THE ANALYSYS OF INFORMATION IMPACTS IN COORDINATING DEFENCE AGAINST MALICIOUS ATTACKS FOR INTERCONNECTED POWER SYSTEMS

Ettore Bompard
Politecnico di Torino
ettore.bompard@polito.it

George Gross
University of Illinois
gross@uiuc.edu

Roberto Napoli
Politecnico di Torino
Roberto.Napoli@polito.it

Fei Xue
Politecnico di Torino
fei.xue@polito.it

Abstract – In the analysis of power systems security recently a new concern related to possible malicious attacks caught much attention. Coordination among different system operators (SO) in an interconnected power system to counteract such attacks has become an important problem. This paper presents a specific model for the analysis of information impacts in handling on-line security after a malicious attack. The model is based on the socially rational multi-agent systems and the equilibrium of a fictitious play is considered to analyze the impacts of various levels of information available to the interconnected system operators on the outcomes of the decision making process under attack. A 34-buses test system, with three systems interconnected by tie-lines, is presented to illustrated the model and compare the impacts of different information scenarios.

Keywords: Homeland security, malicious attack, power system security, interdiction, multi-agent systems

1 INTRODUCTION

Many existent studies have focused on the problem of terrorist attacks against power systems. These efforts mainly concern the defense problems with reference to the physical components of power systems resorting, for example, to strategy interactions in game theory [1] or bilevel programming problems [2][3][4]. At the same time, the importance of cyber risk assessment in the electric power industry has been recognized [5]. However, there are two main problems that have not been specifically addressed.

Firstly, the physical behaviors of power system and the information availability under malicious attacks have generally been studied separately or from different perspectives in contrast to a joint analysis. There is still inadequacy of systematical and mathematical methodologies for taking into account the interaction between the timely communication of information and the physical behaviors of power systems. Secondly, system operators are assumed able to perform certain corrective actions under attack to minimize the impacts often without taking into account the decision making chain and the coordination among autonomous system operators with the inherent human and organizational factors which may make the best feasible solution, in theory, not viable, in practice, due to the rational and self-interest behavior in the coordination.

Compared with much traditional security analysis focusing on physical characteristics of power systems, information exchange has been considered more and more critical, especially in the problem of coordination of interconnected power systems. The possible security-related real time data to be exchanged have been described, at least in Europe, by the UCTE (Union for the Co-ordination of Transmission of Electricity) operation handbook [6].

Meanwhile, multi-agent systems (MAS) have been widely applied in different fields of power system [7]. However, most of these works are "prescriptive" [8] which utilize MAS as a complex adaptive system to perform distributed control. Another promising direction of MAS referred as "descriptive" [8] which asks how nature agents learn in the context of other agents is also important for power system applications. The goal is to investigate formal models that agree with people's behavior or other natural agents to reveal problems and characteristics of the analyzed process. Some former works [9][10] have attempted to do such works related to power system security coordination.

In this paper, a model based on multi-agent system (MAS) and fictitious play to evaluate the impacts of information about active power flow in different information scenarios, when coordinating the defense of interconnected power system against malicious attacks, is introduced. In contrast with traditional security analysis focusing on physical infrastructures, we stress the analysis of the impacts from the dimensions of information and decision making.

The rest of the paper is organized as follows. The next section introduces the MAS model about decision making under various information scenarios; section 3 discusses how to analyze information impact; all proposed methods are applied in a 34-buses test system in section 4; the conclusions are drawn in section 5.

2 DECISION MAKING MODEL OF INTERCONNECTED POWER SYSTEM UNDER VARIOUS INFORMATION SCENARIOS

For the independent SOs, who have the obvious features of rationality, intelligence, self-interest and decision making abilities, the most important issue in response to a malicious attack is to coordinate their decisions to be optimal or acceptable for the whole system and viable for each decision maker.

In MAS, a variety of protocols and structures have been developed to address the coordination problem. They range from long-term social laws, through medium term mechanisms such as Partial Global Planning, organizational structuring and market protocols to one-shot (short-term) mechanisms like the Contract-Net Protocol [11]. Each coordination mechanism should be selected according to the characteristics of the tasks in hand [11]. Here we will resort to socially rational agents [12] as the coordination mechanism in the decision making of distributed SOs. Decentralized socially rational agents have been proved to make coordinated actions by still performing in self-interest manner [13]; the result is a balance between self-interest and cooperation.

2.1 Structure of the Interconnected System and States

The system is composed of n different subsystems interconnected by tie-lines with each other. We define n different agents to represent the independent operators of the subsystems.

Let each agent:

- get information about its local system (such as the active power flow of all transmission lines);
- get information about the other systems;
- determine which action to perform on its local system, based on the maximization of an objective that represents its utility.

The environment consists of the interconnected power system which is simulated using a DC power flow model.

From a conceptual point of view, the key aspect in determining the network impact of any special scheme is the active power flow; of course a more detailed analysis in terms of a detailed analysis of the network and of its dynamics can be included in the model.

There are some traditional and classic methods to classify power system states; in this model we classify the system states in: *Secure state* (no line overloaded); *Emergency state* (at least one line overloaded).

The states transition diagram is shown in Figure 1. Both Secure and Emergency states comprise different operative configurations characterized by different power flows, generation and load distribution. With a given topology, if all power flows in the transmission lines are within the maximum limits, we call a specific distribution of all w_b and d_b ($b \in \mathcal{B}$) as a feasible operative configuration.

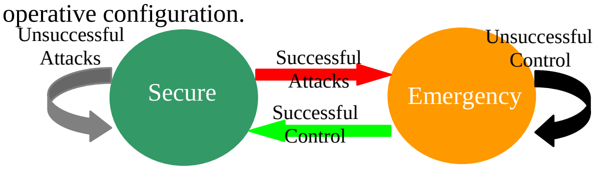

Figure 1: Transition of states.

2.2 Attacking Patterns

We can classify the malicious attacks in two types: *physical attacks* and *cyber attacks*.

For the physical attacks, we will only consider attacks that cause the failure of tie-lines or internal transmission lines since they are the most unprotected and represent a relatively easy target for an attacker [4]. The lines being attacked can be multiple. Furthermore, a discussion about possible attacks of other components such as power plant and substations can be found in [2]. Our model applies, as well, to those attacking scenarios.

For cyber attacks, we generally summarize the following patterns:

- Make the information unavailable or corrupted for decision makers, so that the decision making would be inappropriate and leads to catastrophic results.
- Make the correct control instructions unable to be implemented by attack the SCADA system to make catastrophic results.
- Directly control the SCADA system to make malicious actions against the infrastructures.

According to what some existent models have shown [14], cyber attacks may be more difficult to perform successfully than physical attacks. However, cyber attacks can be accessorial to enlarge the damage of physical attacks. So in this model, we will focus on the problem of decision making by operators without enough or correct information under some most credible physical attacks from off-line security analysis.

2.3 Objective of the SOs

When the overload congestions have not been relieved, the SOs only focus on the extent of congestions. When the congestions are relieved, the SOs focus on how much it costs to achieve this.

In the first place, in case of congestions caused by physical attacks and that cannot be removed, to reflect the security level of the power system, we express the utilities for each SO in terms of the overload rate of the lines. The overload rate associated to line l is:

$$V^l = \begin{cases} 0 \ (If\ P^l \le P^l_{\max}) \\ (P^l_{\max} - P^l)/P^l_{\max} \ (If\ P^l > P^l_{\max}) \end{cases} \quad (l \in \mathcal{L}) \tag{1}$$

By taking into account all internal lines, i.e. those that have both terminal buses in the local system, and tie-lines that have one terminal bus in the local system and the other in another system, the individual overlaod rate for SO i is:

$$V_i^I = \sum_{l \in \mathcal{I}_i} V^l + \sum_{l \in \mathcal{T}_i} 0.5 V^l \tag{2}$$

where coefficient 0.5 means that only half of the overloaded rate of a tie-line would be considered by SO i and the other half would be considered by the other SO connected by the tie-line.

Each SO estimates expected overlaod rate by considering the overload rate of its own system and, with a proper weight, of the systems of its neighbors, according to the socially rational agents approach :

$$V_i^E = k_1 \cdot V_i^I + k_2 \cdot \left(\sum_{\substack{j=1 \\ j \ne i}}^{n} \varphi_j^i \cdot V_j^I \right) \tag{3}$$

where $k_1 + k_2 = 1$

The evaluation of φ_j^i depends on how tight the interaction between each pair of SO *i* and *j* is. We use the absolute value of power exchange between the two parts as the parameter to evaluate this interaction. If the interaction between SO *i* and another SO is more active, then SO *i* would like to consider the overloaded rate of the subsystem corresponding to that SO more important. Then φ_j^i can be expressed as:

$$\varphi_j^i = P_j^i / \sum_{\substack{k=1 \\ k \neq i}}^{n} P_k^i \tag{4}$$

In the second place, in case of secure state following counteracting control actions, the SOs would not focus on overloaded rate any more, but on how many loads must be shed to relieve the congestions. To take the system back to the secure state by shedding fewer loads should be assigned higher utility values.

Then the final definition of utility U_i of a socially rational agent *i* is :

$$U_i = \begin{cases} V_i^E \ (if\ V_i^E < 0) \\ (M_i - L_i)/M_i \ (if\ V_i^E = 0) \end{cases} \tag{5}$$

We suppose that SO *i* has total *e* action schemes, the amount of loads to be shed in MW for each action scheme is denoted as L_i^j *(j=1…e)*. Then

$$M_i = \underset{j}{MAX}(L_i^j) \quad (j = 1 \cdots e) \tag{6}$$

To keep the system secure, we assume that all the operating agents can only select to shed loads in its own system. Under different operative configurations, the possible actions may be different depending on the distribution of loads at the buses.

In subsystem *i* with d_i buses whose loads can be shed, a vector of action scheme α_i , $\mathcal{X}_i$ consists of d_i elements. Each element has two possible values, 0 or 1, which respectively represents no shedding/shedding of the loads on the bus; for example α = *{1,0,0,…,0}* means that only the load on bus 1 is to be shed.

The SOs have estimations about the influence on the line flows of the loads at each bus. Based on some specific distribution factors of different buses (such as PTDFs) which reflect the sensitivities of the active power flows with respect to the variation of loads on different buses, the SO may select some most sensitive buses with loads to be considered to form the action sets and hence the dimension of joint actions set composed by the combination of all individual actions will be tractable.

2.4 Objective Attainment by Learning

When only partial information about active power flows on transmission lines is available, system operators do not have enough information about the structure of neighboring systems and the distributions of generations and loads to rebuild the DC power flow model of the whole interconnected power system. Additionally they may not know the current policies of the neighbor SOs, so they can not directly get the utilities of their joint control actions. Reinforcement learning provides a suitable method for modeling such a context.

We assume that *g* is the joint action which is composed of *n* different actions by *n* SOs ($\alpha_1\alpha_2\cdots\alpha_n$). $\mathcal{G}$ is the set of all possible joint actions under the present operative configuration. We apply the classic Q-learning method to the learning process of all the agents which can be considered as a repeated one stage game [15].

For each SO, when he gets the reward U_i by executing g_t at state s_t, the updating formula for all Q-values of time step *t* is:

$$Q_{t+1}^i(s,g) = \begin{cases} Q_t^i(s,g) + \beta[U_i - Q_t^i(s,g)] \\ \qquad if\ s = s_t\ and\ g = g_t \\ Q_t^i(s,g)\ otherwise \end{cases} \tag{7}$$

where *i =(1,2,…,n)*

The learning rate β decays in the learning process to guarantee the convergence [16]. The criterion of convergence of Q value is that the difference of two consecutive iterations is less than 0.001. Initial utility values are assigned to different action schemes according to their quantity of loads to be shed.

2.5 Equilibrium Search by Fictitious Play

After getting the estimations about the system performance following the possible control actions according to the available information, the SO needs to make the decisions based on its rational self-interest and a strategic interaction with other operators. We resort to fictitious play to find equilibrium to represent the final joint decision.

A *fictitious play* is a process where each player believes that each opponent is using a stationary mixed strategy based on empirical distribution of their past actions until the strategies come to equilibrium [17].

This approach is appropriate for the problems where the players are not aware about the utilities of other opponents because of the lack of information and can only make decisions based on their experiences. Fictitious play is integrated with the model of socially rational agents: each agent *i* keeps a count $C^i(\alpha_j)$ for each individual action α_j of the number of times agent *j* has used it in the past. Agent *i* treats the relative frequencies of each agent *j*'s actions as indication of the current strategy of *j*. Agent *i* assumes that *j* plays action α_j with probability:

$$R_{\alpha_j}^i = C^i(\alpha_j) / [\sum_{b_j \in \mathcal{X}_j} C^i(b_j)] \tag{8}$$

For each player *i*, let its current action choice α_i be selected according to some pure strategy which maximizes the weighted evaluation of utility:

$$U^W(\alpha_i) = \sum_{\alpha_{-i} \in \mathcal{X}_{-i}} Q(\alpha_{-i} \cup \alpha_i) \prod_{j \neq i} \{R_{\alpha_{-i}[j]}^i\} \tag{9}$$

where α_{-i} denotes all the actions implemented by other agents except agent *i*.

The process of fictitious play is integrated with the reinforcement learning which keeps updating the *Q* values of the joint actions. When all the maximum frequencies of individual actions (or estimated probabilities) of each agent are higher than a criterion (such as 0.9), the process can be considered as converged to a pure strategy equilibrium formed by the individual actions of each agent with maximum probabilities.

3 INFORMATION IMPACT ANALYSIS

The different information sets available to the SOs correspond generally to different decisions and consequently different performance of the system in terms of overload removal and required load shedding. In this context the information scenarios in terms of the metrics for quantifying the level of information available need to be defined. In this section, it will be introduced a metric able to evaluate the effect of the information availability on the estimation of the objectives of the SOs, upon which the decision making is based.

3.1 Information Scenarios

An information scenario is defined by the set of values of the power flows on the transmission lines when the system is under attack. The information scenario is represented by the matrix:

$$F = \begin{bmatrix} F_{11}\ F_{12}\ \dots F_{1n} \\ F_{21}\ F_{22}\ \dots F_{2n} \\ \vdots \\ F_{n1}\ F_{n2}\ \dots F_{nn} \end{bmatrix} \qquad (10)$$

where a non diagonal element F_{ij} represents the aggregated information communicated from SO *i* to SO *j* defined as:

$F_{ij} = (p_{x,y}, \dots)$ ($i = 1\dots n, j = 1\dots n,\ i \neq j$) (11)

Each component $p_{x,y}$ of F_{ij}, denotes the active power flow between bus *x* and bus *y*. $p_{x,y} = 0$ if there is no transmission line between these two buses.

A diagonal element F_{ii} in the matrix denotes the information of SO *i* related to his own system.

F^{ϕ} denotes no information exchanged between the SOs. F_{ij}^{ϕ} denotes that there is no information exchanged from operator *i* to operator *j*.

F^f denotes full information scenario. F^f_{ij} denotes all information from SO *i* to SO *j* has been communicated. F^f_{ii} denotes that all information of system *i* is available to SO *i*.

In case of partial information scenario where information about active power flow in some transmission lines is not available to local SO or neighboring SOs, due to cyber attacks or coordination rules, the SOs will consider the overloaded rates of these unknown transmission lines as zero.

3.2 Information Scenarios Comparison

To assess the impacts of information on the outputs of the coordinated decision making, a metric for comparing various information sets available to the SOs is needed. We propose the idea of *information distance* that characterizes the quantitative differences among different information scenarios under the same physical conditions and attacking pattern. This gives us an insight to compare all information scenarios on a common basis.

In the decision making process, the operators utilize the information available in the current scenario to choose its action and estimate the consequent system performance, as measured by its utility. Different information sets correspond to different levels of accuracy in the system knowledge and bring to different estimations of the expected utility of the same actions. The variation of the expected utility under the same physical system conditions provides a way to compare quantitatively different information scenarios regardless to human and organizational factors in decision making.

There would be *n* different utility values of one joint action *g* for *n* different agents from reinforcement learning in a specific information scenario *F*. From equation (7), we can extend Q^i as a function of information scenario *F*: $Q^i(s,g,F)$. We consider the estimated utility values $[Q^1(F^f), Q^2(F^f), \dots, Q^n(F^f)]$ for joint action *g* based on full information scenario F^f where information about active power of all transmission lines could be common knowledge of all operators as the coordinates of a point in a *n*-dimension space, and the estimated utility values $[Q^1(F^p), Q^2(F^p), \dots, Q^n(F^p)]$ for the same joint action *g* based on another partial information scenario F^p as another point in the same utility space. As an example, Figure 2 indicates the situation for three agents in a 3-dimension space.

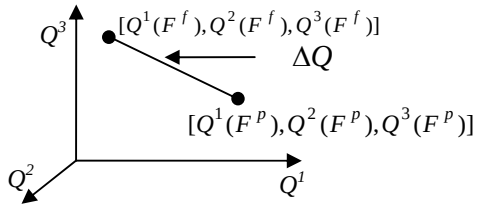

Figure 2: Variation of utility of one joint action.

The variation of estimated utilities of joint action *g* caused by reduction of available information unavailability can be considered as the Euclidean distance between these two points. To have a general evaluation of an information scenario about the corresponding estimating accuracy of system performances, we define:

$$H_p = \sum_{g} \sqrt{\sum_{i=1}^{n} [Q^i(p) - Q^i(f)]^2} \qquad (12)$$

Then the information distance between scenarios F^f and F^p could be defined as:

$$D_p = H_p / H_\phi \quad (13)$$

H_ϕ corresponds to information scenario F^ϕ where there is no information exchange between SOs as a reference.

System performance, information distance and decisions of the SOs at the equilibrium can reveal three different characteristics of the problem; by comparing them, we can have an insight about their interrelations with special reference to the decision making-information relationship.

4 NUMERICAL SIMULATIONS

We consider an interconnected 34-bus system with three SOs connected by 6 tie-lines to exemplify the analysis of the information impacts on coordination of SOs in different information scenarios. The system data are reported in the appendix. By the test results, we will see what factors influence the information impact seriously, the role played by coordination rules and how decision making impacts system performance.

We consider an attacking pattern, derived from an off-line security analysis, characterized by the destroying of two lines (1-3 and 5-14).

We consider two operative configurations in the secure state for which the power exchanges among the SOs are shown in Figure 3.

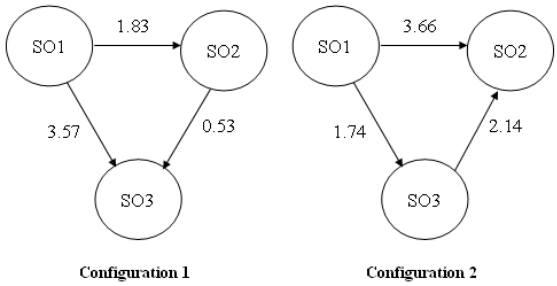

Figure 3: Power exchange at different operative configurations (pu).

We set $k_1 = k_2 = 0.5$ in (3) which means a medium attitude of the SOs in favor of the welfare of the whole system. We assume that each system operator can shed loads on one or two busses in its local subsystem to remove the congestions caused by the attack.

We consider and compare 9 different information scenarios in the operative configurations. The information made available to the neighboring SOs, in scenarios F^a F^b F^c F^d and F^e, is the power flows on the most overloaded lines after the attack.

$$F^a = \begin{bmatrix} F^f_{11} & F^\phi_{12} & F^\phi_{13} \\ (p_{30,32}) & F^f_{22} & F^\phi_{23} \\ F^\phi_{31} & F^\phi_{32} & F^f_{33} \end{bmatrix} \quad F^b = \begin{bmatrix} F^f_{11} & F^\phi_{12} & F^\phi_{13} \\ F^\phi_{21} & F^f_{22} & (p_{30,32}) \\ F^\phi_{31} & F^\phi_{32} & F^f_{33} \end{bmatrix}$$

$$F^c = \begin{bmatrix} F^f_{11} & F^\phi_{12} & F^\phi_{13} \\ (p_{30,32}) & F^f_{22} & (p_{30,32}) \\ F^\phi_{31} & F^\phi_{32} & F^f_{33} \end{bmatrix} \quad F^d = \begin{bmatrix} F^f_{11} & F^\phi_{12} & F^\phi_{13} \\ (p_{33,34}) & F^f_{22} & (p_{33,34}) \\ F^\phi_{31} & F^\phi_{32} & F^f_{33} \end{bmatrix}$$

$$F^e = \begin{bmatrix} F^f_{11} & F^\phi_{12} & F^\phi_{13} \\ (p_{33,32}) & F^f_{22} & (p_{33,32}) \\ F^\phi_{31} & F^\phi_{32} & F^f_{33} \end{bmatrix} \quad F^\phi = \begin{bmatrix} F^f_{11} & F^\phi_{12} & F^\phi_{13} \\ F^\phi_{21} & F^f_{22} & F^\phi_{23} \\ F^\phi_{31} & F^\phi_{32} & F^f_{33} \end{bmatrix}$$

F^f is the case in which the information about active power of all transmission lines would be communicated to all operators. F^ϕ is the case that no information would be communicated to neighbors. In case F^u, the information about active power of all transmission lines except $p_{30,32}$ $p_{33,34}$ and $p_{33,32}$ would be communicated to the neighbors, while in case F^r only the information about active power of lines near to the borders would be communicated to the neighbors.

Firstly, let us consider the *operative configuration 1* (table 1) under the various scenarios.

Scenario	Equilibrium from fictitious play (Bus NO. of shed loads)			Shed loads (p.u.)	Unrelieved overload rate	Info-distance
	SO 1	SO 2	SO 3			
F^a	20, 23	3, 29	26, 27	4.85	0	0.696
F^b	None	None	15	1.0	0.5	0.926
F^c	20, 23	5	27	4.65	0	0.507
F^d	20, 23	3, 29	26, 27	4.85	0	0.627
F^e	20, 23	3, 29	26, 27	4.85	0	0.627
F^u	None	3, 5	None	2.8	0.5	0.420
F^r	None	None	15	1.0	0.5	0.957
F^f	20, 23	5	27	4.65	0	0
F^ϕ	None	None	15	1.0	0.5	1

Table 1: System performance under various information scenarios (operative configuration 1).

In tab. 1, it is obvious that the considered scenarios come to 4 different equilibria from fictitious play. The comparison among scenarios F^a and F^b shows how the same information (power flow on line 30-32) can impact differently the system performance when it is utilized by various SOs; that means that the same information can play a differently important role for different operators.

Considering the information related only to the lines closer to the border, as suggested by the UCTE regulation, may be not sufficient to maintain the system security, as shown in scenario F^r; that prompts for the need of a ranking of the critical information starting from a systematic analysis of the whole systems and not only focusing on the interconnecting lines.

The information dimension plays a major role. However, the decision making dimension can superpose providing surprising results. In scenario F^u the SOs fail to relieve congestion as a result of their control actions, though its information distance to F^f is the smallest, that shows even under better information, the strategy interactions of the rational and self-interest system operators in the decision making process can not guarantee better performance of the system that depends both on the information availability and the corresponding decision making.

System Operator	Bus NO. of shed loads	Total shed loads (p.u.)	Unrelieved overload rate
SO 1	None	1.2	0
SO 2	33 34		
SO 3	None		

Table 2: System performance under various information scenarios(operative configuration 2).

In *operative configuration* 2, compared with configuration 1, all the considered information scenarios provide always the same performance of the system represented by the same and unique output equilibrium from fictitious play (table 2).

Consequently, in *operative configuration* 2, the information availability has no impact on the decisions of the system operators; that indicates that, in this case, the physical dimension of the system is robust enough with reference to information unavailability.

5 CONCLUSIONS

The security of interconnected power system, against contingencies, both natural and malicious, can be properly modeled considering the SOs as socially rational MAS playing a fictitious play. Information plays a major role in determining the decision of each SO and the corresponding performance of the system in terms of line overloading and load shedding. The model proposed can be usefully employed to verify the physical robustness of a system with respect to the availability of information. This can provide a new viewpoint of system robustness by taking into account not only the physical dimension but also the cyber and decision making dimensions.

Each information is operator-sensitive in the sense that the same information may have different relevance to different operators in the grid in determining their performance. The most critical information may be not necessarily those referred to the lines located near to the borders of the sub-systems, as the current regulation in EU assumed. In this respect a systematical analysis and ranking of the critical information all over the system is necessary. Furthermore, the performance of the interconnected system depends considerably on the decision making process of the decision makers and on their attitudes that need to be modeled and quantitatively assessed in security analysis.

APPENDIX

Line NO.	Start bus	End bus	Admittance [p.u.]	P_i^{max} [p.u.]
1	1	2	0.05062	2.286
2	1	3	0.05785	3.0
3	1	4	0.05785	2.286
4	1	4	0.08161	2.286
5	1	8	0.12934	2.286
6	1	10	0.00413	2.477
7	1	10	0.00413	2.477
8	2	4	0.05062	2.286
9	2	11	0.00413	2.286
10	3	4	0.13843	2.286
11	3	5	0.20041	2.286
12	3	12	0.00413	2.286
13	3	12	0.00413	2.286
14	4	15	0.05114	2.286
15	4	7	0.06818	2.286
16	4	13	0.00413	2.286
17	4	13	0.00413	2.286
18	5	15	0.0657	2.477
19	5	14	0.00413	2.286
20	6	15	0.00413	2.286
21	6	15	0.00413	2.286
22	7	8	0.06674	2.286
23	7	16	0.00413	2.286
24	8	17	0.00413	2.286
25	9	14	0.08161	2.286
26	30	29	0.04756	1.039
27	30	29	0.04756	1.039
28	30	29	0.04756	1.039
29	32	30	0.04756	1.039
30	32	30	0.04756	1.039
31	32	31	0.04756	1.039
32	32	31	0.04756	1.039
33	34	33	0.092	1.039
34	33	32	0.092	1.039
35	24	25	0.04756	1.039
36	26	25	0.04756	1.039
37	27	26	0.04756	1.039
38	28	27	0.04756	1.039
39	19	20	0.04756	1.039
40	19	20	0.04756	1.039
41	21	20	0.04756	1.039
42	21	20	0.04756	1.039
43	21	22	0.092	1.039
44	18	21	0.04756	1.039
45	18	21	0.04756	1.039
46	22	23	0.092	1.039
47	29	12	0.01033	3.811
48	31	14	0.01033	2.286
49	34	9	0.02066	2.286
50	24	16	0.02066	2.477
51	28	6	0.02066	2.477
52	19	17	0.01033	3.429
53	18	11	0.01033	2.286
54	23	13	0.04132	2.286

Table 3: Line data

	Operative Configuration 1		Operative Configuration 2	
Bus NO.	Generation [p.u.]	Load [p.u.]	Generation [p.u.]	Load [p.u.]
1	0	0	0	0
2	1.8	0	1.8	0
3	0	1	0	1
4	0	3.8	0	3.8
5	0	1.8	0	1.8
6	0	0.7	2.4	0
7	0	0.4	0	0
8	0	0	0	0
9	3.4	0	2	0
10	3.4	0	3.4	0
11	0	0	0	0
12	0	0	0	0
13	4	0	4	0
14	0	0	0	0

15	0	1.0	0	0
16	0	0	0	0
17	0	0	0	0
18	0	0.9	0	0.9
19	1.15	0	1.15	0
20	0	1.75	0	1.75
21	2.7	0	2.7	0
22	0	0.6	0	0.6
23	0	0.6	0	0.6
24	0	0.5	0	0.5
25	0	0.5	0	0.5
26	0	0.5	0	0.5
27	0	0.5	0	0.5
28	0	0	0	0
29	0	0.5	0	0.9
30	0	0.55	0	0.95
31	0	0.5	0	0.9
32	0	0.05	0	1.05
33	0	0	0	0.6
34	0	0.3	0	0.6

Table 4: Distribution of generations and loads

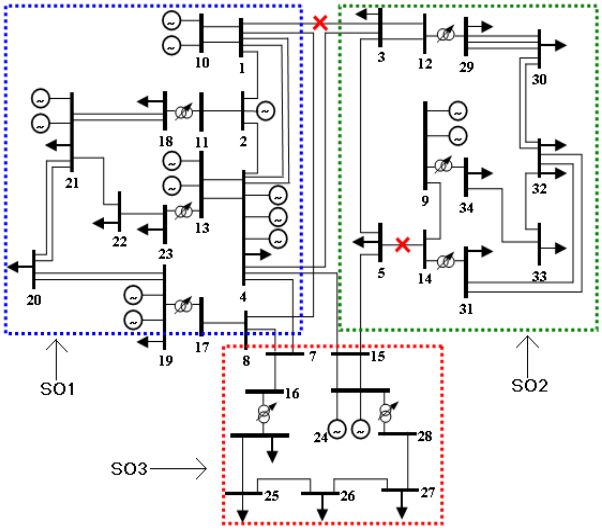

Figure 4: Test system

REFERENCES

[1] Å.J. Holmgren, E. Jenelius, and J. Westin, "Evaluating Strategies for Defending Electric Power Networks Against Antagonistic Attacks," *IEEE Trans. Power Systems*, vol. 22, Feb.2007.

[2] J. Salmeron, K. Wood, and R. Baldick, "Analysis of electric grid security under terrorist threat," *IEEE Trans. Power Systems*., vol. 19, no. 2, pp. 905–912, May 2004.

[3] A. L. Motto, J. M. Arroyo, and F. D. Galiana, "A mixed-integer LP procedure for the analysis of electric grid security under disruptive threat, " *IEEE Trans. Power Systems*., vol. 20, no. 3, pp. 1357–1365, Aug. 2005.

[4] J. M. Arroyo and F. D. Galiana, "On the solution of the bilevel programming formulation of the terrorist threat problem, " *IEEE Trans. Power Systems*., vol. 20, no. 2, pp. 789–797, May 2005.

[5] G. Dondossola, and O. Lamquet, "Cyber Risk Assessment in the Electric Power Industry, " *Electra Magazine,* n. 224, Feb. 2006.

[6] Union for the Co-ordination of Transmission of Electricity, "*Operation Handbook*", [Online]. Available: http://www.ucte.org.

[7] C. Rehtanz, "*Autonomous Systems and Intelligent Agents in Power System Control and Operation*", Springer-Verlag Berlin Heidelberg 2003, ISBN 3-540-40202-0.

[8] Y. Shoham, R. Powers, T. Grenager, "If multi-agent learning is the answer, what is the question?" *Artificial Intelligence* 171(7) (2007) 365-377

[9] E. Bompard, C. Gao, M. Masera, R. Napoli, A. Russo, A. Stefanini, and F. Xue, "Approaches To The Security Analysis Of Power Systems: Defence Strategies Against Malicious Threats". Luxembourg: Office for Official Publications of the European Communities, 2007, EUR 22683 EN, ISSN 1018-5593

[10]E. Bompard, R. Napoli, A. Russo, F. Xue, M. Masera, and A. Stefanini, "The analysis of malicious threats to infrastructures: a conceptual approach based on multi-agent systems", in *Proc.2007 First Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection.*

[11]C.B. Excelente-Toledo, and N. R. Jennings. "Learning When and How to Coordinate", *Web Intelligence and Agent System*, vol. 1, pp. 203-218, 2003.

[12]L. Hogg and N. R. Jennings. "Socially rational agents". In Proc. of AAAI *Fall symposium on Socially Intelligent Agents*, pp. 61–63, 1997.

[13]A. Namatame, "Social Learning in a Society of Decentralized Agents", in *Proc. 1996 IEEE International Conference on Evolutionary Computation.*

[14]B. John Garrick et alii , "Confronting the risks of terrorism: making the right decisions", *Reliability Engineering and System Safety*, Vol. 86, pp. 129-176, 2004.

[15]C. Claus, and C. Boutilier, "The Dynamics of Reinforcement Learning in Cooperative Multiagent Systems", in *Proc. 1998 Fifteenth National Conf. on Artificial Intelligence*.

[16]C.J.C.H. Watkins, and P. Dayan, "Technical Note Q-Learning". *Machine Learning*, vol. 8, pp. 279-292, 1992.

[17]J.S. Shamma, and G. Arslan, "Dynamic Fictitious Play, Dynamic Gradient Play, and Distributed Convergence to Nash Equilibria", *IEEE Trans. Automatic Control*, vol. 50, no. 3, March 2005.