2015 IEEE 16th International Symposium on High Assurance Systems Engineering

A Game-Theoretical Model for Security Risk Management of Interdependent ICT and Electrical Infrastructures

Ziad Ismail, Jean Leneutre*, David Bateman and Lin Chen†
EDF R&D France, *Telecom ParisTech, †University of Paris-Sud 11
{firstName.lastName}@edf.fr, *{jean.leneutre}@telecom-paristech.fr, †{lin.chen}@lri.fr

Abstract—**The communication infrastructure is a key element for management and control of the power system in the smart grid. The communication infrastructure, which can include equipment using off-the-shelf vulnerable operating systems, has the potential to increase the attack surface of the power system. The interdependency between the communication and the power system renders the management of the overall security risk a challenging task. In this paper, we address this issue by presenting a mathematical model for identifying and hardening the most critical communication equipment used in the power system. Using non-cooperative game theory, we model interactions between an attacker and a defender. We derive the minimum defense resources required and the optimal strategy of the defender that minimizes the risk on the power system. Finally, we evaluate the correctness and the efficiency of our model via a case study.**

Keywords-**Cyber-physical System; Non-cooperative Game Theory; SCADA Security;**

I. Introduction

The future power grid known as the smart grid is a modernized grid that enables bidirectional flows of energy, and uses two-way communication and control capabilities that will lead to an array of new functionalities and applications [1]. It is envisioned to increasingly rely on information technology to deliver electricity efficiently, reliably, and securely. The communication infrastructure that enables such services is very important, as it allows control and electrical engineers to track the state of the grid in real time, in such a way that system failures are isolated as soon as they are identified. In addition, tracking the customers' power consumption enables engineers to adapt the generation to the load and to use energy resources more efficiently.

The increased dependence of the smart grid on ICT (Information and Communications Technology) will potentially expose it to additional threats. An attack on a communication equipment used to control an industrial process can have severe impact on critical infrastructures [4]. Reciprocally, an electrical node responsible of providing power to a set of communication equipment is important to the communication infrastructure: if the power source of these equipment is compromised, the communication nodes will not be able to achieve their objectives. The complex interaction between the ICT and the power system makes it difficult to assess the impact of malicious attacks on the reliability and availability of the power grid. Different risk analysis methods exist to assess the reliability of the power grid, and the security of the ICT infrastructure (for example [2] and [3] respectively for power grid and ICT infrastructures). However, most of these methods treat each infrastructure independently. The interdependency between the ICT and the power system needs to be studied. The security of the power and ICT systems needs to be evaluated jointly to determine the risk of an unintended failure or accident or deliberate attack on each component of these systems. In addition, it is important to study the risk propagation between components of the communication and the electrical systems. This will eventually help identify the most critical parts of each system that cause the highest damage on the power grid. Throughout the paper, the communication system refers to the telecommunication infrastructure responsible of controlling and monitoring the electrical system.

Different techniques were used to model the interdependencies between the communication and the electrical systems including agent-based [5], petri nets [6] and co-simulation [7]. However, the choice of the level of abstraction used to represent system components affects the nature and the type of interdependencies that will be investigated and their potential impact on the behavior of the system. A formal model able to model and analyze the impact of complex interactions between the communication and the electrical systems is still needed. In this paper, we propose a mathematical model for identifying the most critical communication equipment used in the power system that must be hardened. To achieve this goal, we use a set of parameters to assess the impact of attacks on system nodes. We suppose that these values are known as a result of a preliminary application of risk assessment methods in each infrastructure.

In addition to classic security approaches, other approaches based on game theory were recently used to study and analyze smart grid security problems [8] [9]. Game theory is a tool that allows the analysis of complex interactions between different players with the same or conflicting interests. In particular, game theory has been used to study distributed control of micro-grids and energy consumption scheduling for demand-side management [9]. The concept of Nash equilibrium (NE) in game theory allows the definition of the optimal strategies of players in which none of them has an incentive to unilaterally deviate from. From a security point of view, it means it is possible to characterize the optimal strategy of the defender that takes into account the attacker's actions. In this paper, we propose to use game theory to identify the optimal distribution of defense resources on vulnerable equipment in the

978-1-4799-8111-3/15 $31.00 © 2015 IEEE
DOI 10.1109/HASE.2015.24

communication system.

The contributions of this paper are organized as follows. In section II, we present different factors that are used to assess the initial risk on each equipment in the communication and power infrastructures. In section III, we extend the model for risk diffusion presented in [10] and extend it to include risk diffusion between nodes of the same infrastructure and prove the existence of an equilibrium. We present in section IV a security game between an attacker who tries to compromise communication equipment to cause the maximum impact on the power grid, and a defender who's objective is to protect the power system by hardening the security on communication equipment, while taking into account the existence of backup control equipment in the communication infrastructure. We prove the existence of a solution and solve the game analytically. In section V, we show via a case study depicting interdependencies between a subset of a control network and the power grid, how our framework can be applied to find optimal security strategies that reduce the risk of cyberattacks on the power system. Section VI discusses related work. Finally, we conclude the paper in section VII.

II. Initial Risk

There are multiple risk analysis methods designed for information systems risk assessment. These methods classify threats and define security objectives that are generally to ensure the integrity, confidentiality and availability of data or communications. However, such methods cannot be applied directly to assess risks on communication equipment in the electrical system due to the interdependency that exists between the two infrastructures. The electrical system main objective is to ensure that electricity is delivered without service disruptions. The integrity of data used to estimate the state of the power system needs to be guaranteed. The combination of the availability and the integrity of data are essential to ensure the dependability and availability of the power grid. The electrical system uses a Supervisory Control and Data Acquisition (SCADA) system to monitor and control electrical equipment in the power system. SCADA uses several telecommunication infrastructures such as telephone lines, cellular networks, etc. to send data to a control center to be analyzed. This renders the power system dependent on the reliability and security of the telecommunication system.

The impact of attacks on an electrical node depends, among other factors, on the nature of the node (e.g. generator, transformer, load). We refer by initial risk, the risk on a node before the impact of an accident or an attack propagates between system nodes. Several methods exist to assess the risk of faults in the power system. For example, PROMAPS [11] calculates the probability and the financial consequences of fault conditions in the power system. However, deliberate attacks on control equipment can have severe impact on the grid. Therefore, this type of events needs to be taken into account when assessing risk on the power system. Different factors affect the initial risk $r_i^e(0)$ on an electric equipment i such as the power P generated/consumed by the node, the cost of recovery in the event of a failure, the number of affected customers if the node fails, etc.

The communication infrastructure is critical in today's power systems. On the other hand, communication equipment need electric power to function. Therefore, the risk on communication equipment should take into account the impact of compromised equipment in the power system. Similarly to electric nodes, we consider an initial risk $r_j^c(0)$ on the communication equipment j. As for $r_i^e(0)$, we do not provide a definition for computing $r_j^c(0)$. However, factors that may affect its value include the criticality/importance of electrical nodes' data processed by j, the number of electric equipment it controls, etc.

In this paper, we assume that initial risk on system nodes are nonnegative real numbers and has been evaluated using risk assessment methods. We are interested in the risk diffusion process between nodes in the same infrastructure as well as between nodes of different infrastructures.

III. Risk Diffusion and Equilibrium

We model the interdependency between the electrical and the communication infrastructures as a weighted directed interdependency graph $\mathcal{D}$. The graph $\mathcal{D}$ is defined as the triplet $(V,\ E,\ f)$. $V = \{v_1, v_2, ..., v_N\}$ 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 $\mathcal{D}$. An element of the set of ordered pairs of vertices E is defined as $e_{ij} = (i, j)$, where i is the tail of the edge and j its head. Depending on the head and the tail of element e_{ij}, the meaning of the edge is different. Finally, $f : E \to \mathbb{R}^+$ is a function where $f(e_{ij})$ refers to the weight associated with the edge e_{ij}.

Let $V = \{\mathcal{T}^e, \mathcal{T}^c\}$, such that $\mathcal{T}^e = \{v_1, v_2, ..., v_{N_e}\}$ 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:

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

$$\text{where} \begin{cases} B = [b_{ij}]_{N_e\times N_e} & s.t \ \sum_i b_{ij} = 1 \ \forall j \\ D = [d_{ij}]_{N_e\times N_c} & s.t \ \sum_i d_{ij} = 1 \ \forall j \\ F = [f_{ij}]_{N_c\times N_e} & s.t \ \sum_i f_{ij} = 1 \ \forall j \\ S = [s_{ij}]_{N_c\times N_c} & s.t \ \sum_i s_{ij} = 1 \ \forall j \end{cases}$$

Matrix M represents the effects of nodes on each other and is a block matrix composed of left stochastic matrices B, D, F and S. Elements of these matrices are nonnegative real numbers. Matrix B represents the dependency between electrical nodes. Each element b_{ij} of B represents the impact of the failure of electrical node i on electrical node j. Dependencies between communication nodes are represented in matrix S. Control engineers use the communication infrastructure to observe the state of the power system. An incident or attack on a set of communication nodes could have severe impact on power system control data routing and analysis. In addition, a failure of electric equipment can deprive communication equipment from their main power supply. We introduce matrices D and F to represent the dependency relation on communication nodes by electric nodes and vice versa respectively. M represents the effect of an accident or an attack on a node to nodes of both communication and electric infrastructures. Fig. 1 shows the cascading risk relation between electrical and communication nodes in the system. In this section, we are interested in computing the risk on communication equipment after an attacker compromises a set of nodes in the communication system. We consider that the first cascading effects of an attack on communication equipment take place in the communication infrastructure itself. Afterwards, the impact of the attack propagates to the electric system. Finally, the failures in the power grid will affect the power supply of communication nodes.

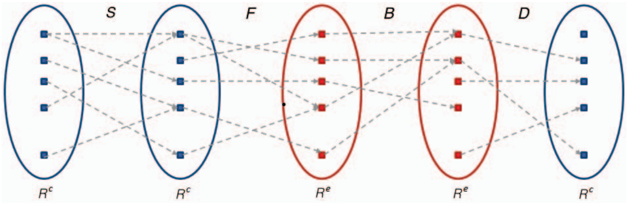

Fig. 1: Cascading risk between the electrical and communication nodes

In the communication system, we consider that a set of Intrusion Detection Systems (IDS) exists. We assume that devices that assure a security function such as IDSs, have security mechanisms protecting the availability of their function. The attacker tries to compromise a set of communication nodes in order to control or disrupt the power system. The probability of being detected increases each time the attacker attempts to compromise a new equipment. Therefore, we consider that the payoff of future attacks decreases at each attack step. Let γ_c be a nonnegative real number that represents the weight of the impact payoff of future attacks. γ_c is a function of the probability of detection of the IDS and attacker's profile. For example, an insider attacker could possess credentials that enables him to legitimately access control equipment without drawing suspicions.

In the power system, different safety and control measures ensure that failures in the electric system do not propagate through the entire grid. When an electric node fails or is compromised, let γ_e be a nonnegative real number that represents the weight of the impact of future cascading failures between electric equipment. γ_e is a function of the probability that safety measures prevent the impact of a failed node of propagating in the power grid.

We introduce two metrics that define the scale of attacks' impacts propagation between systems' nodes. The average propagation time t_c in the communication system is the average time for the impact of an attack on communication equipment to propagate in the communication infrastructure. The average time t_e in the electrical system 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. The time t_e can give an insight on the extent of a failure of electric equipment to propagate in the power grid before impacting the communication infrastructure.

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. We are interested in computing the maximum impact of an attack on communication equipment to reach communication nodes during time t_c. Let the matrix $S^{max} = [s_{ij}^{max}]_{N_c \times N_c}$ represents this maximum impact, where $s_{ij}^{max} = \max_{l=1,\dots,\lfloor t_c \rfloor} \gamma_c^l s_{ij}^l$. The overall impact on node j, given a specific attack path, depends on the number of equipment the attacker needs to compromise to impact node j. At attack step r, the payoff is decreased by γ_c^r. In fact, we consider that each action of the attacker in the system increases the probability of him being detected. Therefore, γ_c^r represents the uncertainty for the attacker of getting the payoff of the r^{th} future attack step.

Similarly, we define the matrix $B^{max} = [b_{ij}^{max}]_{N_e \times N_e}$ that represents the maximum impact of an attack on electrical equipment to reach electrical nodes during time t_e, where $b_{ij}^{max} = \max_{l=1,\dots,\lfloor t_e \rfloor} \gamma_e^l b_{ij}^l$. Let S_n^{max} and B_n^{max} be the normalized matrices of S^{max} and B^{max} with respect to their rows s.t. $\forall j,\ \sum_i {b_n^{max}}_{ij} = 1$ and $\sum_i {s_n^{max}}_{ij} = 1$.

Therefore, the system of equations for inter- and intra-infrastructure risk diffusion is given by:

$$\begin{cases} R^c(t+1) = S_n^{max} R^c(t) \\ R^c(t+1) = F R^e(t) \\ R^e(t+1) = B_n^{max} R^e(t) \\ R^e(t+1) = D R^c(t) \end{cases} \tag{1}$$

Solving the system of equations 1, we will have: $R^c(t+4) = S_n^{max} F B_n^{max} D R^c(t) = H R^c(t)$ where $H = [h_{ij}]_{N_c \times N_c} = S_n^{max} F B_n^{max} D$.

Lemma 1. *Matrix $H = S_n^{max} F B_n^{max} D$ is a left stochastic matrix.*

Proof: Let $Z = [z_{ij}]_{m \times n}$ and $Y = [y_{ij}]_{n \times m}$ s.t $\forall j,\ \sum_i z_{ij} = 1$ and $\sum_i y_{ij} = 1$. Let $X = [x_{ij}]_{m \times m} = ZY$. Therefore:

$$\begin{aligned} \sum_i x_{ij} &= \sum_i \sum_m z_{im} y_{mj} = (\sum_m y_{mj})(\sum_i z_{im}) \\ &= \sum_m y_{mj} = 1 \end{aligned}$$

Similarly, we can prove that the matrix H which is the product of matrices S_n^{max}, F, B_n^{max} and D is a left stochastic matrix. ■

We take a similar approach to [10] by balancing the immediate risk and the future induced one. The value of risk on communication equipment at a given time is defined as:

$$R^c(t+4) = \delta H R^c(t) + \beta R^c(0) + \theta D^T R^e(0) \qquad (2)$$

In equation 2, β, θ and δ are nonnegative real numbers and $\beta + \theta + \delta = 1$. β and θ 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. Finally, δ reflects the weight of future cascading risk w.r.t the value of the total risk on communication equipment.

Theorem 1. *The iterative system of the cascading risk converges. An equilibrium solution exists whenever $\delta < 1$ and is given by:*

$$R^{c*} = (I - \delta H)^{-1}(\beta R^c(0) + \theta D^T R^e(0)) \qquad (3)$$

$$where\ H = S_n^{max} F B_n^{max} D$$

Proof: Refer to Appendix A for full proof. ■

From Theorem 1, we can predict how the risk on communication equipment diffuses between nodes of the communication and electric systems. If an attacker has access to H, he can choose his targets in the communication system intelligently to maximize the impact of his attacks on the power system. In the next section, we propose a security game between an attacker and a defender and analyze the behavior of both players in this scenario.

IV. Security Game

The use of communication equipment has the potential to increase the attack surface of the power system. Attacks on the communication system could have severe impact on the power grid. It is conceivable that an attacker could exploit vulnerabilities in the strategy of the defender to compromise communication equipment that control electric equipment. In this section, we try to analyze the expected behavior of a rational attacker and derive the optimal strategy of the defender. We formulate the problem as a non-cooperative game and analyze the behavior of the attacker and the defender at the Nash equilibrium. 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 a perfect information game. In addition, we assume that both players have complete knowledge of the architecture of the system.

The attacker's strategy is a vector $p = [p_i]_{1 \times N_c}$ where each $0 \leq p_i \leq 1$ is the attack resource allocated to target $i \in \mathcal{T}^c$. The defender's strategy is a vector $q = [q_i]_{1 \times N_c}$ where each $0 \leq q_i \leq 1$ is the defense resource allocated to target $i \in \mathcal{T}^c$. We can interpret p_i (resp. q_i) as the probability that the attacker (resp. defender) attacks (resp. defends) communication node i. We assume that the cost of attacking and defending a communication node i are proportional to the risk on node i and are given by $c_i^a r_i^c(0)$ and $c_i^d r_i^c(0)$ respectively, where $0 \leq c_i^a, c_i^d \leq 1$.

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. In general, the power utility assigns a set K_i of communication nodes to be the backup of another set K_j if equipment in K_j were compromised or became unreachable. The existence of redundant equipment in the communication system increases the resilience of the power grid against cyber attacks. Let $W = [w_{ij}]_{N_c \times N_c}$ be the redundancy matrix where $\forall i$, $w_{ii} = -1$ and $\sum_{j, j \neq i} w_{ij} \leq 1$. 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. In fact, control centers rely on a telecommunication infrastructure to communicate. A telecommunication carrier often manages this infrastructure. A failure in the power system could impact communications between control centers, therefore affecting the possibility that redundant equipment take charge of the load of compromised communication equipment. This effect should be taken into account when evaluating the impact of the existence of redundant equipment on the utilities of the attacker and the defender.

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

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

$R_D^c(0)$, R_D^{c*}, C^a and C^d are diagonal matrices, I is the identity matrix and $e = (1, ..., 1)_{1 \times N_c}$. The players' utilities are composed of three terms:

- Payoff of an attack taking into account both players' actions and the cascading impact of the attack in the communication and electric systems
- Cost of attacking/defending
- Impact of redundant equipment in ensuring the control of the power system when a set of communication nodes are compromised. $\psi \in [0, 1]$ is a parameter that represents the impact of the existence of backup equipment in computing players' utility functions. ψ is a function of the probability that backup equipment are able to take charge of the load of compromised communication equipment.

In the context of non-cooperative games, we are interested in the concept of Nash equilibrium (NE), in which none of the players has an incentive to deviate unilaterally [12]. The Nash equilibrium is considered as the most profitable strategy profile that maximizes each player's utility given the actions of other players. Let $p = (p_1, ..., p_{N_c}) \in \mathscr{P}$ and $q = (q_1, ..., q_{N_c}) \in \mathscr{Q}$ be the strategy profiles of the attacker and the defender respectively, where $\mathscr{P}$ and $\mathscr{Q}$ refer to the strategy spaces of each player. We define the Nash equilibrium as follows:

Definition 1. *A **Nash equilibrium** is a strategy profile (**p*,q***) in which each player cannot improve his utility by altering his decision unilaterally.*

A. One-shot Game

In this section, we investigate the case where both the attacker and the defender take the decisions at the same time while taking into account each others' strategies. This type of interactions falls under the one-shot game category [12].

Let p^* and s^* denote the attacker and defender strategies at Nash equilibrium respectively. Therefore, we have:

$$U_A(p^*, q^*) > U_A(p, q^*) \ \forall p \in \mathscr{P}$$
$$U_D(p^*, q^*) > U_A(p^*, q) \ \forall q \in \mathscr{Q}$$

Theorem 2. *A unique Nash Equilibrium of the game exists and is given by:*

$$q^* = \frac{1}{2}e(R_D^{c*} + \psi L)(R_D^c(0)C^a)^{-1}M[\frac{1}{2}M^T(R_D^c(0)C^a)^{-1}M + 2R_D^c(0)C^d]^{-1} \tag{4}$$

$$p^* = e(R_D^{c*} + \psi L)[\frac{1}{2}M(R_D^c(0)C^d)^{-1}M^T + 2R_D^c(0)C^a]^{-1} \tag{5}$$

$$where \ \ M = R_D^{c*} + \psi L(W + 2I)$$

Proof: Refer to Appendix A for full proof. ■

The analytical solution has multiple advantages. From a scalability point of view, the complexity resides in evaluating the input parameters of the model. In fact, by proving the existence and unicity of the Nash Equilibrium, and characterizing the solution analytically, we avoided the complexity of searching the set of all possible strategies to find the NE. Using an analytical solution, we can compute the optimal strategies of both players directly and be able to assess the sensitivity of players' strategies to estimation errors on the values of parameters used in the model.

B. Stackelberg Game

In most cases, the attacker chooses his attack strategy based on the deployed security measures in the system. In this section, we analyze the interactions between players as a Stackelberg game [12]. In this type of games, a leader chooses his strategy first. Then, the follower, informed by the leader's choice, chooses his strategy. The leader tries to anticipate the follower's response. In our case, the defender is the leader who tries to secure communication equipment in order to best protect the power system.

Stackelberg games are generally solved by backward induction. The solution is known as Stackelberg Equilibrium (SE) or Stackelberg-Nash Equilibrium (SNE). We start by computing the best response strategy of the follower as a function of the leader's strategy. Then, according to the follower's best response, we derive the optimal strategy of the leader.

The attacker solves the following optimization problem:

$$p(q) = \underset{p \in [0;1]^{N_c}}{\operatorname{argmax}} U_A(p, q)$$

On the other hand, the defender solves the following optimization problem:

$$q(p) = \underset{q \in [0;1]^{N_c}}{\operatorname{argmax}} U_D(p(q), q)$$

Theorem 3. *The game admits a unique Stackelberg Nash equilibrium (p^S, q^S) given by:*

$$q^S = e(R_D^{c*} + \psi L)(R_D^c(0)C^a)^{-1}M(Q + 2R_D^c(0)C^d)^{-1} \tag{6}$$

$$p^S = \frac{1}{2}e(R_D^{c*} + \psi L)(R_D^c(0)C^a)^{-1}[I - M(Q + 2R_D^c(0)C^d)^{-1}M^T(R_D^c(0)C^a)^{-1}] \tag{7}$$

$$where \ \ Q = M^T(R_D^c(0)C^a)^{-1}M$$

Proof: The solution can be found by solving the system by backward induction. We start by finding p^S by setting $\nabla U_a(p, q) = 0$. Then we solve the equation $\nabla U_d(p^S, q) = 0$ to find q^S.

Similarly to the proof of Theorem 2, we can prove that $(Q + 2R_D^c(0)C^d)^{-1}$ exists. ■

V. Case Study

In this section, we prove the efficiency of our model via a case study inspired from [13]. We consider a subset $\mathcal{E}$ of the electrical system represented in Fig. 3. We assume that $\mathcal{E}$ is vulnerable to attacks and the attacker has the capability of compromising equipment in $\mathcal{E}$. In our analysis, we assume that the attacker has enough resources and both players know the architecture of the system.

$\mathcal{E}$ is composed of seven building blocks: a Distribution System Operator (DSO) ICT Control Center, two DSO Area Control Centers and four distribution substations. The unique DSO ICT Control Center manages all communication equipment in $\mathcal{E}$. Each Area Control Center is responsible of controlling two substations. Substations SS11 and SS12 are controlled by DSO Area 1 Control Center. Substations SS21 and SS22 are controlled by DSO Area 2 Control Center.

ICT Control Centers. In the DSO ICT Control Center, four types of communication equipment are represented. A Time Server synchronizes the clocks in all communication equipment used in $\mathcal{E}$. 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.

SCADA Control Centers. In this case study, we represent four types of communication equipment in each Area Control Center: a SCADA HMI, a SCADA Server, a SCADA frontend and a SCADA Historian. At each distribution substation, we represented only two communication equipment, the substation HMI and the substation SCADA. In our case study, the substation electric equipment such as generators, transformers, etc. are represented as an electrical node. The substation SCADA controls the electrical node. For example, commands can be sent to power generators or to route electricity through electric buses.

Impact Matrix. Fig. 2 depicts an example of possible impacts between electric and communication equipment. We suppose that substations S11 and S21 have an impact on the power supply of equipment in the DSO ICT Control Center, and on equipment in the DSO Area 1 and Area 2 Control Centers respectively. Substation S12 has an impact on the power supply of equipment in the DSO Area 2 Control Center. Finally, we suppose that communication equipment in DSO Area 2 Control Center are the backup of communication equipment in Area 1 Control Center.

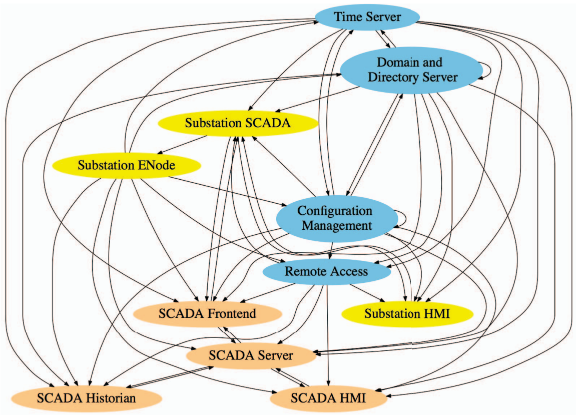

Fig. 2: Example of impacts between communication and electric equipment

Backup equipment can take control of substations of the compromised DSO Area Control Center. This assumes that communication between DSO Control Centers can be established. However, DSO Control and ICT Management networks are generally managed nowadays by third parties. The failure of the power system can lead to a failure of telecommunication equipment. Therefore, a failure in the power system can affect the availability of communication links used by control centers.

In this case study, we assume that the values of the initial risk on equipment have been computed, and we focus on the diffused risk in the system and the behavior of the attacker and the defender. To simplify the analysis, we assume that vectors C^a and C^d are equal, and that $\beta = 0.4$, $\theta = 0$, and $\delta = 0.6$. The future cascading risk has more weight than initial risk w.r.t the value of the total risk on communication equipment.

Table I presents the results of the game between the attacker and the defender.

TABLE I: Nash Equilibrium

		$\mathbf{r_i^{c*}}$	**One-Shot game**		**Stackelberg game**	
			p^*	q^*	p^S	q^S
DSO ICT	**Time Server**	0.761	0.247	0.935	0.128	0.966
	Domain Server	0.758	0.376	0.829	0.206	0.907
	Remote App.	0.4	0.378	0.827	0.207	0.905
	Config. Manag.	0.678	0.159	0.974	0.081	0.987
Area 1	**SCADA Fontend**	0.607	0.362	0.586	0.202	0.654
	SCADA Server	0.285	0.358	0.435	0.207	0.504
	SCADA Historian	0.285	0.377	0.394	0.228	0.476
	SCADA HMI	0.206	0.327	0.414	0.185	0.468
S11	**Subst. HMI**	0.503	0.373	0.833	0.204	0.909
	Subst. SCADA	0.397	0.467	0.678	0.278	0.808
S12	**Subst. HMI**	0.309	0.438	0.741	0.252	0.851
	Subst. SCADA	0.364	0.475	0.657	0.287	0.793
Area 2	**SCADA Fontend**	0.494	0.398	0.719	0.234	0.835
	SCADA Server	0.269	0.405	0.658	0.247	0.792
	SCADA Historian	0.283	0.419	0.598	0.264	0.746
	SCADA HMI	0.204	0.391	0.689	0.235	0.814
S21	**Subst. HMI**	0.454	0.389	0.814	0.214	0.898
	Subst. SCADA	0.378	0.472	0.666	0.283	0.799
S22	**Subst. HMI**	0.243	0.46	0.695	0.272	0.82
	Subst. SCADA	0.341	0.48	0.641	0.292	0.781

1) One-Shot game: In this type of games, both players choose their strategies at the same time. The utilities of the attacker and the defender in the one-shot game are $Ua = 0.7$ and $Ud = -3.384$ respectively. We notice that the Time, Configuration and Domain Servers have the highest risk values. Communication equipment in DSO 2 Control Center are the backup of communication equipment in DSO 1 Control Center. We notice that the attacker and the defender allocate more resources to attack/defend equipment in DSO 2 Control Center than to attack/defend equipment in DSO 1 Control Center. SCADA Frontend in DSO 1 Control Center sends control commands to S11 and S12. This role made it a critical asset for the defender. Attacks on each substation have different impacts on the power system. We notice that substation S11 HMI is identified as the most critical among all substations' HMIs. In addition to the risk on an equipment, the cost and the existence of backup for a communication equipment play an important role in the strategy of both players. Under the assumption of the rationality of both players, the strategy at the Nash equilibrium yields the best payoff for the defender that reduces the impact on the power system taking into account attacker's actions.

2) Stackelberg game: In the Stackelberg game, the defender is the leader who tries to anticipate attacker's actions and secure communication equipment to reduce the impact on the power system. The utilities of the attacker and the defender in the Stackelberg game are $Ua^S = 0.242$ and $Ud^S = -3.095$ respectively. We notice that compared to the one-shot game, the defender increased his defense resources on each equipment. However, the defender's strategy forced the attacker to reduce his attack resources on each equipment. Compared to the one-shot game, an additional security investment by the defender by 1.93 reduced the attacker's allocated resources by 3.245. An increase of the defender resources by 14% allowed the defender to increase his utility by 8.5%. However, the attacker was forced to decrease his attack resources by 41.9%, which reduced his utility by 65.4%. As a result, the benefits of operating at the Stackelberg equilibrium for the defender

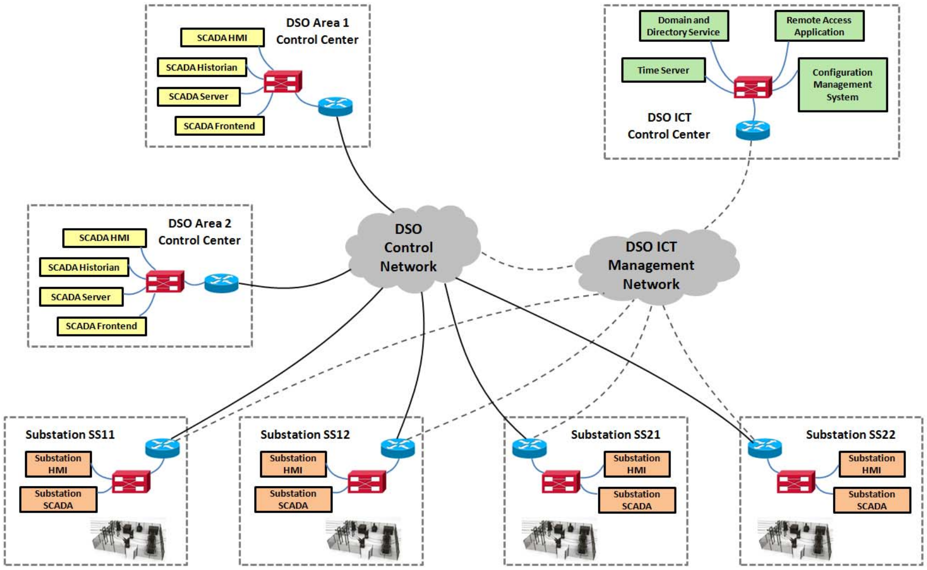

Fig. 3: Example of a subset of the control network in the power grid

outweigh the additional cost of increasing security investments on communication equipment.

3) Sensitivity Analysis: Each parameter used in the model has been submitted to experts of the domains to check whether it is possible to correctly assess its value. However, we performed a sensitivity analysis to evaluate the consequences of an estimation error in one or several parameters. We conducted a sensitivity analysis of the diffused risk R^{c*} and the players' NE strategies in the one-shot and Stackelberg games with respect to the values of the initial risk $R^c(0)$ and the elements of the matrix H. We averaged the results of 1000 iterations. At each iteration, we assume that a random 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 same experiment taking into account errors in a random number of elements of matrix H.

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 (maximum error was 3.8% and 2% respectively).

Sensitivity to H. The maximum error on the values of R^{c*} was around 2%. The worst case error in the attacker strategy was about 18%. The defender strategy at equilibrium in the Stackelberg game is less sensitive to errors in H than his strategy in the one-shot game (maximum error was 8.8% and 13.8% respectively).

VI. Related Work

As we already noted, risk assessment is conducted for the communication and the power system independently (see for example [3] and [2]). With the increased interdependence between ICT and electric systems, different methods were proposed to model the complex interactions including agent-based [5], petri nets [6] and co-simulation [7]. Complex networks have also been used to model interdependencies between these infrastructures and leverage common graph properties to analyze these systems [14] [15].

In our model, we supposed that the attacker knows the topology of the power grid. Even though this assumption does not always hold and depends on the profile of the attacker, Li et al. [16] showed that an attacker, with access to limited data, can learn the topology of the power system. Different models were proposed to identify critical components in the power grid [17]. However, it is important to identify vulnerabilities in the communication system that could impact the power system. Parandehgheibi et al. [18] focus on the interdependency between the power grid and communication networks to study the minimum number of node failures needed to cause total blackout. Beccuti et al. [19] use a SWN (Stochastic Well-formed Nets) and a SAN (Stochastic Activity Network) to model the communication and electric systems respectively. However, their study is limited to the effect of a DoS attack on the communication system to affect the power system. Bloomfield et al. [20] proposed a method and developed a tool to analyze the interdependencies that exist between critical infrastructures. Based on a preliminary description of services and their interdependencies (deterministic or stochastic), an execution engine based on the tool Möbius simulates the model. The authors use a Monte Carlo simulation to quantify the impact of interdependencies on the behavior of the system.

Multiple approaches were proposed to improve the security of the power system. A possible solution to improve the resiliency of the power system could be achieved by adding intelligent equipment to create a reconfigurable grid [21]. Anwar et al. [22] addressed the issue of choosing an optimal combination of security hardening schemes to secure control networks for critical infrastructures under a certain defense cost budget. Sridhar et al. [23] proposed a layered approach to evaluate the risk on the power grid based on the cyber-physical security. However, in these complex interdependent systems, the interactions between the attacker and the defender play an important role. Game theory is a mathematical tool used to study interactions between different players with the same or conflicting interests. It has already been used to analyze the security of the power system. 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, trying to choose the intensity of false data injection, and a defender trying to determine the detection threshold level. Finally, Amin et al. [24] present a framework to assess risks to Cyber-Physical Systems (CPS) when interdependencies between information and physical systems may result in correlated failures. They formulate the problem of security choices of the individual players as a non-cooperative game. After choosing their security strategies, each player chooses a control input sequence to maintain optimal closed-loop performance.

In our work, we propose a mathematical model to represent the risk diffusion process of attacks on communication equipment in the power system. This model has multiple advantages as it allows us to evaluate the efficiency of hardening the security on a set of communication equipment in reducing the impact of attacks on the power grid. We analyze the interactions between an attacker and a defender in the system. The result of the risk diffusion process constitutes an important element in the definition of both players' utility functions. The structure of the utility functions allows us to analytically compute the optimal strategy of both players. The defender is therefore capable of prioritizing the distribution of defense resources on critical communication equipment that most impact the power system and are likely to be the targets of attacks.

VII. Conclusion

In this paper, we proposed 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. We proposed a model to compute the total risk on an equipment as a combination of the initial risk and the diffused/future risk. Using these inputs, we proposed a security game between an attacker and a defender. The objective of the attacker is to compromise communication equipment to cause the maximum impact on the power system, whereas the defender tries to protect the power system by hardening the security on communication equipment. In addition, we take into account backups in the communication system, enabled when a set of equipment are compromised or became unreachable. Finally, we showed via a case study the advantages of our interdependency model and our game framework.

The presented model constitutes an initial, although important, step to formally represent the effects of the interdependency between the communication and the power systems. In our future work, we plan to validate the model on a real use case with the definition of a detailed process to evaluate the initial risk on equipment. Extending the model to include specific control functions in the power grid would allow a more fine grained analysis of the risk on the power system. In addition, investigating the effect of partial knowledge of the parameters of the system on the strategies of both the attacker and the defender is an interesting extension to the presented work. Further explorations would include studying the existence of multiple attackers and the impact of their cooperation on the power system.

Appendix A

Proof of Theorem 1:
From Lemma 1, we know that H is a left stochastic matrix. The spectral radius of any matrix is less than or equal to the norm of the matrix. The 1-norm of the matrix $H = [h_{ij}]_{N_c \times N_c}$ is defined as $\|H\|_1 = \max\limits_{0 \leq j \leq N_c} \{\sum\limits_{i=1}^{N_c} |h_{ij}|\}$. The matrix H is a left stochastic matrix. Therefore, $\|H\|_1 = 1$ and the spectral radius $\rho(H) \leq 1$. The matrix S has at least one eigenvalue equals to 1 since (1,e) is an eigenpair of H^T (where $e = [1...1]^T$). Since the matrix H is multiplied by $\delta < 1$, so as the eigenvalues of H. Therefore, the sequence converges. The equation of the cascading risk $R^c(t+4) = \delta H R^c(t) + \beta R^c(0) + \theta D^T R^e(0)$ converges to the value R^{c*} given by $R^{c*} = \delta H R^{c*} + \beta R^c(0) + \theta D^T R^e(0)$.
The solution of the problem is given by: $\lim\limits_{t \to +\infty} R^c(t) = (I - \delta H)^{-1}(\beta R^c(0) + \theta D^T R^e(0))$. The existence of the solution depends on the existence of the inverse of the matrix $(I - \delta H)$. However, we can notice that:
$\mid 1 - \delta h_{ii} \mid > \mid \delta \sum\limits_{i \neq j} h_{ij} \mid = \mid \delta - \delta h_{ii} \mid \; \forall i$ is true whenever $\delta < 1$.
In this case, the matrix $(I - \delta H)$ is a strictly column diagonally dominant matrix, and therefore nonsingular. As a result, $(I - \delta H)^{-1}$ exists.

Proof of Theorem 2:
Let $\overline{\nabla}$ be the pseudogradient operator of $U = U_a(u) + U_d(u)$ where $u = [p\ q]$.

$$g(u) = \overline{\nabla} U = \left[\begin{array}{c} \nabla_p U_a(u) \\ \nabla_q U_d(u) \end{array} \right]$$

Let $G(u)$ be the Jacobian of $g(u)$.

$$G(u) = \left(\begin{array}{c:c} -diag(2r_i^c(0)c_i^a) & -R_D^{c*} - \psi(W^T + 2I)L \\ \hdashline R_D^{c*} + \psi L(W + 2I) & -diag(2r_i^c(0)c_i^d) \end{array} \right)$$

We suppose that $r_i^c(0)c_i^a \neq 0$ and $r_i^c(0)c_i^d \neq 0 \; \forall i$. Therefore $(G(u) + G(u)^T)$ is a negative definite matrix. As a result, U is diagonally strictly concave. Based on [25], an equilibrium of the game in pure strategy exists and is unique.

To characterize the equilibrium, we need to find vectors p^* and q^* in which the gradients ∇U_a and ∇U_d are equal to 0.

Solving these equations, we find q^* and p^* given in equations 4 and 5 respectively.

Let $M = R_D^{c*} + \psi L(W + 2I)$. The existence of p^* and q^* depend on the existence of the inverse of the matrices ξ and ζ, where:

$$\begin{aligned} \xi &= \tfrac{1}{2}[M(R_D^c(0)C^d)^{-1}M^T + 4R_D^c(0)C^a] \\ and\zeta &= \tfrac{1}{2}[M^T(R_D^c(0)C^a)^{-1}M + 4R_D^c(0)C^d] \end{aligned}$$

The diagonal matrix $4R_D^c(0)C^a$ is a positive definite matrix (diagonal matrix with strictly positive elements).
To prove that $M(R_D^c(0)C^d)^{-1}M^T$ is a positive definite matrix, we need to show that:

$$\forall x \neq 0,\ x^T M(R_D^c(0)C^d)^{-1}M^T x > 0 \qquad .$$

Let $y = M^T x$. Therefore, we need to prove that:

$$\forall y \neq 0,\ y^T(R_D^c(0)C^d)^{-1}y > 0 \qquad (8)$$

However, $(R_D^c(0)C^d)^{-1}$ is a positive definite matrix, and the equation 8 holds. Therefore, the matrix $M(R_D^c(0)C^d)^{-1}M^T$ is a positive definite matrix. Finally, the matrix ξ is a positive definite matrix because it is the sum of two positive definite matrices. Since ξ is a positive definite matrix, the inverse ξ^{-1} exists. Similarly, we prove that ζ^{-1} exists.

Acknowledgment

The authors would like to thank John McDonald in the Department MIRE at EDF for his help and support that improved the quality of this paper.

References

[1] National Institute of Standards and Technology, “NIST framework and roadmap for smart grid interoperability standards, Release 1.0,” january, 2010.

[2] Wenyuan Li, *Risk Assessment Of Power Systems: Models, Methods, and Applications*. Wiley-IEEE Press, 2005.

[3] ANSSI, “EBIOS (Expression of Needs and Identification of Security Objectives) Risk Management Method,” 2010, URL: http://www.ssi.gouv.fr/IMG/pdf/EBIOS-1-GuideMethodologique-2010-01-25.pdf.

[4] K. Poulsen, “Slammer worm crashed Ohio nuke plant network,” *SecurityFocus*, August 19, 2003, URL: http://www.securityfocus.com/news/6767.

[5] E. Casalicchio, E. Galli, and S. Tucci, “Federated agent-based modeling and simulation approach to study interdependencies in it critical infrastructures,” in *11th IEEE International Symposium on Distributed Simulation and Real-Time Applications*, 2007, pp. 182–189.

[6] T. Chen, J. Sanchez-Aarnoutse, and J. Buford, “Petri net modeling of cyber-physical attacks on smart grid,” *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 741–749, 2011.

[7] H. Lin, S. S. Veda, S. K. Shukla, L. Mili, and J. S. Thorp, “GECO: Global Event-Driven Co-Simulation framework for interconnected power system and communication network,” *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1444–1456, 2012.

[8] Y. W. Law, T. Alpcan, and M. Palaniswami, “Security games for voltage control in smart grid,” in *50th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2012, pp. 212–219.

[9] W. Saad, Z. Han, H. V. Poor, and T. Basar, “Game theoretic methods for the smart grid,” IEEE Signal Processing Magazine, Special issue on Signal Processing for the Smart Grid, vol. 29, no. 5, pp. 86-105, September 2012.

[10] T. Alpcan and N. Bambos, “Modeling dependencies in security risk management,” in *Proceedings of the 4th International Conference on Risks and Security of Internet and Systems (Crisis)*, October 2009.

[11] http://www.goodtech.se/en/services/power/promaps.

[12] M. J. Osborne and A. Rubinstein, *A course in game theory*. MIT Press, 1994.

[13] M. Ekstedt, M. Korman, R. Terruggia, and G. Dondossola, “Application of a cyber security assessment framework to smart grid architectures,” in *International Council on Large Electric Systems (Cigré) SC D2 Colloquium*, 2013.

[14] J. Sanchez, R. Caire, and N. Hadjsaid, “ICT and power distribution modeling using complex networks,” in *IEEE Powertech Conference*, 2013.

[15] J. Sanchez, R. Caire, and N. Hadjsaid, “Application of hermitian adjacency matrices for coupled infrastructures interdependencies analysis,” in *4th IEEE PES Innovative Smart Grid Technologies Europe*, 2013.

[16] X. Li, H. Poor, and A. Scaglione, “Blind topology identification for power systems,” in *Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2013.

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

[18] M. Parandehgheibi and E. Modiano, “Robustness of interdependent networks: The case of communication networks and the power grid,” in *IEEE GlobeCom*, 2013.

[19] M. Beccuti, S. Chiaradonna, F. Giandomenico, S. Donatelli, G. Dondossola, and G. Franceschinis, “Quantification of dependencies between electrical and information infrastructures,” *International Journal of Critical Infrastructure Protection*, vol. 5, no. 1, pp. 14–27, 2012.

[20] R. Bloomfield, N. Chozos, P. Popov, V. Stankovic, D. Wright, and R. Howell-Morris, “Preliminary interdependency analysis (PIA): Method and tool support.” Tech. Rep. D/501/12102/2, November 2010.

[21] H. Qi, X. Wang, L. M. Tolbert, F. Li, F. Peng, P. Ning, and M. Amin, “A resilient real-time system design for a secure and reconfigurable power grid,” *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 770–781, 2011.

[22] Z. Anwar, M. Montanari, A. Gutierrez, and R. H. Campbell, “Budget constrained optimal security hardening of control networks for critical cyber-infrastructures,” *International Journal of Critical Infrastructure Protection*, vol. 2, no. 12, pp. 13–25, 2009.

[23] S. Sridhar, A. Hahn, and M. Govindarasu, “Cyber-physical system security for the electric power grid,” *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, 2012.

[24] S. Amin, G. Schwartz, and A. Hussain, “In quest of benchmarking security risks to cyber-physical systems,” *IEEE Network*, vol. 27, no. 1, pp. 19–24, 2013.

[25] J. B. Rosen, “Existence and uniqueness of equilibrium points for concave n-person games,” *Econometrica*, vol. 33, no. 3, pp. 520–534, July 1965.