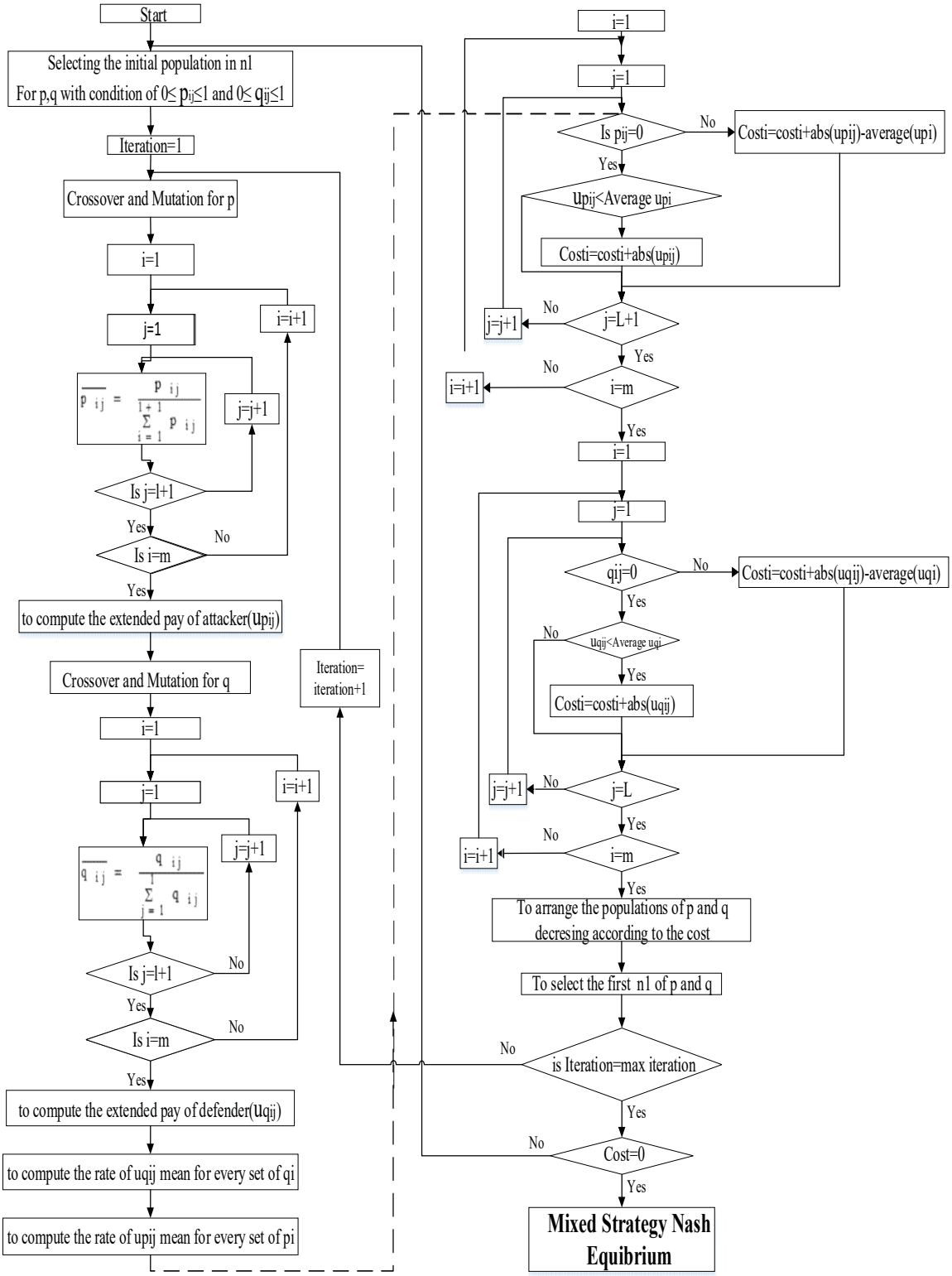

Fig.3. proposed Genetic Algorithm for solving MSNE problem

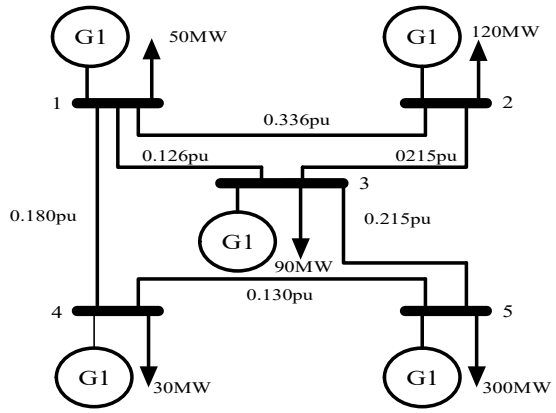

Fig.4. Five-Bus System [19]

The annual inverse load duration curve has been assumed for each load of the system according to per-unit as is shown in figure 5, that the base load is 0.5 per unit and the maximum amount of load is 1 per unit. Using the algorithm of figure 1, the EENS rate can be obtained in the case of attacking each of the powerplants. It is worth mentioning that, because of the similarity of the powerplants, the time of repair and recovery is assumed to be the same for all of them. The rate of Expected Energy Not Served is shown in table II, when there is not yet any defense on power system. Also, the rate of the expected energy loss is shown in table II, when the powerplants features have not been considered, and the load has been assumed to be constant throughout the year.

In this paper, the amount of EENS, which is one of the reliability indexes, is used for the states in which the load features including the graph of annual load, and the powerplants features including FOR and the maximum and minimum amounts of generative power have been considered. The expected energy loss is used for the states in which the load features and generative units have not been considered, and so the powerplants are considered non-stop, and the load has been assumed constant. It means that the load distribution has been done at the moment of attack, and the omitted power has been multiplied in the recovery time. For example, when attacking to the generator 1 and then losing it, if the powerplants are assumed with no loss, and the load graph is not considered, we will not have lack of energy. But this is far from the reality, because by damaging the powerplant 1, the other powerplants (2, 3, 4, 5 and 6) will be available based on FOR, and they will not be sometimes available because of the force outage. So we will have the lack of energy. As it is clear from the table II, the amount obtained for these two states is so different, and therefore, it will effect on the defender decision.(the difference between EENS and Expected Energy Loss, in terms of the mathematical computations, has been also obtained in appendix).

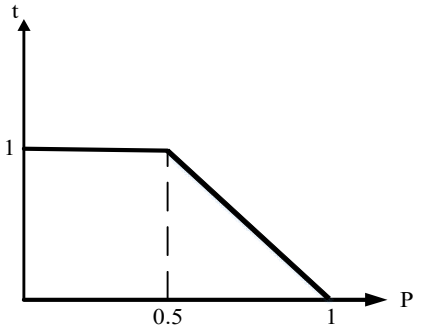

Fig.5. The assumed inverse load duration curve for each load of the system according to per units

As it is seen in table II, at the first state, the rate of EENS is obtained by considering the features of powerplants and loads, and at the second state, the rate of the expected energy loss is obtained without considering the features of powerplants and load, and these two rates are so different from each other because the rate of the expected energy loss is much less than the rate of EENS. It is worth mentioning that the EENS index, as the index of reliability, is more accurate than the expected energy loss. The rates of EENS and expected energy loss are used in the modeling of the defender's and the attacker's behavior. Therefore, not considering the features of power plants and loads and not computing the rate of EENS can cause making a decision which is so different from the optimum decision, and this will cause so much loss to the system.In table III, the rate of MSNE is obtained for two mentioned states according to the amounts obtained for the loss to the system when attacking each of the powerplants (table II), and using the equations (20, 26, 27) and applying the genetic algorithm of figure 3. Considering the rate of the expected energy loss for modeling and using the features of the system, the attacker will attack the generators 3, 4 and 5 by the probability of 0.428, 0.332 and 0.24, and on the opposite side, the defenders will select the generators 3, 4, and 5 to defend them by the probability of 0.139, 0.336, and 0.525. In this state, the amount of loss to the system is equal to 0.1224 in terms of the energy not served. But if we don't consider the powerplants and load features, considering the

defender imagines that, just when attacking generator 5 (table II), the system will be involved in the lack of energy, he will allocate his all defense budget to defend the generator 5. While the attacker will attack the generators 3, 4 and 5 by the probability of 0.428, 0.332 and 0.24. In this state, considering the defender's decision is not optimum, the amount of loss to the system is equal to 0.1649 in terms of the energy not served. As seen in table III, if EENS index and the features of powerplants and loads for modeling and defense decisions are not used, the system will be exposed to the loss which is 0.0425 PU more than the state in which EENS index and the features of powerplants and loads are considered.

The main purpose of using the genetic algorithm is to solve the complicated non-linear and non-cooperative equations, but it is worth mentioning that using the genetic algorithm for optimization causes that the speed of computations for computing MSNE will be more rapid than the mathematical methods. The time of simulation, analyzed by the mathematical methods, is 159 s. While the time of simulation which has been obtained by proposed GA is 35 s, and this shows the speed of proposed algorithm in comparison with the current mathematical methods. When increasing the budget, the expected payoff rate of the defender (the rate of loss to the system) will be reducing until the budget increase does not affect the expected payoff decrease any more. In fact, this is the point in which the budget increase is not economically effective in the solution proposed by MSNE to reduce the expected payoff, and the budget increase does not noticeably affect the expected payoff reduction. In table IV, the rate of the expected payoff has been shown for the different budgets. As is observable from figure 6, after increasing the budget to 120, a considerable decrease in the expected payoff will not be observed, and this means that, based on the strategy obtained by MSNE, the optimum budget needed for a defense strategy is equal to 120. By investing for recovery, the rates of EENS and the expected payoff of the system will be reduced. In table V, the rate of the expected payoff for the different budgets has been presented with and without considering the cost for reducing the recovery time. As it is seen in table V, the expected payoff will be noticeably decreased by investing to reduce the recovery time. Therefore, it can be concluded from this table that the investment to reduce the recovery time is so important in reducing the defenders' loss.

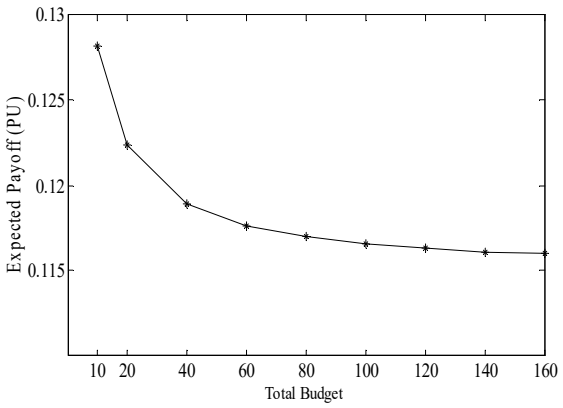

Fig.6 .relation between the rate of the expected payoff and the total budget devoted to defense

Table .II. Expected energy not served and Expected Energy Loss for Each Attack without Defending

Target			considering EENS and the features of powerplants and loads for modeling	without considering EENS and the features of powerplants and loads for modeling[19]
Generator			Expected energy Not served(MWh)	Expected energy loss(MWh)
number	Maximum Capacity	Forced Outage Rates		
1	150	0.2	557670	0
2	150	0.5	444880	0
3	150	0.1	693206	0
4	150	0.1	894691	0
5	150	0.4	1240364	876000

In table VI, it is proved that the defenders, in their planning for the defense budget, must allocate a budget to reduce the recovery time to decrease the amount of the expected payoff. However, this investment should also be purposeful until the allocated budget includes less amount of the expected payoff. So, first, all of the scenarios which the defender may have for his own budget should be obtained (for example: for the budget of 20, the defender can allocate all of the budget for protecting the generators, or allocates it equally to physically protect and reduce the recovery time, or can allocate all of the budget to reduce the recovery time). Then, the defender obtains the amounts of the expected payoff and MSNE for each scenario, and, he selects the best one by comparing the amount of the expected payoff for each scenario. In table VI, the amounts of the expected payoff for different total budgets and the scenarios related to each of them, and finally, the best scenario for investment for different total budgets have been presented. for example, for the defense budget of 20, the best scenario is to allocate the half of the budget to the physical defense, and the rest is allocated to decreasing the recovery time. (in this paper, the investment unit is considered 10, which it can be simply changed.)

Table. III. The defense and attack probabilities computed by MSNE with and without considering EENS and the features of powerplants and loads for modeling

	Defense and attack probabilities computed by MSNE with considering EENS and the features of powerplants and loads for modeling					Defense and attack probabilities computed by MSNE without considering EENS and the features of powerplants and loads for modeling[19]				
	Defender			Attacker		Defender			Attacker	
Generator	Probability of defense strategy	Budget	Successful defense probability	Attack probability	Expected energy Not served(PU)	Probability of defense strategy	Budget	Successful defense probability	Attack probability	Expected energy loss(PU)
3	0.139	2.77	0.48	0.428	0.1224	0	0	0	0.428	0.1649
4	0.336	6.72	0.69	0.332		0	0	0	0.332	
5	0.525	10.51	0.78	0.24		1	20	0.87	0.24	

Table .IV. The amount of expected payoff for different budgets

	Total budget								
	10	20	40	60	80	100	120	140	160
Expected payoff(PU)	0.1282	0.1224	0.1189	0.1176	0.1170	0.1166	0.1163	0.1161	0.1160

Table. V. Defense and attack probabilities computed by MSNE with considering different budgets for defense

		Defense and attack probabilities computed by MSNE with considering EENS and the features of powerplants and loads for modeling				Expected payoff without considering $C_{recovery}$ (PU)	Expected payoff with considering $C_{recovery}$ (PU)						
		Defender			Attacker								
Total budget	generator	Probability of defense strategy	Budget	Defense probability	Attack probability		Budget for recovery						
20	3	0.139	2.77	0.48	0.428	0.1224	**10**	**20**	**30**	**40**	**50**	**60**	**70**
	4	0.336	6.72	0.69	0.332		0.1184	0.1147	0.1113	0.1080	0.1049	0.1020	0.099
	5	0.525	10.51	0.77	0.24								
40	3	0.139	5.55	0.65	0.428	0.1189	**20**	**30**	**40**	**50**	**60**	**70**	**80**
	4	0.336	13.44	0.82	0.332		0.1115	0.1081	0.1049	0.101	0.0991	0.0964	0.0939
	5	0.525	21.01	0.88	0.24								
80	3	0.139	11.1	0.79	0.428	0.1170	**20**	**30**	**40**	**50**	**60**	**70**	**80**
	4	0.336	26.88	0.90	0.332		0.1097	0.1063	0.1032	0.1003	0.0975	0.0948	0.0923
	5	0.525	42.02	0.93	0.24								
120	3	0.139	16.64	0.85	0.428	0.1163	**20**	**30**	**40**	**50**	**60**	**70**	**80**
	4	0.336	40.32	0.93	0.332		0.1090	0.1057	0.1026	0.0997	0.0969	0.0943	0.0918
	5	0.525	63.04	0.95	0.24								

Table. VI .The amounts of the expected payoff for different total budgets and the scenarios related to each of them

Total budget	Scenario for investment		Expected payoff (PU)	The best scenario	
	Budget for defending the Generator	Budget for recovery		Budget for defending the Generator	Budget for recovery
20	0	20	0.1616	10	10
	10	10	0.1240		
	20	0	0.1224		
30	0	30	0.1567	20	10
	10	20	0.1201		
	20	10	0.1184		
	30	0	0.120		
40	0	40	0.1521	20	20
	10	30	0.1165		
	20	20	0.1147		
	30	10	0.1162		
	40	0	0.1189		
50	0	50	0.1477	30	20
	10	40	0.1131		
	20	30	0.1126		
	30	20	0.1113		
	40	10	0.1151		
	50	0	0.1182		

6. Conclusion

Defending the power system, as one of the most significant critical infrastructures, is so important for the countries. But considering the broadness of power system and also the limitation of the determined budget, requiring an optimum strategy for defense investment is of a great importance. Because the relation between defenders and attackers is modeled as a strategic relation, each one's decision- making will not be correct without considering another's decision. So, the game theory is used as an appropriate solution to this strategic problem. In this paper, since it has been proved that the game does not have Nash Equilibrium for the pure strategy, the game has been solved based on MSNE. The noticeable point is that a genetic algorithm has been also used for computing MSNE, which will increase the speed of computing MSNE, and will increase the speed of computing for more complicated systems. Solving MSNE problem with the help of this Genetic Algorithm has provided an appropriate strategy for investment in the power system lines. The results show that the appropriate defense strategy of power system, which has been obtained based on MSNE and according to the attacker's behavior, causes reduction of the loss to system. Increasing the defender's budget will decrease his expected payoff, but the results show that this budget increase should be optimum, because after increasing the budget to a determined rate, the amount of the expected payoff will not have considerable change, and the investment, more than this amount, will not be economically effective.

On the other hand, considering the probability of appropriate defense for each generator, according to the budget determined for it in the mathematical model, it causes more appropriate defense decision-making. Also, it is proved that the allocation of budget for reducing the recovery time causes reducing the expected payoff, and the optimum strategy for the defender has been obtained by considering the budget allocated for reducing the recovery time. In addition, the results show that not considering the

features of powerplants and loads will lead to a decision which is not the optimum one. Therefore, the method presented in this paper for using EENS and the features of powerplants and loads have been proved for modeling.

APPENDIX

the rates of EENS and Expected Energy Loss, which present two different concepts for the energy not served, are obtained by the equations (a- f).

EENS=(X-R).P(R).t

(a)

that:

X=system outage capacity

R=C-L=system reserve capacity

C=system effective capacity

L=maximum load

P(R)= The probability of reservation

Expected Energy Loss=f×t

$f= \min_{j \in load} C_j$

$\sum_{i \in generator} p_i - \sum_{j \in load} c_j - \sum_{j \in lods} d_j = 0$

(b)

That:

p_i:the generated power for generator node i

C_j : the shed load for load nod j

d_j:the initial load of j.

this minimization is implemental with the following constraints:

$0 \leq p_j \leq p_{jmax}$

(c)

$-p_{lmax} \leq p_l \leq p_{lmax}$

(d)

$0 \leq c_j \leq d_j$

(e)

$-\delta \leq \delta_n \leq \delta$

(f)

Where the condition (c) shows the limitation of generators' generative power; the condition (d) shows the limitation of power flow capacity in the lines; the conditions (e) shows the limitation of load shed power; the condition (f)shows the limitation of buses angle.

Reference:

[1] Congress, U. S. *Office of Technology Assessment. Physical vulnerability of electric system to natural disasters and sabotage*. OTA-E-453, Washington, DC: US Government Printing Office, 1990.

[2] Bompard, Ettore, et al. "Classification and trend analysis of threats origins to the security of power systems." *International Journal of Electrical Power & Energy Systems* 50 (2013): 50-64.

[3] Mass GA et al. system disturbance on 4 November 2006.Final, report; 2007.

[4]US-Canada Power System Outage Task Force. (2004) Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and recommendations; 2004 April.

[5] Fovino, Igor Nai, et al. "Cyber security assessment of a power plant." *Electric Power Systems Research* 81.2 (2011): 518-526.

[6] Ren, Hui, Ian Dobson, and Benjamin A. Carreras. "Long-term effect of the n-1 criterion on cascading line outages in an evolving power transmission grid." *Power Systems, IEEE Transactions on* 23.3 (2008): 1217-1225.

[7] Arroyo, José M., and Francisco D. Galiana. "On the solution of the bilevel programming formulation of the terrorist threat problem." *Power Systems, IEEE Transactions on* 20.2 (2005): 789-797.

[8] J. Salmeron, K. Wood, R. Baldick, “Analysis of Electric Grid Security under Terrorist Threat”, *IEEE Trans. Power Syst*. vol. 19, no. 2, may (2004).

[9] Motto, Alexis L., José M. Arroyo, and Francisco D. Galiana. "A mixed-integer LP procedure for the analysis of electric grid security under disruptive threat." *Power Systems, IEEE Transactions on* 20.3 (2005): 1357-1365.

[10] Åke J. Holmgren, “Quantitative Vulnerability Analysis of Electric Power Networks”, PhD Thesis, Royal Institute of Technology, Stockholm, Sweden, (2006).

[11] Arroyo, José M., and Francisco D. Galiana. "On the solution of the bilevel programming formulation of the terrorist threat problem." *Power Systems, IEEE Transactions on* 20.2 (2005): 789-797.

[12]Soleymani, S. "Bidding strategy of generation companies using PSO combined with SA method in the pay as bid markets." *International Journal of Electrical Power & Energy Systems* 33.7 (2011): 1272-1278.

[13] Bell, Michael GH. "The use of game theory to measure the vulnerability of stochastic networks." *Reliability, IEEE Transactions on* 52.1 (2003): 63-68.

[14] Dabbagh, Saeed Rahmani, and Mohammad Kazem Sheikh-El-Eslami. "Risk-based profit allocation to DERs integrated with a virtual power plant using cooperative Game theory." *Electric Power Systems Research* 121 (2015): 368-378.

[15] Romero, Natalia, et al. "Investment planning for electric power systems under terrorist threat." *Power Systems, IEEE Transactions on* 27.1 (2012): 108-116.

[16] Arroyo, José M., and Francisco D. Galiana. "On the solution of the bilevel programming formulation of the terrorist

threat problem." *Power Systems, IEEE Transactions on* 20.2 (2005): 789-797.
[17] Holmgren, Åke J., Erik Jenelius, and Jonas Westin. "Evaluating strategies for defending electric power networks against antagonistic attacks." *Power Systems, IEEE Transactions on* 22.1 (2007): 76-84.
[18] Bricha, Naji, and Mustapha Nourelfath. "Critical supply network protection against intentional attacks: a game-theoretical model." *Reliability Engineering & System Safety* 119 (2013): 1-10.
[19] Chen, Guo, et al. "Exploring reliable strategies for defending power systems against targeted attacks." *Power Systems, IEEE Transactions on* 26.3 (2011): 1000-1009.

SoodabehSoleymani
Received the Ph.D. degree in electrical engineering from the Sharif University of Technology, Tehran, Iran, in 2007.
She is now an Associate professor of science and research branch, Islamic Azad University, Tehran, Iran. Her research interest includes Electric machines, Generation and Transmission expansion planning; Electricity Market and Energy Audit.

Ali Marjanian born in Shahrekord, Iran. He received the degree in Electrical Engineering from the University of Shahrekord, Iran, in 2008, and received the M.Sc degree in Power systems from the Islamic Azad University of Dezfol, Iran, in 2011. Now, he is PHD student at the Department of Electrical Engineering, Islamic Azad University of Science & Research. His interests include FACTS devices, transient stability, game theory, optimization, reactive power compensation, and power distribution systems.