HAL
open science

A general framework for the assessment of power system vulnerability to malicious attacks

R. Piccinelli, G. Sansavini, R. Lucchetti, Enrico Zio

To cite this version:

R. Piccinelli, G. Sansavini, R. Lucchetti, Enrico Zio. A general framework for the assessment of power system vulnerability to malicious attacks. Risk Analysis, 2017, 37 (11), pp.2182 - 2190. 10.1111/risa.12781 . hal-01786942

HAL Id: hal-01786942

https://hal.science/hal-01786942

Submitted on 23 Mar 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

A general framework for the assessment of power system vulnerability to malicious attacks

R. Piccinelli,[4] G. Sansavini,[1] R. Lucchetti,[2] and E. Zio[3,4,*]

1 Reliability and Risk Engineering Laboratory, Institute of Energy Technology, Department of Mechanical and Process Engineering, ETH Zurich, Zurich, Switzerland.

2 Dipartimento di Matematica - Politecnico di Milano, Milano, Italy.

3 Chair System Science and The Energy Challenge, Fondation Electricite' de France (EDF), CentraleSupelec, Universit ´e Paris-Saclay, Chatenay-Malabry, France.

4 Dipartimento di Energia – Politecnico di Milano, Milano, Italy.

∗ Address correspondence to Enrico Zio; enrico.zio@polimi.it

Abstract. The protection and safe operations of power systems heavily rely on the identification of the causes of damage and service disruption. This paper presents a general framework for the assessment of power system vulnerability to malicious attacks. The concept of susceptibility to an attack is employed to quantitatively evaluate the degree of exposure of the system and its components to intentional offensive actions. A scenario with two agents having opposing objectives is proposed, i.e. a defender having multiple alternatives of protection strategies for system elements, and an attacker having multiple alternatives of attack strategies against different combinations of system elements. The defender aims to minimize the system susceptibility to the attack, subjected to budget constraints; on the other hand, the attacker aims to maximize the susceptibility. The problem is defined as a zero-sum game between the defender and the attacker. The assumption that the interests of the attacker and the defender are opposite, makes it irrelevant whether or not the defender shows the strategy he/she will use. Thus, the approaches "Leader-Follower game" or "simultaneous game" do not provide differences as far as the results are concerned. The results show an example of such a situation, and the von Neumann theorem is applied to find the (mixed) equilibrium strategies of the attacker and of the defender.

Keywords: Susceptibility, zero-sum game, power systems, vulnerability, intentional attacks.

1. INTRODUCTION

Energy supply systems, such as power grids, are critical assets as any incapacity or destruction can have a debilitating impact on the Society's efficiency, safety, security and economics [1]. Determining their degree of exposure to hazards and intentional attacks has become a topic of great concern. An analysis aimed at identifying the causes of damage or disruption of services in power systems is necessary for safe operations and protection. This requires an evaluation of the susceptibility to different hazards, including threats of malevolent acts.

A key part of this analysis is the explicit modeling of the adversary behavior during an attack. To this aim, game theoretic methods are particularly attractive and have been widely used in risk analysis [2-6]. By focusing on the strategic interaction between the adversaries, these methods lead to behavioral predictions that explicitly account for the adaptive, intelligent nature of the adversary. A sense of the span, dimension and depth of the literature on the defense and attack of a system can be found in the review paper [7] and references therein. This review classifies and categorizes recent published papers according to the system structures, defense measures, and attack tactics and circumstances. Bier [8] describes a strategic model in which a defender must allocate defensive resources to a collection of locations and an attacker must choose a location to attack. The attacker – defender interaction focus on security investments and costs but choose different payoffs for a given target. Major [9] assumes that defenders and attackers have exactly the same valuations for potential targets: the value to the attacker is given only on the damage inflicted on the defender. But in principle, the value of the attacker of successfully attacking a given target may depend on factors different from the physical damage, such as the social impact of the damage inflicted.

In this paper, a framework is proposed to assess the degree of exposure of a system to intentional attacks. The concept of susceptibility to an attack is employed to quantitatively assess the degree of exposure of the system and its components to intentional offensive actions. The susceptibility of a component is evaluated as a function of the characteristics of the system, i.e. size, level of protection and social criticality, and of the factors underpinning an intentional attack, i.e. attractivity and accessibility. The total susceptibility of a specific system configuration is quantified as the sum of the susceptibilities of its components.

The defender-attacker dynamics is modeled as a two-player zero-sum game, in which the attacker aims to incapacitate the component with the highest degree of exposure to threats, i.e. to maximize system susceptibility, and the defender aims to minimize the degree of exposure to attacks of the different components, i.e. to minimize system susceptibility. Attacker and defender are supposed to select their strategies independently, without observing the strategy chosen by the other player before choosing his own strategy. In infrastructure security, this hypothesis has been referred as non realistic since, for example, the defender may engage in costly defensive improvements over time and some of those defensive investments may be observable by the attacker [10]. However, some terrorist acts suggest that the attackers may indeed be choosing their targets regardless of the observed defense level [11] or attackers may choose to act without acquiring costly information about the security strategy, especially if security measures (e.g. surveillance, alarms) are difficult to obtain [12]. In such instances, the competition between the attacker and the defender may be realistically represented by a simultaneous-move zero-sum game. On the other hand, this type of games may fail in capturing the conflicting and partly conflicting interests between operator and generators in power markets [13]. To this aim, Leader-Follower games are deployed in which the generator, i.e. the follower, chooses his strategy after observing the strategies announced by the operator, i.e. the leader [13]. By assuming that the interests of the attacker and the defender are opposite, it is irrelevant whether or not the defender shows the strategy he will use. In this perspective, the objective of the study is (I) to find the less vulnerable configuration of the system that can be deployed, given a budget constraint, and (II) to identify the best strategies for the attacker and the defender.

The paper is structured as follows: in Section 2, the concept of susceptibility and its quantitative assessment are introduced. In Section 3, the scheme of the game is proposed, and in Section 4 the game is applied to a conceptual example of a power system in which the components are aggregated according to their operational role. Conclusions are presented in Section 5.

2. QUANTIFICATION OF SUSCEPTIBILITY

The concept of vulnerability follows the degree of impact that a hazard has on Critical Infrastructures (CIs). In [14], vulnerability is defined as the “manifestation of inherent states of the system (e.g., physical,

technical, organizational, cultural) that can be exploited by an adversary to harm or damage the system". Along the same line of thought, in [15] and [16] vulnerability is defined as "the degree to which a system, a subsystem or a system component is likely to experience harm due to exposure to a hazard, either a perturbation or stress". In this paper, we adopt a similar perspective, considering vulnerability as the inability of a system to withstands strains and attacks. These definitions focus on the degree of loss and damages due to the impact of a hazard, i.e. on the technical dimensions of vulnerability: a weaker target is as likely to be attacked as a more secure target. But this assumption may not hold. The degree of loss and damages is determined by the degree of exposure to hazards and threats: all elements at risk do not show the same level of exposure to a hazard and when considering malevolent attacks, human actors are influenced by the vulnerability of a target.

The concept of susceptibility has been introduced in [16] to measure the degree to which a critical infrastructure is prone and accessible both to hazards and threats. Susceptibility refers to the property of the system of being potentially damaged and combines the likelihood of a hazardous event, the differential exposure, the potential sensitivity of a system or element of the system exposed, i.e. the degree to which a system or the element could be potentially damaged or affected by a given hazard, and the existing capacity of this system that could potentially reduce this level of damage (e.g. existing measures of prevention, mitigation, etc.) [17].

In this context, the idea of susceptibility is meant to encompass that of probability for random events, while grasping the intentionality that is behind malevolent attacks. To relate the centrality of the state variables that describe the exposure of the system to threats, two key-points are the *intent* and the *capability* to attack a target and cause adverse effects [18]. Intent and capability define a threat to the system.

Indeed, susceptibility must be a function of those factors that are involved in planning and performing an attack, i.e., the attractivity and the accessibility of a target. Attractivity considers the appeal of the target to intentional attacks and relates to the intent of causing damages. Accessibility considers that components have been designed for efficiency and convenience, yet access must be easy for maintenance staff but difficult for attacks [16], and relates to the capability of attack. Thus, the concept of susceptibility includes both a measure of how accessible and how attractive to terrorists a particular target is.

Therefore, the identification of the features of the system influencing its susceptibility to attacks, attractivity and accessibility, plays a key role in the vulnerability assessment of technical systems.

Three influencing variables were identified as components of attractivity and accessibility (Figure 1) [19]:

- Size (physical) of the component;
- Level of protection: the logical and physical barriers deployed to prevent or discourage malevolent acts;
- Social criticality: given that the attack will be successfully accomplished, the impact on public opinion is influenced by the (conditional) effects caused by the achieved intentional act. The most relevant consequences here considered are in terms of human lives and geographic extension of the event.

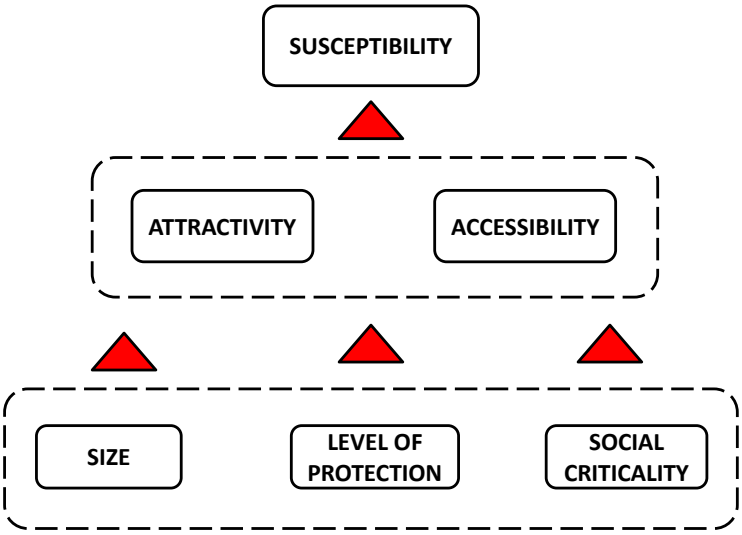

Figure 1. Pictorial representation of the susceptibility as a function of the characteristics of the system (size, level of protection and social criticality) and of the factors underpinning an intentional attack (attractivity and accessibility).

In order to compute the susceptibility function, i.e., the payoff function, we need to quantify its influencing variables, namely size, level of protection and social criticality. The system under study is a power transmission system in which each component is considered according to its functional role. Three main roles can be identified: generating units, which supply power, load buses, which receive the power supplied by generators and transmission lines which spread the power from the source to the target. For the

moment, we neglect the influence of the component physical size on attractivity and on accessibility, and we propose a quantitative expression for susceptibility.

We quantify the social criticality (SC) of a component *i* as proportional to the extent of the damage to the unprotected component, i.e. with a zero level of protection, $LOP_i = 1$:

$$SC_i = m_i \cdot DAMAGE_i + q_i \qquad (1)$$

Depending on the role of the component, $DAMAGE_i$ represents the power not supplied, transmitted or received and is expressed in terms of MW, so to be consistent with the size of medium transmission power systems. The coefficient m_i in Eq. 1 also depends on the functionality of the component *i* and it weights the "importance" of the loss: for example, it is expected that the damage to a single transmission line can cause no loss if the power flow can be redistributed on other transmission lines (N-1 criterion), so the transmission line coefficient m_i will be lower than m_i for a bus (user) that does not receive power due to its incapacitation. Finally, q_i expresses the perception of the disutility of the component *i* which subsumes the geographic extension and the number of potential victims. As a result, we have:

$$SC_{Transmitter} \leq SC_{User} \leq SC_{Provider} \qquad (2)$$

This inequality considers that an attack launched to a generating unit can have a larger impact on the public opinion than an attack to transmission lines or to users.

Six levels of protection (LOP) were introduced and identified in [16] by means of linguistic terms. The safeguards adopted for a component are gathered in 6 levels, from level 1, which identifies components with no protection such as transmission towers, to level 6 which denotes components such as power plants that need to be made inaccessible to possible attackers. These levels are, then, transposed in protection percentage values as shown in Table I:

Level of Protection (LOP)	Description (Examples)	Associated Percentage (%)
6 – Extreme	Completely secure, inaccessible	100
5 – High	Guarded, secure area, locked, alarmed, complex closure	86
4 – Moderate	Secure area, locked, complex closure	69
3 – Low	Complex barrier, security patrols, video surveillance	35
2 – Very low	Unlocked, noncomplex barriers (door or access panel)	17
1 – Zero	Completely open, no controls, no barriers	0

Table I. Level of protection and associated percentage values. A range from 1 to 100 has been divided in six parts in order to associate a percentage to the linguistic description of the safeguards of the system.

Given the values of social criticality (Eq. 1) and of the level of protection (Table I), we quantified the susceptibility of the component *i* as:

$$S_i = a \cdot SC_i \cdot e^{\left(-\frac{b}{SC_i} LOP_i\right)} + constant_i \qquad (3)$$

In Eq.3 it is assumed that a component whose attack has a great social impact on public opinion is more exposed to an attack, that is, has a greater susceptibility. On the other hand, if the component has high level of protection, the exposure to possible attacks should diminish.

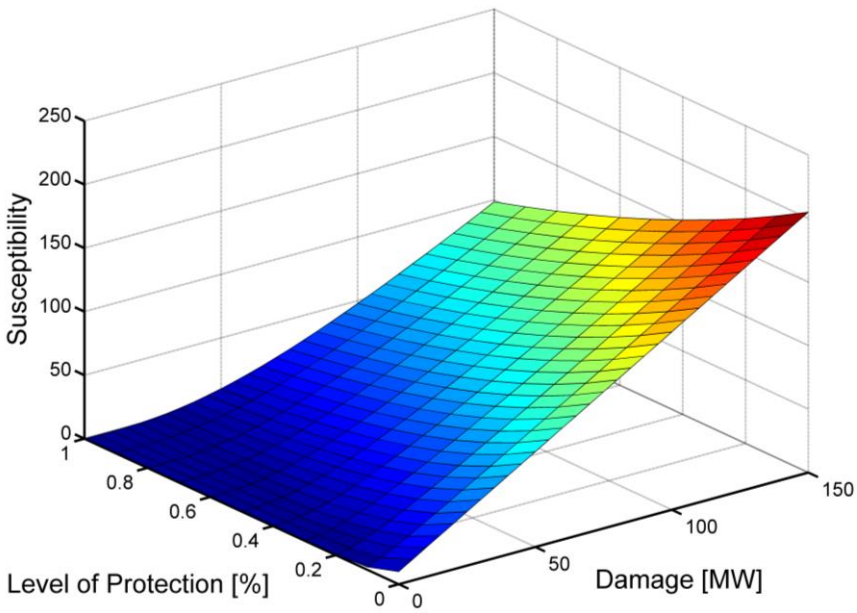

Figure 2. Susceptibility of the "User" component evaluated from Eq. (3) as a function of the damage and level of protection. For the "User" component m_i = 1.3, q_i = 10 a = 1, b = 100 and $constant_i$ = 0.

Figure 2 shows how our assumptions in the definition of susceptibility translate into the susceptibility function for the component "User". Similar plots are obtained also for the other two types of components. Components which are poorly protected and whose incapacitation results in large damage are ranked high with respect to susceptibility. On the other hand, components which are well protected and whose incapacitation results in small damage are ranked low with respect to susceptibility.

The sensitivity of the susceptibility indicator developed in Eq. (3) with respect to the damage extent and the level of protection is shown in Figure 3 and Figure 4, respectively.

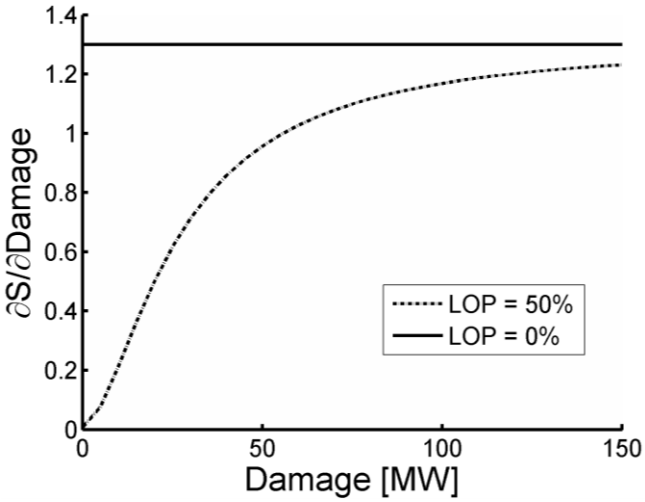

Figure 3. Sensitivity of susceptibility of the "User" component with respect to the damage for two values of level of protection, i.e. *LOP* = 50% (dashed curve) and *LOP* = 0% (solid curve). For the "User" component m_i = 1.3, q_i = 10 a = 1, b = 100 and $constant_i$ = 0.

The sensitivity of the variable Y with respect to the variable X_i is evaluated through a local method as the partial derivative $\left.\partial Y / \partial X_i\right|_{\overline{X_0}}$ where the remaining variables $\overline{X_0}$ have constant value. Figure 3 shows the sensitivity of the susceptibility, $\left.\partial S / \partial Damage\right|_{LOP}$, of the "User" component with respect to the damage for two values of level of protection, i.e. *LOP* = 50% (dashed curve) and *LOP* = 0% (solid curve). The developed susceptibility function is more sensitive for critical scenarios, i.e. when the level of protection is small. For constant level of protection, the susceptibility is more sensitive with increasing damage extent, which is a reasonable result of our assumptions.

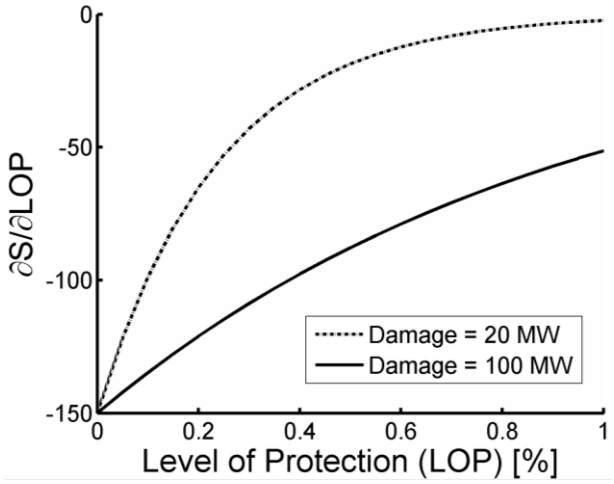

Figure 4. Sensitivity of susceptibility of the "User" component with respect to the level of protection for two values of damage, i.e. *Damage* = 20 MW (dashed curve) and *Damage* = 100 MW (solid curve). For the "User" component m_i = 1.3, q_i = 10 a = 1, b = 100 and $constant_i$ = 0.

Figure 4 shows the sensitivity of the susceptibility, $\partial S / \partial LOP \big|_{Damage}$, of the "User" component with respect to the damage for two values of level of protection, i.e. *Damage* = 20 MW (dashed curve) and *Damage* = 100 MW (solid curve). The developed susceptibility function is more sensitive for critical scenarios, i.e. when the damage extent is large. For constant damage extent, the susceptibility is more sensitive with decreasing level of protection, which is a reasonable result of our assumptions.

For the entire system, the total susceptibility is the sum of the susceptibilities of the components:

$$S = \sum_i \left(a \cdot SC_i \cdot e^{\left(-\frac{b}{SC_i} LOP_i \right)} + constant_i \right) \tag{4}$$

3. THE TWO-PLAYER ZERO-SUM GAME

Our model of the game considers two players: an attacker and a defender. We assume that the attacker aims at the destruction of the system or of a part of it: his aim is to maximize the losses he can cause to the system. From this point of view, an attacker will aim at incapacitating the component with the highest

degree of exposure to threats which could guarantee a successful attack. On the other side, the defender wants to minimize the damage produced on the system by malevolent acts, and he will try to protect the system by changing the levels of protection of the different components. His/her aim is to minimize the degree of exposure to attacks of the different components.

The objective of the game is to find the less vulnerable configuration of the system that can be deployed, given a constraint on the applicable level of protections. We assume the susceptibility function to represents the utility (payoff) function for the game: one player, i.e. the attacker, wants to maximize it; the other player, i.e. the defender, needs to minimize it. Both players compete on the same quantity and try to maximize or minimize it, therefore the game outlines as a zero-sum game: a gain for the attacker entails a corresponding loss for the defender and vice versa.

As for the strategies, we assume that the attacker takes the offensive and strikes a component. The strategy of the defender will be to arrange all the possible protections to limit the damage caused by possible attacks. To this aim, each component of the system is assigned a value of susceptibility, which will depend on its social criticality (SC_i) and on its current level of protection (LOP_i). The susceptibility values are computed using Eq. 4 and they represent the original system configuration.

The defender can act by changing the LOP of different components. The changes executed on the system identify a protection strategy. The susceptibility of the system will change with reference to the initial configuration accordingly to the protection strategy *X* carried out:

$$\Delta S_X = \left[\sum_i S_i \left(SC_i, LOP_i \right) \right]_{STRATEGY(X)} - \left[\sum_i S_i \left(SC_i, LOP_i \right) \right]_{INITIAL_CONFIGURATION} \qquad (5)$$

where the sum extends over all components *i*.

The payoff definition in Eq. (5) is consistent with the aim of the present study to quantify the variations of susceptibility which result from different protection strategies. As a matter of fact, different

components have different levels of protection (LOP_i) and alternative attack strategies have different values for the attacker. On the other hand, our focus is on the variations of susceptibility with respect to the current system configuration. Therefore, the payoffs for the different strategies are normalized to be able to capture the changes with respect to the initial configuration.

Our model assumes that the players know both the own and the opponent's strategy spaces and the associated utility functions, i.e. the defender knows the possible attack strategies and the attacker knows the defensive options. On the other hand, the model assumes that one player does not observe the actions of the other player, e.g. the attacker will not see/know the level of protection chosen by the defender when deciding his attack, and is configured as a simultaneous game. The situation in which the defender shows the current level of protection and the attacker can observe it, would be modeled as a Leader-Follower game. However, it is immediate to observe that for a zero-sum game both the simultaneous game and the Leader-Follower game lead to the same results. Therefore, the adopted model is robust with respect to the assumption of observability. For the basics on game theory, see [20], [21], for application to security games see [12], [22].

4. RESULTS

We exemplify the power grid with its functional model. In the conceptual representation of the system (Figure 5), only the operational role of the components is considered: generating units (G), load buses (B) and transmission lines (T).

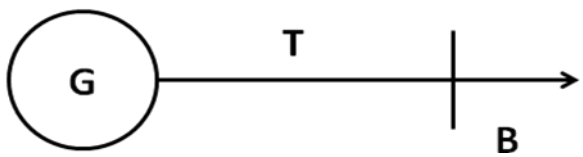

Figure 5. Schematic representation of the functional components of a transmission network. The fundamental components here considered are: a generator unit (G), a bus or load (B) and transmission lines (T).

Starting from the initial configuration (Config. 0 in Table II), the level of protection (LOP) of the different components may be increased (+) or decreased (-) by a certain amount or can be left unchanged (0). In this example, we assume that, for each component, only a unitary increase or decrease of LOP is allowed, i.e. $\Delta LOP = \pm 1$ compared to the initial configuration. Moreover, we assume that the cost of increasing LOP by one is the opposite of the cost of decreasing LOP by the same amount, and that for each configuration the aggregated cost of changing LOP is constrained to be zero. This reflects the limitations of constrained budget. The possible configuration variations for the conceptual example are represented in Table II:

Component	Config.0	Config.1	Config.2	Config.3	Config.4	Config.5	Config.6
G	0	+	+	0	0	-	-
T	0	-	0	+	-	+	0
B	0	0	-	-	+	0	+

Table II. Table of the possible configuration variations for the conceptual system. The first column represents the variation with respect to the reference configuration (0 means no variation). In each consecutive column, an increase in the level of protection is specified with a (+) if there is an increase in the level of protection, whereas (-) represents a decrease and 0 represents no variation.

In order to maintain a zero cost constraint, for an increase in the level of protection on one component we need to have a decrease of the same amount on another element of the system. For example (Table III), in the configuration number 2, the defender chooses to elevate the level of protection for the generating units from level 3 to level 4 and, in order to maintain the constraint on costs, he diminishes the protection on bus from level 3 to level 2. The components with 0, the transmission line in strategy 2, undergo no changes.

Component	Config.0	Config.1	Config.2	Config.3	Config.4	Config.5	Config.6
G	3	4	4	3	3	2	2
T	3	2	3	4	2	4	3

B	3	3	2	2	4	3	4

Table III. Table of the levels of protection in each configuration for the conceptual system. The levels of protection are specified according to the levels shown in Table I.

Given the possible choices of levels of protection, for each component of the system, the incremental susceptibilities (Eq. 5) are computed and collected in Table IV. Each element of Table IV represents the incremental susceptibility due to the variation of the degree of exposure to an attack, i.e., the susceptibility function due to a change in the level of protection with respect to the susceptibility computed for the initial configuration. If the level of protection of component *i* is increased with respect to Config. 0, the susceptibility of component *i* to attack decreases and the incremental value is negative. On the other hand, if the level of protection of component *i* is decreased with respect to Config. 0, its exposure to attacks increases, the susceptibility to attack raises and the incremental value is positive. Finally, if the level of protection of component *i* is unchanged, there is no variation in the susceptibility with respect to the initial configuration.

The simulation of the game was performed on the system, and the output susceptibility values are summarized in Table IV.

			DEFENDER						
			0	**1**	**2**	**3**	**4**	**5**	**6**
			0.0000	**0.0000**	**0.4028**	**0.0000**	**0.0000**	**0.1668**	**0.4304**
ATTACKER	**G**	**0.2138**	0	-31	-31	0	0	17	17
	T	**0.4410**	0	11	0	-13	11	-13	0
	B	**0.3452**	0	0	12	12	-17	0	-17

Table IV. Table of the possible strategies for the conceptual system.

The value of the game is -2.2388. This means that in the described situation the defender is able to increase his/her advantage with respect to the attacker. In order to do this, we observe that his best strategy

assigns null probability to some strategies (columns 0, 1, 3, 4). In particular, he will always change his current status in presence of an attack. On the other hand, it may happen that this is not true in other cases. For instance, the best strategy assigns a probability p_6 = 0.4304, to strategy 6, probability p_2= 0.4028, to strategy 2 and probability p_5 = 0.1668 to strategy 5. The result is not surprising, pure equilibrium strategies are unusual in the context of zero-sum games, as the example of the world-famous rock-paper-scissors game shows.

Compared to the initial configuration of the system, in strategy 6 the defender has increased the level of protection for the bus unit (corresponding to a decrease in the susceptibility) and has decreased the level of protection of the generating unit. In strategy 2, the defender can do exactly the opposite: he can increase the level of protection of the generating unit and decrease the level of protection of the load bus. Finally, in strategy 5 there is an increase in the level of protection of the transmission lines to the detriment of the protection for the generating unit.

On the other hand, the attacker can use all strategies when acting optimally, because all his pure strategies are a best reaction to the defender's strategy. Nonetheless, his target will more likely be component T. So in case of multiple attacks, we should see T attached more frequently.

5. CONCLUSIONS

Determining the power grid degree of exposure to hazards and intentional attacks has become a topic of great concern. An analysis aimed at identifying the causes of damage or disruption of services in power systems is necessary for safe operation and protection. In this paper, a general framework for the assessment of power systems vulnerability to malicious attacks has been presented. A two-player zero-sum game is envisaged between an attacker and a defender. The Nash equilibrium provides a useful overall measure of the network susceptibility to an attack, based on the inherent characteristic of the system. The results identify the best strategies for both the attacker and the defender under the following adopted assumptions:

- The social criticality of a component is linearly dependent on the damage extent;
- The susceptibility of a component can be described in terms of attractivity and accessibility;

- The attacker-defender dynamics can be modeled as a zero-sum game;
- The possible system modifications are subjected to cost constraints.

In the described situation, when acting optimally, the defender is able to increase his/her advantage with respect to the attacker. In particular, he will change his current status in presence of an attack. When the option is to reconfigure the system protection with the constraint of zero additional costs, the defender's optimal strategies will be (1) to increase the protection of buses at the expenses of protection of generators and, vice versa, (2) to increase the protection of generators at the expenses of protection of buses. On the other hand, the attacker can use all strategies when acting optimally, because all his pure strategies are a best reaction to the defender's strategy. Based on the specific case study in which the defender can reconfigure the system protection with the constraint of zero additional costs and the attacker can strike only one component, the attacker shows a preferential target, i.e. the transmission system.

Zero-sum games are a special class of the strictly competitive games. However, every strictly competitive game can be transformed in a zero-sum game with admissible transformation of utilities of the players. Thus, they can well describe contests in which the players have opposite goals. Therefore, all outcomes are efficient, i.e. by switching from an outcome to another one, one player necessarily increases his payoff, and the other one necessarily decreases his. This behavior realistically represents an attacker-defender situation, like the one illustrated here.

The method has been applied to a conceptual case study in which components have been aggregated according to their operational role, and it can be extended to account for a large-scale spatial-distributed infrastructure.

REFERENCES

[1] Kröger W, Zio E. Vulnerable systems. Springer-Verlag London Limited; 2011.

[2] Pate-Cornell E, Guikema S. Probabilistic modeling of terrorist threats: A systems analysis approach to setting priorities among countermeasures. Military Operations Research. 2002;7(4):5–20.

[3] Sandler T. Terrorism & game theory. Simulation & Gaming. 2003;34(3):319–337.

[4] Bier VM, Nagaraj A, Abhichandani V. Protection of simple series and parallel systems with components of different values. Reliability Engineering and System Safety. 2005;87(3):315-323.

[5] Rothschild C, McLay L, Guikema S. Adversarial risk analysis with incomplete information: a level-k approach. Risk Analysis. 2012;32(7):1219-1231.

[6] Bell MG. The Use of Game Theory to measure the vulnerability of stochastic networks. IEEE Transactions on Reliability. 2003;52(1):63-68.

[7] Hausken K, Levitin G. Review of systems defense and attack models. International Journal of Performability Engineering. 2012;8(4):355-366.

[8] Bier VM. Choosing what to protect. Risk Analysis. 2007;27(3):563-587.

[9] Major JA. Advanced techniques for modeling terrorism risk. Journal of Risk Finance. 2002; 4(1):15–24.

[10] Bier VM, Tas S. Game theory in infrastructure security. WIT Transactions on State of the Art in Science and Engineering. 2012;54:91-104.

[11] Nikoofal M, Mehmet Gumus M. What would you know about the next terrorist attack? Target Information vs. Rationality of the Attacker. Annual INFORMS Conference; 2011 Nov 13-16; Charlotte, NC.

[12] Korzhyk D, Yin Z, Kiekintveld C, Conitzer V, Tambe M. Stackelberg vs. Nash in security games: an extended investigation of interchangeability, equivalence, and uniqueness. Journal of Artificial Intelligence Research. 2011;41(2):297–327.

[13] Salehizadeh MR, Ashkan RK, Hausken K. A leader-follower game on congestion management in power systems. In Hausken, K. and Zhuang, J. (eds.). Game theoretic analysis of congestion, safety and security: networks, air traffic and emergency departments, New York, Springer; 2015. 81-112p.

[14] Haimes YY, Horowitz B.M. Modeling interdependent infrastructures for sustainable counterterrorism. Journal of Infrastructure Systems. 2004;8:67 -75.

[15] Konce AM, Apostolakis GE, Cook BK. Bulk power risk analysis: ranking infrastructure elements according to their risk significance. Electrical Power and Energy Systems. 2008;30:169-183.

[16] Apostolakis EG, Lemon MD. A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism. Risk Analysis. 2005;25(2):361-376.

[17] Bouchon S. The vulnerability of interdependent critical infrastructure systems: epistemological and conceptual state-of-the art. EUR 22205 EN; 2006.

[18] Haimes YY. On the definition of vulnerabilities in measuring risks to infrastructures. Risk Analysis. 2006;26(2): 293–6.

[19] Zio E, Piccinelli R, Sansavini G. A framework for ranking the attack susceptibility of components of critical infrastructures. Chemical Engineering Transactions. 2012;26:309-314.

[20] Von Neumann J, Morgenstern O. Theory of games and economic behavior (60th anniversary commemorative edition). Princeton University press; 2007.

[21] Maschler M, Solan E, Zamir S. Game Theory. Cambridge University Press; 2013.

[22] Basilico N, Gatti N, Amiconi F. Patrolling security games: definition and algorithms for solving large instances with single patroller and single intruder. Artificial intelligence. 2012;184:78–123.