Infrastructure Resilience Using Cyber-Physical Game-Theoretic Approach

Nageswara S. V. Rao*, Steve W. Poole*, Chris Y. T. Ma†, Fei He‡, Jun Zhuang‡, David K. Y. Yau§
*Oak Ridge National Laboratory
†Advanced Digital Sciences Center
‡State University of New York at Buffalo
§Purdue University

***Abstract*—We consider a class of infrastructures supported by cyber and physical components, which are subject to disruptions. We study reinforcement strategies for cyber and physical components to achieve resilience, specified by the probability of infrastructure survival, against disruptions using a game-theoretic formulation. The game utility function is a sum of the infrastructure survival probability term and a cost term. We account for cyber-physical interactions at two different levels: (i) the conditional survival probability of cyber sub-infrastructure is specified by a linear function of the marginal probability, and (ii) the survival probabilities of components are determined by the numbers of cyber and physical component attacks as well as reinforcements. At Nash Equilibrium, we identify 12 performance regions based on cyber-physical correlations and component costs, where each is determined by a lower survival probability of either cyber or physical sub-infrastructure. We also derive sensitivity functions that highlight the dependence of infrastructure survival probability on cost parameters and component probabilities as well as cyber-physical correlations, under statistical independence conditions. We apply this approach to models of the energy grid derived at different levels of abstraction.**

I. Introduction

The operation of infrastructures such as smart grids, requires the continued functioning of cyber components such as Supervisory Control And Data Acquisition (SCADA) systems, and also physical components such as power or fiber routes [10]. Even infrastructures used for exclusively cyber services, such as network connectivity and cloud computing, rely on physical components such as fiber routes and HVAC systems, in addition to cyber components such as servers, switches and routers [14]. The components may be disabled and/or disconnected by cyber and physical attacks, which will degrade the infrastructure performance. To counter such disruptions, infrastructure providers are required to adopt strategies that ensure required levels of operation and availability of both cyber and physical components, specified by the survival probability of the infrastructure, by taking into account the attacker strategies and incidental failures.

In this paper, we consider a class of infrastructures consisting of discrete cyber and physical components, which must be *operational* as individual units and also be *available* such as being connected to the network. These components are subject to direct cyber and physical disruptions, and in addition, there are *cyber-physical interactions* that make them unavailable when others are disrupted. For example, a physical attack on a fiber connection to a SCADA site will render it unavailable over the network even though it is operational. The cyber components form the *cyber sub-infrastructure*, and the physical components form the *physical sub-infrastructure*, which may be operated by different domain experts. For example, SCADA systems may be maintained by operations staff, whereas the physical power routes may be maintained by engineering staff. A disruption of either sub-infrastructure will lead to that of the entire infrastructure due to cyber-physical correlations. We model such dependency using the conditional failure probability of one sub-infrastructure given the failure of other as a linear function of the marginal probability of the former. These dependencies are derived from the underlying structure information of the infrastructure.

We consider that the infrastructure consists of a large number of components, so that its performance is adequately characterized by the number of components that are operational and available. This characterization is intended for infrastructures such as smart grid with hundreds to thousands of smart meters, wherein the sheer number of components makes it much too complex to account for the variability among components. The attacker launches a certain number of cyber or physical attacks but not both, but the provider needs to reinforce both cyber and physical components. We focus on reinforcing a certain number of cyber and physical components to defend against the degradations of both kinds. A component can be reinforced so that it cannot be disabled by a direct attack, but it can fail due to incidental causes such as device fatigue, or can be rendered unavailable due to attacks on other components.

We consider a class of infrastructures characterized by the following considerations:

(a) knowledge about physical and cyber component locations is available to the attacker, primarily from public sources;
(b) costs incurred by the provider and attacker are private information and not available to the other;
(c) strategies used by the provider in choosing which components to reinforce, and by the attacker in choosing which components to attack are not revealed to the other; and
(d) information about the success or failure of the attacks is known to both.

This discrete model is simpler than those used in critical infrastructures such as power distribution, transportation and agriculture [5], that model the dynamics of the underlying phenomena, for example, using partial differential equations to model traffic dynamics. We study methods to ensure certain levels of infrastructure survival probability in presence of

cyber and physical degradations within the framework of game theory [7], [11], [12]. The characterizations that address system reliability and robustness using a game-theoretic formulation have been considered recently in several applications [4], for example, smart grids [9], [3], [6], [15], cloud computing infrastructures [13], and power systems [8], [18]. Also, our formulation is more reactive and sensitive to dynamic disruptions compared to long-term strategies used in Markov game models [1], [9].

The results of this paper are generalizations of works in [13] in two ways: (a) in terms of analytical results, our linear model introduces an additive term in the conditional sub-infrastructure failure probability, which increases the number of performance zones from 4 to 12, and leads to more complex cyber-physical interaction terms in the infrastructure survival probability; and (b) in terms of applications, the smart grid models are enhanced in this paper to include additional component types including power generators and smart sensors for dynamic line controls.

We formulate a game between the provider and attacker, wherein their utility functions are in the form of sum of two terms: (a) infrastructure survival probability term, and (b) cost term. The infrastructure survival probability accounts for cyber-physical aspects in two ways: (i) the conditional survival probabilities of cyber and physical sub-infrastructures are specified by linear functions of marginal probabilities derived at the structure-level, and (ii) component survival probabilities are derived based on the number of cyber or physical attacks, the number of cyber and physical components reinforced, and incidental failure probabilities.

Nash Equilibrium (NE) of this game represents the attack and reinforcement actions that optimize the utility of attacker and provider based on their individual information, from which neither has a motivation to unilaterally deviate [7]. We derive NE conditions in terms of cost terms and the component survival probabilities, which are expressed in terms of number of cyber and physical attacks and reinforcements and incidental component failure rates. We identify 12 performance regions based on cyber-physical correlations and component costs, where each is determined by a lower survival probability of either cyber or physical sub-infrastructure. We also estimate the partial derivatives that indicate sensitivities of sub-infrastructure survival probabilities with respect to cost parameters and conditional success and failure probabilities of components, under statistical independence conditions.

We apply this approach to models of energy grids at different levels of abstraction. We first consider a simple power grid with two types of components, namely, SCADA systems and power lines, We then consider different types of cyber components, namely SCADA systems and power meters. Then, we consider a smart grid model consisting of generators and sensors that measure and regulate power flows on the lines. In these cases, we derive estimates of component survival probabilities and sensitivity functions at NE.

In Section II, we present our discrete component model for the infrastructure and derive survival probabilities at structure- and component-levels, and describe simple power grid models in Section II-C. We present our game-theoretic formulation in Section III, and derive NE conditions and sensitivity estimates, and apply these results to more detailed smart grid models in Section III-D.

II. Discrete System Models

The infrastructure consists of a cyber sub-infrastructure of N_C components, and a physical sub-infrastructure of N_P physical components. Each cyber and physical component must be *operational and available* to contribute to the infrastructure operation. A cyber attack may render a physical component unavailable even if it is physically operational, for example, an attack on a SCADA system might disable power flow on a line. And, a physical attack on a component might render cyber components unavailable, for example, fiber cuts to SCADA site would make it unavailable even though it is up and running.

A. Cyber-Physical Structural Interactions

The probability that the infrastructure is operational is denoted by P_{CP}. At the structure-level, the probabilities that the cyber and physical sub-infrastructures are operational are denoted by P_C and P_P, respectively, and $P_{\bar{C}} = 1 - P_C$ and $P_{\bar{P}} = 1 - P_P$. For the infrastructure to be operational *both* cyber and physical sub-infrastructures must necessarily be operational, and their availabilities are determined by the component-level cyber-physical interactions. Then, we have

$$P_{CP} = 1 - [P_{\bar{C}} + P_{\bar{P}} - P_{\bar{C}\bar{P}}] = P_C + P_P - 1 + P_{\bar{C}\bar{P}}. \quad (2.1)$$

To capture the relative importance of cyber and physical parts, the joint probability $P_{\bar{C}\bar{P}} = P_{\bar{C}|\bar{P}} P_{\bar{P}}$ is derived in terms of *multiplicative* and *additive* coefficients, denoted by a_C and b_C respectively, such that $P_{\bar{C}|\bar{P}} = a_C P_{\bar{C}} + b_C$. Here, a_C represents a proportional change in P_C due to the physical sub-infrastructure failure, whereas b_C represents an independent factor; in particular, the certainty of failure of the former due to latter can be presented by $a_C = 0$ and $b_C = 1$ (in [13] only a_C is used). For example, in a power grid with 5 generators per site, disabling the transmission link would disconnect all generators at the site, which can be reflected by choosing $a_C = 5$ and $b_C = 0.001$. If $a_C > 1$ and $b_C > 0$, the cyber failures are *positively correlated* to physical failures, that is, they occur with higher probability following physical failures, since $P_{\bar{C}|\bar{P}} > P_{\bar{C}}$. If $a_C < 1$ and $b_C < 0$ means that cyber failures are *negatively correlated* to physical failures, since $P_{\bar{C}|\bar{P}} < P_{\bar{C}}$.

Condition 2.1: The probability that infrastructure is operational depends on cyber and physical sub-infrastructures such that $P_{CP} = P_C + P_P - 1 + [a_C(1 - P_C) + b_C](1 - P_P)$, where a_C and b_C are multiplicative and additive coefficients. □

B. Component Survival Probabilities

Let p_R be the probability that a component is reinforced, such that $p_{CR} = p_{C|R} p_R$ where $p_{C|R}$ is the conditional probability that a reinforced component will survive direct and indirect attacks. Similarly, $p_N = 1 - p_R$ is the probability that a component is not reinforced, and $p_{CN} = p_{C|N} p_N$ where $p_{C|N}$ is the probability that a non-reinforced component will survive direct and indirect attacks. We now consider that there are different types of cyber and physical components such that x_c^a, $a \in \mathcal{A}_C$, corresponds to cyber components of type a, and x_p^b, $b \in \mathcal{A}_P$, corresponds to physical components of

type b. Then, we have $x_c = \sum_{a\in\mathcal{A}_C} x_C^a$ and $x_p = \sum_{b\in\mathcal{A}_P} x_p^b$. Now we consider that the conditional survival probabilities are statistically independent as follows.

Condition 2.2: The component failures are statistically independent such that

$$P_C = \prod_{a\in\mathcal{A}_C} \left(p_{C|R}^a\right)^{x_c^a} p_{C|N}^{N_C - x_c}$$

$$P_P = \prod_{b\in\mathcal{A}_P} \left(p_{P|R}^b\right)^{x_p^b} p_{P|N}^{N_P - x_p}.\square$$

The partial differentials on the left hand side for these terms are estimated using a Lemma from [13]: for $a \in \mathcal{A}_C$, $b \in \mathcal{A}_P$

$$\frac{\partial P_C}{\partial x_c^a} = P_C \ln\left(\frac{p_{C|R}^a}{p_{C|N}}\right) \quad \text{and} \quad \frac{\partial P_P}{\partial x_p^b} = P_P \ln\left(\frac{p_{P|R}^b}{p_{P|N}}\right),$$

where $p_{C|R}^a$ and $p_{P|R}^b$ denote the survival probabilities of reinforced cyber component of type a and reinforced physical component of type b, respectively.

C. Energy Grid Cyber Infrastructure

We first describe a simplified illustrative example of energy grid [17], [2] controlled by a (cyber) network of SCADA systems [16], where each system controls the power flow on 5 lines. A SCADA system may be disabled by cyber means, and such event will disrupt the power flow on all 5 associated lines. Then, we estimate the survival probability of a reinforced power line in presence of y_c cyber attacks, as

$$p_{P|R} = \frac{f_P}{1 + 5[y_c - x_c]_+},$$

where $0 \le f_P \le 1$ is appropriately chosen to reflect the latent failure rate (namely when $y_c = 0$) that corresponds to factors such a device failures, and $[.]_+$ is the non-negative part, that is $[x]_+ = x$ for $x > 0$, and $[x]_+ = 0$ otherwise. A power line can be physically disrupted if not reinforced, and a component is more likely to be unavailable for higher values y_p. Thus, an attack on a SCADA system will have an amplified effect on power lines compared to direct physical attacks such that

$$p_{P|N} = \frac{f_P}{1 + y_p + 5[y_c - x_c]_+}$$

provides an estimate of the probability of survival of a non-reinforced power line.

We now enhance the model with smart meters on the lines that provide demand information to the generation and distribution control systems. The smart meters can be attacked by cyber means so that the demand information can be manipulated, for example, to make it zero. Let $x_c = x_c^S + x_c^M$ such that x_c^S and x_c^M denote the number of reinforced SCADA systems and meters, respectively. Similarly, $y_c = y_c^S + y_c^M$ such that y_c^S and y_c^M denote the number of SCADA systems and meters attacked, respectively. A SCADA system or a meter may be disabled by cyber means, which will disrupt the power flow on the lines so that

$$p_{P|R} = \frac{f_P}{1 + 5[y_c^S - x_c^S]_+ + [y_c^M - x_c^M]_+},$$

for physically-reinforced power lines; notice that cyber attacks on SCADA systems are amplified 5 times compared to attacks on smart meters. Each power line can be directly disrupted by physical means such that it can be brought down if not reinforced, and thus we have

$$p_{P|N} = \frac{f_P}{1 + [y_p - x_p]_+ + 5[y_c^S - x_c^S]_+ + [y_c^M - x_c^M]_+},$$

which reflects the amplified effect of cyber attacks on SCADA systems compared to physical line attacks.

III. Game-Theoretic Formulation

In this section, for simplicity of presentation, we consider single types of cyber and physical components, and extensions to multiple types are straight-forward, where the analysis is carried out separately for each component type. The provider's objective is to keep the infrastructure operational and available, which involves selecting a number of components to reinforce at certain costs. We express the provider utility function as a sum of system probability and cost terms

$$U_D = \left[P_{CP}(x_c, x_p, y_c, y_p)\right] g_D - C_D(x_c, x_p),$$

where g_D represents the reward of keeping the infrastructure available and $C_D(.)$ represents the cost incurred in reinforcing the components. When the component reinforcement costs are uniform, we use $C_D\left(x_c, x_p\right) = c_{CD}x_c + c_{PD}x_p$, where c_{CD} and c_{PD} are reinforcement costs of cyber and physical components, respectively.

Similarly, the attacker's utility function is given by

$$U_A = \left[1 - P_{CP}(x_c, x_p, y_c, y_p)\right] g_A - C_A(y_c, y_p)$$

where g_A represents the reward of disabling the infrastructure and $C_A(.)$ represents the cost of attacking the components. When the attack costs are uniform, we use $C_A\left(y_c, y_p\right) = c_{CA}y_c + c_{PA}y_p$, where c_{CA} and c_{PA} are the attack costs of cyber and physical components, respectively, and only one of y_c and y_p is non-zero.

A. Nash Equilibrium Conditions

We consider that the numbers of cyber and physical components are large enough that the system behavior can be qualitatively described using derivatives with respect to x_a and y_a, $a = c, p$. Then, Nash Equilibrium conditions are derived by equating the corresponding derivatives to zero such that

$$\frac{\partial U_D}{\partial x_a} = \frac{\partial P_{CP}}{\partial x_a} g_D - \frac{\partial C_D}{\partial x_a} = 0$$

for $a = c, p$ for the provider, and

$$\frac{\partial U_A}{\partial y_a} = -\frac{\partial P_{CP}}{\partial y_a} g_A - \frac{\partial C_A}{\partial y_a} = 0$$

for $a = c, p$ for the attacker.

We now consider that the effects of reinforcement and attacks on cyber and physical sub-infrastructures can be separated such that most of the interactions are captured at the component level, more precisely, $\frac{\partial P_P}{\partial z_c} \approx 0$ and $\frac{\partial P_C}{\partial z_p} \approx 0$ for $z = x, y$. Intuitively, these conditions indicate that at the structure-level, only direct impacts are dominant, for example,

cyber reinforcements contribute to improving the cyber sub-infrastructure but not directly to physical sub-infrastructure. Consequently, we have for the defender the following condition.

Condition 3.1: For P_{CP} in Condition 2.1, we have

$$\frac{\partial P_{CP}}{\partial x_c} \approx [1 - a_C + a_C P_P] \frac{\partial P_C}{\partial x_c}$$
$$\frac{\partial P_{CP}}{\partial x_p} \approx [1 - a_C - b_C + a_C P_C] \frac{\partial P_P}{\partial x_p}$$

for the defender. □

B. Performance Regions of Cyber and Physical Sub-Infrastructures

We now compare the survival probabilities of cyber and physical sub-infrastructures, P_C and P_P, respectively, at the Nash Equilibrium. At NE, we have $\frac{\partial P_{CP}}{\partial x_c} = \frac{1}{g_D}\frac{\partial C_D}{\partial x_c}$ and $\frac{\partial P_{CP}}{\partial x_p} = \frac{1}{g_D}\frac{\partial C_D}{\partial x_p}$. By using the formulae in Condition 3.1, we have

$$[1 - a_C + a_C P_P] \frac{\partial P_C}{\partial x_c} = \frac{1}{g_D}\frac{\partial C_D}{\partial x_c}$$
$$[1 - a_C - b_C + a_C P_C] \frac{\partial P_P}{\partial x_p} = \frac{1}{g_D}\frac{\partial C_D}{\partial x_p}.$$

We now substitute expressions for $\frac{\partial P_C}{\partial x_c}$ and $\frac{\partial P_P}{\partial x_p}$ from Section II-B and utilize the component costs on the right hand side to obtain the system of equations:

$$P_C\left[1 - a_C + a_C P_P\right] = \frac{\frac{\partial C_D}{\partial x_c}}{g_D \ln\left(\frac{p_{P|R}}{p_{P|N}}\right)} = d_{CD}\left(x_c, y_c, y_p\right)$$

$$P_P\left[1 - a_C - b_C + a_C P_C\right] = \frac{\frac{\partial C_D}{\partial x_p}}{g_D \ln\left(\frac{p_{C|R}}{p_{C|N}}\right)} = d_{PD}\left(x_p, y_c, y_p\right).$$

Then, we have

$$P_C = P_P\left(1 - \frac{b_C}{1 - a_C}\right) + \frac{d_{CD} - d_{PD}}{1 - a_C},$$

where we represent $d_{PD}\left(x_p, y_c, y_p\right)$ and $d_{CD}\left(x_c, y_c, y_p\right)$ by simply d_{PD} and d_{CD}, respectively. The relationship between P_C and P_P can be described by 12 different regions determined by a_C, b_C, d_{CD} and d_{PD}. We first consider $a_C > 1$ for which we have the following cases:

(a1) $a_C > 1$; $d_{CD} < d_{PD}$; $b_C > 0$:
$$P_C = P_P + \Delta_a \quad \text{for} \quad \Delta_a \geq 0$$

(b1) $a_C > 1$; $d_{CD} > d_{PD}$; $b_C < 0$:
$$P_C = P_P - \Delta_b \quad \text{for} \quad \Delta_b \geq 0$$

(c1) $a_C > 1$; $d_{CD} > d_{PD}$; $b_C > 0$:
(c1-1) $P_P > \frac{d_{CD} - d_{PD}}{b_C}$:
$$P_C = P_P + \Delta_c \quad \text{for} \quad \Delta_c \geq 0$$
(c1-2) $P_P < \frac{d_{CD} - d_{PD}}{b_C}$:
$$P_C = P_P - \Delta_c \quad \text{for} \quad \Delta_c \geq 0$$

(d1) $a_C > 1$; $d_{CD} < d_{PD}$; $b_C < 0$:
(d1-1) $P_P < \frac{d_{CD} - d_{PD}}{b_C}$:
$$P_C = P_P + \Delta_d \quad \text{for} \quad \Delta_d \geq 0$$
(d1-2) $P_P > \frac{d_{CD} - d_{PD}}{b_C}$:
$$P_C = P_P - \Delta_d \quad \text{for} \quad \Delta_d \geq 0$$

Then, for $a_C < 1$, we have the following cases:

(a2) $a_C < 1$; $d_{CD} < d_{PD}$; $b_C > 0$:
$$P_C = P_P - \Delta_a \quad \text{for} \quad \Delta_a \geq 0$$

(b2) $a_C < 1$; $d_{CD} > d_{PD}$; $b_C < 0$:
$$P_C = P_P + \Delta_b \quad \text{for} \quad \Delta_b \geq 0$$

(c2) $a_C < 1$; $d_{CD} > d_{PD}$; $b_C > 0$:
(c2-1) $P_P > \frac{d_{CD} - d_{PD}}{b_C}$:
$$P_C = P_P - \Delta_c \quad \text{for} \quad \Delta_c \geq 0$$
(c2-2) $P_P < \frac{d_{CD} - d_{PD}}{b_C}$:
$$P_C = P_P + \Delta_c \quad \text{for} \quad \Delta_c \geq 0$$

(d2) $a_C < 1$; $d_{CD} < d_{PD}$; $b_C < 0$:
(d2-1) $P_P < \frac{d_{CD} - d_{PD}}{b_C}$:
$$P_C = P_P - \Delta_d \quad \text{for} \quad \Delta_d \geq 0$$
(d2-2) $P_P > \frac{d_{CD} - d_{PD}}{b_C}$:
$$P_C = P_P + \Delta_d \quad \text{for} \quad \Delta_d \geq 0$$

These cases show that both relative component costs and cyber-physical coefficients a_C and b_C can independently determine which sub-infrastructure has a higher probability of survival. The difference in the survival probabilities of cyber and physical parts depends on the difference in component costs, as expected. But, the exact nature depends on the $1-$ and $0-$ crossing points of a_C and b_C, respectively; in particular, the dependence reverses as the cyber and physical parts are switched from being positively correlated to negatively correlated.

C. NE Sensitivity Functions

We now estimate approximations of P_C and P_P under Conditions 2.1, 2.2 and 3.1, to obtain qualitative information about their sensitivities to different parameters from the provider's perspective.

Theorem 3.1: Under Conditions 2.1, 2.2 and 3.1, an estimate of the survival probability of physical sub-infrastructure is

$$\hat{P}_{P;D}\left(x_c, x_p, y_c, y_p\right) = \frac{d_{PD} - d_{CD}}{2(1 - a_C - b_C)} - \frac{(1 - a_C)}{2a_C} \pm \frac{1}{2a_C} \times \sqrt{\left(\frac{a_C(d_{PD} - d_{CD})}{1 - a_C - b_C} - (1 - a_C)\right)^2 + \frac{4a_C d_{PD}(1 - a_C)}{(1 - a_C - b_C)}},$$

for $a_C + b_C \neq 1$, and an estimate of the survival probability of cyber sub-infrastructure is

$$\hat{P}_{C;D}\left(x_c, x_p, y_c, y_p\right) = \frac{d_{CD} - d_{PD}}{2(1 - a_C)} - \frac{(1 - a_C - b_C)}{2a_C} \pm \frac{1}{2a_C} \times \sqrt{\left(\frac{a_C(d_{CD} - d_{PD})}{1 - a_C} - (1 - a_C - b_C)\right)^2 + \frac{4a_C d_{CD}(1 - a_C - b_C)}{(1 - a_C)}},$$

for $a_C \neq 1$.

Proof: At NE, by using $P_C = d_{CD}/[1 - a_C + a_C P_P]$ in

$$[1 - a_C - b_C + a_C P_C]\, P_P = d_{PD}$$

we obtain the quadratic equation

$$\begin{aligned} &a_C(1 - a_C - b_C)P_P^2 \\ &-[(d_{PD} - d_{CD})a_C + (1 - a_C)(1 - a_C - b_C)]\, P_P \\ &-(1 - a_C)d_{PD} = 0. \end{aligned}$$

Solution to this equation provides $\hat{P}_{P;D}\left(x_c, x_p, y_c, y_p\right)$, which in turn yields $\hat{P}_{C;D}\left(x_c, x_p, y_c, y_p\right)$. □

To facilitate a qualitative discussion of $\hat{P}_{P;D}$ and $\hat{P}_{C;D}$, we briefly consider OR Systems [13], where the probability of simultaneous failures of cyber and physical sub-infrastructures is negligible such that $P_{\bar{C}\bar{P}} = P_{\bar{C}} + P_{\bar{P}}$. The estimates for the survival probabilities are:

$$\tilde{P}_{P;D}\left(x_p, y_c, y_p\right) = \frac{c_{PD}}{g_D \ln\left(\frac{p_{P|R}}{p_{P|N}}\right)} = d_{PD}$$

$$\tilde{P}_{C;D}\left(x_c, y_c, y_p\right) = \frac{c_{CD}}{g_D \ln\left(\frac{p_{C|R}}{p_{C|N}}\right)} = d_{CD}.$$

These estimates provide qualitative information about the survival probabilities of cyber and physical sub-infrastructures in terms of component costs and component survival probabilities. But, they involve only component probabilities of the same type, namely $\tilde{P}_{P;D}$ and $\tilde{P}_{C;D}$ depend only on the probabilities of physical and cyber components, respectively, and they do not involve structure-level interactions.

Compared to OR systems, there are significant cyber-physical interactions in the above $\hat{P}_{P;D}\left(x_c, x_p, y_c, y_p\right)$ and $\hat{P}_{C;D}\left(x_c, x_p, y_c, y_p\right)$ in that they both depend on $d_{PD}\left(x_p, y_c, y_p\right)$ and $d_{CD}\left(x_c, y_c, y_p\right)$. In particular, they both are affected by the survival probabilities of cyber and physical components, each of which in turn depends on the number of both cyber and physical component attacks and reinforcements.

The multiplier a_C and additive factor b_C affect these quantities in much more complicated manner than their "linear" roles in Condition 2.1. Since $0 \leq P_{\bar{C}|\bar{P}} \leq 1$, both a_C and $a_C + b_C$ can take values higher and lower than 1. Both $\hat{P}_{P;D}\left(x_c, x_p, y_c, y_p\right)$ and $\hat{P}_{C;D}\left(x_c, x_p, y_c, y_p\right)$ depend on the difference of components costs, as opposed to depending on components of the same type as in the case of OR Systems. Furthermore, the nature of dependence of $\hat{P}_{P;D}$ and $\hat{P}_{C;D}$ reverses as $a_C + b_C$ and a_C cross 1, respectively, reflecting the effects of positive and negative correlations between the cyber and physical parts. For $a_C + b_C < 1$ and $a_C < 1$, $\hat{P}_{P;D}$ and $\hat{P}_{C;D}$, respectively, are directly proportional to physical and cyber component costs, respectively, and this relationship reverses for $a_C + b_C > 1$ and $a_C > 1$, respectively. Similarly, for $a_C + b_C < 1$ and $a_C < 1$, $\hat{P}_{P;D}$ and $\hat{P}_{C;D}$, respectively, depend on components of the corresponding type, namely physical and cyber component survival probabilities, respectively, as follows: (a) higher survival probability of reinforced component leads to lower sub-infrastructure survival probability, and (b) higher survival probability of non-reinforced component leads to higher sub-infrastructure survival probability. And, $\hat{P}_{P;D}$ and $\hat{P}_{C;D}$ depend on components of other type, namely cyber and physical component survival probabilities, respectively, in the opposite way. For $a_C + b_C > 1$ and $a_C > 1$, respectively, the qualitative behavior reverses in the cases above, which illustrates the significant impact of the structure-level cyber-physical correlation on the overall behavior of the infrastructure.

D. Smart Grid Infrastructure

Continuing the smart grid model in Section II-C, we have

$$d_{PD} = \frac{c_{PD}}{g_D \ln\left(1 + \frac{[y_p - x_p]_+}{1 + 5[y_c^S - x_c^S]_+ + [y_c^M - x_c^M]_+}\right)},$$

which decreases in the number of attacks on non-reinforced power lines, and increases in the number of attacks on non-reinforced SCADA systems and non-reinforced meters but the former effect is amplified 5 times. We also have

$$d_{CD}^B = \frac{c_{PD}}{g_D \ln\left(\frac{1 + y_c^B}{1 + [y_c^B - x_c^B]_+}\right)}$$

for $B = S, M$, which decreases in the total number of cyber attacks but increases in the number of attacks on non-reinforced cyber attacks. The net effect of the numbers of attacks and reinforcements on the survival probabilities of cyber and physical sub-infrastructures is also determined by correlation multiplier a_C and additive coefficient b_C in addition to d_{PD} and d_{CD}^B, for $B = S, M$, as described in Section III-C.

We now consider more details of the smart grid example [17], [2]. In this system, transmission lines are equipped with sensors for dynamic line rating, which dynamically adjust the transmission flow of a transmission line according to weather conditions and line temperature, and all of the users are connected using smart meters. We also include generators into consideration. Hence, there are two types of physical components, namely lines and generators, and $x_p = x_p^L + x_p^G$ such that x_p^L and x_p^G denote the number of reinforced lines and generators, respectively; and there are three types of cyber components, namely dynamic rate sensors, smart meters, and the SCADA systems, and $x_c = x_c^D + x_c^M + x_c^S$ such that x_c^D, x_c^M, and x_c^S denote the number of reinforced dynamic rate sensors, smart meters, and the SCADA systems, respectively. Physical attacks on lines or cyber attacks on dynamic rate sensors will also affect generators and smart meters, while cyber attacks on SCADA systems will affect physical and cyber components. The physical component survival probabilities are estimated separately for the lines and the generators, while the cyber component survival probabilities are estimated separately for the dynamic rate sensors, smart meters, and the SCADA systems. The survival probabilities of the transmission lines with and without reinforcement are denoted by $p_{P|R}^L$ and $p_{P|N}^L$, respectively. The power flow on the transmission lines may be disrupted by cyber attacks on the SCADA system or the dynamic rate sensors, so that

$$p_{P|R}^L = \frac{f_P}{1 + 5[y_c^S - x_c^S]_+ + [y_c^D - x_c^D]_+},$$

for physically-reinforced transmission lines; notice that cyber attacks on SCADA systems are amplified 5 times compared to attacks on the dynamic rate sensors. Each transmission line can also be directly disrupted by physical means such that it can be bought down if not reinforced, and thus, we have

$$p_{P|N}^L = \frac{f_P}{1 + [y_p^L - x_p^L]_+ + 5[y_c^S - x_c^S]_+ + [y_c^D - x_c^D]_+}.$$

Combining the two formulae, we have

$$d^L_{PD} = \frac{c_{PD}}{g_D \ln\left(1 + \frac{[y^L_p - x^L_p]_+}{1+5[y^S_c - x^S_c]_+ + [y^D_c - x^D_c]_+}\right)},$$

which decreases in the number of physical attacks on the non-reinforced transmission lines, and increases in the number of attacks on the non-reinforced SCADA systems and the non-reinforced dynamic line rating sensors but the former effect is amplified 5 times. Similarly, the survival probabilities of the generators are given by

$$p^G_{P|R} = \frac{f_P}{1 + [y^L_p - x^L_p]_+ + 5[y^S_c - x^S_c]_+ + [y^D_c - x^D_c]_+},$$

$$p^G_{P|N} = \frac{f_P}{1 + [y^G_p - x^G_p]_+ + [y^L_p - x^L_p]_+ + 5[y^S_c - x^S_c]_+ + [y^D_c - x^D_c]_+},$$

and we have $d^G_{PD} = \frac{c_{PD}}{g_D \ln\left(1+\frac{[y^G_p - x^G_p]_+}{1+[y^L_p - x^L_p]_+ + 5[y^S_c - x^S_c]_+ + [y^D_c - x^D_c]_+}\right)}$.
The survival probabilities of the dynamic rate sensors and the smart meters are given by

$$p^B_{C|R} = \frac{f_C}{1 + [y^B_c - x^B_c]_+ + 5[y^S_c - x^S_c]_+},$$

$$p^B_{C|N} = \frac{f_C}{1 + y^B_c + 5[y^S_c - x^S_c]_+},$$

for $B = D, M$, and we have

$$d^B_{PD} = \frac{c_{PD}}{g_D \ln\left(\frac{1+y^B_c+5[y^S_c - x^S_c]_+}{1+[y^B_c - x^B_c]_+ + 5[y^S_c - x^S_c]_+}\right)},$$

for $B = D, M$. The survival probabilities of the SCADA systems are

$$p^S_{C|R} = \frac{f_C}{1 + [y^S_c - x^S_c]_+} \text{ and } p^S_{C|N} = \frac{f_C}{1 + y^S_c},$$

and we have $d^S_{CD} = \frac{c_{CD}}{g_D \ln\left(\frac{1+y^S_c}{1+[y^S_c - x^S_c]_+}\right)}$. The qualitative effects of the numbers of cyber and physical attacks and reinforcements as well as the performance regions in this case are quite similar to the simpler case in Section III-C, except they are assessed separately for each component type.

IV. Conclusions

We considered infrastructures composed of a large number of discrete components that can be disrupted by cyber and physical attacks, and can be reinforced against the attacks. We captured the cyber-physical interactions using: (a) conditional survival probabilities of cyber and physical sub-infrastructures at the structure-level, and (b) survival probabilities of components determined by the number of cyber and physical component attacks and reinforcements. We studied provider's strategies for ensuring certain probability of infrastructure survival against incidental component failures and attacks on cyber and physical components, using a game-theoretic formulation. We derived Nash Equilibrium conditions in terms of cost terms and component survival probabilities, and estimated the sensitivity functions that indicate the dependence of sub-infrastructure survival probabilities on cost parameters, component probabilities and correlation coefficients. This analysis shows 12 performance regions, each determined by a lower survival probability of either cyber or physical sub-infrastructure (but not both). We applied this approach to models of smart energy grid at different levels of abstraction.

This formulation may be extended in several ways in future studies. It would be interesting to study sequential game formulations of this problem, and cases where different levels of knowledge, including mis-information, are available to each party. More detailed models of smart energy grid infrastructures, cloud computing infrastructures and high-performance computing complexes would be of future interest.

Acknowledgments

This work is funded by the Mathematics of Complex, Distributed, Interconnected Systems Program, Office of Advanced Computing Research, U.S. Department of Energy, and by Extreme Scale Systems Center, sponsored by U. S. Department of Defense, and performed at Oak Ridge National Laboratory managed by UT-Battelle, LLC for U.S. Department of Energy under Contract No. DE-AC05-00OR22725.

References

[1] T. Alpcan and T. Basar. *Network Security: A Decision and Game Theoretic Approach*. Cambridge University Press, 2011.

[2] M. Amin. Toward self-healing energy infrastructure systems. *IEEE Computer Applications in Power*, 2001.

[3] S. Backhaus, R. Bent, J. W. Bono, R. Lee, B. Tracey, D. Wolpert, D. Xie, and Y. Yildiz. Cyber-physical security: A game theory model of humans interacting over control systems. *IEEE Transactions on Smart Grids*, 2013. under review.

[4] V. M. Bier and M. N. Azaiez, editors. *Game Theoretic Risk Analysis of Security Threats*. Springer, 2009.

[5] G. Brown, M. Carlyle, J. Salmern, and K. Wood. Defending critical infrastructure. *Interfaces*, 36(6):532–544, 2006.

[6] Z. M. Fadlullah, Y. Nozaki, A. Takeuchi, and N.Kato. A survey of game theoretic approaches in smart grid. In *International Conference on Wireless Communications and Signal Processing (WCSP 2011)*, 2011.

[7] D. Fudenberg and J. Tirole. *Game Theory*. MIT Press, 2003.

[8] C. Y. T. Ma, D. K. Y. Yau, and N. S. V. Rao. Markov game analysis for attack-defense of power networks under possible misinformation. *IEEE Transactions on Power Systems*, 28(2):1676–1886, 2013.

[9] C. Y. T. Ma, D. K. Y. Yau, and N. S. V. Rao. Scalable solutions of Markov games for smart-grid infrastructure protection. *IEEE Transactions on Smart Grid*, 4(1):47–55, 2013.

[10] Y. Mo, J. Kim T. H, D. Dikinson, H. Lee, A. Perrig, and B. Sinopoli. Cyber-physical security of smart grid infrastructure. *Proceedings of the IEEE*, 100(1), 2012.

[11] R. B. Myerson. *Game Theory: Analysis of Conflict*. Harvard University Press, 1991.

[12] N. Nisan, T. Roughgarden, E. Tardos, and V. V. Vazirani, editors. *Algorithmic Game Theory*. Cambridge University Press, 2007.

[13] N. S. V. Rao, S. W. Poole, C. Y. T. Ma, F. He, J. Zhuang, and Yau D. K. Y. Cyber and physical information fusion for infrastructure protection: A game-theoretic approach. In *International Conference on Information Fusion*, 2013.

[14] N. S. V. Rao, S. W. Poole, C. Y. T. Ma, F. He, J. Zhuang, and Yau D. K. Y. Game-theoretic approach to cyber-physical aspects of UltraScience Net. In *Workshop on Design, Modeling and Evaluation of Cyber Physical Systems*. 2013.

[15] W. Saad, Z. Han, H. V. Poor, and T. Basar. Game theoretic methods for the smart grid. *IEEE Signal Processing*, 2012.

[16] P. Sauer, K. Tomsovic, and V. Vittal. Chapter 15: Dynamic security assessment. In *Power System Stability and Control*, volume 5, pages 421–430. CRC Electric Power Engineering Handbook, 2007.

[17] G. N. Sorebo and M. C. Echols. *Smart Grid Security*. CRC Press, 2012.

[18] F. Wu, Z. Hu, and K. Chen. Game theory based power system security analysis. In *International Conference on Control, Automation and Systems Engineering*, 2011.