Game-Theoretic Strategies for Asymmetric Networked Systems

Nageswara S. V. Rao*, Chris Y. T. Ma†, Kjell Hausken‡, Fei He§, David K. Y. Yau¶, Jun Zhuang‖
*Oak Ridge National Laboratory, Oak Ridge, TN, USA
†Hang Seng Management College, Hong Kong
‡University of Stavanger, Norway
§Texas A&M University, Kingsville, TX, USA
¶Singapore University of Technology and Design, Singapore
‖State University of New York at Buffalo, Buffalo, NY, USA

***Abstract*—We consider an infrastructure consisting of a network of systems each composed of discrete components that can be reinforced at a certain cost to guard against attacks. The network provides the vital connectivity between systems, and hence plays a critical, asymmetric role in the infrastructure operations. We characterize the system-level correlations using the aggregate failure correlation function that specifies the infrastructure failure probability given the failure of an individual system or network. The survival probabilities of systems and network satisfy first-order differential conditions that capture the component-level correlations. We formulate the problem of ensuring the infrastructure survival as a game between an attacker and a provider, using the sum-form and product-form utility functions, each composed of a survival probability term and a cost term. We derive Nash Equilibrium conditions which provide expressions for individual system survival probabilities, and also the expected capacity specified by the total number of operational components. These expressions differ only in a single term for the sum-form and product-form utilities, despite their significant differences. We apply these results to simplified models of distributed cloud computing infrastructures.**

Keywords and phrases: networked systems, aggregated correlation function, game theory, Nash Equilibrium

I. Introduction

A number of infrastructures, such as cloud computing complex and smart energy grid, consist of networked systems. Here, the network plays an important, asymmetric role by providing the vital connectivity between the systems: its complete failure makes them all unreachable, thereby rendering the entire infrastructure unavailable. We represent such an infrastructure by its constituent systems, S_i, $i = 1, 2, \ldots, N$, and the network represented as the system S_{N+1}. Each system consists of several discrete cyber and physical components that must be *operational* as individual units and also be *available*, namely, being connected to the network. The individual components of S_i may be individually disabled, and S_i as a system may be disconnected from the network by component cyber and physical attacks. The components can be reinforced at a certain cost to withstand such attacks. Non-reinforced components can be disabled by attacks at a cost to the attacker. Additionally, effects of component attacks may propagate to other components within S_i, and furthermore, they may propagate to components of other systems S_j, $j \neq i$. For example, consider a cloud computing infrastructure with multiple sites, each housing several servers. A server may be brought down by a cyber attack, but a single physical attack on the network fiber to the site may disconnect all servers at the site. In general, correlations between components and systems lead to the propagation of disruptions within and beyond the individual systems, respectively. In an extreme case, effects of attacks may propagate across the network to all other systems, and possibly degrade the entire infrastructure.

The infrastructure provider is tasked with strategically reinforcing the components against attacks by taking into account various system-level and component-level correlations. Let n_i denote the number of components of S_i, and y_i and x_i be the number of components of S_i attacked and reinforced, respectively. A reinforced component survives a direct attack but may be disrupted indirectly, for example, an operational server being disconnected due to an attack on network fiber. Let P_i be the survival probability of S_i, and P_I be the survival probability of entire infrastructure. Also, let S_{-i} denote the infrastructure without S_i, and P_{-i} be its survival probability. The *aggregate failure correlation function* C_i is the failure probability of "rest" of the infrastructure S_{-i} (namely, without S_i) given the failure of S_i. Intuitively, it indicates the relative importance of S_i by capturing the disruption propagation from S_i to entire infrastructure. We consider an important special case of an asymmetric network such that: (a) $C_{N+1} = 1$ indicating that the network failure will disrupt the entire infrastructure, and (b) $C_i = 0$, for $i = 1, 2, \ldots, N$ indicating that disruptions of individual systems are uncorrelated.

In addition to system-level correlations, the interdependencies between components of individual systems are captured by simple first-order differential conditions on P_i which generalize the contest success functions and statistical independence conditions of component failures [21]. This two-level characterization helps to conceptualize the basic correlations in infrastructures such as cloud computing and smart grid infrastructures [24]. In addition, it leads to a simplified analysis

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.

by "separating" the system- and component-level aspects, and also provides insights into the needed defense strategies.

We formulate a game between the attacker and provider wherein the costs of attacks and reinforcements of systems, given by $L_A(y_1, \ldots, y_{N+1})$ and $L_D(x_1, \ldots, x_{N+1})$, respectively, are not known to the other. The provider maximizes the *sum-form utility function* given by

$$U_{D+} = [P_I(x_1, \ldots, x_{N+1}, y_1, \ldots, y_{N+1})]\, g_D - C_D(x_1, \ldots, x_{N+1}),$$

where g_D represents the benefit of keeping the infrastructure operational. We also consider the *product-form utility function* given by

$$U_{D\times} = [1 - P_I(x_1, \ldots, x_{N+1}, y_1, \ldots, y_{N+1})] \times C_D(x_1, \ldots, x_{N+1}),$$

which will be minimized by the provider. It represents the "wasted" cost to the provider since it is the expected cost under the condition that the infrastructure has failed. The attacker's utility functions are similarly defined. We are interested in the *expected capacity* of the infrastructure expressed in terms of the expected number of available components, given by

$$N_I = \sum_{i=1}^{N} n_i P_i,$$

which reflects the average size of part of the infrastructure that survives attacks.

In previous work, the sum-form utility function [21] and the product-form utility function [22] have been considered separately for a generic version of this game. They represent two different ways of representing the value of keeping the infrastructure operational: the sum-form represents a weaker coupling of probability and cost terms, whereas the product-form utility function is their product. In general they lead to qualitatively different defense strategies that are derived separately, and the expressions for the survival probabilities appear to be structurally different. In this paper, we show that under the asymmetric correlations, the Nash Equilibrium (NE) of this game [9] leads to expressions for P_i's and N_I with the same structure. We derive NE conditions that show the dependence of P_i on cost terms, and their partial derivatives and aggregate correlation functions. The estimates of P_i for sum-form and product-form utilities have the same expression in Theorem 4.1 except for one term, given by $\xi_i^+ = \frac{1}{g_D}\frac{\partial C_D}{\partial x_i}$ and $\xi_i^\times = (1 - P_I)\frac{\partial \ln C_D}{\partial x_i} = \frac{(1-P_I)}{C_D}\frac{\partial C_D}{\partial x_i}$. To consider the case where the sum-form and the product-form utilities are equivalent, we equate the two terms and obtain the following "equivalent" gain term of the sum-form

$$g_D = C_D/(1 - P_I) = C_D\left[1 + \sum_{i=1}^{\infty} P_I^i\right],$$

which is an increasing function in both P_I and C_D. Or, equivalently we have, $P_I = 1 - C_D/g_D$. This similarity is striking since the sum-form and product-form utilities represent two quite different objectives.

We apply these results to a simplified model of cloud computing infrastructure with multiple server sites connected over a network. We derive expressions for P_i, $i = 1, 2, \ldots, N$, and N_I for both sum-form and product-form utilities. Even under simple uniform independent distributions of component attacks and reinforcements, they reveal useful and also complex underlying relationships.

Our results extend previous results on interconnected systems in [11], [12] and cyber-physical infrastructures in [23], [24] by considering more general systems and correlations. Our results specialize results in [21], [22] by explicitly considering the communications network, and also unify their results which are derived separately for sum-form and product-form utilities.

The organization of this paper is as follows. We briefly describe related work in Section II. In Section III, we describe the infrastructure model along with the aggregate correlation function and differential conditions on system survival probabilities. We present a game-theoretic formulation in Section IV, and derive NE conditions and estimates for system survival probabilities and the expected capacity. We apply the analytical results to a model of cloud computing infrastructure in Section V. We present conclusions in Section VI.

II. Related Work

Critical infrastructures of power grids, cloud computing, and transportation systems provide vital public and private services [8], [15]. They depend on complex communications networks that connect the constituent systems, which by themselves consist of many disparate cyber and physical components [15]. The communications network plays a very critical role in these infrastructures [6], in some ways more so than the constituent systems, and its failure can significantly degrade the entire infrastructure [3], [25]. These infrastructures are under increasing cyber and physical attacks, which the providers are required to counter by applying defense measures and strategies.

By capturing the interactions between providers and attackers of these infrastructures, game-theoretic methods have been extensively applied to develop the needed defense strategies [1], [4], [16], which attempt to ensure continued infrastructure operations in presence of evolving threats [26]. Partial differential equations and discrete components models have been used in several of these infrastructures to model the physical and cyber systems [2] in formulating the underlying games. The game-theoretic formulations and the solutions developed for such infrastructures are quite varied and extensive. They include: multiple-period games that address multiple time-scales of system dynamics [14]; incomplete information games that account for partial knowledge about the system dynamics and attack models [18]; and multiple-target games that account for possibly competing objectives [27].

A comprehensive review of the defense and attack models in various game-theoretic formulations has been presented in [13]. Recent interest in cyber and cyber-physical systems led to the application of game theory to a variety of cyber security scenarios [16], [28], and, in particular, for securing cyber-

physical networks [5] with applications to power grids [6], [10], [17], [19].

The system availability, reliability and robustness aspects can be explicitly integrated into the game formulations [1] for infrastructures such as power grids, cloud computing and transportation systems. In particular, discrete models of cyber-physical infrastructures have been studied in various forms under Stackelberg game formulations [7]. A subclass of these models using the number of cyber and physical components that are attacked and reinforced as the main variables have been studied in [24]. These models characterize infrastructures with a large number of components, and are coarser compared to the models that consider the attacks and reinforcements of individual cyber and physical components. Various forms of correlation functions [21], [22], [24] are used in these works to capture the dependencies between the survival probabilities of constituent systems, such as the cyber and physical sub-infrastructures.

Complex interacting collections of systems have been studied using game-theoretic formulations in [12], and their two-level correlations have been studied using the sum-form utility functions in [21] and the product-form disutility functions in [22]. The sum-form utility represents a *gain-centric priority*, wherein an independent gain term weighted by P_I represents the gain to be maximized by the provider. The product-form disutility, on the other hand, represents a *cost-centric priority*, wherein the expected cost is to be minimized. The sum-form utility function [21] and the product-form utility function [22] are considered separately for a generic version of this game wherein all systems play a similar role, unlike the asymmetric role of the network considered here. In terms of analysis, these two formulations have a certain degree of commonality but there are also differences; in particular, estimates of P_I can be obtained somewhat directly for the product-form as shown in [22]. These two utility functions also lead to qualitatively different defense strategies, and in particular P_I appears explicitly in the sensitivity estimates of system survival probabilities in product-form but not in sum-form. In this paper, we show that under the asymmetric correlations, these results can be unified so that they have the same form and differ only in ξ_i^+ and $\xi_i^\times$. Additionally, we derive expressions for the expected capacity of the infrastructure that also differ only in these two terms.

III. Discrete System Models

We consider infrastructures wherein the constituent systems consists of discrete components. We capture the underlying correlations at the system-level using aggregate correlation functions as well as those within each system using differential conditions.

A. Aggregate Correlations

We capture the interactions between systems and also between systems and network of the infrastructure in terms of their survival probabilities using the aggregate correlation functions in the following definition.

Condition 3.1: **Aggregate Correlation Function:** [21], [22] The probability that infrastructure is operational is given by

$$\begin{aligned} P_I &= P_i + P_{-i} - 1 + C_i(1 - P_i) \\ &= P_i + P_{-i} - 1 + C_{-i}(1 - P_{-i}), \end{aligned}$$

where C_i and C_{-i} are the aggregate correlation functions of S_i and S_{-i}, respectively, such that

$$C_i(1 - P_i) = C_{-i}(1 - P_{-i}),$$

for $i = 1, \ldots, N + 1$. □

The aggregate failure correlation function captures the interdependence of rest of the system S_{-i} on the failure of S_i, which can be illustrated using the following special cases.

(a) *Asymmetric Network:* In a cloud computing infrastructure consider that the fiber connections to N sites, each with l servers, constitute the network system $S_F = S_{N+1}$. Then, we have

$$P_{-F} = 1 - l(1 - P_F)/K,$$

where K is a normalization constant, since the fiber failure rate is amplified by l in rendering the servers unavailable. Thus, we have

$$P_I = [1 - (C_F - l/K)]\, P_F + C_F - l/K.$$

(b) *Statistical Independence:* The system failures satisfy a statistical independent condition given by $C_i = 1 - P_{-i}$, indicating that the failure probability of S_{-i} is not dependent on P_i. This condition in turn leads to $P_I = P_i P_{-i}$, which indicates the statistical independence of the survival processes of S_i and S_{-i}. More generally, if $C_i > 1 - P_{-i}$, the failures in S_{-i} are *positively correlated* to failures in S_i, that is, they occur with a higher probability following the latter. If we denote the failure probability of S_i by $P_{\bar{i}}$, then we have $P_{\overline{-i}|\bar{i}} > P_{\overline{-i}}$, or equivalently failure in S_i leads to a higher probability of failure in S_{-i}. If $C_i < 1 - P_{-i}$, failures in S_{-i} are *negatively correlated* to latter failures, that is $P_{\overline{-i}|\bar{i}} < P_{\overline{-i}}$.

(c) *Definite Failure:* In another case, when the failure of S_i leads to a definite failure of rest of the infrastructure, we have $C_i\,(P_i) = 1$ such that $P_I = P_{-i}$. This condition indicates that the infrastructure survival probability solely depends on the marginal failure probability of S_{-i}.

(d) *OR Systems:* The OR systems as modeled in [24] correspond to the special case $N = 2$ where the infrastructure consists of cyber and physical systems (denoted by $i = C$ and $-i = P$, respectively) that can be independently analyzed. For OR systems, the failure probability of cyber or physical sub-infrastructure is $P_{\bar{i} \cup \overline{-i}} = P_{\bar{i}} + P_{\overline{-i}}$ or equivalently $P_{\bar{i} \cap \overline{-i}} = 0$. Thus, we have $P_I = P_i + P_{-i} - 1$ and $C_i = 0$. This condition indicates that the failure processes of S_i and S_{-i} are uncorrelated. We generalize this condition next in Condition 3.2 for N systems considered in this paper.

We now consider an important special case where network plays a strong asymmetric role in that its failure disconnects all systems S_i, $i = 1, 2, \ldots, N$. Furthermore, these systems

are suitably shielded so that their failures are uncorrelated in that they do not escalate to the infrastructure level. We capture such scenarios using the following condition.

Condition 3.2: **Asymmetric Network and Uncorrelated Systems Conditions:** The aggregated correlation functions of S_i, $i = 1, 2, \ldots, N+1$ satisfy the conditions: (i) for the network S_{N+1}, we have $C_{N+1} = 1$, and (ii) for the constituent systems, we have $C_i = 0$, $i = 1, 2, \ldots, N$. □

The part (i) of this condition implies that $P_I = P_{-(N+1)}$, thereby indicating the role of rest of the infrastructure $S_{-(N+1)}$ without the network. The part (ii) of this condition implies $P_I = P_i + P_{-i} - 1$, $i = 1, 2, \ldots, N$ which separates failures of the constituent systems from rest of the infrastructure S_{-i}.

We further consider that the effects of reinforcements and attacks can be separated at the system level such that

(i) $\frac{\partial P_{-i}}{\partial x_i} \approx 0$ for $i = 1, 2, \ldots, N$ which indicates that reinforcing S_i does not directly impact the survival probability of the rest of the infrastructure, and

(ii) $\frac{\partial P_i}{\partial x_j} \approx 0$ for $i = 1, 2, \ldots, N+1$, $j = 1, 2, \ldots, N$ and $j \neq i$, which indicates that reinforcing S_j does not directly impact the survival probability of S_i.

We capture such system-level considerations for the provider using the following condition.

Condition 3.3: For P_I in Condition 3.1, we have for $i = 1, 2, \ldots, N+1$,

$$\frac{\partial P_I}{\partial x_i} \approx (1 - C_i) \frac{\partial P_i}{\partial x_i} + (1 - P_i) \frac{\partial C_i}{\partial x_i}$$

for the provider. □

In the cases C_i is constant, we note that $\frac{\partial C_i}{\partial x_i} = 0$, which is the case under both parts of Condition 3.2.

The conditions in this section correspond to system-level correlations, and are not fine enough to capture the component-level correlations. In the next section, we consider generic differential conditions that characterize component-level correlations.

B. System Survival Probabilities

We consider that the system survival probabilities satisfy the following differential condition, which was originally defined for cyber and physical sub-infrastructures [21], [23].

Condition 3.4: **System Multiplier Functions:** The survival probabilities P_i and P_{-i} of system S_i and S_{-i}, respectively, satisfy the following conditions: there exist *system multiplier functions* Λ_i and Λ_{-i} such that

$$\frac{\partial P_i}{\partial x_i} = \Lambda_i(x_1, \ldots, x_N, y_1, \ldots, y_N) P_i$$
$$\frac{\partial P_{-i}}{\partial x_i} = \Lambda_{-i}(x_1, \ldots, x_N, y_1, \ldots, y_N) P_{-i}$$

for $i = 1, 2, \ldots, N+1$. □

The derivative in the above condition is *linear* in P_i for $\Lambda_i = 1$, and is faster than linear if $\Lambda_i > 1$ and slower than linear if $\Lambda_i < 1$. This somewhat abstract condition is satisfied in two special cases studied in literature.

1) Statistically Independent Components: The special case when component survival probabilities are statistically independent with and without reinforcements has been studied in [23]. Let $p_{i|R}$ and $p_{i|N}$ denote the conditional survival probability of a component of S_i with and without reinforcement, respectively. Under the statistical independence condition of component failures, the probability that S_i with n_i components survives the attacks is

$$P_i = p_{i|R}^{x_i} p_{i|N}^{n_i - x_i}$$

as in [23], or equivalently

$$\ln P_i = n_i \ln p_{i|N} + x_i \ln \left(\frac{p_{i|R}}{p_{i|N}} \right).$$

By differentiating with respect to x_i we obtain

$$\frac{\partial P_i}{\partial x_i} = \ln \left(\frac{p_{i|R}}{p_{i|N}} \right) P_i.$$

The condition for faster than linear derivative is $p_{i|R} > e p_{i|N}$. The condition that the survival probability of a reinforce component is higher than that of non-reinforced component but less than $e p_{i|N}$, namely, $e p_{i|N} > p_{i|R} > p_{i|N}$, corresponds to only slower than linear derivative.

2) Contest Survival Functions: The contest survival functions are to express P_i in [12] such that $P_i = \frac{\xi + x_i}{\xi + x_i + y_i}$ for a suitably selected slack variable ξ, which in turn leads to

$$\frac{\partial P_i}{\partial x_i} = \left[\frac{y_i}{(\xi + x_i + y_i)(\xi + x_i)} \right] P_i.$$

The condition for slower than linear derivative is

$$y_i[1 - (x_i + \xi)] < (\xi + x_i)^2$$

which is satisfied for larger values of x_i sufficient to make the left hand side negative.

IV. Game Theoretic Formulation

The provider's objective is to make the infrastructure resilient by reinforcing x_i components of S_i by optimizing the corresponding utility function, namely, minimizing the sum-form or maximizing the product-form. Similarly, the attacker's objective is to disrupt the infrastructure by attacking y_i components of S_i by optimizing the corresponding utility function. NE conditions are derived by equating the corresponding derivatives of the utility functions to zero, which yields the following for sum- and product-form utilities, respectively:

$$\frac{\partial U_{D+}}{\partial x_i} = \frac{\partial P_I}{\partial x_i} g_D - \frac{\partial C_D}{\partial x_i} = 0$$

$$\frac{\partial U_{D\times}}{\partial x_i} = -\frac{\partial P_I}{\partial x_i} C_D + (1 - P_I) \frac{\partial C_D}{\partial x_i} = 0$$

for $i = 1, 2, \ldots, N+1$ for the provider.

A. NE Sensitivity Functions

We now derive estimates for P_i at NE using partial derivatives of the cost and failure correlation functions to infer qualitative information about their sensitivities to different parameters.

Theorem 4.1: Under Conditions 3.1, 3.3, and 3.4, estimates of the survival probability of system S_i, for $i = 1, 2, \ldots, N+1$ is given by

$$\hat{P}^A_{i;D} = \frac{\frac{\partial C_i}{\partial x_i} - \xi^A_i}{\frac{\partial C_i}{\partial x_i} - (1 - C_i)\Lambda_i}$$

where $A = +$ and $A = \times$ correspond to sum-form and product-form, respectively, such that

$$\xi^A_i = \begin{cases} \frac{1}{g_D}\frac{\partial C_D}{\partial x_i} & \text{if } \ A = + \\ (1 - P_I)\frac{\partial \ln C_D}{\partial x_i}, & \text{if } \ A = \times \end{cases}$$

for $i = 1, 2, \ldots, N + 1$ under the condition: $C_i < 1$ or $\frac{\partial C_i}{\partial x_i} \neq 0$. Under the asymmetric network correlation coefficient $C_{N+1} = 1$, the survival probability of the network is given by

$$P^A_{-(N+1);D} = \frac{\xi^A_{N+1}}{\Lambda_{-(N+1)}}$$

for $A = +, \times$.

Proof: Our proof is based on deriving NE conditions separately for sum-form and product-form utility functions, and then comparing them to identify their common structure and the difference terms. At NE, for sum-form we have

$$\frac{\partial P_I}{\partial x_i} = \frac{1}{g_D}\frac{\partial C_D}{\partial x_i} = \xi^+_i.$$

Then, using the equation in Condition 3.3 and $\frac{\partial P_i}{\partial x_i} = \Lambda_i P_i$ from Condition 3.4, we have

$$(1 - C_i)\Lambda_i P^+_{i;D} + (1 - P^+_{i;D})\frac{\partial C_i}{\partial x_i} = \frac{1}{g_D}\frac{\partial C_D}{\partial x_i}. \quad (1)$$

Under the condition $C_i < 1$ or $\frac{\partial C_i}{\partial x_i} \neq 0$, we have $\frac{\partial C_i}{\partial x_i} - (1 - C_i)\Lambda_i \neq 0$, and hence, we obtain

$$P^+_{i;D} = \frac{\frac{\partial C_i}{\partial x_i} - \frac{1}{g_D}\frac{\partial C_D}{\partial x_i}}{\frac{\partial C_i}{\partial x_i} - (1 - C_i)\Lambda_i} = \frac{\frac{\partial C_i}{\partial x_i} - \xi^+_i}{\frac{\partial C_i}{\partial x_i} - (1 - C_i)\Lambda_i},$$

for $i = 1, 2, \ldots, N + 1$. Similarly, for product-form we have

$$\frac{\partial P_I}{\partial x_i} = (1 - P_I)\frac{1}{C_D}\frac{\partial C_D}{\partial x_i} = (1 - P_I)\frac{\partial \ln C_D}{\partial x_i} = \xi^\times_i. \quad (2)$$

Then, using the equation in Condition 3.3 and $\frac{\partial P_i}{\partial x_i} = \Lambda_i P_i$ from Condition 3.4, we have

$$(1 - C_i)\Lambda_i P^\times_{i;D} + (1 - P^\times_{i;D})\frac{\partial C_i}{\partial x_i} = (1 - P_I)\frac{\partial \ln C_D}{\partial x_i}.$$

Then, we have

$$P^\times_{i;D} = \frac{\frac{\partial C_i}{\partial x_i} - (1 - P_I)\frac{\partial \ln C_D}{\partial x_i}}{\frac{\partial C_i}{\partial x_i} - (1 - C_i)\Lambda_i},$$

for $i = 1, 2, \ldots, N + 1$.

Consider the survival probability of the infrastructure, under the asymmetric network condition, we have $C_{N+1} = 1$ and $\frac{\partial C_{N+1}}{\partial x_{N+1}} = 0$, which imply the condition $C_i < 1$ or $\frac{\partial C_i}{\partial x_i} \neq 0$ is not satisfied; hence, the above formula cannot be used directly since the denominator $\frac{\partial C_i}{\partial x_i} - (1 - C_i)\Lambda_i = 0$. Instead, using $C_{N+1} = 1$ in Condition 3.1, we obtain $P_I = P_{-(N+1)}$, which implies

$$\frac{\partial P_I}{\partial x_{N+1}} = \frac{\partial P_{-(N+1)}}{\partial x_{N+1}}.$$

Then, NE condition for the sum-form is given by

$$\frac{\partial P_I}{\partial x_{N+1}} = \frac{\partial P^+_{-(N+1);D}}{\partial x_{N+1}} = \Lambda_{-(N+1)}P^+_{-(N+1);D} = \frac{1}{g_D}\frac{\partial C_D}{\partial x_{N+1}}.$$

Similarly, for the product-form we obtain,

$$\frac{\partial P_I}{\partial x_{N+1}} = \Lambda_{-(N+1)}P^\times_{-(N+1);D} = (1 - P_I)\frac{\partial \ln C_D}{\partial x_{N+1}},$$

which completes the proof. □

The estimates $\hat{P}_{i;D}$ above provide sensitivity information about the corresponding survival probabilities with respect to various parameters (the estimates may not necessarily lie within [0,1]). In particular, they qualitatively relate P_i to the corresponding aggregate correlation function C_i and its derivative, and also to Λ_i. These dependencies are identical for both sum-form and product-form utility functions. Indeed, the difference between the two formulae is captured by the single term ξ^A_i, which is proportional to the derivative term $\frac{\partial C_D}{\partial x_i}$ in both cases. The main difference is that $\xi^\times_i$ is an increasing function of P_I, whereas ξ^+_i does not depend on P_I. Also, the dependence on C_D is different for these two terms. Since $\xi^+_i = \frac{1}{g_D}\frac{\partial C_D}{\partial x_i}$ and $\xi^\times_i = (1-P_I)\frac{1}{C_D}\frac{\partial C_D}{\partial x_i}$, the role of g_D in the former is played by $C_D/(1 - P_I)$ in the latter. Typically, g_D is chosen as a constant in the sum-form, and P_I is a function of x_i and y_i.

We now consider that the network failure renders entire infrastructure unavailable, and those of individual systems are uncorrelated with others given by Condition 3.2. The following theorem provides a single, simplified expression for the expected capacity under these conditions.

Theorem 4.2: **Asymmetric Network Correlations:** Under Conditions 3.1-3.4, the expected capacity is given by

$$N^A_I = \sum_{i=1}^{N}\left(n_i\frac{\xi^A_i}{\Lambda_i}\right)$$

where $A = +$ and $A = \times$ correspond to sum-form and product-form, respectively, such that

$$\xi^A_i = \begin{cases} \frac{1}{g_D}\frac{\partial C_D}{\partial x_i} & \text{if } \ A = + \\ (1 - P_I)\frac{\partial \ln C_D}{\partial x_i}, & \text{if } \ A = \times \end{cases}$$

for $i = 1, 2, \ldots, N$.

Proof: Equations (1) and (2) in Theorem 4.1 under part (ii) of Condition 3.2 simplify to the same equation $\Lambda_i P^A_{i;D} = \xi^A_i$ for $A = +, \times$ and $i = 1, 2, \ldots, N$. Thus, we have $P^A_i = \frac{\xi^A_i}{\Lambda_i}$, which provides the expression for N^A_I. □

For the sum-form,

$$N^+_I = \sum_{i=1}^{N}\left(\frac{n_i\frac{\partial C_D}{\partial x_i}}{g_D\Lambda_i}\right)$$

indicates that higher gain g_D leads to lower number of operational components. For the product form,

$$N_I^{\times} = (1 - P_I) \sum_{i=1}^{N} \left(\frac{n_i \frac{\partial C_D}{\partial x_i}}{C_D \Lambda_i} \right)$$

indicates that higher survival probability of the network leads to lower number of operational components. The dependence on Λ_i is similar in both cases, namely, faster than linear leads to lower number of available component, and vice versa. The dependence on C_D is somewhat different due its presence in the denominator for product-form, even though $\frac{\partial C_D}{\partial x_i}$ appears in the numerator in both forms.

V. Distributed Cloud Computing Infrastructure

A distributed cloud computing infrastructure consisting of N sites, each with l_i servers at site i, $i = 1, 2, \ldots, N$ has been studied in [20] by using separate cyber and physical models for each site. The sites are connected over a communication network S_{N+1} as shown in Figure 1. The network consists of a number of routers each of which manages l_{N+1} connections as shown in Figure 2.

This infrastructure is subject to a variety of cyber and physical attacks on its components. Cyber attacks on the servers may be launched remotely over the network since they are accessible to users. Meanwhile, routers are located at geographically separated sites and access to them is limited (to network administrators), and they are not as easily accessible over the network. Cyber attacks on routers require different techniques and represent different costs to the attacker compared to server attacks. Furthermore, this infrastructure is subject to physical attacks in the form of fiber cuts, which require a proximity access by the attacker. In particular, the network fibers that connect server sites to routers may be physically cut, and disconnect the entire site making it inaccessible to the users. And, such attacks may also be launched on the network fibers between routers at different locations on the network.

The infrastructure provider may employ a number of reinforcements to protect against attacks, including replicating the servers and routers to support fail-over operations, and installing physically separated redundant fiber lines to the sites and between router locations. These measures could require significant costs, and hence must be strategically chosen.

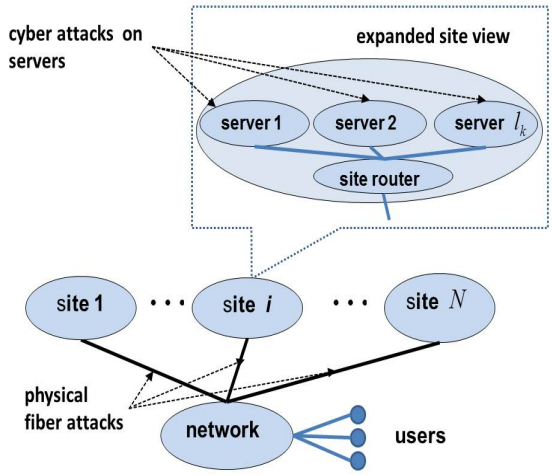

Fig. 1. Cloud computing infrastructure with N sites.

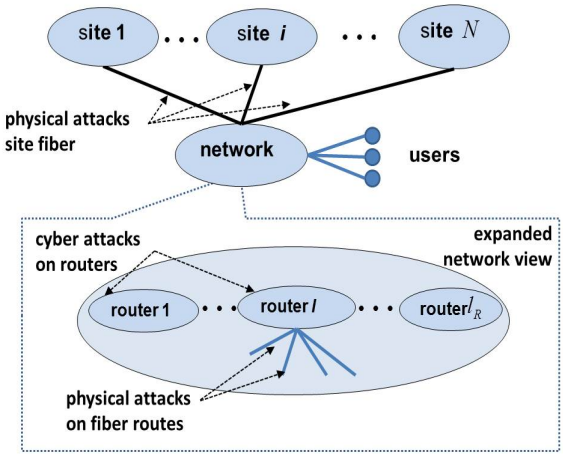

Fig. 2. Network of cloud computing infrastructure.

A. System-Level Correlations

The cyber and physical aspects of a site S_i can be represented by using $S_{(i,c)}$ and $S_{(i,p)}$ that correspond to cyber and physical model, respectively. Similarly, those of the network S_{N+1} are represented by $S_{(N+1,c)}$ and $S_{(N+1,p)}$, which are the cyber and physical models as illustrated in Figure 3. The relationships between these system-level models can be captured using the the aggregate correlation functions as follows (as described in [21], [20]). For the communications network, we have

$$C_{(N+1,c)} = l_{N+1} C_{(N+1,p)}$$

which reflects that a cyber attack on a router will disrupt all its l_{N+1} connections, thereby illustrating the amplification effect of cyber attacks. For the server sites, we have a similar effect due to physical fiber attacks reflected by

$$C_{(i,p)} = l_i C_{(i,c)}$$

which indicates that at site S_i the fiber disruption will disconnect all its l_i servers.

B. Component-Level Correlations

We now consider a special case where the attacker and provider choose the components to attack and reinforce, respectively, according to uniform distribution. Let $n_{(i,c)}$ and $n_{(i,p)}$ represent the number of cyber and physical components, respectively, of site S_i such that $n_i = n_{(i,c)} + n_{(i,p)}$. Similarly, let $x_{(i,c)}$ and $x_{(i,p)}$ represent the number of cyber and physical components reinforced at site S_i such that $x_i = x_{(i,c)} + x_{(i,p)}$, and let $y_{(i,c)}$ and $y_{(i,p)}$ represent the number of cyber and physical components reinforced at site S_i such that $y_i = y_{(i,c)} + y_{(i,p)}$. Then, corresponding to the site physical model $S_{(i,p)}$, $i = 1, 2, \ldots, N$, there are $[n_{(i,p)} - x_{(i,p)}]_+$ non-reinforced fiber connections, where $[x]_+ = x$ for $x > 0$, and $[x]_+ = 0$ otherwise. Similarly, there are $[n_{(i,c)} - x_{(i,c)}]_+$

non-reinforced servers. If a cyber component (i.e., a server) is reinforced, it will survive a cyber attack but can be brought down indirectly by a fiber attack. Then, the probability that a cyber-reinforced component survives $y_{(i,p)}$ fiber attacks is approximated by

$$p_{(i,c)|R} = \frac{f_{(i,c)}}{1 + l_i \left[y_{(i,p)} - x_{(i,p)}\right]_+},$$

where the normalization constant $f_{(i,c)}$ is appropriately chosen.

On the other hand, if a cyber component is not reinforced, it can be brought down by either a direct cyber attack, or indirectly through a fiber attack. Thus, we approximate the survival probability of a cyber component at site k as

$$p_{(i,c)|N} = \frac{f_{(i,c)}}{1 + y_{(i,c)} + l_i \left[y_{(i,p)} - x_{(i,p)}\right]_+},$$

which reflects the additional lowering of the survival probability in inverse proportion to the level of cyber attack $y_{(i,c)}$. Using these formulae, for cyber model $S_{(i,c)}$ of site S_i, we have, under the independence of component attacks

$$\Lambda_{(i,c)}(x_{(i,p)}, y_{(i,c)}, y_{(i,p)}) = \ln\left(1 + \frac{y_{(i,c)}}{1 + l_i \left[y_{(i,p)} - x_{(i,p)}\right]_+}\right).$$

It is interesting to note that it does not depend on the cyber reinforcements term $x_{(i,c)}$ even though it corresponds to $\frac{\partial P_{(i,c)}}{\partial x_{(i,c)}}$. It, however, depends on the physical reinforcement term $x_{(i,p)}$.

Under the statistical independence of cyber and physical attacks, we have the following generalization of the condition derived in Section III-B1

$$P_i = p_{(i,c)|R}^{x_{(i,c)}} p_{(i,c)|N}^{n_{(i,c)} - x_{(i,c)}} p_{(i,p)|R}^{x_{(i,p)}} p_{(i,p)|N}^{n_{(i,p)} - x_{(i,p)}}$$

or equivalently

$$\begin{aligned}\ln P_i = {} & n_{(i,c)} \ln p_{(i,c)|N} + x_{(i,c)} \ln\left(\frac{p_{(i,c)|R}}{p_{(i,c)|N}}\right) \\ & + n_{(i,p)} \ln p_{(i,p)|N} + x_{(i,p)} \ln\left(\frac{p_{(i,p)|R}}{p_{(i,p)|N}}\right)\end{aligned}$$

By differentiating by $x_{(i,c)}$ we obtain

$$\frac{\partial P_i}{\partial x_{(i,c)}} = \ln\left(\frac{p_{(i,c)|R}}{p_{(i,c)|N}}\right) P_i = \Lambda_{(i,c)} P_i.$$

Then, by noting that $\frac{\partial x_i}{\partial x_{(i,c)}} = 1$, we obtain

$$\frac{\partial P_i}{\partial x_i} = \Lambda_{(i,c)} P_i,$$

which enables us to approximate Λ_i by $\Lambda_{(i,c)}$.

Consider $\hat{P}^A_{i;D}$ in Theorem 4.1, the term Λ_i appears in the denominator with a negative sign. Thus, in qualitative terms, it depends linearly with a multiplier a on the logarithm of the number of cyber attacks $y_{(i,c)}$, and inversely on the logarithm of $\left[y_{(i,p)} - x_{(i,p)}\right]_+$ which is the number of attacks exceeding the reinforcements. The sign of the multiplier a could be positive or negative based on the other factors $\frac{\partial C_i}{\partial x_i}$ and ξ_i^A, where $A = +, \times$. This condition may appear somewhat counter-intuitive at the surface but note that it only characterizes the states that satisfy NE conditions, and in particular, it illustrates the richness of infrastructure behavior at NE.

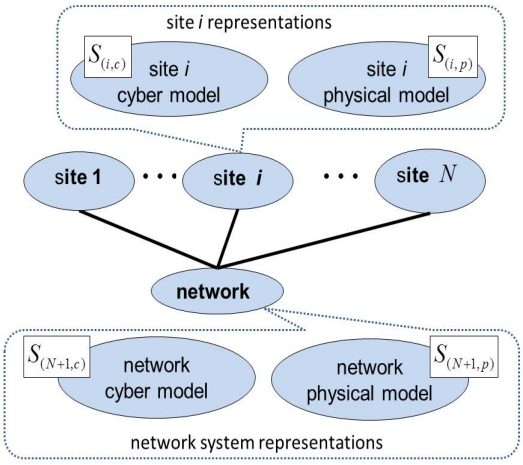

Fig. 3. Representation of cloud computing infrastructure.

C. Expected Capacity

In terms of the expected capacity N_I^A, the dependence on $y_{(i,c)}$ and $\left[y_{(i,p)} - x_{(i,p)}\right]_+$ is more direct, and qualitatively similar for both sum-form and product-form, since the term Λ_i appears in the denominator. Based on Theorem 4.2 we obtain the following expressions: for the sum-form,

$$N_I^+ = \sum_{i=1}^{N} \left(\frac{n_i \frac{\partial C_D}{\partial x_i}}{g_D \ln\left(1 + \frac{y_{(i,c)}}{1 + l_i \left[y_{(i,p)} - x_{(i,p)}\right]_+}\right)}\right),$$

and for the product form,

$$N_I^\times = (1 - P_I) \sum_{i=1}^{N} \left(\frac{n_i \frac{\partial C_D}{\partial x_i}}{C_D \ln\left(1 + \frac{y_{(i,c)}}{1 + l_i \left[y_{(i,p)} - x_{(i,p)}\right]_+}\right)}\right).$$

In both cases, the multipliers n_i, g_D and C_D are positive, and it is reasonable to assume the condition $\frac{\partial C_D}{\partial x_i} \geq 0$, since the reinforcement cost does not decrease with x_i. Thus, the expected capacity decreases with $y_{(i,c)}$ and the opposite is true with respect to $\left[y_{(i,p)} - x_{(i,p)}\right]_+$. In both cases, the dependence on the number of servers l_i at site i is qualitatively similar in that the expected capacity increases proportional to its logarithm.

In summary, the overall dependencies considered here are quite simple, namely, under the statistical independence and uniform distributions of components chosen by both defender and attacker. Even under such simple conditions, the detailed NE conditions are quite complex to characterize.

VI. Conclusions

We consider a class of infrastructures with multiple systems, each with discrete cyber and physical components.

These systems are connected over a communications network which plays an important asymmetric role by providing the critical connectivity that makes these systems available, and consequently requires an explicit consideration in ensuring the performance of the infrastructure. Individual components of a system can be disrupted directly or indirectly by either a cyber or physical attack. The components are reinforced against such attacks by explicitly taking into account the correlations between the systems and also between the components within individual systems. We characterize the system-level correlations using the aggregate failure correlation function that specifies the infrastructure failure probability given the failure of an individual system or network. The survival probabilities of systems and network satisfy first-order differential conditions that capture the component-level correlations.

We formulated the problem of ensuring the infrastructure survival as a game between an attacker and a provider, using two different utility functions, namely, the sum-form and product-form; the former is the sum of a survival probability term and a cost term, and the latter is their product. We derived Nash Equilibrium conditions in terms of the partial derivatives of cost terms and failure correlation functions. In particular, we derive expressions for individual system survival probabilities, and also the expected capacity specified by the total number of operational components. These expressions differ only in a single term for the sum-form and product-form utilities, despite their significant differences in modeling objectives. We applied this approach to simplified models of cloud computing infrastructures.

These results extend or specialize previous results on interconnected systems [11], [12] and cyber-physical infrastructures [23] by using the general utility functions. They also unify the results that were separately developed for the sum-form utility functions in [21] and the product-form disutility functions in [22] for the cases wherein the network plays a critical, asymmetric role.

Several extensions of the formulation studied in this paper can be pursued in future studies, including cases where the effects of attacks and reinforcements of specific individual components are explicitly accounted for. It is of future interest to compare this formulation to one where the utility function contains the expected capacity term in place of infrastructure survival probability. Another future direction is to consider the simultaneous cyber and physical attacks on multiple components. It would be interesting to study sequential game formulations of this problem, and cases where different levels of knowledge are available to each party. Applications of our approach to more detailed models of cloud computing infrastructure, smart energy grid infrastructures and high-performance computing complexes would be of future interest. It would also be of future interest to explore the applicability of this overall method to continuous models such as partial differential equations describing individual systems or the entire infrastructure.

REFERENCES

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

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

[3] G. Brown, M. Carlyle, J. Salmeron, and K. Wood. Analyzing the vulnerability of critical infrastructure to attack and planning defenses. *Tutorials in Operations Research: Emerging Theory, Methods, and Applications*, pages 102–123, 2005.

[4] S. Bu and F. R. Yu. A game-theoretical scheme in the smart grid with demand-side management: Towards a smart cyber-physical power infrastructure. *Emerging Topics in Computing, IEEE Transactions on*, 1(1):22–32, 2013.

[5] A. A. Cardenas, S. Amin, and S. Sastry. Secure control: Towards survivable cyber-physical systems. In *The 28th International Conference on Distributed Computing Systems Workshops*, pages 495–500. IEEE, 2008.

[6] P.-Y. Chen, S.-M. Cheng, and K.-C. Chen. Smart attacks in smart grid communication networks. *Communications Magazine, IEEE*, 50(8):24–29, 2012.

[7] S. K. Das, K. Kant, and N. Zhang, editors. *An analytical framework for cyber-physical networks*. Morgan Kaufman, 2012.

[8] DHS. Critical Infrastructure Sectors. lhttp://www.dhs.gov/critical-infrastructure-sectors, 2015. [Online; accessed in October 2015].

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

[10] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu. Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid. *Smart Grid, IEEE Transactions on*, 4(2):847–855, 2013.

[11] K. Hausken. Strategic defense and attack of complex and dependent systems. *Reliability Engineering*, 95(1):29–42, 2009.

[12] K. Hausken. Defense and attack for interdependent systems. 2016.

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

[14] V. R. R. Jose and J. Zhuang. Technology adoption, accumulation, and competition in multi-period attacker-defender games. *Military Operations Research*, 18(2):33–47, 2013.

[15] T. G. Lewis. *Critical infrastructure protection in homeland security: defending a networked nation*. John Wiley & Sons, 2014.

[16] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Bacşar, and J.-P. Hubaux. Game theory meets network security and privacy. *ACM Computing Surveys (CSUR)*, 45(3):25, 2013.

[17] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli. Cyber–physical security of a smart grid infrastructure. *Proceedings of the IEEE*, 100(1):195–209, 2012.

[18] M. Nikoofal and J. Zhuang. Robust allocation of a defensive budget considering an attackers private information. *Risk Analysis*, 32(5):930–943, 2012.

[19] F. Pasqualetti, F. Dörfler, and F. Bullo. Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design. In *Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on*, pages 2195–2201. IEEE, 2011.

[20] N. S. V. Rao, N. Imam, C. Y. T. Ma, K. Hausken, F. He, and J. Zhuang. On defense strategies for system of systems using aggregated correlations. In *11th Annual IEEE International Systems Conference*, 2017.

[21] N. S. V. Rao, C. Y. T. Ma, K. Hausken, F. He, and J. Zhuang. Defense strategies for infrastructures with multiple systems of components. In *International Conference on Information Fusion*, 2016.

[22] N. S. V. Rao, C. Y. T. Ma, K. Hausken, F. He, and J. Zhuang. Game-theoretic strategies for systems of components using product-form utilities. In *IEEE International Conference on Multisensor Fusion and Integration for Intelligent Systems*, 2016.

[23] 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 *International Conference on Information Fusion*, 2014.

[24] N. S. V. Rao, C. Y. T. Ma, U. Shah, J. Zhuang, F. He, and D. K. Y. Yau. On resilience of cyber-physical infrastructures using discrete product-form games. In *International Conference on Information Fusion*, 2015.

[25] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly. Identifying, understanding, and analyzing critical infrastructure interdependencies. *Control Systems, IEEE*, 21(6):11–25, 2001.

[26] T. Sandler et al. Terrorism & game theory. *Simulation & Gaming*, 34(3):319–337, 2003.

[27] 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*, 228(1):262–272, 2013.

[28] S. Shiva, S. Roy, and D. Dasgupta. Game theory for cyber security. In *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, page 34. ACM, 2010.