

RISK ASSESSMENT OF MALICIOUS ATTACKS AGAINST POWER SYSTEMS

*Original*

RISK ASSESSMENT OF MALICIOUS ATTACKS AGAINST POWER SYSTEMS / Bompard, Ettore Francesco; Gao, Ciwei; Napoli, Roberto; Russo, Angela; Masera, M; Stefanini, A.. - In: IEEE TRANSACTIONS ON SYSTEMS MAN AND CYBERNETICS PART A-SYSTEMS AND HUMANS. - ISSN 1083-4427. - STAMPA. - 39:5(2009), pp. 1074-1085. [10.1109/TSMCA.2009.2020687]

*Availability:*

This version is available at: 11583/1915067 since:

*Publisher:*

IEEE

*Published*

DOI:10.1109/TSMCA.2009.2020687

*Terms of use:*

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

*Publisher copyright*

(Article begins on next page)

# Risk Assessment of Malicious Attacks Against Power Systems

Ettore Bompard, *Member, IEEE*, Ciwei Gao, Roberto Napoli, *Member, IEEE*,  
Angela Russo, Marcelo Masera, and Alberto Stefanini

**Abstract**—The new scenarios of malicious attack prompt for their deeper consideration and mainly when critical systems are at stake. In this framework, infrastructural systems, including power systems, represent a possible target due to the huge impact they can have on society. Malicious attacks are different in their nature from other more traditional cause of threats to power system, since they embed a strategic interaction between the attacker and the defender (characteristics that cannot be found in natural events or systemic failures). This difference has not been systematically analyzed by the existent literature. In this respect, new approaches and tools are needed. This paper presents a mixed-strategy game-theory model able to capture the strategic interactions between malicious agents that may be willing to attack power systems and the system operators, with its related bodies, that are in charge of defending them. At the game equilibrium, the different strategies of the two players, in terms of attacking/protecting the critical elements of the systems, can be obtained. The information about the attack probability to various elements can be used to assess the risk associated with each of them, and the efficiency of defense resource allocation is evidenced in terms of the corresponding risk. Reference defense plans related to the online defense action and the defense action with a time delay can be obtained according to their respective various time constraints. Moreover, risk sensitivity to the defense/attack-resource variation is also analyzed. The model is applied to a standard IEEE RTS-96 test system for illustrative purpose and, on the basis of that system, some peculiar aspects of the malicious attacks are pointed out.

**Index Terms**—Game theory, malicious attack, mixed-strategy equilibrium (MSE), power-system security, vulnerability.

## NOMENCLATURE

### Indexes and Sets:

$i$	Index for attack plans.
$j$	Index for defense plans.
$k$	Index for components.
$l$	Index for lines.

Manuscript received May 5, 2008; revised October 17, 2008. First published July 14, 2009; current version published August 21, 2009. This work was supported in part by Next Generation Infrastructures Foundation (NGI), Delft, The Netherlands, and in part by SiTI, Turin, Italy. This paper was recommended by Associate Editor H. R. Rao.

E. Bompard is with the Politecnico di Torino, 10129 Torino, Italy and also with the Institute for Economic Research Firms and Growth (CERIS-CNR), National Research Council, Mancalieri (TO), 10024 Italy (e-mail: ettore.bompard@polito.it).

C. Gao is with the School of Electrical Engineering, Southeast University, Nanjing 210096, China.

R. Napoli and A. Russo are with the Politecnico di Torino, 10129 Torino, Italy.

M. Masera is with the Institute for the Protection and Security of the Citizen, Joint Research Centre, European Commission, 21020 Ispra, Italy.

A. Stefanini was with the Institute for the Protection and Security of the Citizen, Joint Research Centre, European Commission, 21020 Ispra, Italy.

Color versions of one or more of the figures in this paper are available online at <http://ieeexplore.ieee.org>.

Digital Object Identifier 10.1109/TSMCA.2009.2020687

$m$	Index for buses.
$\Phi$	Set of the lines of the system.
$\Theta$	Set of the buses of the system.
$\mathcal{A}_i$	Set of components of the $i$ th attack plan.
$\mathcal{D}_j$	Set of components of the $j$ th defense plan.
$\mathcal{G}_1$	Set of components that have not been defended and are destroyed.
$\mathcal{G}_2$	Set of components that have not been defended and are not destroyed.
$\mathcal{H}_1$	Set of components that have been defended but are destroyed.
$\mathcal{H}_2$	Set of components that have been defended and are not destroyed.
$\mathcal{R}$	Set of components of the entire system.
$\mathcal{X}$	Set of components that have been destroyed.
$B^A$	Budget of the attacker.
$B^D$	Budget of the defender.
$C$	Monetary measure of the damage incurred by the attack action.
$C_A$	Attacker's cost of its attacking.
$C_D$	Defender's cost of its defending measures.
$C_i^A$	Cost of implementation of $\mathcal{A}_i$ .
$C_j^D$	Cost of implementation of $\mathcal{D}_j$ .
$C_{ij}$	Damage evaluation under the scenario with the attack plan $\mathcal{A}_i$ and defense $\mathcal{D}_j$ .
$C_k^{oa}$	Cost of attack of the $k$ th component.
$C_k^{od}$	Cost of defense of the $k$ th component.
$E_{ij}$	Expected costs/losses of the system under the scenario with the attack plan $\mathcal{A}_i$ and defense $\mathcal{D}_j$ .
$F_l$	Power flow on line $l$ .
$F_{l_{\max}}$	Maximum power flow on line $l$ .
$G_m$	Value of the damage at the bus $m$ .
$L_m$	Load demand at bus $m$ before the contingency occurrence.
$M_{\mathcal{X}}$	Total economic value of the lost load due to the destruction of the components of $\mathcal{X}$ .
$N_A$	Number of the feasible attack plans.
$N_D$	Number of the feasible defense plans.
$O_k^A$	$k$ th component in an attack plan.
$P_m$	Generated power before the contingency at bus $m$ .
$P_{m_{\max}}$	Maximum value of the generated power at bus $m$ .
$S_A$	Payoff of the attacker.
$S_D$	Payoff of the defender.
$S_i^A$	Attacker's utility corresponding to $\mathcal{A}_i$ .
$S_j^D$	Defender's utility corresponding to $\mathcal{D}_j$ .
$n_A$	Number of the component candidates for the attack.
$n_D$	Number of the component candidates for the defense.
$p_i^A$	Probability of choosing the $i$ th attack plan.
$p_j^D$	Probability of choosing the $j$ th defense plan.

$p_k^{oa}$	Probability of the $k$ th component to be attacked.
$p_k^{od}$	Probability of the $k$ th component to be defended.
$\alpha_k$	Probability of the $k$ th component to be successfully destroyed without any defending measure.
$\beta_k$	Probability of the $k$ th component to be successfully destroyed with a defending measure.
$\gamma$	Risk.
$\lambda_m$	Evaluation factor with reference to the load shedding at bus $m$ .
$\Delta L_m$	Load shedding at the bus $m$ .
$\Delta P_m$	Variation of the generated power at bus $m$ .

## I. INTRODUCTION

A VAST number of hazards can threaten power systems both due to accidental reasons and to intentional attacks; both of them can have disastrous effects on the society from the social and economic point of view. Potential deliberate attacks draw more attention nowadays when threats such as international terrorism have become a very serious issue.

Since terrorist attacks aim at having the largest impact on society, critical infrastructures are a credible target. Therefore, systems such as the power one, which is vital to the whole society and whose failure can cause severe consequences, have to be properly protected. Recent accidental blackouts have demonstrated the vulnerability of those systems (e.g., the 2003 U.S. blackout, 9300 km<sup>2</sup>, 50 millions of inhabitants involved, \$39 billion/day of economic lost; 2003 Italy blackout, 57 millions of inhabitants, 4 persons died, 120 M€ of economic loss [1]). Authorities have already realized the threat of malicious attacks [2] and taken several countermeasures against their possible occurrence. For instance, for power systems, the North American Electric Reliability Council (NERC) defined for the North American electricity sector a set of physical/cyber-response security guidelines with the actions that they should consider when responding to the malicious-threat-level alerts issued by the U.S. Department of Homeland Security or Public Safety and Emergency Preparedness Canada [3], [4].

The conventional power-system security and risk analysis is based on the physical nature of the power system. System failures depend on components' reliability (transformer [5], the specific protection system [6], etc.) and the randomly happening of natural accidents (lightning, fires, animal intrusion, etc.). Online security-assessment approaches are developed to examine the status of the system [7], [8].

However, research on modeling malicious attack against power systems is at a preliminary stage. A greedy algorithm is applied in [9] to identify promising interdiction strategies in transmission system. A max–min model is introduced in [10], and a more general model of bilevel formulation is proposed in [11]. In [12], the power-system vulnerability is treated with Bayesian networks, which is based on statistical data. Nevertheless, the papers mentioned above neglect the fact that both the terrorist and the defender are intelligent, and their actions are guided by their strategic analysis. For instance, Bier *et al.* [9] study the impact of different system-hardening strategies but only with respect to already-identified interdiction strategies. In this respect, strategic interactions, which are not taken into account in conventional security analysis, should be emphasized in the research on malicious attack. New approaches and tools are indispensable to that aim.

Game theory, as an effective tool for the analysis of strategic behavior and the formal study of conflict and cooperation [13], has already been resorted for capturing the thoughts of terrorists in negotiation or nonnegotiation processes [14]–[17], to analyze how terrorist select the target country [18], and how governments choose deterrence and preemption strategies [19].

In this paper, we present a mixed-strategy game-theory model, which is able to capture the strategic interaction among attacker and defender for power systems under malicious threat. The model provides an effective way to assess the risk of attacks against specific power-system components, so as to support the proper allocation of resources for the protection of the system. This paper presents the concept of the probability of components being attacked/defended, derived from the similar “probability” conception in traditional reliability analysis. Moreover, the method presented can calculate the risk sensitivity of the target system to the resources of the defender and the attacker, an attribute that helps in making optimal defense resource allocation and shows the links between attack/defense resources and consequence of the attack. Game-theory application to the power system introduced in [20] takes a relative macroperspective, namely, it focuses on resource allocation between measures of protection and recovery, while attacks are analyzed with reference to various scenarios in terms of combination of normal/extreme operational situations and different attack strategies. In this paper, resource allocation is computed for each specific component, namely, it shares the same objective as [21], i.e., to optimally allocate the resources in response to a threat of malicious attack.

Of course, multiagent systems will be more effective to simulate the real world [22], [23], but game theory is usually more suitable to illustrate the essence of the problem.

The remainder of this paper is composed of the following sections. In Section III, malicious and natural threats are analyzed and compared. The actions of the attacker and defender, the interaction between the attacker and the defender, and the technique for efficiently finding the mixed-strategy equilibrium (MSE) are explained in Section IV. System vulnerability and risk assessment with reference to malicious attacks are studied in Section V. In Section VI, the proposed model is tested with numerical simulations, and finally, conclusions are drawn in Section VII.

## II. MALICIOUS VERSUS NATURAL THREATS

A threat is the danger of adversarial events, such as malicious attacks. Attacks may impair systems security by acting upon some existing vulnerabilities or faults. Malicious attacks are conducted with criminal, belligerent, or political purposes. Defense measures for diminishing the probability of such attacks may be either online or offline. The former ones consist of countermeasures taken before the happening of the contingency, including responses to threat warnings; the latter are performed after the contingency. From this point of view, this paper centers on the analysis of the vulnerability of infrastructure and the effectiveness of defense measures.

### A. Natural Hazards, Systemic Failures, and Human Errors

Natural hazards happen due to acts of nature and, therefore, occur without the intentional intervention of any human

being. Natural phenomena, such as atmospheric discharges (lightning), animals, winds, etc., may impact on infrastructures' integrity and their operation and are typically analyzed by means of statistical method. Systemic failures come about due to the activation of faults in components, following stochastic reliability laws. They are subject to the lifecycle of the system: operation, maintenance and repair, aging, production, and so on. System failures follow some physical laws that can be discovered by statistical and experimental methods, extensively developed in the field of reliability engineering. Failures caused by human action, although without intention, are normally known as human errors, since there is *no willingness*. The three of these phenomena (i.e., natural hazards, systemic failures, and human errors) are characterized by a key common element: They may cause system failures on a random basis, independent on the intention of any human being.

### B. Malicious Threats

Malicious attacks are brought about by human beings with the willingness to provoke damage. They are critical for the infrastructures' security. The resulting damage can be evaluated in various respects, e.g., operational, financial, psychological, etc. Some features of malicious threats are as follows.

- 1) Malicious threats are potential hazards that can materialize as attacks—i.e., threats cause damage, when executed as offensive actions.
- 2) Attacks are the actual implementation of threats, and therefore, they are the effective cause of damages.
- 3) Malicious threats are selective: The more the target can produce disruptive effects, the more it is likely to be attacked; the more the target is protected, the less likely it will be attacked.
- 4) Attacks are carried through as processes, where actions of the attackers and defenders follow and affect each other. In other words, an attack is a chain of mutually dependent offensive and defensive events. In few occasions, the hostile part of an attack can consist of just one step, but more generally, it will comprehend several steps, possibly organized in successive phases.

The level of threat, for a given component, depends on the attitudes, decisions, and interaction between attackers and defenders at a given point in time and space.

Therefore, the study of malicious threats must take into account the interactions between attackers and defenders. We propose in this paper to approach this problem using game theory.

### C. Comparison Between Accidental and Malicious Threats

As pointed out, there are huge distinctions in various respects between malicious threats and accidental ones. Conventional risk-analysis methods for dealing with accidental failures provide limited answer to malicious ones. When considering deliberate attacks, strategic interaction between the actors determines the probability of an attack (in time and in space, i.e., which element will be targeted), while accidental acts occur on a random basis. This is based on the assumption that malicious actors are rational agents and, hence, will thoroughly scrutinize the cost and potential effects of their acts. Their analyses will include the means and ways, the target, and the time of the

attack. For instance, malicious attackers are likely to select the target that appears assailable for their available resources and with more potential impact. Obviously, both the difficulty of the attack and its effects are dependent upon the defender's countermeasures. Therefore, the decision of the malicious attacker will vary according to the corresponding decisions of the defender. In other words, strategic interaction between attackers and defenders affects the probability distribution of the contingency. Attackers will adapt their goals, tactics, resources, timing, and modes of operation according to the (perceived) actions of the defenders.

Conventional methods for analyzing accidental failures, like probabilistic approaches and Monte Carlo simulation, are not always suitable for malicious attacks, particularly when the chain of events during an attack expands in complex series of actions and counteractions, with the attackers dynamically adapting to the new conditions defined by the technical and organizational measures of the defenders. In addition, there is little statistical information of aggressive actions that could serve as probabilistic basis for typical risk-assessment processes. Traditional risk-assessment approaches can not provide an answer to situation characterized by the changing nature of the capabilities and strategic goals of the attackers and their evaluation of the attractiveness of the targets.

Another distinctive difference among malicious and accidental threats is that, by taking some special preemptive measures, for instance, systems hardening by vulnerabilities elimination, system operators are able to substantially diminish the probability of success of malicious attacks. To be noticed, the model of the strategic interaction depends on the specific reference scenario. For example, if defenders' online countermeasures can be neglected and information is perfect, terrorists face a certain scenario and choose the target that could have the major effect. Nevertheless, conventional probabilistic approaches could provide some contribution to the analysis of malicious threats. For instance, if the attacker knows little about the defender's countermeasure, the choice of the target will be based on history or experience about which one could greatly disturb the system. If one hypothesizes an attack with few steps, the interactions between attacker and defender are limited, and therefore, one can apply probabilistic approaches.

Table I introduces a side-by-side comparison between the two types of threats. In particular, we want to point out that the societal actors that will suffer the consequences of natural threats (the "sufferers" mentioned in the table) are different from the "other affected actors" related to malicious threats, since the former are randomly affected (i.e., nature has no specific aim) and are basically passive targets, while the latter refers to those influenced by the malicious threat, who are not necessarily the first targets of an attack.

## III. STRATEGIC INTERACTION MODEL

The rational player hypothesis, according to which each player will act so as to maximize a measure of his/her own utility, is assumed.

As discussed in Section III, defenders take countermeasures against malicious attacks against power systems. In this paper, we consider that the system may be strengthened by offline countermeasures in case there is warning of malicious threats.

TABLE I  
COMPARISON BETWEEN NATURAL AND MALICIOUS THREATS

	Natural, systemic and human error threats	Malicious threats
motivation	accidental	deliberate
distribution on the failure	random	critical component preferred
risk assessment	probabilistic approaches (Monte-Carlo simulation)	rational interactions models
counter-actions	1.re-enforce the system, make the system less vulnerable, e.g. double critical components 2.increase components reliability	1. re-enforce the system, make the system less vulnerable, e.g. double the critical component 2. preemptive measures against attackers
strategic interaction	no	yes
players	1. system operators 2. sufferers 3. government	1.system operators 2. attackers 3. government 4. other affected actors (e.g., society)

Our aim is to compute the risk of the power system in terms of the resources and the action sets available to the defender and attacker. The action selected by one side will surely influence the action of the other side. Obviously, malicious threats shall be directed against the more critical and vulnerable components; hence, these attacker targets shall be the subjects of the defenders' highest attention; on the contrary, the less critical and vulnerable components are also less likely to be attacked. Therefore, there is a complex interaction between decisions on both sides. The concept of "equilibrium" can be used to represent the game outcome. A Nash equilibrium is a set of strategies, one for each player, such that no player has the incentive to unilaterally change his/her action. Players are in equilibrium if a change in strategies by any one of them would lead that player to have less utility than if he/she keeps the current strategy. Therefore, the equilibrium is the foreseen outcome of the game with a given set of conditions and may be an important reference for the players to make their decisions.

The defender and the attacker are both rational entities and will analyze the situation to find their optimal actions. When these actions are the best choices of rational agents with respect to a given set of conditions, the result is the state of equilibrium. Considering the specific features of power systems, the next sections present a game model to represent the interaction between malicious attackers and defenders when attacking/defending the network.

#### A. Game Representation of the Malicious Attack

In a malicious attack, the roles and the corresponding action sets are defined as follows.

##### 1) Players:

Attacker) All malicious actors that want to attack power-system components to maximize the damage.

Defender) Various entities (e.g., system operators, authorities) whose goal is to minimize the power-system vulnerability and the potential damage caused by malicious attacks.

2) *Action Set*: The scenario considered includes the possibility of simultaneous attack actions (and the corresponding defense ones) against several components of the target systems. This relates to the fact that, in power systems, the occurrence of a simultaneous failure is usually much more severe. Moreover, simultaneous occurrence of multiple natural failures is usually with much lower probability, which makes " $n - 1$ " criterion widely adopted to assure the system feasibility and operability after the occurrence of any major single failure. However, this condition does not apply to the malicious attack.

*Attacker's action set*: The attack action is a plan that aims at several components as the attacking targets. The candidate components are considered to be either lines or buses.

Line attacked) The line (or parallel lines) attacked remain inoperative with a certain successful destruction rate (i.e., the lines are open from the electrical viewpoint).

Bus attacked) All lines, generation, and load connected to the bus are disconnected with a certain successful destruction rate.

*Defender's action set of defender*: The defense action is a plan that defines the components to be protected. Two types of defense actions are considered, with different time frames.

- 1) Online defense action, which can be deployed at once. For instance, more strict inspection and security control or patrols guarding specific components. This follows the response to malicious threats defined by NERC [3], [4]. The effect of this defense actions is the lowering of the destruction rate of the specific components attacked.
- 2) Offline defense action with a time delay, which refers to general actions that enhance the protection of the entire electric network. For instance, construction of new lines or new buses—all measures that may require a long time to be implemented. As a result, the topology of the network will change, together with the power-flow patterns.

3) *Payoff*: The payoff functions of the malicious attackers and of the defenders will be different, as their goals and perception of potential benefits have opposing views. For this reason, our model makes use of the same bilevel approach introduced in [11] that allows this parallel modeling of the objective functions for the attacker and the defender. However, it is still reasonable to model the interaction as a zero-sum game, since the utilities of the two sides are complementary, namely, the loss of one side is the gain of the other side. The utility of the attacker and the defender can be formulated as

$$\text{Attacker : } S_A = C_D + C - C_A \quad (1)$$

$$\text{Defender : } S_D = C_A - C_D - C \quad (2)$$

where

- $S_A$  the payoff of the attacker;
- $S_D$  the payoff of the defender;
- $C_A$  the attacker's cost of its attacking;
- $C_D$  the defender's cost of its defending measures;
- $C$  the monetary measure of the damage incurred by the attack action.

Usually, the damage is much bigger than the defense/attack cost; hence, the latter can be omitted.

The damage to the systems due to an attack can be quantified in terms of the economic value of the lost load that, for a generic bus  $2m$ , can be determined as

$$G_m = \lambda_m \Delta L_m. \quad (3)$$

$G_m$  and  $\Delta L_m$  are, respectively, the value of the damage and the load shedding at the bus  $m$ , while  $\lambda_m$  is an evaluation factor that expresses the importance of the loads connected at the bus. Buses with different levels of importance can be represented by imposing various values of  $\lambda_m$ , which not only considers the economic aspect of the load loss at that bus but also the potential social, political, environmental, or even psychological impact on the end users and other affected stakeholders. For sake of simplicity, we adopt the simple damage expression shown in (3), which is based on a per-load-interrupted basis. In fact, the economic impact is not the crucial factor for malicious attackers. Terrorists aim to create fear in the public so as to exert pressure on the government and eventually attain their political goals in an indirect way. Although comprehensive modeling of malicious attacks is undoubtedly necessary, in this paper, we focus on modeling the strategic interactions between attackers and defenders only, taking into account the economic value of the damage for sake of simplicity.

Cascading failures play a very important role in spreading the effect of an initial power-system fault, power-system dynamic characteristics, stability, and relay protections interplay to limit/spread such failures. In this paper, cascading outages are not considered so as to simplify the analysis. Consequences are evaluated with a simple dc model. Defenders, after a successful attack, will try to minimize the economic value of the lost load to keep the system feasible. This is similar to what people do in traditional power-system adequacy evaluation.

When an attack successfully destroys the components contained in the set  $\mathcal{X}$ , the defender has to face the contingency, and the system restoration can be decided by solving the following optimization problem:

$$\min M_{\mathcal{X}} = \sum_{m \in \Theta} G_m \quad (4)$$

s.t.

$$F_l \leq F_{l_{\max}}, \quad l \in \Phi \quad (5)$$

$$0 \leq \Delta L_m \leq L_m, \quad m \in \Theta \quad (6)$$

$$0 \leq P_m + \Delta P_m \leq P_{m_{\max}}, \quad m \in \Theta \quad (7)$$

where  $M_{\mathcal{X}}$  is the total economic value of the lost load due to the destruction of the components contained in the set  $\mathcal{X}$ .  $P_m$ ,  $\Delta P_m$ , and  $P_{m_{\max}}$  are, respectively, the generated power before the contingency, the variation of the generated power, and the maximum generated power at bus  $m$ .  $F_l$  and  $F_{l_{\max}}$  are, respectively, the power flow and the maximum power flow on line  $l$ .  $L_m$  is the load demand at bus  $m$  before the contingency occurrence.  $\Theta$  and  $\Phi$  are the sets of the buses and of the lines of the system, respectively.

Transmission constraints are respected with (5), in which power flows are determined by the nodal net-power injection and the line impedance, only considering the dc power-flow model. Therefore, binding of the constraint (5) means that the nodal power is adjusted, which may possibly result in a nonzero

TABLE II  
ENUMERATION OF ATTACK PLANS WITH  $n_A$  COMPONENTS CONSIDERED

Number of components contained in the attack plan	Possible attack plans	Number of possible attack plans
1	$\{O_1^A\}, \{O_2^A\}, \dots, \{O_{n_A}^A\}$	$\binom{1}{n_A} = n_A$
2	$\{O_1^A, O_2^A\}, \{O_1^A, O_3^A\}, \dots, \{O_{n_A-1}^A, O_{n_A}^A\}$	$\binom{2}{n_A} = \frac{n_A!}{2!(n_A-2)!}$
...	...	...
$x$	$\{O_1^A, O_2^A, \dots, O_x^A\}, \dots, \{O_{n_A-x+1}^A, O_{n_A-x+2}^A, \dots, O_{n_A}^A\}$	$\binom{x}{n_A} = \frac{n_A!}{x!(n_A-x)!}$
...	...	...
$n_a$	$\{O_1^A, O_2^A, \dots, O_{n_A}^A\}$	$\binom{n_A}{n_A} = 1$
Total number of possible attack plans		$\sum_{x=1}^{n_a} \binom{x}{n_A} = 2^{n_a} - 1$

value of  $\Delta L_m$ , so as to impact the value of  $G_m$  as well as the objective function  $M_x$  according to the formula (3) and (4). Moreover, the restoration time, which will surely impact the consequence, can be considered in (3) but needs much more complicated modeling. Since the purpose of this paper is just to introduce strategic interaction in risk evaluation, we do not further investigate this point in-depth.

The set of system components is  $\mathcal{R}$ . The attack plan may target several power-system components simultaneously, and the components that are candidate for the attack may be, in the most general case, a subsystem of  $\mathcal{R}$ . If we assume that there are  $n_A$  components candidate for the attack and that an attack plan can contain any number of components between 1 and  $n_A$ , the possible attack plans can be enumerated as in Table II. Under those assumptions, the total number of the attack plans can be determined and equals  $2^{n_A} - 1$ .

Analogously, on the defender's side, the defense plan contains the components for which some defense measures have been taken and, in the most general case, is a subsystem of  $\mathcal{R}$ . If we assume that there are  $n_D$  candidate components to be defended and that a defense plan can contain any number of components between 1 and  $n_D$ , the possible defense plans can be similarly enumerated, and the total number of the defense plans equals  $2^{n_D} - 1$ .

All the possible scenarios determined by the combination of a defense plan and an attack plan should be examined to account for the security situation in light of possible malicious activities.

The action set, which is composed of the plans of both the attacker and the defender, is confined by their respective resources. Since it is reasonable to assume limited resources for implementing attack and defense plans, some constraints related to the available resources of the attacker and the defender can be included.

If the attacker realizes the  $i$ th attack plan, referred to as  $\mathcal{A}_i$ , the cost of implementation  $C_i^A$

$$C_i^A = \sum_{k \in \mathcal{A}_i} C_k^{oa} \quad (8)$$

should meet the resource constraint

$$C_i^A \leq B^A. \quad (9)$$



Analogously, if the defender implements the  $j$ th defense plan, referred to as  $\mathcal{D}_j$ , the cost of implementation  $C_j^D$

$$C_j^D = \sum_{k \in \mathcal{D}_j} C_k^{od} \quad (10)$$

should meet the resource constraint

$$C_j^D \leq B^D. \quad (11)$$

In (8) and (9),  $C_k^{oa}$  and  $C_k^{od}$  are the costs representing attack and defense resources with respect to the component  $k$ , respectively; in (10) and (11),  $B^A$  and  $B^D$  are the budgets representing resources of the corresponding attackers and defenders. Changing the system operational state could be also an effective countermeasure for the defender, but in this paper, we only study the online hardening action with respect to the specific components of the system under analysis.

As a consequence of the resource constraints, not all the possible enumerated plans can be realized, and the number of feasible attack and defense plans, referred to as  $N_A$  and  $N_D$ , are

$$N_A \leq (2^{n_A} - 1) \quad (12)$$

$$N_D \leq (2^{n_D} - 1). \quad (13)$$

Obviously, with the variation of the resource, the action-set sizes of the defender and attacker will change as well as the final game results. Therefore, the sensitivity of the risk to the defender's/attacker's resource allocation can be quantified, and the optimal defense resource allocation can be obtained.

A scenario is defined as the set composed of the attack plan chosen by the attacker and the defense plan chosen by the defender. Therefore, there are  $N_A \times N_D$  feasible scenarios with respect to the various attack and defense plans to be analyzed.

Let us consider a scenario in which the attacker implements the attack plan  $\mathcal{A}_i$  and the defender chooses the defense plan  $\mathcal{D}_j$ . We assume that, once the component  $k \in \mathcal{A}_i$  is attacked, it has a probability  $\alpha_k$  to be successfully implemented if no protection measures have been taken by the defender for that component, i.e., when  $k \notin \mathcal{D}_j$ . It has the probability  $\beta_k$  to be successfully implemented with the corresponding protection measures taken by the defender; in other words, if the component  $k \in \mathcal{D}_j$ .

Considering that each component in the set  $\mathcal{A}_i$  has a probability to be successfully destroyed, the damage evaluation of the attack in terms of the economic loss of load  $C_{ij}$  should take into account all the possible cases and, therefore, is expressed as

$$C_{ij} = \sum_{\substack{\forall G_1 \cup G_2 = \mathcal{A}_i \\ \forall H_1 \cup H_2 = \mathcal{D}_j}} \left[ \prod_{k \in G_1} \alpha_k \cdot \prod_{k \in G_2} (1 - \alpha_k) \cdot \prod_{k \in H_1} \beta_k \cdot \prod_{k \in H_2} (1 - \beta_k) \cdot M_{G_1 \cup H_1} \right] \quad (14)$$

where

- $G_1$  the set of components that have not been defended and are destroyed;
- $G_2$  the set of components that have not been defended and are not destroyed;

TABLE III  
ENUMERATION OF POSSIBLE EVENTS WITH REFERENCE  
TO THE COMPONENT STATE AFTER THE ATTACK

Event	State of component after the attack			Probability
	1	2	3	
1	destroyed	not destroyed	not destroyed	$\beta_1 (1 - \alpha_2) (1 - \beta_3)$
2	destroyed	not destroyed	destroyed	$\beta_1 (1 - \alpha_2) \beta_3$
3	destroyed	destroyed	not destroyed	$\beta_1 \alpha_2 (1 - \beta_3)$
4	destroyed	destroyed	destroyed	$\beta_1 \alpha_2 \beta_3$
5	not destroyed	not destroyed	not destroyed	$(1 - \beta_1) (1 - \alpha_2) (1 - \beta_3)$
6	not destroyed	not destroyed	destroyed	$(1 - \beta_1) (1 - \alpha_2) \beta_3$
7	not destroyed	destroyed	not destroyed	$(1 - \beta_1) \alpha_2 (1 - \beta_3)$
8	not destroyed	destroyed	destroyed	$(1 - \beta_1) \alpha_2 \beta_3$

$\mathcal{H}_1$  the set of components that have been defended but are destroyed;

$\mathcal{H}_2$  the set of components that have been defended and are not destroyed.

To illustrate the calculation of  $C_{ij}$ , let  $\mathcal{A}_i$  contain the components 1, 2, and 3 and  $\mathcal{D}_j$  contain the components 1 and 3. The possible events that could occur in relation to the state of the components after the attack are mutually exclusive, and they are listed in Table III. The value of  $C_{ij}$  can be derived by adding up the products of the probability of each event (please see the last column in Table III) and the consequent economic damage.

The analysis considers a worst-case scenario: i.e., the destruction of the components. Although the pure tripping of the component might cause important consequences (even a blackout), their complete destruction will result in more difficulty for recovering the system and, hence, causes more significant losses/impact. Thorough investigations need to be made for studying the effects of attacks onto complex power systems. In this paper, the extent of the successful attack is expressed by assigning to it a probability, but the difference between tripping and destroying components is not highlighted. Since this paper's focus is on the strategic interactions in malicious attack, the modeling of the attack effects is simplified.

### B. Framework of the Game Evolution

The evolution of power-system configurations with respect to the risk of blackouts from nonterrorist cascading failures is introduced in [24]. In this paper, the system vulnerability and the associated risk analysis are carried out in terms of the equilibrium of the game between the defender and the attacker. With the variation of the system configuration/topology, and the resources of the defender and the attacker, the equilibrium changes accordingly—hence, the risk assessment should be performed repetitively at successive moments, as shown in Fig. 1. For each variation of the situation of the power system, the defender, and the attacker, a new game is established with a new equilibrium. For example, at time point  $t_i$ , the defender's decision of online defense action takes effect at once, therefore, will participate in the game at  $t_i$ , while the defender's decision of the defense action with time delay changes the system topology at  $t_j$ ; hence, it will influence the equilibrium at  $t_j$ .

### C. Equilibrium of the Game

We propose to consider an MSE, in which, at the equilibrium (theoretically, it always exists), a probability is given to each

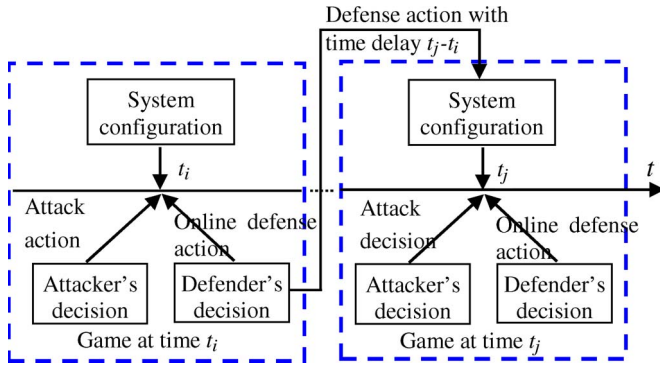


Fig. 1. Risk analysis based on game model along the time axis.

action in the action set. The equilibrium may not be unique—in some cases, in fact, multiple equilibria can arise from the game. Considering mixed strategies, the expected payoff of the players can be evaluated, and the probabilities assigned to the actions are derived. Therefore, it is possible to evaluate the risk with reference to the associated utility of the defender. Searching the equilibrium is always a difficult problem, since it is computationally expensive, particularly with a large action set. Proper algorithms need to be developed to handle real-case problems.

The traditional enumeration approach is applied to solve the game treated in this paper. It is an indirect way to search the equilibrium, which derives from the nature of the MSE. Namely, at equilibrium, the probability assignment to the defender's/attacker's actions should make uniform the utilities of the attacker's/defender's nonzero-probability actions. Moreover, the utility of the nonzero-probability actions should be greater than that of the zero-probability actions. According to this property, an enumeration approach is recommended in [25], where, with different cases of the zero-probability distribution, a set of the linear equations can be listed and solved for limited action sets. If the action set is not big, the approach is very direct and efficient and it is widely used to demonstrate solutions of MSE problems. However, the computation will be exponentially increased with the action-set expansion. Usually, the evolutionary computation will be resorted to for big action set [26], [27], but global optimum is not assured.

We propose an alternative approach based on optimization, in which the uniform utilities property can be transformed to minimize the difference among the utilities.

Let us suppose that  $p_i^A$  and  $p_j^D$  are, respectively, the probabilities of choosing the  $i$ th attack plan  $A_i$  and the  $j$ th defense plan  $D_j$ . Starting from the evaluation of the attack in terms of the economic loss of load, i.e.,  $C_{ij}$ , the expected costs/losses of the system is determined as

$$E_{ij} = p_i^A p_j^D C_{ij}. \quad (15)$$

The expected utility of the attacker corresponding to the  $i$ th plan  $S_i^A$  is

$$S_i^A = p_i^A A_i \quad (16)$$

where

$$A_i = -C_i^A + \sum_{j=1}^{N_D} p_j^D (C_{ij} + C_j^D). \quad (17)$$

The expected utility of the defender corresponding to the  $j$ th defense plan  $S_j^D$  is

$$S_j^D = p_j^D D_j \quad (18)$$

where

$$D_j = -C_j^D + \sum_{i=1}^{N_A} p_i^A (C_{ij} + C_i^A). \quad (19)$$

Therefore, the utility of the attacker  $S^A$  and of the defender  $S^D$  are given by

$$S^A = \sum_{i=1}^{N_A} S_i^A \quad (20)$$

$$S^D = \sum_{j=1}^{N_D} S_j^D. \quad (21)$$

The problem of the search of the MSE can be therefore formulated, as explained in the following. For the attacker, the search of MSE can be found by solving

$$p_k^A \left( \sum_{i=1}^{N_A} p_i^A A_i - A_k \right) = 0 \quad (k = 1, \dots, N_A) \quad (22a)$$

$$\sum_{i=1}^{N_A} p_i^A A_i - A_k \geq 0 \quad (k = 1, \dots, N_A) \quad (22b)$$

$$0 \leq p_i^A \leq 1 \quad (i = 1, \dots, N_A) \quad (22c)$$

$$\sum_{i=1}^{N_A} p_i^A = 1 \quad (22d)$$

where the rules for determining the equilibrium can be explained as follows.

- 1) Since the actions with nonzero probabilities have a uniform utility and  $\sum_{i=1}^{N_A} p_i^A = 1$ , therefore, if  $p_k^A \neq 0$ , then  $\sum_{i=1}^{N_A} p_i^A A_i = A_k$ , and this makes the (22a) true.
- 2) Since the utility of the nonzero-probability actions is greater than that of the zero-probability actions and  $\sum_{i=1}^{N_A} p_i^A A_i$  is equal to the utility of any nonzero-probability action, therefore, if  $p_k^A = 0$ , then  $\sum_{i=1}^{N_A} p_i^A A_i > A_k$ .
- 3) Considering both 1) and 2), (22b) is proved.

Analogously, for the defender, the following equations should be satisfied:

$$p_k^D \left( \sum_{j=1}^{N_D} p_j^D D_j - D_k \right) = 0, \quad k = 1, \dots, N_D \quad (23a)$$

$$\sum_{j=1}^{N_D} p_j^D D_j - D_k \geq 0, \quad k = 1, \dots, N_D \quad (23b)$$

$$0 \leq p_i^D \leq 1, \quad k = 1, \dots, N_D \quad (23c)$$

$$\sum_{i=1}^{N_D} p_i^D = 1. \quad (23d)$$



In (22) and (23), the variables are the probabilities of the attacker's actions  $p_k^A (k = 1, \dots, N_A)$  and of the defender's actions  $p_k^D (k = 1, \dots, N_D)$ .

Solving jointly (22) and (23), the MSE is identified. An effective way to approach the solution point is to transform (22) and (23) into an optimization problem as

$$\min \left\{ \left[ \sum_{k=1}^{N_A} p_k^A \left( \sum_{i=1}^{N_A} p_i^A A_i - A_k \right)^2 \right] + \left[ \sum_{k=1}^{N_D} p_k^D \left( \sum_{i=1}^{N_D} p_i^D D_i - D_k \right)^2 \right] \right\} \quad (24a)$$

s.t.

$$\sum_{i=1}^{N_A} p_i^A A_i - A_k \geq 0, \quad k = 1, \dots, N_A \quad (24b)$$

$$0 \leq p_i^A \leq 1, \quad \sum_{i=1}^{N_A} p_i^A = 1 \quad (24c)$$

$$\sum_{i=1}^{N_D} p_i^D D_i - D_k \geq 0 \quad (k = 1, \dots, N_D) \quad (24d)$$

$$0 \leq p_i^D \leq 1, \quad \sum_{i=1}^{N_D} p_i^D = 1. \quad (24e)$$

The optimization problem (24) is a constrained quadratic optimization problem and can be conveniently solved. The objective function (24a) is the sum of  $N_A + N_D$  quadratic terms, and so to minimize (24a) is to actually minimize the  $N_A + N_D$  quadratic terms, the minimum of (24a) should be zero, and it is acquired at the equilibrium, where (22) and (23) are both respected. Moreover, since every term of (24a) can be zero, to minimize (24a) is to minimize the difference among the utilities of the nonzero-probability actions. The equilibrium is found when the objective function (24a) is zero, which can be taken as true in practice when the objective function is below a threshold.

#### IV. RISK ASSESSMENT OF MALICIOUS THREATS

With the actions set and the corresponding utilities computed, the game can be solved by the approaches provided in the previous section, and the MSE can be obtained as well as the probabilities of the various plans. The risk is defined as the product of the probability and the corresponding damages, which can be taken as the utility of the attacker. Namely, the risk can be expressed as

$$\gamma = \sum_{i=1}^{N_A} p_i^A \cdot S_i^A \quad (25)$$

which is also the expected payoff of the attacker. According to [25, Lemma 364.1] which states that “the expected payoff of each player in any mixed strategy Nash equilibrium of a strategic game is at least equal to his/her maximized payoff,” we propose a more general model of that in [10], which can be considered as a special case of our model.

It should be noticed that, in our MSE model, probabilities are assigned to the actions, and each action may contain several components. The probability of being attacked/defended prob-

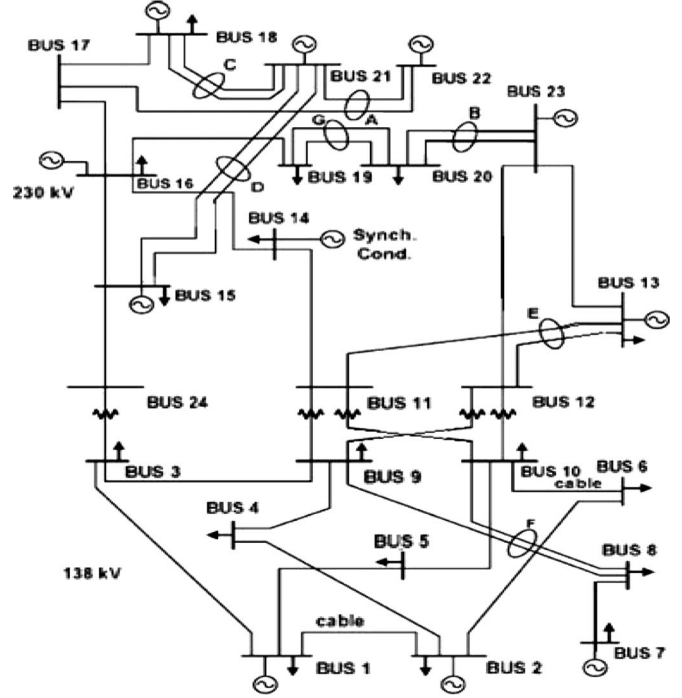


Fig. 2. IEEE RTS 96 24-bus system.

ability of a specific component is the sum of the probabilities of the attack/defense actions that contain the component.

The probability of the  $k$ th component to be attacked is

$$p_k^{oa} = \sum_{\substack{i=1 \\ \text{if } \{k\} \subseteq \mathcal{A}_i}}^{N_A} p_i^A. \quad (26)$$

Therefore, the vulnerability of the system can be assessed with respect to the ranking of system components regarding their probability of being attacked.

The probability of the  $k$ th component to be defended is

$$p_k^{od} = \sum_{\substack{j=1 \\ \text{if } \{k\} \subseteq \mathcal{D}_j}}^{N_D} p_j^D. \quad (27)$$

The defense probability of each component at the equilibrium, which is the outcome of the game, is also obtained. At the equilibrium, once the defender keeps its strategy, no matter which decision the attacker takes, the expected consequence will not be altered. Namely, if the defender follows the strategy defined at the equilibrium, there is a corresponding fixed risk. Adopting the defense strategy at the equilibrium, the risk can be controlled below the risk at equilibrium. Therefore, on the one hand, the risk evaluation establishes a link between the resources (budgets) and the risk so as to set a reference for budget allocation; on the other hand, it provides an effective strategy to control the risk.

#### V. NUMERICAL SIMULATIONS

To illustrate the application of our model to the security assessment of malicious threats to, the IEEE RTS 96 System [28] is taken as the test system.

TABLE IV  
BUDGET AND THE ACTION COST IN BASE CASE\*

Player	Action	Cost	Budget
Attacker	Attack single line	30	60
	Attack single bus	60	
Defender	Defending single line	60	60
	Attacking single bus	30	

The IEEE RTS 96 24-bus system is composed of 24 buses, 38 lines, and 32 generators (Fig. 2). The load profile is defined as that of the winter weekday at 1800 [28].

The base case of the attack and defense budgets and costs of a single line or a single bus is shown in Table IV. The successful destruction rate with/without protection (online defense action) of the power-system components are, respectively,  $\beta_k = 0.2$  and  $\alpha_k = 0.8$ . For the unserved energy, we take the direct cost of \$0.66/kWh and the indirect cost \$3.45/kWh [2], and the average recovery time of the failure is 72 h [10]; therefore the cost-shedding evaluation factor is assumed as  $l_m = (0.66 + 3.45) \$/\text{kWh} \cdot 72 \text{ h} = 0.296 \$/\text{W}$ .

The objectives are to determine the vulnerability of the system, assess the risk sensitivity to the resources of the attacker and the defender, and obtain the optimal resource allocation for the defender. The defense actions refer only to the online defense action, since the impacts of the action with a time delay can be considered as changes in the system topology.

In the following points, we present the simulation in three steps. First, we test the proposed approach with respect to the computational burden, in order to justify the performance of the algorithm. Second, the risk assessment of the base case of the test system is carried out; the risk sensitivity and the sensitivity analysis of the probabilities of being attacked/defended with reference to the variation of the destruction rate  $\beta_i$ , and the defense and attack resource are presented.

#### A. Algorithm Testing

To carry out the risk analysis, the MSE should be efficiently found. We tested the approaches proposed in Section IV for solving the MSE as shown in Table V, where “—” means the approach cannot get convergence or cannot find the equilibrium in half an hour. The efficiency of the traditional approach, which is detailed in Section IV-C, rapidly goes down with the increase of the action set size. It takes more 2325 s with the set size 15 for the traditional approach but only 0.328 s for the approach proposed. The efficiency of the algorithm is acceptable (840.7 s for the set with 232 actions). Moreover, the optimization algorithm presents good performance with respect to its accuracy, which is assured by the value of the objective function approaching to zero (in Table V, the maximum objective function value is  $1.09 \times 10^{-6}$ ). Therefore, the optimization approach is selected as the MSE algorithm for the following steps of the analysis.

Even when considering resource constraints, the sizes of the action sets are usually huge with middle-scale systems. When studying the probabilities of MSE, we find that they are unevenly distributed, and the nonzero probabilities are always assigned to a few actions. Therefore, for the sake of simplifica-

TABLE V  
MSE APPROACHES TEST WITH ACTION SETS OF DIFFERENT SIZES

Size of the action set	Traditional approach T (s)	Optimization approach T (s)	Obj
2	0	0.015	$9.57 \times 10^{-27}$
6	1.28	0.125	$4.26 \times 10^{-12}$
15	2325	0.328	$2.46 \times 10^{-11}$
30	-	0.578	$9.35 \times 10^{-11}$
67	-	5.25	$1.09 \times 10^{-6}$
137	-	200.03	$1.27 \times 10^{-23}$
232	-	840.7	$7.70 \times 10^{-10}$

tion, we reduce the size of the action set by only considering a certain number of possible actions. For example, 50 attack actions ( $i$ ) with the largest  $\sum_j C_{ij}$  are considered, and 50 defense actions ( $j$ ) with the largest  $\sum_i C_{ij}$  are considered.

#### B. Risk Assessment and Sensitivity Analysis

With the given power-system configuration and the data of the defender and attacker, the MSE of the game is solved. Being the foreseen result of the game, the MSE provides a way to assess the power-system vulnerability and the associated risk in terms of the stable situation at the equilibrium. At equilibrium, the defense/attack plans with nonzero probabilities and the risks are shown in Table VI, which is obtained by solving the optimization problem (24). The vulnerability of the system can be represented by the probability of the components to be attacked and defended as shown in Table VII. The equilibrium is a steady state where the attacker chooses the buses 8, 13, 15, and 18 and lines 15–21 and 16–17 as the target of the offensive actions, and the defender chooses to defend buses 8, 13, 15, and 18 and line 15–21 with the probabilities given in Table VII. For each attack action in Table VI, the expected payoff of the attacker is \$60 560 and that of the defender is  $-\$60 560$ , since it is modeled as a zero-sum game. Namely, at this state, neither the attacker nor the defender will unilaterally change their decision.

1) *Variation of the Destruction Rate  $\beta_k$  ( $\beta_k \leq \alpha_k$ ):* From the technical point of view, the lower the  $\beta_k$ , the better the corresponding component is protected. The risk variation with the decrease of  $\beta_k$  is shown in Fig. 3.  $\beta_k = 0.8$  and  $\beta_k = 0$  are two extreme cases; the former one means that the defense measures cannot make any difference with regard to the attacks, and the latter one means that the defended component will definitely not be destroyed. In Fig. 3, we find that the decrease of  $\beta_k$  is an effective way of decreasing the risk; the risk decrease rate is diminishing with the diminution of  $\beta_k$ , which implies that if  $\beta_k$  is high, it is more effective to lower  $\beta_k$ . For instance, if  $\beta_k$  decreases from 0.8 to 0.7, the risk decreases of \$14 370, but the corresponding risk reduction is only \$2736 when  $\beta_k$  decrease from 0.1 to 0. Moreover, even with  $\beta_k = 0$  there is an obvious bottleneck of the minimum risk \$54 718.

Fig. 4 shows the evolution of all the nonzero-attack probabilities of the components. When the defense measures have no effect (i.e.,  $\beta_k = 0.8$ ), the attacking pattern is definite with the targets line 15–21 and line 16–17. With the decrease of

TABLE VI  
MSE OF THE GAME WITH REFERENCE TO THE IEEE RTS 96 SYSTEM

Attacker		$S_i^A(k\$)$	$\gamma_i$	Defender		$p_i^d$	$\Sigma\gamma_i$
Attack action	$p_i^a$			Defense action	$p_i^d$		
1 Bus: 8	0.1946	60.56	11.78	1 Bus: 8, 15	0.071	60.56	
2 Bus:13	0.2174	60.56	13.17	2 Bus: 8, 18	0.0945		
3 Bus:15	0.1817	60.56	11.00	3 Bus: 13, 15	0.0289		
4 Bus:18	0.173	60.56	10.48	4 Bus: 15, 18	0.1719		
5 Line: 15-21,16-17	0.2332	60.56	14.12	5 Line: 15-21	0.6338		

TABLE VII  
BEING ATTACKED AND DEFENDED PROBABILITIES OF THE COMPONENTS AT THE MSE

Component	Bus8	Bus13	Bus15	Bus18	Line 15-21	Line 16-17
Probability of being attacked	0.1946	0.2174	0.1817	0.173	0.2332	0.2332
Probability of being defended	0.1655	0.0289	0.2718	0.2664	0.6338	0

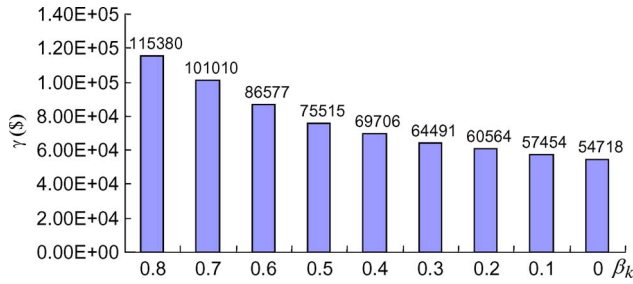


Fig. 3. Risk sensitivity to the variation of the destroy rate  $\beta_k$ .

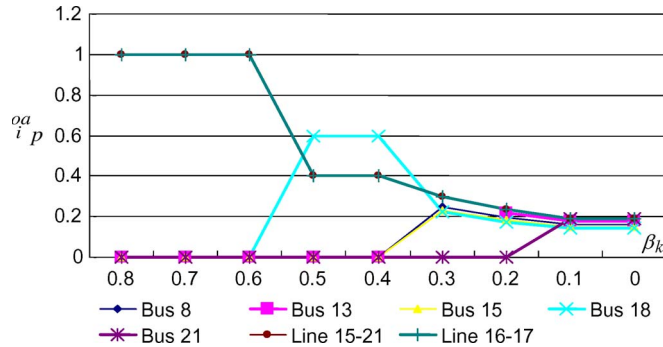


Fig. 4. Being-attacked probabilities of the components with the variation of  $\beta_k$ .

$\beta_k$ , the targeting becomes dispersed; when  $\beta_k = 0$ , the attacked probabilities of the components are very similar.

Fig. 5 shows the evolution of the nonzero probabilities for all the defended components. When the defense measures have no effect ( $\beta_k = 0.8$ ), the defender would choose to implement no defense. With the decrease of  $\beta_k$ , there will be more and more components to be defended, and it is interesting to find that the components seem to have various relative priorities with respect to the probabilities for being defended. This phenomenon is more distinctive for the buses, for instance, bus 18 always keeps its advantage of  $p_k^{od}$  over the other buses.

2) *Variation of the Defense Resources*: The defense resources are a key contributor to the risk variation. Fig. 6 shows the risk sensitivity with respect to the variation of the defense resource  $B^D$ . With the increase of  $B^D$ , the risk diminishes accordingly. Once  $B^D$  is just over the threshold of defending two lines (i.e., 60, as defending one line is meaningless, since the “ $n - 1$ ” principle should be kept), the risk is greatly reduced.

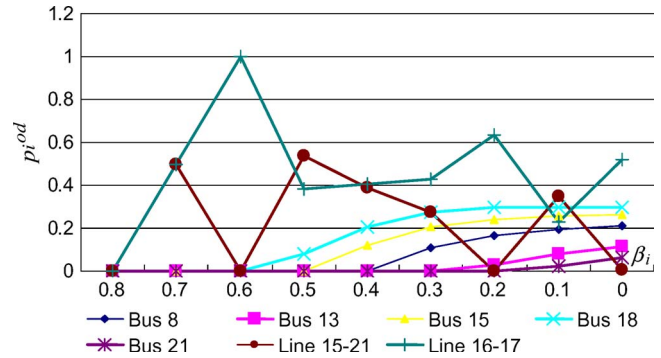


Fig. 5. Being-defended probabilities of the components with the variation of  $\beta_k$ .

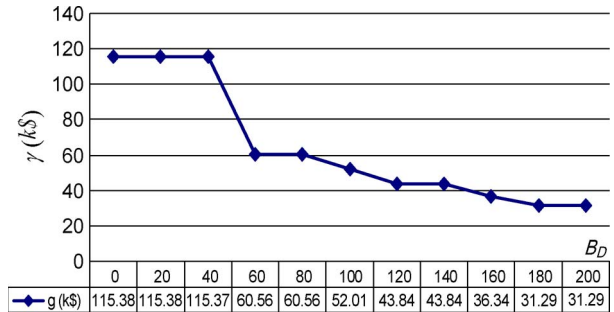


Fig. 6. Risk sensitivity to the variation of the defense resource  $B^D$ .

But with the continuous increase of the defense resources, the reduction rate of the risk will be gradually decreased. This fact provides a basis for the optimal allocation of the defense resources. Compared with Fig. 3, there must be a tradeoff between the limited available resources and the resources devoted to the single components. At a certain level of  $\beta_i$ , to allocate the limited resources to defend more components might be more effective for decreasing the risks.

The evolution of the probabilities of being attacked as function of the increase of the  $B^D$  is shown in Fig. 7. It is quite similar to Fig. 4: When  $B^D$  is under a threshold, the defense is not effective, and the targeted components will be definitely attacked. With the increase of  $B^D$ , more and more components are targeted with various probabilities, namely, the increase of  $B^D$  will disperse the probability of being attacked among the various components.

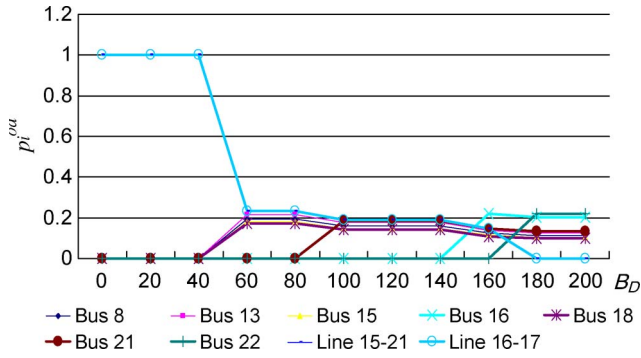


Fig. 7. Being-attacked probabilities of the components with the increase of the defense resources  $B^D$ .

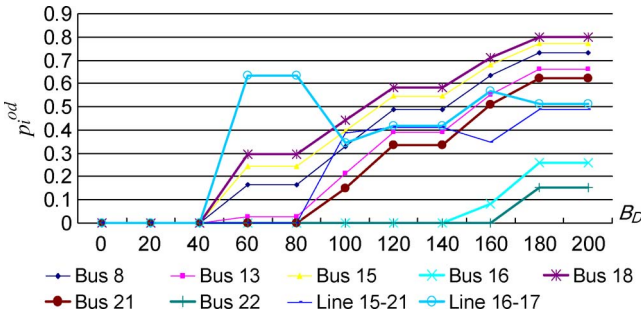


Fig. 8. Being-defended probabilities of the components with the increase of the defense resources  $B^D$ .

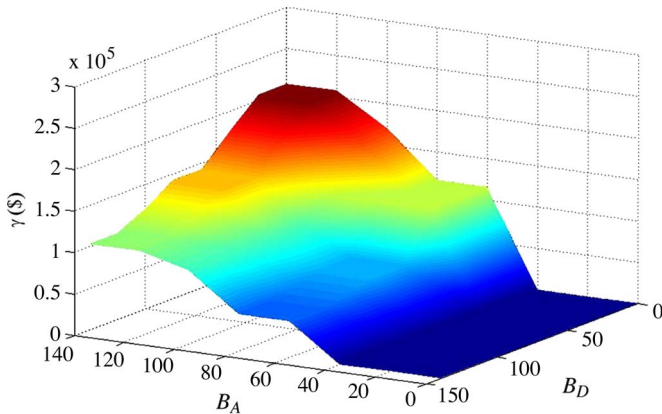


Fig. 9. Risk sensitivity to the variation of the resource of the defender and the attacker.

The evolution of the probabilities of being defended as a function of  $B^D$  is shown in Fig. 8. In the beginning, there are no enough resources to implement the defense action, while with the increase of the defense resources, the probabilities of being defended have an obvious increasing tendency, and some components gain more probability of being defended.

3) *Risk Sensitivity to the Defense/Attack Resources*: Fig. 9 shows the risk variation with respect to the various resources of the defender and attacker.

The increase of the attack resources increases the impact of the attack, rapidly showing the effect of the infrastructure as a consequence amplifier. On the contrary, to curb the attack effects, the increase of the defense budget is much less effective. In other words, the risk of the attacker is very sensitive to the

budget of the attacker, but much less sensitive to the budget of the defender. With reference to the objective of diminishing the risk, this quantitative analysis allows the understanding of how effective is the increase of the defense resources as well as how effective it would be to control the resources of the attacker.

## VI. CONCLUSION

The specificity of malicious attacks lies in the interaction between entities with conflicting interests and cannot be fully studied with traditional approaches suitable for natural threats (as, for instance, probabilistic risk analysis).

Game theory provides a sound approach to model strategic interaction between defenders and attackers in the context of malicious attacks. This paper shows how useful analytical tools, based on the hypothesis of MSE, can be implemented for those strategic interaction models and used to study different attack–defense scenarios. A key point is that, for finding the MSE, we developed an efficient optimization algorithm, which accounts for the model application to a real-size system. Particularly, our approach supports the assessment of the likelihood of attacks to different components of power systems, for then ranking those components in terms of the associated risk. This kind of analysis can be exploited for designing proper defense plans and for allocating scarce resources to the most convenient defense actions in protecting the most sensitive targets.

As an example of the possibilities provided by the approach and the tool, the analysis undertaken for the simple test system brings preliminary conclusions. The risk sensitivity of the resources, in terms of the amount of resources and budget allocated to pursue their targets, is much higher for the attacker than for the defender, showing the amplifying effect of the network structure of power systems with respect to action of the attackers. Defense measures to strengthen the power systems have the effect of causing the dispersion of the offensive actions deployed by the attacker.

## REFERENCES

- [1] S. Corsi and C. Sabelli, "General blackout in Italy Sunday September 28, 2003, h. 03:28:00," in *IEEE Power Eng. Soc. Gen. Meet.*, Jun. 6–10, 2004, vol. 2, pp. 1691–1702.
- [2] U.S. Congress Office of Technology Assessment, *Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage*, 1990, Washington, DC: U.S. Government Printing Office. OTA-E-453. [Online]. Available: <http://www.wvns.princeton.edu/cgi-bin/byteserv/prl/~ota/disk2/1990/9034/9034.PDF>
- [3] *Security Guidelines for the Electricity Sectors: Physical Response*, NERC, Princeton, NJ, Nov. 1, 2005.
- [4] *Threat Alert System and Cyber Response Guidelines for the Electricity Sector—Definitions of Cyber Threat Alert Levels*, NERC, Princeton, NJ, Oct. 8, 2002.
- [5] W. Fu and J. D. McCalley, "Risk assessment for transformer loading," *IEEE Trans. Power Syst.*, vol. 16, no. 3, pp. 346–353, Aug. 2001.
- [6] J. D. McCalley and W. Fu, "Reliability of the special protection system," *IEEE Trans. Power Syst.*, vol. 14, no. 4, pp. 1400–1406, Nov. 1999.
- [7] M. Ni, J. D. McCalley, and V. Vittal, "Online risk-based security assessment," *IEEE Trans. Power Syst.*, vol. 18, no. 1, pp. 258–265, Feb. 2003.
- [8] M. Ni, J. D. McCalley, V. Vittal, S. Greene, C.-W. Ten, V. S. Ganugula, and T. Tayyib, "Software implementation of online risk-based security assessment," *IEEE Trans. Power Syst.*, vol. 18, no. 3, pp. 1165–1172, Aug. 2003.
- [9] V. M. Bier, E. R. Gratz, N. J. Haphuriwat, W. Magua, and R. W. Kevin, "Methodology for identifying near-optimal interdiction strategies for a power transmission system," *Reliab. Eng. Syst. Saf.*, vol. 92, no. 9, pp. 1155–1161, Sep. 2007.

- [10] J. Salmeron, K. Wood, and R. Baldick, "Analysis of electric grid security under terrorist threat," *IEEE Trans. Power Syst.*, vol. 19, no. 2, pp. 905–912, May 2004.
- [11] J. M. Arroyo and F. D. Galiana, "On the solution of the bilevel programming formulation of the terrorist threat problem," *IEEE Trans. Power Syst.*, vol. 20, no. 2, pp. 789–797, May 2005.
- [12] C. Tranchita, N. Hadsaid, and A. Torres, "Ranking contingency resulting from terrorism by utilization of the Bayesian networks," in *IEEE Melecon*, Benalmadena, Spain, May 16–19, 2006, pp. 964–967.
- [13] D.-Z. Zeng, L. Fang, K. W. Hipel, and D. M. Kilgour, "Policy equilibrium and generalized metarationalities for multiple decision-maker conflicts," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 37, no. 4, pp. 456–463, Jul. 2007.
- [14] T. Sandler, J. T. Tschirhart, and J. Cauley, "A theoretical analysis of transnational terrorism," *Amer. Polit. Sci. Rev.*, vol. 77, no. 1, pp. 36–54, Mar. 1983.
- [15] J. Cauley and E. I. Im, "Intervention policy analysis of skyjackings and other terrorist incidents," *Amer. Econ. Rev.*, vol. 78, no. 2, pp. 27–31, 1988.
- [16] H. E. Lapan and T. Sandler, "To bargain or not to bargain: That is the question," *Amer. Econ. Rev.*, vol. 78, no. 2, pp. 16–20, 1998.
- [17] R. Selten, "A simple game model of kidnappings," in *Models of Strategic Rationality*, R. Selten, Ed. Boston, MA: Kluwer, 1988, pp. 77–93.
- [18] T. Sandler and H. E. Lapan, "The calculus of dissent: An analysis of terrorists' choice of targets," *Synthese*, vol. 76, no. 2, pp. 245–261, Aug. 1988.
- [19] G. Daniel, M. Arce, and T. Sandler, "Counter terrorism—A game theoretic analysis," *J. Confl. Resolut.*, vol. 49, no. 2, pp. 183–200, 2005.
- [20] J. Holmgren, E. Jenelius, and J. Westin, "Evaluating strategies for defending electric power networks against antagonistic attacks," *IEEE Trans. Power Syst.*, vol. 22, no. 1, pp. 76–84, Feb. 2007.
- [21] O. Berman and A. Gavious, "Location of terror response facilities: A game between state and terrorist," *Eur. J. Oper. Res.*, vol. 177, no. 2, pp. 1113–1133, Mar. 2007.
- [22] E. J. Bass and A. R. Pritchett, "Human-automated judge learning: A methodology for examining human interaction with information analysis automation," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 38, no. 4, pp. 759–776, Jul. 2008.
- [23] A. Padovitz, S. W. Loke, and A. Zaslavsky, "Multiple-agent perspectives in reasoning about situations for context-aware pervasive computing systems," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 38, no. 4, pp. 729–742, Jul. 2008.
- [24] H. Ren, I. Dobson, and B. A. Carreras, "Long-term effect of the n-1 criterion on cascading line outages in an evolving power transmission grid," *IEEE Trans. Power Syst.*, vol. 23, no. 3, pp. 1217–1225, Aug. 2008.
- [25] M. J. Osborne, *An Introduction to Game Theory*. London, U.K.: Oxford Univ. Press, 2004.
- [26] A. Shubham, Y. Dashora, and M. K. Tiwari, "Interactive particle swarm: A Pareto-adaptive metaheuristic to multiobjective optimization, systems," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 38, no. 2, pp. 258–277, Mar. 2008.
- [27] B.-B. Li, L. Wang, and B. Liu, "An effective PSO-based hybrid algorithm for multiobjective permutation flow shop scheduling," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 38, no. 4, pp. 818–831, Jul. 2008.
- [28] C. Grigg, P. Wong, P. Albrecht, R. Allan, M. Bhavaraju, R. Billinton, Q. Chen, C. Fong, S. Haddad, S. Kuruganty, W. Li, R. Mukerji, D. Patton, N. Rau, D. Reppen, A. Schneider, M. Shahidepour, and C. Singh, "The IEEE reliability test system—1996," *IEEE Trans. Power Syst.*, vol. 14, no. 3, pp. 1010–1020, Aug. 1999.



**Ciwei Gao** was born in Chun'an County, Zhejiang Province, China, in 1977. He received the B.S. degree from the North China Electrical Power University, Beijing, China, in 1999, the M.S. degree from Wuhan University, Wuhan, China, in 2002, the Ph.D. degree from the Politecnico di Torino, Torino, Italy, in 2006, and the Ph.D. degree from Shanghai Jiaotong University, Shanghai, China, in 2007.

He is currently an Associate Professor with the School of Electrical Engineering, Southeast University, Nanjing, China.



**Roberto Napoli** (M'74) was born in Palermo, Italy, in 1945. He received the degree in electrotechnical engineering from the Politecnico di Torino, Torino, Italy, in 1969.

He is currently with Politecnico di Torino, where he is a Full Professor of electric power systems, a member of the Board of Directors of Politecnico di Torino, and the Deputy Dean of the 1st Engineering Faculty. He is also the leader of the local Power System Group and is heavily involved in many national and international research projects. He has

been a National Coordinator of several boards (the Italian Power System Group GUSEE, Italian Power System Board of Electrical Engineering Presidents, etc.). His broad international academic experiences have been coupled with a top professional activity, designing and directing several important power system projects inside and outside Italy. His main scientific interests cover various aspects of electric systems, including analysis and modeling, transmission planning, market modeling, distributed generation, and renewable energy sources.



**Angela Russo** was born in Cassino, Italy, in 1972. She received the M.S. degree in electrical engineering and the Ph.D. degree in industrial engineering from the Università degli Studi di Cassino, Cassino, Italy, in 1996 and 2000, respectively.

She is currently an Assistant Professor of electrical power systems with the Dipartimento di Ingegneria Elettrica, Politecnico di Torino, Torino, Italy. Her research interests concern power-system analysis.



**Marcelo Masera** was born on September 22, 1956. He has the Engineering degree in electronics and electricity from the University of Mendoza, Argentina, in 1980.

From 1981 to 1989, he was a Researcher in the areas of risk and reliability with the National Research Council of Argentina. He was a Visiting Scientist at the Joint Research Centre (JRC), Ispra, Italy, from 1990 to 1992 and from 1997 to 1998. Since November 2000, he has been a Scientific Officer with the Institute for the Protection and Security of the

Citizen, JRC, European Commission, where he is in charge of the "Security of Critical Networked Infrastructures" area. His interests include the dependability and security of complex socio-technical systems and, specifically, those related to critical infrastructures, large-scale systems-of-systems, information and communication technologies, and the information society. He has published more than 60 papers in the fields of dependability, security, and risk.



**Alberto Stefanini** received the degree in electronic engineering from the University of Bologna, Bologna, Italy, 1974.

He was with the Joint Research Centre, Institute for the Protection and Security of the Citizen, European Commission, Ispra, Italy, until November 2008, and was involved in studies on critical infrastructure protection (CIP), with specific focus on power systems. He is currently a private consultant. His current interests include cyber security assessment of control systems and participation to

standardization efforts, coordination of research activities on CIP, and dissemination of relevant best practices.



**Ettore Bompard** (M'99) received the M.S. and Ph.D. degrees in electrical engineering from the Politecnico di Torino, Torino, Italy.

Since May 1997, he has been with the Politecnico di Torino, where he is currently an Associate Professor with the Dipartimento di Ingegneria Elettrica. He is also with the Institute for Economic Research Firms and Growth (CERIS-CNR), National Research Council, Mancalieri (TO), Italy. He was a Visiting Assistant Professor in the Electrical and Computer Engineering Department, University of

Illinois at Urbana-Champaign, Urbana, in 2001. He was in charge for the scientific direction of many research projects within the Italian System Research on power systems in the fields related with electricity industry restructuring. His research activities include power systems and electricity market analysis and simulation.