A Methodology to Apply a Game Theoretic Model of Security Risks Interdependencies Between ICT and Electric Infrastructures

Ziad Ismail[1(✉)], Jean Leneutre[1], David Bateman[2], and Lin Chen[3]

[1] Télécom ParisTech, Université Paris-Saclay, 46 rue Barrault, 75013 Paris, France
{ismail.ziad,jean.leneutre}@telecom-paristech.fr
[2] EDF, 1 Place Pleyel, 93282 Saint-Denis, France
david.bateman@edf.fr
[3] University of Paris-Sud 11, 15 Rue Georges Clemenceau, 91400 Orsay, France
lin.chen@lri.fr

Abstract. In the last decade, the power grid has increasingly relied on the communication infrastructure for the management and control of grid operations. In a previous work, we proposed an analytical model for identifying and hardening the most critical communication equipment used in the power system. Using non-cooperative game theory, we modeled the interactions between an attacker and a defender and derived the minimum defense resources required and the optimal strategy of the defender that minimizes the risk on the power system. In this paper, we aim at validating the model using data derived from real-world existing systems. In particular, we propose a methodology to assess the values of the parameters used in the analytical model to evaluate the impact of equipment failures in the power system and attacks in the communication infrastructure. Using this methodology, we then validate our model via a case study based on the polish electric power transmission system.

Keywords: Cyber-physical system · Non-cooperative game theory · SCADA security

1 Introduction

The power grid stands as one of the most important critical infrastructures on which depends an array of services. It uses a Supervisory Control and Data Acquisition (SCADA) system to monitor and control electric equipment. Traditionally, the reliability of the power grid and the security of the ICT infrastructure are assessed independently using different methodologies, for instance [1] and [2] respectively for electric and ICT infrastructures. More recently, a growing body of research has been dedicated to the modeling of interdependencies in critical infrastructures, focusing in particular on communication and electric systems. For example, Laprie et al. [3] proposed a qualitative model to address cascading, escalating, and common cause failures due to interdependencies between these infrastructures. In the case of quantitative models, we can

Q. Zhu et al. (Eds.): GameSec 2016, LNCS 9996, pp. 159–171, 2016.
DOI: 10.1007/978-3-319-47413-7_10

distinguish two main categories: analytical-based and simulation-based models. In the first category of models, we find the work of Buldyrev et al. [4] in which a theoretical framework was developed to study the process of cascading failures in interdependent networks caused by random initial failures of nodes. In simulation-based models, the main techniques used include agent-based [5], petri nets [6] and co-simulation [7].

In complex interdependent systems, the interactions between the attacker and the defender play an important role in defining the optimal defense strategy. In this context, game theory offers a mathematical framework to study interactions between different players with the same or conflicting interests. For example, Law et al. [8] investigate false data injection attacks on the power grid and formulate the problem as a stochastic security game between an attacker and a defender. Amin et al. [9] present a framework to assess risks to cyber-physical systems when interdependencies between information and physical systems may result in correlated failures.

In [10], we proposed an analytical model based on game theory for optimizing the distribution of defense resources on communication equipment taking into account the interdependencies between electric and communication infrastructures. Due to the abstract nature of such analytical models, assessing their relevance in real-world scenarios is a challenging task. In this paper, we propose a methodology for assessing the values of the parameters in the analytical model related to the electric and communication infrastructures, and validate our approach on a case study based on the polish electric transmission system. Throughout the paper, the communication system refers to the telecommunication infrastructure responsible of controlling and monitoring the electrical system.

The paper is organized as follows. In Sect. 2, we present a slight adaptation of the analytical model presented in [10]. In Sect. 3, we propose an approach to evaluate the values of a number of parameters used in the analytical model. In Sect. 4, we validate our model via a case study based on the polish electric power transmission system. Finally, we conclude the paper in Sect. 5.

2 A Game Theoretical Model for Security Risk Management of Interdependent ICT and Electric Systems

In this section, we briefly recall our analytical model for identifying critical communication equipment used to control the power grid that must be hardened. The proofs are omitted, and we refer the reader to [10] for complete details.

2.1 Interdependency Model

We refer by initial risk, the risk on a node before the impact of an accident or an attack propagates between system nodes. We will denote by $r_i^e(0)$ and $r_j^c(0)$ the initial risk on electrical node i and communication equipment j respectively.

We assume that initial risk on a system node is a nonnegative real number and has been evaluated using risk assessment methods.

We use the framework proposed in [11] as a basis to represent the risk dependencies using a graph-theoretic approach. We model the interdependency between the electrical and the communication infrastructures as a weighted directed interdependency graph $\mathcal{D} = (V,\ E,\ f)$, where $V = \{v_1, v_2, ..., v_N\}$ is a finite set of vertices representing the set of electrical and communication nodes, E is a particular subset of V^2 and referred to as the edges of $\mathcal{D}$, and $f : E \rightarrow \mathbb{R}^+$ is a function where $f(e_{ij})$ refers to the weight associated with the edge e_{ij}.

Let $V = \{\mathcal{T}^e, \mathcal{T}^c\}$ where $\mathcal{T}^e = \{v_1, v_2, ..., v_{N_e}\}$ represents the set of electrical nodes in the grid and $\mathcal{T}^c = \{v_{N_e+1}, v_{N_e+2}, ..., v_{N_e+N_c}\}$ represents the set of communication nodes. Let $\mathcal{D}$ be represented by the weighted adjacency matrix $M = [m_{ij}]_{N\times N}$ defined as follows:

$$M = \begin{pmatrix} B & D \\ F & S \end{pmatrix}$$

where $B = [b_{ij}]_{N_e\times N_e}$, $D = [d_{ij}]_{N_e\times N_c}$, $F = [f_{ij}]_{N_c\times N_e}$, and $S = [s_{ij}]_{N_c\times N_c}$. Matrix M represents the effects of nodes on each other and is a block matrix composed of matrices B, D, F and S. Elements of these matrices are nonnegative real numbers. Without loss of generality, we assume that these matrices are left stochastic matrices. Therefore, for each node k, we evaluate the weight of other nodes to impact node k. For example, matrices B and S represent the dependency between electrical nodes and communication nodes respectively.

2.2 Risk Diffusion and Equilibrium

We consider that the first cascading effects of an attack on communication equipment take place in the communication infrastructure itself. We introduce a metric t_c in the communication system that refers to the average time for the impact of an attack on communication equipment to propagate in the communication infrastructure. In this model, as opposed to our model in [10], we do not consider the average time t_e in the electrical system that refers to the average time elapsed between the failure of a set of electric equipment and the response time of safety measures or operators manual intervention to contain the failures and prevent them from propagating to the entire grid.

Let $R^e(t) = [r_i^e(t)]_{N_e\times 1}$ and $R^c(t) = [r_i^c(t)]_{N_c\times 1}$ be the electrical and communication nodes risk vectors at time t respectively. We take discrete time steps to describe the evolution of the system. Let $S^l = [s_{ij}^l]_{N_c\times N_c}$ be the l-th power of the matrix S. At attack step r, the payoff is decreased by a factor of γ_c^r. In fact, we consider that each action of the attacker in the system increases the probability of him being detected. Let the matrix $S^{max} = [s_{ij}^{max}]_{N_c\times N_c}$ represents the maximum impact of an attack on communication equipment to reach communication nodes during time t_c, where $s_{ij}^{max} = \max\limits_{l=1,...,\lfloor t_c \rfloor} \gamma_c^l s_{ij}^l$. Let S_n^{max} be the normalized matrices of S^{max} with respect to their rows s.t. $\forall j,\ \sum\limits_i {s_n^{max}}_{ij} = 1$.

We take a similar approach to [11] by balancing the immediate risk and the future induced one. Let β and τ refer to the weight of the initial risk on communication nodes and the weight of the diffused risk from electric nodes to communication nodes at time $t = 0$ respectively, and δ the weight of future cascading risk w.r.t. the value of the total risk on communication nodes. We can prove that the iterative system of the cascading risk converges and an equilibrium solution exists whenever $\delta < 1$ and is given by $R^{c*} = (I - \delta H)^{-1}(\beta R^c(0) + \tau D^T R^e(0))$, where $H = S_n^{max} FBD$, and β, τ, and δ are nonnegative real numbers and $\beta + \tau + \delta = 1$.

2.3 Security Game

We formulate the problem as a non-cooperative game and analyze the behavior of the attacker and the defender at the Nash equilibrium (NE), in which none of the players has an incentive to deviate unilaterally. The attacker's/defender's objective is to distribute attack/defense resources on the communication nodes in order to maximize/minimize the impact of attacks on the power system. We consider the worst-case scenario where both players have complete knowledge of the architecture of the system.

We associate for each communication equipment, a load l_i that represents the amount of computational work the equipment performs. Let $L = diag(l_i)_{N_c \times N_c}$ be the load matrix. Let $W = [w_{ij}]_{N_c \times N_c}$ be the redundancy matrix where $\forall i$, $w_{ii} = -1$ and $\sum\limits_{j, j \neq i} w_{ij} \leq 1$. If $i \neq j$, w_{ij} represents the fraction of the load of node i, node j will be responsible of processing when node i is compromised.

The utility U_a and U_d of the attacker and the defender respectively are as follows:

$$U_a(p, q) = pR_D^{c*}(e^T - q^T) - pR_D^c(0)C^a p^T - \psi pL(Wq^T - I(e^T - 2q^T))$$

$$U_d(p, q) = -pR_D^{c*}(e^T - q^T) - qR_D^c(0)C^d q^T + \psi pL(Wq^T - I(e^T - 2q^T))$$

where $p = [p_i]_{1 \times N_c}$ refers to the attacker's strategy where $0 \leq p_i \leq 1$ is the attack resource allocated to target $i \in \mathcal{T}^c$, $q = [q_j]_{1 \times N_c}$ refers to the defender's strategy where $0 \leq q_j \leq 1$ is the defense resource allocated to target $j \in \mathcal{T}^c$, $R_D^c(0)$, R_D^{c*}, C^a and C^d are diagonal matrices and C^a and C^d refer to the cost of attacking and defending communication nodes respectively, I is the identity matrix, and $e = (1, ..., 1)_{1 \times N_c}$.

The players' utilities are composed of three parts: the payoff of an attack, the cost of attacking/defending, and the impact of redundant equipment in ensuring the control of the power system when a set of communication nodes is compromised. $\psi \in [0, 1]$ is a function of the probability that backup equipment are able to take charge of the load of compromised communication equipment.

We analyze the interactions between the attacker and the defender as a one-shot game [12] in which players take their decisions at the same time.

Theorem 1. *A unique NE of the one-shot game exists and is given by:*

$$\begin{aligned}
q^* &= \frac{1}{2}e(R_D^{c*} + \psi L)(R_D^c(0)C^a)^{-1}M[\frac{1}{2}M^T(R_D^c(0)C^a)^{-1}M + 2R_D^c(0)C^d]^{-1} \\
p^* &= e(R_D^{c*} + \psi L)[\frac{1}{2}M(R_D^c(0)C^d)^{-1}M^T + 2R_D^c(0)C^a]^{-1} \\
&\quad \textit{where} \;\; M = R_D^{c*} + \psi L(W + 2I)
\end{aligned}$$

We also analyze the interactions between players as a Stackelberg game [12]. In our case, the defender is the leader who tries to secure communication equipment in order to best protect the power system. We have the following theorem:

Theorem 2. *The game admits a unique Stackelberg equilibrium* (p^S, q^S) *given by:*

$$\begin{aligned}
q^S &= e(R_D^{c*} + \psi L)(R_D^c(0)C^a)^{-1}M(Q + 2R_D^c(0)C^d)^{-1} \\
p^S &= \frac{1}{2}e(R_D^{c*} + \psi L)(R_D^c(0)C^a)^{-1}[I - M(Q + 2R_D^c(0)C^d)^{-1}M^T(R_D^c(0)C^a)^{-1}] \\
&\quad \textit{where} \;\; Q = M^T(R_D^c(0)C^a)^{-1}M
\end{aligned}$$

3 Parameters Evaluation

In this section, we present our approach to assess the impact of attacks in the electric and communication infrastructures, and therefore evaluate matrices B and S respectively. While the problem of the assessment of the other parameters of the model remains, we discuss at the end of this section potential avenues for their evaluation.

3.1 Evaluation of Matrix *B*

We assess the impact of cascading failures in the power grid by solving power flow equations using the DC power flow approximation [13]. Following a similar approach as in [14], we simulate individual failures and assess their impact on the power grid such as identifying generators with insufficient capacities to meet the demand and overloaded lines.

In our model, we analyze the impact of tripping transmission lines or loosing generators on the power grid. The flowchart diagram in Fig. 1 shows the cascading algorithm used in our model to analyze the impact of tripping transmission lines. In general, this could have a significant impact on the power grid and could lead to the formation of islands in the electric system. In our algorithm, we shut down islands where the demand (denoted as d in Fig. 1) exceeds the maximum generation capacity in the island (denoted as $max(g)$ in Fig. 1). We then solve the DC power flow problem in the electric transmission system using MATPOWER [15] and check the existence of overloaded lines. These lines are tripped and the process is repeated until a balanced solution emerges. Similarly, we assess the impact of loosing generators on the power grid.

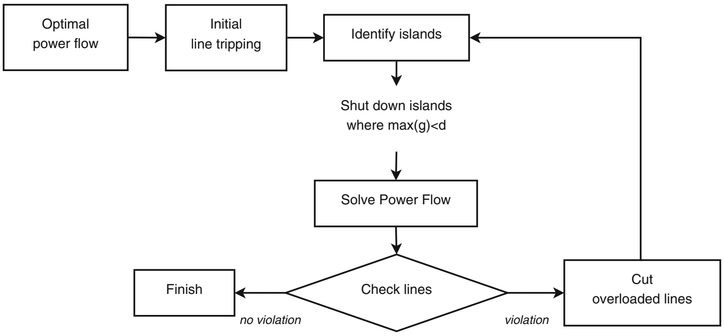


Fig. 1. Flowchart of the cascade algorithm in the case of tripped transmission lines

In our approach, we consider the worst-case scenario where load shedding is not an option when we conduct our analysis of the impact of cascading failures on the power grid. Further work taking into account more fine grained analysis of the behavior of the power grid will allow us to quantify more precisely the values of elements of matrix B.

3.2 Evaluation of Matrix S

To address the challenge of evaluating the impact of cyber attacks on the communication infrastructure, attack graphs [16] are a promising solution to generate all possible attack steps to compromise a target node. These graphs could be used in conjunction with risk assessment methods to evaluate the impact of each attacker action on the communication infrastructure.

Let $\mathcal{G} = (\mathcal{X}, \mathcal{E})$ be an attack graph where $\mathcal{X}$ refers to the set of nodes in the graph and $\mathcal{E}$ refers to the set of edges. In our case, a node $x \in \mathcal{X}$ in the graph refers to a state of the attacker in the system, and an edge $e = (x_i, x_j) \in \mathcal{E}$ refers to an action executed by the attacker after which the state of the attacker in the system transits from x_i to x_j. A state of the attacker refers to his knowledge at a particular time of the topology and the configuration of the system, the set of access levels acquired on equipment, and the set of credentials at his disposal. $\mathcal{G}$ represents all attack paths that can be used by the attacker to compromise a set of equipment or services in the system. In [17], we defined such graph and implemented a proof of concept for constructing it.

Let θ_{lm}^r be the number of paths of length r an attacker can use to compromise communication equipment m from communication equipment l. Let $\Theta_{lm} = \sum_r \gamma_c^r \theta_{lm}^r$ refer to the impact metric of a communication equipment l on a communication node m. Θ_{lm} is a measure of the cumulated impact on communication equipment m of an attack originating from equipment l. We consider that each action of the attacker in the system increases the probability of him being detected. Therefore, at attack step r, the payoff is decreased by a factor of γ_c^r representing the uncertainty for the attacker of getting the payoff of the r^{th} future attack step. In this case, $s_{lm} = \dfrac{\Theta_{lm}}{\sum\limits_i \Theta_{im}}$, where $S = [s_{lm}]_{N_c \times N_c}$.

3.3 Other Parameters

In our case study, we rely on experts' knowledge to evaluate matrices D and F, which represent the dependency relation on communication nodes by electric nodes and vice versa respectively. However, at the end of the case study in the next section, we conduct a sensitivity analysis to evaluate errors in the outputs of our model to estimation errors on the values of the elements of matrix F.

In our model, we introduced parameters β and τ, which represent the weight of the initial risk on communication nodes and the weight of the diffused risk from electric equipment to communication equipment at time $t = 0$ respectively, and δ which reflects the weight of future cascading risk w.r.t. the value of the total risk on communication equipment. These parameters can be evaluated as a result of the application of a risk assessment method coupled with quantitative metrics derived from the attack graph of the communication infrastructure. In fact, depending on the assessment of the efficiency of deployed defense mechanisms in thwarting threats, the value of β and τ w.r.t. δ can be adjusted. In particular, by analyzing the attack graph, we can evaluate the probability of compromising critical communication equipment given existing defense measures in the system.

4 Case Study

In this section, we validate our model on a case study based on the dataset of the polish electric transmission system at a peak load in the summer of 2004 provided in the MATPOWER computational package [15]. The dataset consists of 420 generators and 3504 transmission lines. The analysis of an electric system at a peak load is important, as it allows us to assess the maximum impact on the power grid as a result of a cyber attack.

4.1 System Architecture

We made a number of assumptions on the architecture of the communication infrastructure that we use in our case study to assess the impact of attacks on the power grid. In addition, to simplify our analysis, we combined a set of communication equipment in a single communication node depending on their functions, thus reducing the number of nodes to be represented in each electric transmission system control center. Let $\mathcal{Y}$ represent the polish electric transmission system. We assume that $\mathcal{Y}$ is controlled by 10 TSO (Transmission System Operator) control centers. Each center controls 42 generators and about 350 transmission lines in a specific area of the power grid. We assume that communication equipment in control centers are vulnerable to attacks, and the attacker has enough resources and both players know the architecture of the system. As we study the impact of attacks on the power grid in the worst-case scenario, this assumption holds. A unique TSO ICT control center is introduced to manage all communication equipment in TSO control centers.

TSO ICT Control Center. In the TSO ICT control center, four types of communication equipment are represented. A Time Server synchronizes the clocks in all communication equipment. A Domain and Directory Service manages access controls on communication equipment. The Remote Access Application is used by ICT administrators to access equipment remotely via secured connections. Finally, the Configuration Management System is responsible of pushing OS and software updates to equipment. Updates can be installed automatically or require specific authorizations on equipment performing critical operations.

TSO Area Control Centers. We represent four types of communication equipment in each TSO area control center: a SCADA HMI, a SCADA server, a SCADA frontend and a SCADA historian. The SCADA HMI is a human-machine interface that provides a graphics-based visualization of the controlled area of the power system. The SCADA server is responsible of processing data collected from sensors in the power grid and sending appropriate control commands back to electric nodes. The SCADA frontend is an interface between the SCADA server and electric nodes control equipment. It formats data in order to be sent through communication channels and to be interpreted when received by control equipment and vice versa. Finally, the SCADA historian is a database that records power state events.

Impact Matrix. We use the algorithm presented in the previous section to assess the impact of stopping generators or tripping transmission lines on the electric transmission system and compute matrix B. We rely on experts' knowledge to evaluate matrices F and D. In the communication infrastructure, we consider that each equipment in a TSO control center is also the backup of an equipment in another TSO control center.

In this case study, we assume that the values of the initial risk on communication equipment have been computed, and for each communication equipment, the cost to defend is always greater than the cost to attack. We fix $\beta = 0.4$, $\tau = 0$, $\delta = 0.6$, and $\psi = 0.5$. Therefore, the future cascading risk has more weight than initial risk w.r.t. the value of the total risk on communication equipment.

4.2 Results

Figure 2 shows the value of risk on communication equipment in each TSO area control center after the impact of attacks propagates in the interdependent communication and electric infrastructures. We can notice that the highest risk values in TSO control centers are on SCADA servers. In particular, risk values on SCADA servers in TSO 1 and TSO 2 control centers are significantly higher than risk values on SCADA servers in the other TSO control centers.

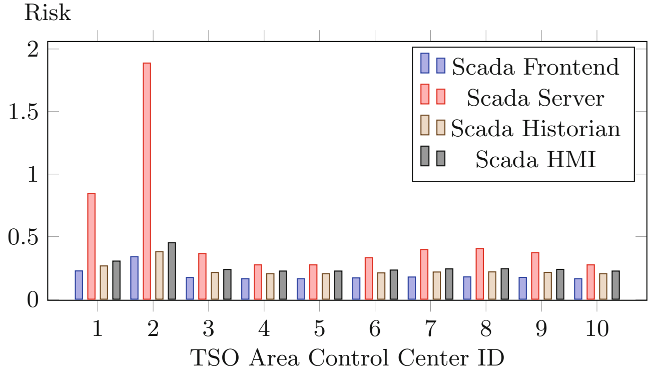


Fig. 2. Risk on communication equipment in TSO area control centers

Table 1 presents the results of the one-shot and Stackelberg games between the attacker and the defender for the TSO ICT and TSO area 1 and area 2 control centers.

Table 1. Nash Equilibrium

		$\mathbf{r_i^{c*}}$	**One-Shot game**		**Stackelberg game**	
			p^*	q^*	p^S	q^S
TSO ICT	**Time Server**	2.547	0.287	0.972	0.146	0.986
	Domain Server	2.885	0.183	0.972	0.093	0.986
	Remote App.	2.089	0.202	0.966	0.103	0.9823
	Config. Manag.	3.073	0.21	0.985	0.106	0.992
TSO 1	**SCADA Fontend**	0.226	0.275	0.537	0.15	0.591
	SCADA Server	0.844	0.295	0.688	0.156	0.744
	SCADA Historian	0.266	0.315	0.515	0.177	0.584
	SCADA HMI	0.305	0.329	0.51	0.187	0.586
TSO 2	**SCADA Fontend**	0.339	0.302	0.648	0.162	0.697
	SCADA Server	1.888	0.213	0.895	0.108	0.909
	SCADA Historian	0.379	0.344	0.618	0.189	0.684
	SCADA HMI	0.451	0.358	0.631	0.197	0.7

One-Shot game. From Fig. 2 and Table 1, we notice that the Time, Configuration and Domain Servers have the highest risk values. These equipment are often connected to the internet which significantly increases their attack surface. In addition, given their functions, compromising these equipment could lead to important disruptions in the communication infrastructure. As a result, at equilibrium, the defender allocates a large amount of defense resources to protect these equipment. However, this does not prevent the attacker from allocating attack resources on these equipment considering their potential impact on the power grid in the case of a successful attack.

The utilities of the attacker and the defender in the one-shot game are $U_a = 0.941$ and $U_d = -6.151$ respectively. In our case study, we noticed that in the case where the values of risk on equipment in two different TSO control centers are similar, the attacker/defender allocate more resources to attack/defend backup equipment. Therefore, by attacking backup equipment, the attacker improves the efficiency of his attacks and increases the probability of succeeding in his attempts to disrupt the power system. On the other hand, the defender responds by allocating more defense resources to protect backup equipment.

Stackelberg game. The utilities of the attacker and the defender in the Stackelberg game are $U_a^S = 0.307$ and $U_d^S = -5.746$ respectively. Compared to the one-shot game, the defender allocates more defense resources on each communication equipment, which forces the attacker to reduce his attack resources on these equipment. In fact, an additional security investment by the defender by 2.908 reduced the attacker's allocated resources by 6.082. As a result, from the point of view of the defender, the benefits of operating at the Stackelberg equilibrium outweigh the additional cost of increasing security investments on communication equipment.

Impact of redundancies. Figure 3 shows the variation of total attack and defense resources w.r.t. the weight of the existence of redundancies in players' utility functions ψ. We notice that ψ has a negative effect on the total amount of resources allocated by the attacker. This is consistent with the fact that increasing the weight of redundancies in player's utilities leaves the attacker with fewer choices to achieve a better payoff since the defender will increase the protection of backup equipment. In addition, we notice that when the value of ψ increases, the difference between the one-shot and Stackelberg games total defense resources allocation decreases.

Figure 4 shows the variation of the attacker and the defender strategies on two communication equipment in TSO area 2 control center w.r.t. variation of elements of the redundancy matrix W. We analyze the behavior of the attacker and the defender when varying elements w_{ij}, the fraction of the load of node i, node j will be responsible of processing when node i is compromised. We notice that the behavior of the attacker and the defender depends on the type of the communication equipment. For example, the behavior of both players does not change significantly with respect to W for critical equipment such as the SCADA server. However, this behavior is different for the other equipment in TSO area 2 control center. Finally, increasing w_{ij} leads both the attacker and the defender to decrease their attack and defense resources on communication equipment.

Sensitivity Analysis. We conducted a sensitivity analysis of the diffused risk R^{c*}, the NE in the one-shot game, and the Stackelberg equilibrium w.r.t. the values of the initial risk $R^c(0)$ and the elements of matrices S and F. We averaged the results of 10000 iterations. At each iteration, we assume that a random

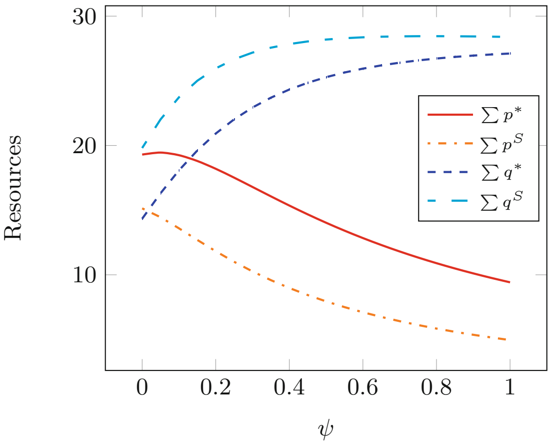
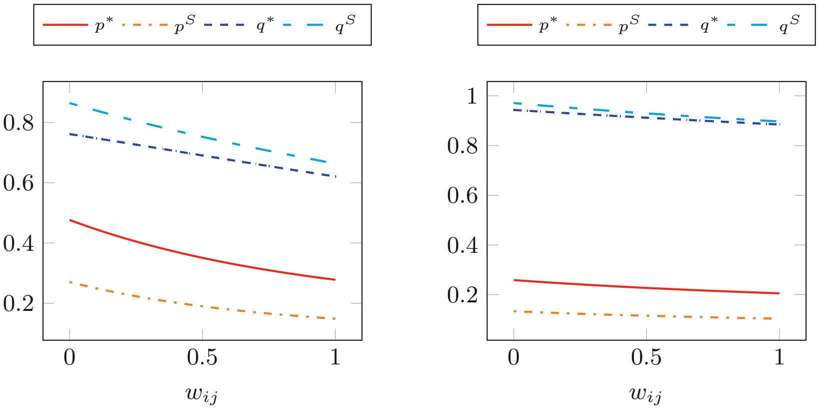


Fig. 3. Variation of attack and defense resources w.r.t. ψ



(a) SCADA frontend

(b) SCADA server

Fig. 4. Variation of attack and defense resources on TSO 2 w.r.t. redundancy matrix W

number of elements of $R^c(0)$ deviate from their correct values by $\pm 10\,\%$ (sign of the deviation is chosen randomly). We repeat the experiment taking into account errors in a random number of elements in matrices S and F.

Sensitivity to $\mathbf{R^c(0)}$. The maximum error on the values of R^{c*} was around $4\,\%$. The attacker strategy seems more sensitive than the defender strategy with respect to errors in $R^c(0)$ at equilibrium. In the one-shot game, the maximum error on the attacker strategy was about $4.1\,\%$ whereas the error on the defender strategy was about $2.1\,\%$. However, in the Stackelberg game, we noticed that the maximum error on the attacker strategy has increased compared to the one-shot game and was about 5.1 %. In the case of the defender, the maximum error has decreased and was about 1.2 %.

Sensitivity to matrices S and F. The maximum error on the values of R^{c*} was around 3.4 %. We do not note a significant change in the maximum errors on the attacker and defender strategies in the case of the one-shot game compared to the Stackelberg game. The maximum error on the attacker and defender strategies was about 2.1 % and 1.3 % respectively.

5 Conclusion

In [10], we presented a quantitative model, based on game-theoretic analysis, to assess the risk associated with the interdependency between the cyber and physical components in the power grid. In this paper, we proposed a method to evaluate the values of parameters used in our model to assess the impact of equipment failures in the power system and attacks in the communication infrastructure. We rely on experts' knowledge to assess all the other parameters of our model. However, the structure of player's utility functions, taking into account the existence of backups in the communication system, allows us to characterize analytically players' strategies at the NE. Therefore, we are able to evaluate potential changes in the behavior of players to estimation errors on the values of a set of model parameters. We validated our model via a case study based on the polish electric transmission system.

References

1. Li, W.: Risk Assessment of Power Systems: Models, Methods, and Applications. Wiley-IEEE Press, New York (2005)
2. Agence Nationale de la sécurité des systèmes d'information. EBIOS Risk Management Method (2010). http://www.ssi.gouv.fr/IMG/pdf/EBIOS-1-GuideMethodologique-2010-01-25.pdf
3. Laprie, J., Kanoun, K., Kaniche, M.: Modeling interdependencies between the electricity and information infrastructures. In: SAFECOMP, pp. 54–67 (2007)
4. Buldyrev, S., Parshani, R., Paul, G., Stanley, H.E., Havlin, S.: Catastrophic cascade of failures in interdependent networks. Nature **464**, 1025–1028 (2010)
5. Casalicchio, E., Galli, E., Tucci, S.: Federated agent-based modeling and simulation approach to study interdependencies in it critical infrastructures. In: IEEE 11th International Symposium on Distributed Simulation and Real-Time Applications, pp. 182–189 (2007)
6. Chen, T., Sanchez-Aarnoutse, J., Buford, J.: Petri net modeling of cyber-physical attacks on smart grid. IEEE Trans. Smart Grid **2**(4), 741–749 (2011)
7. Lin, H., Veda, S.S., Shukla, S.K., Mili, L., Thorp, J.S.: GECO: global event-driven co-simulation framework for interconnected power system and communication network. IEEE Trans. Smart Grid **3**(3), 1444–1456 (2012)
8. Law, Y.W., Alpcan, T., Palaniswami, M.: Security games for voltage control in smart grid. In: 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton), pp. 212–219 (2012)

9. Amin, S., Schwartz, G., Hussain, A.: In quest of benchmarking security risks to cyber-physical systems. IEEE Netw. **27**(1), 19–24 (2013)
10. Ismail, Z., Leneutre, J., Bateman, D., Chen, L.: A game-theoretical model for security risk management of interdependent ict and electrical infrastructures. In: IEEE 16th International Symposium on High Assurance Systems Engineering (HASE), pp. 101–109 (2015)
11. Alpcan, T., Bambos, N.: Modeling dependencies in security risk management. In: Proceedings of the 4th International Conference on Risks and Security of Internet and Systems (Crisis) (2009)
12. Osborne, M.J., Rubinstein, A.: A Course in Game Theory. MIT Press, Cambridge (1994)
13. Zhu, J.: Optimization of Power System Operation. Wiley-IEEE Press, Hoboken (2009)
14. Pfitzner, R., Turitsyn, K., Chertkov, M.: Statistical classification of cascading failures in power grids. In: 2011 IEEE Power and Energy Society General Meeting, pp. 1–8 (2011)
15. Zimmerman, R., Murillo-Snchez, C., Thomas, R.: Matpower: steady-state operations, planning, and analysis tools for power systems research and education. IEEE Trans. Power Syst. **26**(1), 12–19 (2011)
16. Ingols, K., Lippmann, R., Piwowarski, K.: Practical attack graph generation for network defense. In: 22nd Annual Computer Security Applications Conference (ACSAC), pp. 121–130 (2006)
17. Ismail, Z., Leneutre, J., Fourati, A.: An attack execution model for industrial control systems security assessment. In: Proceedings of the First Conference on Cybersecurity of Industrial Control Systems (CyberICS) (2015)