18th International Conference on Information Fusion
Washington, DC - July 6-9, 2015

# On Resilience of Cyber-Physical Infrastructures Using Discrete Product-Form Games

Nageswara S. V. Rao*, Chris Y. T. Ma†, Urvashi Shah‡, Jun Zhuang‡, Fei He§, David K. Y. Yau†¶
*Oak Ridge National Laboratory
†Advanced Digital Sciences Center
‡State University of New York at Buffalo
§Texas A&M University
¶Singapore University of Technology and Design

***Abstract*—In critical infrastructures consisting of discrete cyber and physical components, the correlations between them may be exploited to launch strategic component attacks that may degrade the entire system. We capture such correlations between cyber and physical sub-infrastructures using the conditional probabilities, and between cyber and physical components using first-order differential conditions. By using a resilience measure specified by the infrastructure's survival probability, we formulate a discrete game between the provider and attacker. Their disutility functions are products of the survival (or failure) probability and cost terms expressed in terms of the number of components attacked and reinforced by the attacker and provider, respectively. The Nash Equilibrium conditions of the game provide the sensitivity functions that clearly show the dependence of the infrastructure resilience on cost terms, correlation function and sub-infrastructure survival probabilities. These results for product-form disutility functions complement the sum-form results from previous works, and more closely represent the provider's objectives for a certain class of infrastructures. We apply these results to simple models of network testbed infrastructures and cyber infrastructures of smart energy grids.**

## I. Introduction

The increasing proliferation of cyber technologies in critical infrastructures leads to complex cyber-physical correlations that can be exploited by attackers to launch novel attacks. These attacks, while utilizing only physical or cyber components, can disrupt the other components and possibly bring down the entire infrastructure. For example, a physical fiber cut in a network testbed may disconnect all switches and routers at a site, and a cyber attack on a supervisory control and data acquisition (SCADA) system may disrupt all power lines under its control. More generally, the operation of infrastructures such as network testbeds and smart grids, requires the uninterrupted operation of cyber components such as routers, servers, and SCADA systems as well as physical components such as optical fibers, electrical bus cables, and heating, ventilation and air conditioning (HVAC) systems.

One of the key measures of resilience of such infrastructures is the probability that the infrastructure remains operational under various attack conditions, and thus it constitutes a primary goal of the provider. The cyber and physical components of the infrastructure may be reinforced by the provider by balancing the costs against attack profiles that reflect the underlying cyber-physical correlations. These considerations lead to game theoretic formulations wherein the attacker and provider utility functions include the survival probability and cost terms [1]. The effectiveness of such approaches is determined by the Nash Equilibrium (NE) of the underlying game, which in turn specifies the reinforcement and attack strategies for the provider and attacker, respectively.

We consider infrastructures composed of discrete cyber and physical components, whose performance critically depends on both components being *operational* and *available*. The cyber and physical components could be disrupted in various ways: they may be disabled by direct attacks, for example, a cyber attack on a server, or by indirect attacks, such as a physical attack on a fiber conduit to a regional network. Furthermore, in several infrastructures, the cyber and physical sub-infrastructures depend on different technologies, and are operated by separate domain teams. For example, in network infrastructures, switches and routers are maintained by networking staff, fiber routes are maintained by engineering staff, and HVAC systems are maintained by physical plant staff. Hence, it may not be feasible for the provider to dynamically reallocate the defenses between different domains, and hence it is important to deploy them using optimal defense resource allocations.

Consider an infrastructure characterized by the number of discrete components, wherein an attacker launches $y_c$ cyber or $y_p$ physical component attacks (not both), and the provider reinforces $x_c$ cyber and $x_p$ physical components. In essence this formulation captures critical infrastructures with a large number of components such as a network testbed with thousands of servers, routers, and switches, or a power grid with hundreds of SCADA systems. The provider's main objective is to ensure that the infrastructure is operational by strategically reinforcing a certain number of cyber and physical components. A reinforced component survives a direct attack, but can become (indirectly) unavailable as a result of an attack on another component, and we attempt to explicitly model such dependencies. Let $P_C$ and $P_P$ denote the marginal survival probabilities of cyber and physical sub-infrastructures, respectively. The *failure correlation function* $f(P_C, P_P)$ is the failure probability of cyber sub-infrastructure given the other's failure; it is typically estimated using the structural properties of the infrastructure. Furthermore, we consider that $P_C$ and $P_P$ satisfy first-order differential conditions [1] involving $x_c$, $x_p$, $y_c$, and $y_p$, which are derived based on component-level considerations.

We formulate a game between the provider and attacker with the following considerations:

TABLE I. NOTATIONS

| Notations | Meaning | Function of |
|---|---|---|
| $x_c$ | Number of cyber components reinforced by provider | NA |
| $x_p$ | Number of physical components reinforced by provider | NA |
| $y_c$ | Number of cyber components attacked | NA |
| $y_p$ | Number of physical components attacked | NA |
| $P_{CP}$ | Probability of survival of the cyber-physical infrastructure | $(x_c, x_p, y_c, y_p)$ |
| $P_C$ | Probability of survival of cyber sub-infrastructure | $(x_c, x_p, y_c, y_p)$ |
| $P_P$ | Probability of survival of physical sub-infrastructure | $(x_c, x_p, y_c, y_p)$ |
| $Q_{CP} = 1 - P_{CP}$ | Probability of failure of cyber-physical infrastructure | $(x_c, x_p, y_c, y_p)$ |
| $C_D$ | Total cost incurred by the provider | $(x_c, x_p)$ |
| $C_A$ | Total cost incurred by the attacker | $(x_c, x_p)$ |
| $C_{CD}$ | Cost of reinforcing a cyber component by the provider | $(x_c)$ |
| $C_{PD}$ | Cost of reinforcing a physical component by the provider | $(x_p)$ |
| $C_0$ | Cost of initial system deployment by the provider | NA |
| $U_{D\times}$ | Disutility function of the provider in product form | $(x_c, x_p, y_c, y_p)$ |
| $U_{A\times}$ | Disutility function of the attacker in product form | $(x_c, x_p, y_c, y_p)$ |

(a) sufficient knowledge about the cyber-physical correlation in the infrastructure is available to the attacker to launch component attacks that impact others;
(b) costs of attacks and reinforcements (including initial deployment) of components, denoted by $C_A(y_c, y_p)$, and $C_D(x_c, x_p)$, respectively, are 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) attack incidents and their results on components will be known to the provider and attacker.

Let $P_{CP}$ denote the survival probability of the infrastructure. The *provider disutility function* is

$$U_{D\times} = [1 - P_{CP}(x_c, x_p, y_c, y_p)]\, C_D(x_c, x_p),$$

which is the expected reinforcement and deployment cost under the condition that the infrastructure failed, and thus is to be minimized. Intuitively, it represents the average "wasted cost" since the infrastructure failed (with probability $1 - P_{CP}$) despite the component reinforcements. Notice that $C_D$ includes the initial system deployment cost, $C_0 > 0$, to preclude the degenerate solution at $x_c = 0$ and $x_p = 0$, wherein the provider achieves zero wasted cost by not reinforcing any component. Similarly, the *attacker disutility function* is

$$U_{A\times} = [P_{CP}(x_c, x_p, y_c, y_p)]\, C_A(y_c, y_p),$$

which is the expected attack cost under the condition that the infrastructure survives, and is to be minimized. For the attacker, it represents the "wasted cost" since the infrastructure survived (with probability $P_{CP}$) despite the attacks.

The organization of this paper is as follows. We compare the above formulation with existing ones in Section II. In Section III, we briefly present a discrete component model for cyber-physical infrastructures, and discuss the failure correlation function and the differential conditions on sub-infrastructure survival probabilities. In Section IV, we present the game-theoretic formulation, and derive NE conditions and sensitivity estimates. We discuss the special cases of linear failure correlation function, OR systems, and statistical independence conditions in Section V. We discuss NE conditions for simplified models of network testbeds and smart energy grids in Section VI.

## II. COMPARISON WITH OTHER WORKS

Game-theoretic methods have been extensively applied in the risk analysis of critical infrastructures by explicitly accounting for the interactions between providers and attackers [2]. In particular, infrastructures such as power distribution, transportation, and agriculture have been analyzed using complex dymamic models of the underlying physical systems [3], for example, using partial diffential equations. Both the formulation and solution space of such works is quite extensive, including, multiple-period games [4] that address multiple timescales of system dynamics; incomplete information games [5], [6], [7] that account for partial knowledge about the system dynamics and attack models; and multiple-target games [8], [9] that account for possibly competing objectives. A comprehensive review of the defense and attack models in various game-throretic model has been presented in [10]. While many of these formulations utilize detailed dynamics models, they do not explicitly account for the underlying cyber-physical correlations. In another direction, game-theoretic methods have been utilized to fuse information from muliple sources in defense applications [11]. Due to the wide spectrum of these game-theoretic and information fusion methods, we limit our discussion to the ones that are directly related to our discrete cyber-physical component formulation.

Discrete infrastructure models have been developed for a certain class of cyber infrastructures [1], which are simpler than ones used in above critical infrastructures, for example, partial differential equations used to model traffic dynamics [3]. Also, game-theoretic methods have been developed specifically to address the system reliability and robustness

for several applications [2], including, smart grids [12], cloud computing infrastructures [13], and power systems [14]. For cyber-physical infrastructures, the Stackelberg formulations (where the provider chooses options based on instantaneous information) have been developed [1], [13]; typically, this formulation leads to more reactive strategies that are sensitive to dynamic disruptions compared to long-term strategies used in Markov game models [15].

The overall formulation of this paper is closely related to that in [1] in terms of correlation characterization, but its product-form disutility function is different from the other's sum-form. For the provider, the sum-form utility function, which is to be maximized, is given by

$$U_{D+} = [P_{CP}(x_c, x_p, y_c, y_p)]\, g_D - C_D(x_c, x_p),$$

where $g_D$ represents the reward of keeping the infrastructure operational. Thus, it represents the cases where explicit revenue terms can be identified. Similarly, the attacker incurs a cost proportional to the attack efforts to bring down the network. For the attacker, the sum-form utility function, which again is to be maximized, is given by the utility function

$$U_{A+} = [1 - P_S(x_c, x_p, y_c, y_p)]\, g_A - C_A(y_c, y_p),$$

where $g_A$ represents the reward for disrupting the infrastructure.

In contrast, the product-form represents the cases where facility provider's main objective is to keep the infrastructure operational at the lowest cost. For example, there is no "explicit" revenue from running the system as is the case for many research infrastructures and government services. Consequently, the NE conditions are different in these two cases. Interestingly, they will turn out (in Section IV-D) to be surprisingly similar at a fundamental level: the sensitivity conditions show that the role of $1/g_D$ in the sum-form is effectively replaced by $1/C_D^2$ in the product-form. However, the cyber-physical differential at NE differs in its dependence on the unit costs of components: in the product-form it depends on the positive ratio of the unit costs, whereas in the sum-form it depends on their negative ratio.

## III. Correlations in Discrete Cyber-Physical Network Infrastructures

A *Cyber-Physical Network Infrastructure* (CPNI) consists of cyber and physical sub-infrastructures with $N_C$ cyber components and $N_P$ physical components, respectively. Both components must be *operational* and *available* as part of the infrastructure, but they can be functionally disabled or operationally disconnected from the infrastructure through attacks. The cyber-physical interactions are captured by the survival probabilities of cyber and physical sub-infrastructures using the failure correlation function $f(P_C, P_P)$ that captures the correlations at the sub-infrastructure level, and differential conditions on $P_C$ and $P_P$ that capture the component-level correlations [1].

*Condition 3.1:* The probability that the CPNI is operational is given by

$$P_{CP} = P_C + P_P - 1 + f\,(P_C, P_P)\,(1 - P_P),$$

where $f\,(P_C, P_P) = P_{\bar{C}|\bar{P}}$ is the sub-infrastructure *failure correlation* function [1]. □

The failure correlation function captures the dependence of cyber sub-infrastructure failure on that of physical sub-infrastructure. For example, in a network testbed (e.g., [16]) with $N_S$ switches at each site, disabling the fiber would disconnect all of them from the infrastructure, which can be captured by choosing $f\,(P_C, P_P) = N_S(1 - P_P)$; this shows that the physical failure rate is amplified by $N_S$ times by making all switches unavailable. The following two special cases lead to a simplified yet illustrative analysis of $P_{CP}$.

(a) *Linear Form:* The special case of a linear form

$$f(P_C, P_P) = a_C(1 - P_C) + b_C$$

has been studied in [1] that expresses the failure correlation in terms of *multiplicative* and *additive* coefficients, denoted by $a_C$ and $b_C$ respectively. Here, $a_C$ represents a proportional change in $P_{\bar{C}}$ due to the physical sub-infrastructure failure, whereas $b_C$ represents an independent factor. If $a_C > 1$ and $b_C \geq 0$, or $a_C \geq 1$ and $b_C > 0$, cyber failures are positively correlated to physical failures, that is, $P_{\bar{C}|\bar{P}} > P_{\bar{C}}$; and if $a_C < 1$ and $b_C \leq 0$, or $a_C \leq 1$ and $b_C < 0$, cyber failures are negatively correlated to physical gfailures, that is, $P_{\bar{C}|\bar{P}} < P_{\bar{C}}$. If the cyber and physical sub-infrastructures are *statistical independent*, then we have the special case of $a_C = 0$ and $b_C = 1$, that is, $f\,(P_C, P_P) = 1 - P_C$.

(b) *OR Systems:* From a cyber-physical correlations perspective, the OR systems defined in [1] are amenable to much simpler analysis in that the cyber and physical sub-infrastructures can be independently studied. For OR systems, the probability of failure of cyber or physical sub-infrastructure is $P_{\bar{C}\cup\bar{P}} = P_{\bar{C}} + P_{\bar{P}}$ or equivalently $P_{\bar{C}\cap\bar{P}} = 0$. Thus, we have $P_{CP} = P_C + P_P - 1$ and $f\,(P_C, P_P) = 0$, and their implications to the formulation of this paper will be discussed in Section V-B.

The sub-infrastructure survival probabilities satisfy the following differential conditions [1]:

*Condition 3.2:* The survival probabilities of cyber and physical sub-infrastructures are given by

$$\frac{\partial P_C}{\partial x_c} = h_C\,(P_C, x_c, x_p, y_c, y_p) = \Lambda_C(x_c, x_p, y_c, y_p) P_C$$

$$\frac{\partial P_P}{\partial x_p} = h_P\,(P_P, x_c, x_p, y_c, y_p) = \Lambda_P(x_c, x_p, y_c, y_p) P_P$$

respectively. □

We now consider that the effects of reinforcements and attacks can be "separated" at the sub-infrastructure level by utilizing the following conditions $\frac{\partial P_P}{\partial z_c} \approx 0$ and $\frac{\partial P_C}{\partial z_p} \approx 0$ for $z = x, y$. Intuitively, these conditions indicate that only the direct cyber (physical) impacts are dominant at the level of cyber (physical) sub-infrastructure. For example, cyber reinforcements contribute to improving the cyber sub-infrastructure but not directly to physical sub-infrastructure. However, both $P_C$ and $P_P$ capture the correlations between cyber and physical components through $\Lambda_C(x_c, x_p, y_c, y_p)$ and $\Lambda_P(x_c, x_p, y_c, y_p)$, respectively. We capture the sub-infrastructure correlations for the provider using the following condition from [1].

*Condition 3.3:* For $P_{CP}$ in Condition 3.1, we have

$$\frac{\partial P_{CP}}{\partial x_c} \approx \left[1 + (1 - P_P)\frac{\partial f}{\partial P_C}\right]\frac{\partial P_C}{\partial x_c} \quad (1)$$

$$\frac{\partial P_{CP}}{\partial x_p} \approx \left[1 - f(P_C, P_P) + (1 - P_P)\frac{\partial f}{\partial P_P}\right]\frac{\partial P_P}{\partial x_p} \quad (2)$$

for the provider. □

## IV. Game-Theoretic Analysis

In this section, we first present a simple example that illustrates the non-monotonic dependence of the survival probaibilty of cyber-physical infrastructure $P_{CP}$ on some system paramters. We then present general results that characteize the Nash equilibrium and the sensitivity functions of suvival probabilties of cyber and physical sub-infrastructures.

### A. Dependence of Infrastructure Survival Probability

We consider a simple case of a network testbed with $N_S = 4$ switches at each site with the number of sites ranging from 2 to 100. Each site is connected to the wide-area network via a single fiber connection, and thus its failure rate is amplified such that $f(P_C, P_P) = N_S(1 - P_P)$. We consider two scenarios: (a) all components are reinforced, and (b) only half of the randomly chosen components are reinforced. We assume that the component failures are statistically independent, and the probability that a reinforced component survives is 0.95, and that a non-reinforced component survives is 0.5.

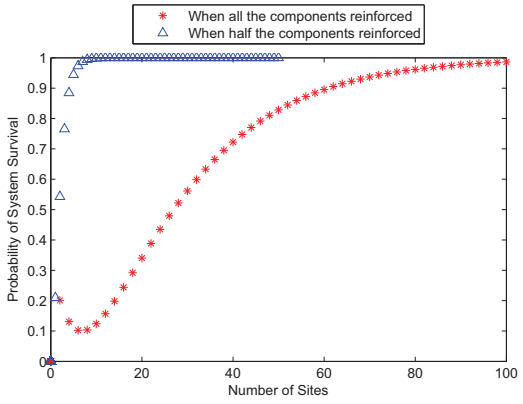


Fig. 1. Probability of survival of cyber-physical infrastructure $P_{CP}$ as a function of the number of sites.

As the number of sites is increased, $P_{CP}$ monotonically increases for case (a) as shown in Figure 1. However, for case (b), $P_{CP}$ initially decreases and then exponentially increases, and such non-monotonic dependence in general requires a closer examination of the reinforcement strategies at the Nash equilibrium. Nevertheless, there are several other monotonic relationships between the parameters of infrastructure. As shown in Figure 2, the probability of survival of the physical sub-infrastructure $P_C$ is generally higher when all components are reinforced, and it decreases exponentially with increase in number of fiber links. Together, these results indicate that even under very simple conditions (namely, statistical independence of component failures and simple network connectivity), the underlying dependences are non-monotonic, and hence simple reinforcement strategies are not sufficient to address the cyber-phyisical dependencies of these infrastructures.

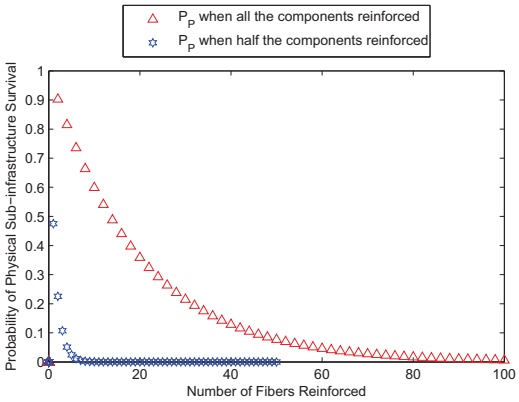


Fig. 2. Probability of physical sub-infrastructure survival $P_P$ as a function of number of fiber links reinforced.

### B. Nash Equilibrium Conditions

At Nash Equilibrium (NE) of this game, the attack and reinforcement actions, given by $(y_c, y_p)$ and $(x_c, x_p)$ respectively, represent the attempts of attacker and provider to minimize the respective expected costs based on their individual information (from which neither has a motivation to unilaterally deviate.

Partial derivatives for the provider's disutility function are calculated as follows

$$\frac{\partial U_{D\times}}{\partial x_c} = -\frac{\partial P_{CP}}{\partial x_c}C_D(x_c, x_p) + C_{CD}[1 - P_{CP}]$$

$$\frac{\partial U_{D\times}}{\partial x_p} = -\frac{\partial P_{CP}}{\partial x_p}C_D(x_c, x_p) + C_{PD}[1 - P_{CP}]$$

Equating these to zero, we get Nash Equilibrium conditions

$$\frac{\partial P_S}{\partial x_c} = \frac{C_{CD}[1 - P_{CP}]}{C_D(x_c, x_p)} \quad \text{and} \quad \frac{\partial P_S}{\partial x_p} = \frac{C_{PD}[1 - P_{CP}]}{C_D(x_c, x_p)}$$

The NE conditions highlight the dependence of $P_{CP}$ on cost terms, correlation function, and sub-infrastructure survival probabilities and their partial derivatives. In particular, the provider strategy is derived by combining both cyber and physical parameters and their correlations. We can also estimate the sensitivity functions of $P_{CP}$ using the partial derivatives of parameters $C_A(\cdot)$, $C_D(\cdot)$, $P_C$, $P_P$, and $f(P_C, P_P)$ that indicate their relative importance.

We apply this method to study simplified models of network testbed infrastructures such as Global Environment for Network Innovations (GENI) [16] and UltraScienceNet [17] that provide users with network configurations or slices consisting of connections, switches, routers and/or host systems. We also consider simplified models of cyber infrastructures for smart energy grids that consist of smart meters, SCADA systems, power lines and generators [18]. In these examples,

we derive the NE conditions and sensitivity functions under certain statistical independence conditions on component failures.

### C. System Survival Dependence on Players' Cost

The disutility function of the provider can be written as

$$U_{D\times} = [Q_{CP}(x_c, x_p, y_c, y_p)]\, C_D(x_c, x_p),$$

for $Q_{CP} = 1 - P_{CP}$, wherein the initial infrastructure cost is represented by $C_0 = C_D(0,0) > 0$. Even with no reinforcements, this cost will be wasted if the infrastructure does not survive, and the consideration of this cost precludes the degenerate solution at $x_c = 0$ and $x_p = 0$. At Nash equilibrium, we have

$$\frac{\partial U_{D\times}}{\partial x_c} = \frac{\partial Q_{CP}}{\partial x_c} C_D(x_c, x_p) + \frac{\partial C_D(x_c, x_p)}{\partial x_c} Q_{CP} = 0,$$

which leads to the partial differential condition

$$\frac{\partial Q_{CP}}{\partial x_c} = \frac{\frac{-\partial C_D(x_c, x_p)}{\partial x_c}}{C_D(x_c, x_p)} Q_{CP}.$$

A sensitivity-based estimate $\hat{P}_{CP}$ for the system survival probability $P_{CP}$ can be obtained using an approximation to this condition. Consider the approximate solution $\hat{Q}_{CP} = q_d e^{-p_d[\ln C_D(x_c, x_p)]} = 1 - \hat{P}_{CP}$, which is parameterized by the scalars $q_d$ and $p_d$. As $p_d \mapsto 1$, this differential relationship of $\hat{Q}_{CP}$ approaches that of $Q_{CP}$, that is, the solution satisfies

$$\frac{\partial \hat{Q}_{CP}}{\partial x_c} = -q_d \frac{\frac{\partial C_D(x_c, x_p)}{\partial x_c}}{C_D(x_c, x_p)} \hat{Q}_{CP},$$

which in turn approaches the NE condition as $q_d \mapsto 1$. This approximation

$$\hat{P}_{CP;D} = 1 - q_d e^{-p_d[\ln C_D(x_c, x_p)]} \tag{3}$$

qualitatively shows the dependence of system survival on the provider's cost with the underlying cyber-physical correlations absorbed by the normalization constant $q_d$.

The disutility function of the attacker is given by

$$U_{A\times} = [P_{CP}(x_c, x_p, y_c, y_p)]\, C_A(x_c, x_p).$$

To avoid the degenerate solution, we have assumed that at least one component is eventually attacked such that $y_c + y_p \geq 1$. By using the above approach we obtain the following similar approximation for the attacker,

$$\hat{P}_{CP;A} = q_a e^{-p_a[\ln C_A(y_c, y_p)]},$$

which shows the qualitative effect of the attacker's cost on the system survival with the underlying cyber-physical correlations absorbed by the normalization constant $q_a$.

### D. NE Sensitivity Functions

We now derive sensitivity-based approximations for $P_C$ and $P_P$ at NE using the partial derivatives of the cost and failure correlation function to obtain qualitative information about their sensitivities to different parameters from the provider's perspective.

*Theorem 4.1:* Under Conditions 3.1, 3.2 and 3.3, an estimate of the survival probability of physical sub-infrastructure, for $\frac{\partial f}{\partial P_P} \neq 0$, is

$$\hat{P}_{P;D}(x_c, x_p, y_c, y_p) = \frac{1 - f(P_C, P_P) + \frac{\partial f}{\partial P_P}}{2\frac{\partial f}{\partial P_P}} \pm \sqrt{\left(\frac{1 - f(P_C, P_P) + \frac{\partial f}{\partial P_P}}{2\frac{\partial f}{\partial P_P}}\right)^2 - \frac{\frac{\partial C_D}{\partial x_p}(1 - \hat{P}_{CP;D})}{C_D \Lambda_P(x_c, x_p, y_c, y_p)\frac{\partial f}{\partial P_P}}},$$

and, for $\frac{\partial f}{\partial P_P} = 0$, is

$$\hat{P}_{P;D}(x_c, x_p, y_c, y_p) = \frac{\frac{\partial C_D}{\partial x_p}(1 - \hat{P}_{CP;D})}{C_D \Lambda_P(x_c, x_p, y_c, y_p)\,[1 - f(P_C, P_P)]}.$$

An estimate of the survival probability of cyber sub-infrastructure is

$$\hat{P}_{C;D}(x_c, x_p, y_c, y_p) = \frac{\frac{\partial C_D}{\partial x_c}(1 - \hat{P}_{CP;D})}{C_D \Lambda_C(x_c, x_p, y_c, y_p)\left[1 + (1 - \hat{P}_{P;D})\frac{\partial f}{\partial P_C}\right]}.$$

*P*roof: At NE, we have

$$\frac{\partial P_{CP}}{\partial x_c} = \frac{C_{CD}[1 - P_{CP}]}{C_D(x_c, x_p)} \quad \text{and} \quad \frac{\partial P_{CP}}{\partial x_p} = \frac{C_{PD}[1 - P_{CP}]}{C_D(x_c, x_p)}.$$

By using the formulae in Condition 3.3, we have

$$\left[1 + (1 - P_P)\frac{\partial f}{\partial P_C}\right]\frac{\partial P_C}{\partial x_c} = \frac{C_{CD}[1 - P_{CP}]}{C_D(x_c, x_p)},$$

$$\left[1 - f(P_C, P_P) + (1 - P_P)\frac{\partial f}{\partial P_P}\right]\frac{\partial P_P}{\partial x_p} = \frac{C_{PD}[1 - P_{CP}]}{C_D(x_c, x_p)}.$$

We now substitute expressions for $\frac{\partial P_C}{\partial x_c}$ and $\frac{\partial P_P}{\partial x_p}$ based on Condition 3.2, and obtain the system of equations:

$$\left[1 + (1 - P_P)\frac{\partial f}{\partial P_C}\right] P_C = \frac{C_{CD}[1 - P_{CP}]}{\Lambda_C C_D(x_c, x_p)}, \tag{4}$$

$$\left[1 - f(P_C, P_P) + (1 - P_P)\frac{\partial f}{\partial P_P}\right] P_P = \frac{C_{PD}[1 - P_{CP}]}{\Lambda_C C_D(x_c, x_p)}. \tag{5}$$

The expression for $\hat{P}_{P;D}$ is obtained by solving for $P_P$ using the quadratic Eq. 5, and the expression for $\hat{P}_{C;D}$ follows from Eq. 4. □

The expression $\hat{P}_{P;D}(x_c, x_p, y_c, y_p)$ shows the dependence on both $f(\cdot)$ and its partial derivatives with respect to $P_P$, and the partial derivative of $C_D$ with respect to $x_p$; it also depends on the cost factor $C_D$, $\Lambda_P$ and $P_{CP}$ as expected. Its dependence on $P_C$ is implicit through the failure correlation function

$f(P_C, P_P)$. The qualitative behavior of $\hat{P}_{C;D}(x_c, x_p, y_c, y_p)$ is quite similar with respect to $C_D$ but its dependence on $P_P$ is also through $f$. And, they both are affected by $\Lambda_C(\cdot)$ and $\Lambda_P(\cdot)$, and each of them in turn depends on the number of both cyber and physical component attacks and reinforcements. Thus, the estimates $\hat{P}_{P;D}$ and $\hat{P}_{C;D}$ reflect the correlations between the sub-infrastructures explicitly through $f$, as well as those captured by the survival probabilities of individual sub-infrastructures by themselves.

### E. Comparison with Sum-Form Utility Functions

We have seen from Section IV-A that by using the limiting approximation with $p_d = 1$ and $q_d = 1$ in Eq. 3, we obtain the approximation

$$\hat{P}_{CP;D} = 1 - \frac{1}{C_D(x_c, x_p)}$$

By substituting this term in $\hat{P}_{P;D}(x_c, x_p, y_c, y_p)$ of Theorem 4.1, we obtain the following:

$$\hat{P}_{P;D}(x_c, x_p, y_c, y_p) = \frac{1 - f(P_C, P_P) + \frac{\partial f}{\partial P_P}}{2\frac{\partial f}{\partial P_P}} \pm \sqrt{\left(\frac{1 - f(P_C, P_P) + \frac{\partial f}{\partial P_P}}{2\frac{\partial f}{\partial P_P}}\right)^2 - \frac{\frac{\partial C_D}{\partial x_p}}{C_D^2 \Lambda_P(x_c, x_p, y_c, y_p)\frac{\partial f}{\partial P_P}}}$$

We now compare it with the corresponding expression of the sum-form given by

$$\hat{P}_{P;D}(x_c, x_p, y_c, y_p) = \frac{1 - f(P_C, P_P) + \frac{\partial f}{\partial P_P}}{2\frac{\partial f}{\partial P_P}} \pm \sqrt{\left(\frac{1 - f(P_C, P_P) + \frac{\partial f}{\partial P_P}}{2\frac{\partial f}{\partial P_P}}\right)^2 - \frac{\frac{\partial C_D}{\partial x_p}}{g_D \Lambda_P(x_c, x_p, y_c, y_p)\frac{\partial f}{\partial P_P}}}$$

These two expressions for $\hat{P}_{P;D}(x_c, x_p, y_c, y_p)$ are strikingly similar in that $g_D$ of the sum-form is simply replaced by $C_D^2$ in the product form. Such similarity is not apparent from the formulation since the sum-form appears to account for two separate terms namely cost and resilience, whereas the product-form more closely combines the two. However, despite the similarity, these two quantities have opposite effects on $\hat{P}_{CP;D}$, namely, increase in $g_D$ is qualitatively similar to decrease in $C_D^2$, since the utility functions are maximized in the sum-form compared to the minimization in the product-form. Also, due to the presence of power 2, $\hat{P}_{CP;D}$ is more sensitive to $C_D$ compared to $g_D$.

## V. Special Cases of Infrastructure Models

In this section, we present special cases wherein simpler forms of results of Theorem 4.1 can be derived.

### A. Linear From

For the special case of the linear form of the failure correlation function (Section III), we first derive a simplified version of the Condition 3.3. Then, by substituting the expression for the correlation coefficients in Eq. 1 we obtain

$$\frac{\partial P_{CP}}{\partial x_c} = \left[1 + (1 - P_P)\frac{\partial\left(a_C(1 - P_C) + b_C\right)}{\partial P_C}\right]\frac{\partial P_C}{\partial x_c} = [1 - a_C + a_C P_P]\frac{\partial P_C}{\partial x_c}$$

Since we have considered the effects of reinforcements and attacks can be "separated" at the sub-infrastructure level, the probability of survival of cyber infrastructure does not depend on the probability of survival of physical infrastructure and vice versa. Also, by substituting the expression for correlation coefficients in Eq. 2 we obtain

$$\frac{\partial P_{CP}}{\partial x_p} = \left[1 - a_C(1 - P_C) - b_C + (1 - P_P)\frac{\partial\left(a_C(1 - P_C) + b_C\right)}{\partial P_P}\right]\frac{\partial P_P}{\partial x_p} = [1 - a_C - b_C + a_C P_C]\frac{\partial P_P}{\partial x_p}$$

Thus, we have much simpler dependences of $P_{CP}$ on $P_C$ and $P_P$ compared to the general forms in Theorem 4.1.

### B. OR Systems

In the special case of OR systems [1], the infrastructure will fail if either of the physical or cyber sub-infrastructures fails under the condition $P_{\bar{C}\cup\bar{P}} = P_{\bar{C}} + P_{\bar{P}}$, which requires that $P_{\bar{C}\cap\bar{P}} = 0$, that is, the simultaneous failure of cyber and physical sub-infrastructures is not possible. While practical interpretations or verifications of these conditions are not apparent, these systems are of interest from an analytical perspective. In particular, we have a much simpler form of Condition 3.3 for these systems given by $\frac{\partial P_{CP}}{\partial x_c} \approx \frac{\partial P_C}{\partial x_c}$ and $\frac{\partial P_{CP}}{\partial x_p} \approx \frac{\partial P_P}{\partial x_p}$ [1]. At NE, using the limiting approximation for $\hat{P}_{CP;D}$ we have

$$\frac{\partial P_C}{\partial x_c} = \frac{1}{C_D^2}\frac{\partial C_D}{\partial x_c} \quad \text{and} \quad \frac{\partial P_P}{\partial x_p} = \frac{1}{C_D^2}\frac{\partial C_D}{\partial x_p}.$$

Using Condition 3.2, we obtain the following estimates for the survival probabilities of cyber and physical sub-infrastructures:

$$\tilde{P}_{C;D}(x_c, x_p, y_c, y_p) = \frac{\frac{\partial C_D}{\partial x_c}}{C_D^2 \Lambda_C(x_c, x_p, y_c, y_p)},$$

$$\tilde{P}_{P;D}(x_c, x_p, y_c, y_p) = \frac{\frac{\partial C_D}{\partial x_p}}{C_D^2 \Lambda_P(x_c, x_p, y_c, y_p)}.$$

These estimates do not involve $f(P_C, P_P)$ – the cyber-physical interactions are captured by $\Lambda_C(\cdot)$ and $\Lambda_P(\cdot)$ at the component level instead. Both survival probability estimates $\tilde{P}_{C;D}$ and $\tilde{P}_{P;D}$ are proportional to the corresponding cost derivatives and inversely proportional to the square of the cost term $C_D$. However, such seemingly counter-intuitive trend applies only to the set of Nash equilibria and not to the overall system behavior.

Compared to OR Systems, there are significant cyber-physical interactions in the general case at the sub-infrastructure level in both $\hat{P}_{P;D}(x_c, x_p, y_c, y_p)$ and $\hat{P}_{C;D}(x_c, x_p, y_c, y_p)$ as seen in Theorem 4.1.

### C. Statistical Independence

Condition 3.2 is satisfied under the special case of *Statistical Independence* as defined in Section III. Let $p_{C|R}$, $p_{C|N}$ and $p_{P|R}$, $p_{P|N}$ denote the conditional probability of survival of a cyber or physical component, respectively where *'R'* denotes *reinforcement* and *'N'* denotes *no reinforcement*.

Under the assumption of statistical independence of component failures, the probability that the cyber and physical components survive the attacks are given by [1]:

$$P_C = p_{C|R}^{x_c} p_{C|N}^{N_C - x_c} \quad \text{and} \quad P_P = p_{P|R}^{x_p} p_{P|N}^{N_P - x_p}$$

respectively.

The partial differentials are estimated using a Lemma from [1] that leads to:

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

which provide simpler expressions for the terms used in formulae in Theorem 4.1.

## VI. Applications

We apply the analytical results to simplified models of network testbed infrastructures and smart grid cyber infrastructures in this section. In both cases, we attempt to capture the provider's perspective of primarily keeping the system operational. In these examples, we derive the NE conditions and sensitivity functions under certain statistical independence conditions on component failures.

### A. Testbeds for Network Experiments

Network infrastructure testbeds have been established by the research community to support the development and testing of new network configurations, technologies and applications. For example, they enable the researches to setup novel network configurations and connections, and test the performance of new devices, protocols and network applications. In cases such as GENI [16] and USN [17], these testbeds provide connections that span the country and beyond; they may connect the local networks consisting of switches, routers and/or host systems at individual sites over the long-haul backbone networks. In particular, certain GENI slices provide entire infrastructure of backbone and local area networks, and certain USN configurations provide networking devices and end hosts. There testbed infrastructures are different from the traditional network infrastructures in some ways: the devices tend to be more dynamically configured, and each site may house multiple types of devices such as routers, switches and hosts. Also, because of their research-oriented objectives, they do not have revenue measures that are common in commercial network infrastructures. As such, the provider may aim at keeping the system operational against possible attacks with least cost. In terms of game-theoretic models, these infrastructure models are somewhat more complex than simplified cloud computing infrastructures in [1] in that these sites consist of more networking devices.

A simplified model of a network testbed consists of multiple sites, each with $N_N$ network devices and $N_S$ servers. Assess to the site networks may be blocked by cyber attacks on gateway routers, and communication fiber routes to the sites may be physically cut. Similar effect may also result from multiple cyber attacks on the network devices that effectively disconnect the site network. Reinforcements to these components may be in the form of replicated standby servers, switches and routers, and redundant, physically separate fiber routes. Since a physical fiber cut disconnects all network devices and servers at the site from the network, to a first-order approximation, we consider $f(P_C, P_P) = (N_N + N_S)(1 - P_P)$, which indicates the multiplicative effect of physical attacks. We now consider that the attacker and provider choose the components according to the uniform distribution. Then, there are $[y_p - x_p]_+$ non-reinforced fiber connections, where $[\cdot]_+$ represent the non-negative part, that is, $[x]_+ = x$ for $x > 0$, and $[x]_+ = 0$ otherwise. Then, the probability that a cyber-reinforced component survives the fiber attacks is estimated by

$$p_{C|R} = \frac{g_C}{1 + (N_N + N_S)[y_p - x_p]_+},$$

where $0 \leq g_C \leq 1$ is appropriately chosen. This estimate reflects that a random attack on a cyber component is more likely to be effective for higher values of $[y_p - x_p]_+$. If a cyber component is not reinforced, it can be brought down by a direct cyber attack, or indirectly through a fiber attack. Thus, we estimate the survival probability of a cyber component as

$$p_{C|N} = \frac{g_C}{1 + y_c + (N_N + N_S)[y_p - x_p]_+},$$

which reflects the additional lowering of survival probability, in inverse proportion to the level of cyber attack $y_c$. Using these formulae, we have [1]

$$\Lambda_C(x_p, y_c, y_p) = \ln\left(1 + \frac{y_c}{1 + (N_N + N_S)[y_p - x_p]_+}\right),$$

which does not depend on $x_c$.

### B. Smart Grid Infrastructures

In some power grids, the cyber infrastructure of the transmission and distribution network is operated by an independent entity who is not directly involved in the retail market. Indeed, it may be hard for such providers to accurately estimate the total revenue from an operating network. On the other hand, the deployment cost of the network is usually huge, so that there is a strong incentive for the provider to protect the system against attacks. There have been recent efforts to develop smart grid technologies [18] that utilize cyber technologies to achieve high levels of automation and adaptation of power systems. We consider simplified models of such smart energy grids that consist of smart meters, SCADA system, power lines and generators.

We consider a simplified model of a power grid infrastructure controlled by a SCADA system using information fed with a network of sensors monitoring the condition of each major transmission and distribution line, related by communication

sinks located at strategic locations for the best connectivity of the sensors. We assume that each communication sink relates information from sensors of $N_L$ lines. Each sink may be disabled by a direct cyber attack, which will disrupt the information flow to the SCADA system, and hence, the power flow on all its $N_L$ lines. By using the reasoning analogous to Example 1, we have $P_{\bar{P}|\bar{C}} = N_L(1 - P_C)$; then by using the Bayes formula $P_{\bar{C}|\bar{P}} = P_{\bar{P}|\bar{C}}P_{\bar{C}}/P_{\bar{P}}$, we have $f(P_C, P_P) = \frac{N_L(1-P_C)^2}{(1-P_P)}$. We then estimate the survival probability of reinforced smart grid communication system that can be disconnected by $y_c$ cyber attacks, as

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

where $0 \leq g_P \leq 1$ is appropriately chosen. Meanwhile, each power line can be directly disrupted by physical means such that it can be brought down if not reinforced, and the physical sub-infrastructure is more likely to be unavailable if there are more physical attacks, namely, higher $y_p$. Thus, an attack on a communication sink will have an amplified effect on power lines compared to direct physical attacks such that

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

provides an estimate of the probability of survival of a non-reinforced power line. Using the above formulae, we have

$$\Lambda_P(x_c, y_c, y_p) = \ln\left(1 + \frac{y_p}{1 + N_L[y_c - x_c]_+}\right),$$

which does not depend on $x_p$.

## VII. Conclusion

We considered simple models of critical infrastructures consisting of discrete cyber and physical components. The cyber-physical correlations in these systems may be exploited to launch strategic component attacks that may degrade the entire infrastructure. We modeled such correlations using conditional probabilities and first-order differential conditions. By using an infrastructure resilience measure specified by its survival probability, we have formulated a discrete game between the provider and attacker. Their disutility functions are the products of survival (or failure) probability and cost terms expressed in terms of the number of components attacked and reinforced by the attacker and provider, respectively. The Nash Equilibrium conditions of the game provide the sensitivity functions that clearly show the dependence of infrastructure resilience on the cost terms, correlation function and sub-infrastructure survival probabilities.

The product-form results presented here complement sum-form results from previous works, and more closely represent the considerations of a class of infrastructure operators. The model is flexible and applicable to numerous practical cases. The application of the framework is neither limited to the examples described in this paper, nor to the computer security modeling. The basic framework can be utilized to solve problems in which the game theoretical models can be formulated for modeling strategic interactions between rational players. This includes a wide range of problems from political and economic analysis to perspective and normative analysis.

Applications of the analytical results presented here to more detailed models of network and smart grid infrastructures would be of future interest. Also, it would be of future interest to extend this formulation to account for different types of cyber and physical components, which may represent different benefits and costs to the provider and attacker. In these cases, the utility functions must capture the specific effects of inidividual components such as identifying critical components (for example, core connections of a network testbed) as well as critical correlations between certain components.

## References


[1] N. S. V. Rao, C. Y. T. Ma, F. He, J. Zhuang, and D. K. Y. Yau, "Cyber-physical correlations for infrastructure resilience: A game-theoretic approach," in *Information Fusion (FUSION), 2014 17th International Conference on*. IEEE, 2014, pp. 1–8.

[2] V. M. Bier and M. N. Azaiez, *Game theoretic risk analysis of security threats*. Springer Science & Business Media, 2008, vol. 128.

[3] G. Brown, M. Carlyle, J. Salmerón, and K. Wood, "Defending critical infrastructure," *Interfaces*, vol. 36, no. 6, pp. 530–544, 2006.

[4] V. R. R. Jose and J. Zhuang, "Technology adoption, accumulation, and competition in multi-period attacker-defender games," *Military Operations Research*, vol. 18, no. 2, pp. 33–47, 2013.

[5] F. He and J. Zhuang, "Modelling 'contracts' between a terrorist group and a government in a sequential game," *Journal of the Operational Research Society*, vol. 63, no. 6, pp. 790–809, 2012.

[6] E. Jenelius, J. Westin, and A. J. Holmgren, "Critical infrastructure protection under imperfect attacker perception," *International Journal of Critical Infrastructure Protection*, vol. 3, no. 1, pp. 16–26, 2010.

[7] M. Nikoofal and J. Zhuang, "Robust allocation of a defensive budget considering an attacker's private information," *Risk Analysis*, vol. 32, no. 5, pp. 930–943, 2012.

[8] X. Shan and J. Zhuang, "Hybrid defensive resource allocations in the face of partially strategic attackers in a sequential defender-attacker game," *European Journal of Operational Research*, vol. 228, no. 1, pp. 262–272, 2013.

[9] ——, "Cost of equity in homeland security resource allocations in the face of partially strategic attacker," *Risk Analysis*, vol. 33, no. 6, pp. 1083–1099, 2013.

[10] K. Hausken and G. Levitin, "Review of systems defense and attack models," *International Journal of Performability Engineering*, vol. 8, no. 4, pp. 355–366, 2012.

[11] J. Brynielsson and S. Arnborg, "An information fusion game component," *Journal of Adnavces in Information Fusion*, vol. 1, no. 2, pp. 108–121, 2006.

[12] C. Y. T. Ma, D. K. Y. Yau, and N. S. V. Rao, "Scalable solutions of markov games for smart-grid infrastructure protection," *Smart Grid, IEEE Transactions on*, vol. 4, no. 1, pp. 47–55, 2013.

[13] N. S. Rao, S. W. Poole, C. Y. Ma, F. He, J. Zhuang, and D. K. Yau, "Defense of cyber infrastructures against cyber-physical attacks using game-theoretic models," *Risk Analysis*, 2015, in press.

[14] C. Y. T. Ma, D. K. Y. Yau, X. Lou, and N. S. V. Rao, "Markov game analysis for attack-defense of power networks under possible misinformation," *Power Systems, IEEE Transactions on*, vol. 28, no. 2, pp. 1676–1686, 2013.

[15] T. Alpcan and T. Başar, *Network security: A decision and game-theoretic approach*. Cambridge University Press, 2010.

[16] "GENI: Global environment for network innivations," http://www.geni.net.

[17] N. S. V. Rao, W. R. Wing, S. M. Carter, and Q. Wu, "Ultrascience net: Network testbed for large-scale science applications," *IEEE Communications Magazine*, vol. 43, no. 11, pp. s12–s17, 2005.

[18] T. Flick and J. Morehouse, *Securing the Smart Grid*. Elsevier Pub., 2011.