On Defense Strategies for System of Systems Using Aggregated Correlations

Nageswara S. V. Rao[*], Neena Imam[*], Chris Y. T. Ma[†], Kjell Hausken[‡], Fei He[§], 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
[¶]State University of New York at Buffalo, Buffalo, NY, USA

***Abstract*—We consider a System of Systems (SoS) wherein each system S_i, $i = 1, 2, \ldots, N$, is composed of discrete cyber and physical components which can be attacked and reinforced. We characterize the disruptions using aggregate failure correlation functions given by the conditional failure probability of SoS given the failure of an individual system. We formulate the problem of ensuring the survival of SoS as a game between an attacker and a provider, each with a utility function composed of a survival probability term and a cost term, both expressed in terms of the number of components attacked and reinforced. The survival probabilities of systems satisfy simple product-form, first-order differential conditions, which simplify the Nash Equilibrium (NE) conditions. We derive the sensitivity functions that highlight the dependence of SoS survival probability at NE on cost terms, correlation functions, and individual system survival probabilities. We apply these results to a simplified model of distributed cloud computing infrastructure.**

I. Introduction

Critical infrastructures such as cloud computing facilities and smart grids can be perceived as System of Systems (SoS), wherein each system S_i, $i = 1, 2, \ldots, N$, is composed of discrete cyber and physical components. The components of a system must be *operational* as individual units and also be *available*, such as being connected to the network. A component may be disrupted by a direct cyber or physical attack; in addition, it may be made unavailable by attacks on other components, even though it is operational by itself. The effects of disruptions may propagate among the components of S_i, and also beyond to other systems S_j, $j \neq i$. For example, consider a distributed cloud computing infrastructure with multiple server sites connected over a wide area network. A cyber attack on a server may bring it down, and a physical attack on a fiber line that connects a site to the network may render all servers at the site unavailable to cloud users. In an extreme case, the effects of component attacks may spread to entire SoS. The SoS provider is tasked with developing defense strategies to reinforce components of S_i's against attacks, by accounting for both types of disruption propagation, namely, within and between the systems.

Let y_i and x_i be the number of components of S_i attacked and reinforced, respectively, wherein a reinforced component survives a direct attack but may be disrupted indirectly. Let P_i be the survival probability of S_i, and P_S be the survival probability of entire SoS. The *aggregate failure correlation function* $C_i(P_i)$ is the failure probability of "rest" of SoS (namely, without S_i) given the failure of S_i. Intuitively, it indicates the relative importance of S_i by capturing the fault propagation from S_i to rest of SoS, which is denoted by S_{-i}. In addition to these system-level correlations, those among the components of individual systems are characterized by simple product-form, first-order differential conditions on P_i [20] using the system multiplier functions. These conditions subsume the contest success functions and statistical independence conditions as special cases, and lead to simplified estimates of survival probabilities at the Nash Equilibrium (NE). This two-level characterization of correlations is natural to SoS, for example, cloud computing and smart grid infrastructures [23], and leads to a simplified analysis of NE conditions by "separating" system-level aspects from component-level details.

The reinforcements and attacks on components entail certain costs to the provider and attacker, respectively. In developing defense strategies, the provider should weigh the costs against benefits in terms of keeping SoS operational. This task requires taking into account both types of correlations described above as well as the costs incurred by the provider. We formulate a game wherein individual system components can be disrupted by the attacker, and can be reinforced by the provider to defend against them. The costs of attacks and reinforcements of systems are denoted by $L_A(y_1, \ldots, y_N)$ and $L_D(x_1, \ldots, x_N)$, respectively. The provider minimizes the *disutility function* given by a sum of two parts:

$$\begin{aligned}
&U_D\left(x_1, \ldots, x_N, y_1, \ldots, y_N\right) \\
&= F_{D,G}(x_1, \ldots, x_N, y_1, \ldots, y_N) G_D(x_1, \ldots, x_N, y_1, \ldots, y_N) \\
&\quad + F_{D,L}(x_1, \ldots, x_N, y_1, \ldots, y_N) L_D(x_1, \ldots, x_N),
\end{aligned}$$

where the first part corresponds to reward and the second part corresponds to cost. Each part is a product of two terms: (i) first terms $F_{D,G}$ and $F_{D,L}$ are the reward and cost multiplier functions, respectively, of the provider, and (ii) second terms G_D and L_D represent the reward and cost of keeping SoS

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.

operational, respectively. Similarly, the attacker's *disutility function* is given by

$$\begin{aligned} &U_A\left(x_1,\ldots,x_N,y_1,\ldots,y_N\right) \\ &= F_{A,G}(x_1,\ldots,x_N,y_1,\ldots,y_N)G_A(x_1,\ldots,x_N,y_1,\ldots,y_N) \\ &\quad + F_{A,L}(x_1,\ldots,x_N,y_1,\ldots,y_N)L_A(y_1,\ldots,y_N), \end{aligned}$$

where (i) $F_{A,G}$ and $F_{A,L}$ are the reward and cost multiplier functions, respectively, of the attacker, and (ii) G_A and L_A represent the reward and cost of disrupting the operation of SoS, respectively. At NE, the attacker and provider minimize their respective disutility functions [8]. The previously studied sum-form [20] and product-form [21] utility functions are special cases of these disutility functions. The sum-form utility function is a linear combination of survival probability and cost parts such that $G_D = g_D$ is a constant, and $F_{D,G} = 1 - P_S$, $F_{D,L} = 1$ [20], and it is given by

$$\begin{aligned} &U_{D+}\left(x_1,\ldots,x_N,y_1,\ldots,y_N\right) \\ &= \left[1 - P_S(x_1,\ldots,x_N,y_1,\ldots,y_N)\right] g_D + L_D(x_1,\ldots,x_N). \end{aligned}$$

The product-form utility function is a product of the two terms such that $F_{D,G} = 0$, $F_{D,L} = 1 - P_S$, and it is given by

$$\begin{aligned} &U_{D\times}\left(x_1,\ldots,x_N,y_1,\ldots,y_N\right) \\ &= \left[1 - P_S(x_1,\ldots,x_N,y_1,\ldots,y_N)\right] L_D(x_1,\ldots,x_N). \end{aligned}$$

The sum-form utility function represents a weaker coupling of the two terms, $1 - P_S$ and L_D, and leads to qualitatively different defense strategies compared to the product-form disutility. Typically, NE conditions for these two disutilities are obtained using somewhat different derivations. Our generalization provides a unified treatment of both forms, and also provides simple expressions for the sensitivity functions at NE involving a single gain-cost term that encompasses both forms.

We derive NE conditions that show the dependence of P_S on cost terms, correlation functions, system survival probabilities, and their partial derivatives. We also estimate the sensitivity functions of P_i in terms of: (i) gain-cost term involving the cost and gain terms and their partial derivatives, (ii) system multiplier functions defined in Condition 3.3, and (iii) terms involving the correlation function and its partial derivative. These "separate" terms clearly indicate the relative importance of the correlations and system multiplier functions on P_i at NE. These results extend previous results on interconnected systems in [10], [11] by utilizing the aggregated correlations and system multiplier functions to capture more general dependencies. Also, the cyber-physical infrastructures considered in [22], [23] constitute a special SoS class with $N = 2$.

The organization of this paper is as follows. We briefly describe related work in Section II. In Section III, we describe the discrete component 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 sensitivity estimates. We also describe the special case of OR systems in Section IV-A, wherein the correlation effects are significantly simplified. We apply the analytical results to a simple model of cloud computing in Section V. We present conclusions in Section VI.

II. Related Work

Critical infrastructures [14], [3], [17] that support smart grids, cloud computing, and transportation systems are vital to national security. They can be viewed as system of systems, since they rely on complex networked systems each with disparate components. Game-theoretic methods have been extensively applied to capture the interactions between providers and attackers of critical infrastructures [1], [4], [24]; they lead to strategies that ensure their continued operation in the presence of evolving threats. Several of these infrastructures are modeled using complex dynamic models of the underlying physical systems [2], in particular, using partial differential equations. In general, both game-theoretic formulations and their solutions are quite extensive for such infrastructures, including: games with multiple time-scales of system dynamics [13]; incomplete information games under partial knowledge of system dynamics and attack models [18]; and multiple-target games with possibly competing objectives [25]. A comprehensive review of the defense and attack models in various game-theoretic formulations has been presented in [12]. In particular, game theory has been applied in a variety of cyber security applications [15], [26], and in particular for securing cyber-physical networks [5] with applications to power grids [6], [16], [19], [9].

The system reliability and robustness parameters and variables can be explicitly integrated into these game formulations [1], for example for smart grids, cloud computing infrastructures and transportation systems. Within this class, Stackelberg game formulations using discrete models of cyber-physical infrastructures have been studied in various forms [7], and a subclass of them is formulated using the number of cyber and physical components that are attacked and reinforced [23]. These formulations characterize the infrastructures with a large number of components, and are coarser than formulations that consider the attack and defense of individual cyber and physical components. In particular, these works utilize the correlation functions to capture the dependencies between the survival probabilities of two systems, namely, the cyber and physical sub-infrastructures. Complex interacting systems that consist of several such systems have been studied using game-theoretic formulations in [11], and their two-level correlations have been studied using the sum-form utility functions [20] and the product-form disutility functions [21].

The sum-form utility represents a *gain-centric priority*, wherein the gain term g_D weighted by $1 - P_S$ plus the cost term is minimized by the provider. The product-form disutility, on the other hand, represents a *cost-centric priority*, wherein the expected cost is to be minimized. In terms of analysis, these two formulations have a certain degree of commonality but there are also differences; in particular, estimates of P_S can be obtained somewhat directly for the product-form as shown in [21]. Also, they lead to qualitatively different defense strategies, and in particular P_S appears explicitly in the sensitivity estimates of system survival probabilities in the product-form but not in the sum-form. The sum-form and product-form disutility functions are specific examples of the general diutility function presented in this paper.

III. Discrete System Models

We capture the interactions between a system S_i and rest of SoS S_{-i} in terms of their survival probabilities using the aggregate correlation function C_i and its companion function C_{-i} represented by the conditional failure probability of S_i given the failure of S_{-i} [20]. We denote the failure probability of S_j by $P_{\bar{j}} = 1 - P_j$, $j = -N, \ldots, -(N-1), -1, 1, 2, \ldots, N-1, N$. The survival probability of SoS is given by

$$P_S = P_{i,-i} = 1 - P_{\bar{i}\cup\overline{-i}},$$

where the last term corresponds to the probability that either of S_i and S_{-i} is non-operational. Then, we have

$$P_{\bar{i}\cup\overline{-i}} = P_{\bar{i}} + P_{\overline{-i}} - P_{\bar{i}\cap\overline{-i}}$$

wherein the last term is the joint failure probability of S_i and S_{-i} given by

$$P_{\bar{i}\cap\overline{-i}} = C_i\left(P_i\right)\left(1 - P_i\right) = C_{-i}\left(P_i\right)\left(1 - P_{-i}\right).$$

We highlight the dependence on P_i by explicitly showing it as an operand of C_i and C_{-i}.

Condition 3.1: **Aggregate Correlation Function:** The probability that SoS is operational is given by

$$P_S = P_i + P_{-i} - 1 + C_{-i}\left(P_i\right)\left(1 - P_{-i}\right),$$

where $C_i\left(P_i\right) = C_{-i}\left(P_i\right)\frac{1-P_{-i}}{1-P_i}$ is the aggregate failure correlation function of system S_i, $i = 1, \ldots, N$. □

We now present illustrative cases for the aggregate correlation function. In the special case where the failure of S_i leads to definite failure of rest of SoS, we have $C_i\left(P_i\right) = 1$ such that $P_S = P_{-i}$, that is, the survival probability of SoS solely depends on S_{-i}. Under the statistical independence of failures of S_i and S_{-i}, we have $C_{-i}\left(P_i\right) = 1 - P_i$, since the failure probability of S_i does not depend on that of S_{-i}. Consequently we have $P_S = P_i P_{-i}$. In a simple cloud infrastructure with N_S servers where the fiber connections are represented by system S_F, we have $P_S = 1 - N_S(1 - P_F)/K$, where K is a normalization constant. In this case, we have $C_F = N_S/K$, which shows that the fiber failure rate is amplified by N_S in rendering the servers unavailable.

We now consider that the effects of reinforcements and attacks can be separated at the system level such that (i) $\frac{\partial P_{-i}}{\partial x_i} \approx 0$, which indicates that reinforcing S_i does not directly impact the survival probability of the rest of SoS, and (ii) $\frac{\partial P_i}{\partial x_j} \approx 0$ for $j \neq i$, 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 3.2: For P_S in Condition 3.1, we have for $i = 1, 2, \ldots, N$, $j = 1, 2, \ldots, N$, $j \neq i$,

$$\frac{\partial P_S}{\partial x_i} \approx \left[1 + (1 - P_{-i})\frac{\partial C_{-i}}{\partial P_i}\right]\frac{\partial P_i}{\partial x_i}$$

$$\frac{\partial P_S}{\partial x_j} \approx \left[1 - C_{-i}(P_i) + (1 - P_{-i})\frac{\partial C_{-i}}{\partial P_{-i}}\right]\frac{\partial P_{-i}}{\partial x_j}$$

for the provider. □

A special class called OR systems corresponds to zero correlations such that $P_{\bar{i}\cup\overline{-i}} = P_{\bar{i}} + P_{\overline{-i}}$ or equivalently $P_{\bar{i}\cap\overline{-i}} = 0$. Thus, we have $P_S = P_{i,-i} = P_i + P_{-i} - 1$, $C_i = 0$, and $C_{-i} = 0$. These systems represent some of the simplest systems [20] to analyze due to the absence of correlations as will be shown in Section IV-A.

A. *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 [22].

Condition 3.3: 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 $i = 1, 2, \ldots, N$. □

We now illustrate two cases for which the above condition is satisfied.

(a) *Statistically Independent Component Failures:* 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 $P_i = p_{i|R}^{x_i} p_{i|N}^{N_i - x_i}$ [22], which in turn leads to

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

(b) *Contest Survival Functions:* The contest survival functions are to express P_i in [11] such that $P_i = \frac{\xi + x_i}{\xi + x_i + y_i}$, which in turn leads to

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

IV. Game Theoretic Formulation

The provider's objective is to make the infrastructure resilient by reinforcing x_i components of S_i and minimizing the corresponding disutility function. Similarly, the attacker's objective is to disrupt the infrastructure by attacking y_i components of S_i and minimizing the corresponding disutility function. NE conditions are derived by equating the corresponding derivatives of disutility functions to zero, which yields

$$\frac{\partial U_D}{\partial x_i} = \left(G_D\frac{\partial F_{D,G}}{\partial P_S} + L_D\frac{\partial F_{D,L}}{\partial P_S}\right)\frac{\partial P_S}{\partial x_i} + F_{D,G}\frac{\partial G_D}{\partial x_i} + F_{D,L}\frac{\partial L_D}{\partial x_i} = 0$$

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

$$L^D_{G,L} = G_D\frac{\partial F_{D,G}}{\partial P_S} + L_D\frac{\partial F_{D,L}}{\partial P_S}$$

as the *composite gain-cost* term, and

$$F^{D,i}_{G,L} = F_{D,G}\frac{\partial G_D}{\partial x_i} + F_{D,L}\frac{\partial L_D}{\partial x_i}$$

as the *gain-cost gradient* with respect to x_i, $i = 1, 2, \ldots, N$. Hence, at NE we have the following simplified condition

$$\frac{\partial P_S}{\partial x_i} = -\frac{F_{G,L}^{D,i}}{L_{G,L}^{D}}.$$

For the attacker, we similarly obtain

$$\frac{\partial U_A}{\partial y_i} = \left(G_A \frac{\partial F_{A,G}}{\partial P_S} + L_A \frac{\partial F_{A,L}}{\partial P_S} \right) \frac{\partial P_S}{\partial y_i} + F_{A,G} \frac{\partial G_A}{\partial y_i} + F_{A,L} \frac{\partial L_A}{\partial y_i} = 0$$

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

A. OR Systems

The OR systems [22] constitute a SoS sub-class where simultaneous failures of two or more systems is extremely unlikely, namely, their probability is zero. These systems are simpler to analyze due to the absence of system-level correlation terms, and indeed an estimate of P_i can be derived as a simple ratio of gain-cost gradient and system multiplier function Λ_i. Using $P_S = P_i + P_{-i} - 1$, we obtain

$$\frac{\partial P_i}{\partial x_i} = -\frac{F_{G,L}^{D,i}}{L_{G,L}^{D}} = -\Theta_i \left(x_1, \ldots, x_N, y_1, \ldots, y_N \right),$$

where $\Theta_i\left(\cdot\right)$ is called the *scaled gain-cost gradients* of system S_i. Then, Condition 3.3 provides us an estimate for the survival probability of S_i as the ratio of scaled gain-cost gradient and system multiplier function given by

$$\tilde{P}_{i;D}\left(x_1, \ldots, x_N, y_1, \ldots, y_N\right) = -\frac{\Theta_i \left(x_1, \ldots, x_N, y_1, \ldots, y_N\right)}{\Lambda_i(x_1, \ldots, x_N, y_1, \ldots, y_N)},$$

for $i = 1, 2, \ldots, N$. These estimates for individual systems depend mainly on the corresponding scaled gain-cost gradients, and thus represent a “separation” of the individual systems at this level. In this sense, OR systems constitute an important analytical case wherein the correlations between the individual systems may be ignored. In addition, these estimates provide the sensitivity information of the survival probabilities of the individual systems with respect to various quantities of S_i. In particular, the survival probability estimate $\tilde{P}_{i;D}$ is proportional to the corresponding weighted cost and reward functions and inversely proportional to their weighted derivatives. This seemingly counter-intuitive trend applies only to the set of Nash equilibria and not to the overall system behavior. In the rest of the paper, we denote $\Lambda_i\left(x_1, \ldots, x_N, y_i, \ldots, y_N\right)$ and $\Theta_i\left(x_1, \ldots, x_N, y_i, \ldots, y_N\right)$, by Λ_i and Θ_i, respectively, to simplify the notation.

B. NE Sensitivity Functions

We now derive estimates for P_i and 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: Aggregate Correlation Function: Under Conditions 3.1, 3.2, and 3.3, an estimate of the survival probability of rest of the infrastructure S_{-i}, for

$$\hat{P}_{-i;D}\left(x_1, \ldots, x_N, y_1, \ldots, y_N\right) = \frac{1 - C_{-i}\left(\hat{P}_{i;D}\right) + \frac{\partial C_{-i}}{\partial P_{-i}}}{2\frac{\partial C_{-i}}{\partial P_{-i}}} \pm \sqrt{\left(\frac{1 - C_{-i}\left(\hat{P}_{i;D}\right) + \frac{\partial C_{-i}}{\partial P_{-i}}}{2\frac{\partial C_{-i}}{\partial P_{-i}}}\right)^2 + \frac{\Theta_j}{\Lambda_{-i}\frac{\partial C_{-i}}{\partial P_{-i}}}},$$

and, for $\frac{\partial C_{-i}}{\partial P_{-i}} = 0$, is

$$\hat{P}_{-i;D}\left(x_1, \ldots, x_N, y_1, \ldots, y_N\right) = -\frac{\Theta_j}{\Lambda_{-i}\left[1 - C_{-i}\left(P_i\right)\right]}.$$

An estimate of the survival probability of system S_i is

$$\hat{P}_{i;D}\left(x_1, \ldots, x_N, y_1, \ldots, y_N\right) = -\frac{\Theta_i}{\Lambda_i\left[1 + (1 - \hat{P}_{-i;D})\frac{\partial C_{-i}}{\partial P_i}\right]}.$$

Proof: At NE, we have $\frac{\partial P_S}{\partial x_i} = -\Theta_i$ and $\frac{\partial P_S}{\partial x_j} = -\Theta_j$. By using the formulae in Condition 3.2, we have

$$\left[1 + (1 - P_{-i})\frac{\partial C_{-i}}{\partial P_i}\right]\frac{\partial P_i}{\partial x_i} = -\Theta_i$$

$$\left[1 - C_{-i}(P_i) + (1 - P_{-i})\frac{\partial C_{-i}}{\partial P_{-i}}\right]\frac{\partial P_{-i}}{\partial x_j} = -\Theta_j.$$

We now substitute expressions for $\frac{\partial P_i}{\partial x_i}$ and $\frac{\partial P_{-i}}{\partial x_j}$ based on Condition 3.3, and obtain the system of equations:

$$\left[1 + (1 - P_{-i})\frac{\partial C_{-i}}{\partial P_i}\right] P_i = -\frac{\Theta_i}{\Lambda_i} \tag{1}$$

$$\left[1 - C_{-i}(P_i) + (1 - P_{-i})\frac{\partial C_{-i}}{\partial P_{-i}}\right] P_{-i} = -\frac{\Theta_j}{\Lambda_{-i}}. \tag{2}$$

The expression for $\hat{P}_{-i;D}$ is obtained by solving for P_{-i} using quadratic Equation 2, and the expression for $\hat{P}_{i;D}$ follows from quadratic Equation 1. □

The estimates $\hat{P}_{-i;D}$ and $\hat{P}_{i;D}$ 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 and P_{-i} to the aggregate correlation function C_{-i} between them. In these estimates, however, the quantities related to S_i are essentially captured by the ratios $\frac{\Theta_j}{\Lambda_{-i}}$ and $\frac{\Theta_i}{\Lambda_i}$, which do not involve the aggregate correlation function. In fact, the dependence on the correlation function can be discussed separately from these ratios.

As indicated above, there are significant system-level interactions reflected in both $\hat{P}_{-i;D}$ and $\hat{P}_{i;D}$ compared to OR systems. In particular, $\hat{P}_{-i;D}$ depends on both $C_{-i}(\cdot)$ and its partial derivative with respect to P_{-i}; while an increase in the former leads to a decrease in $\hat{P}_{-i;D}$, the effect of the latter depends on its sign and it can in some cases

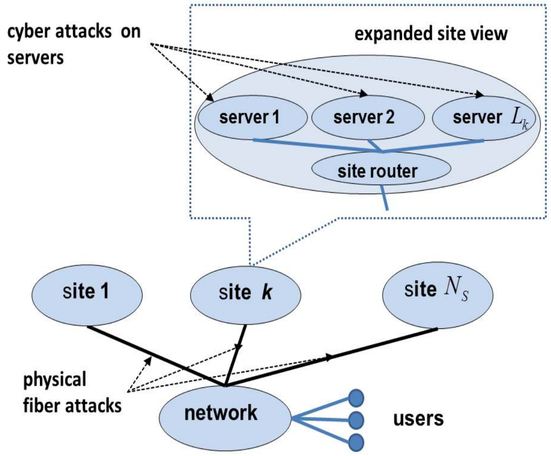

Fig. 1. Cloud computing infrastructure with N_S sites.

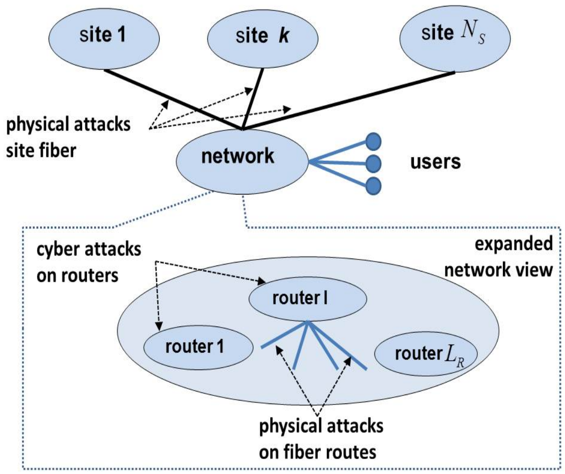

Fig. 2. Network of cloud computing infrastructure.

mitigate the decrease due to the former. Also $\hat{P}_{-i;D}$ depends on the partial derivative of L_D with respect to x_j multiplied by $(1-P_S)$, and this multiplication factor is not present in similar expressions derived for sum-form utilities [20]. It also depends on Θ_j (which involves the cost factor L_D and its derivative) and Λ_{-i} as expected. Its dependence on P_i is through the failure correlation function $C_{-i}(P_i)$. The qualitative behavior of $\hat{P}_{i;D}$ is quite similar with respect to L_D in Θ_i. And, they both are affected by Λ_{-i} and Λ_i, and each of them in turn depends on the number of component attacks and reinforcements of system S_i. Thus, the estimates $\hat{P}_{-i;D}$ and $\hat{P}_{i;D}$ reflect the system-level correlations between S_{-i} and S_i explicitly through $C_{-i}(P_i)$ term; they also represent component-level correlations indirectly through Λ_{-i} and Λ_i terms.

V. Distributed Cloud Computing Infrastructure

A distributed cloud computing infrastructure consists of N_S sites, with L_k servers at site k, $k=1,2,\ldots,N_S$ as shown in Figure 1. These sites are connected over a communication network wherein each router manages L_N connections as shown in Figure 2. Servers and routers can be brought down by cyber attacks, and the communication fibers that connect server sites to routers may be physically cut. To reinforce the components of this infrastructure, servers and routers may be replicated, and redundant fiber lines may be installed.

This infrastructure is modeled by SoS consisting of $2N_S+2$ systems where $S_{(k,c)}$ and $S_{(k,p)}$ represent the cyber and physical models of server site k, and $S_{(N_S+1,c)}$ and $S_{(N_S+1,p)}$ represent the cyber and physical models of the communications network as illustrated in Figure 2. Thus, in terms of original indices, we have:

(i) $S_l = S_{(l,c)}$, for $l=1,2,\ldots,N_S$, $S_{N_S+1}=S_{(N_S+1,c)}$,
(ii) $S_{N_S+1+l}=S_{(l,p)}$, for $l=1,2,\ldots,N_S$, and
(iii) $S_{2N_S+2}=S_{(N_S+1,p)}$.

The relationships between the aggregate correlation functions can be captured as follows (as described in [20]). For the communications network, we have

$$C_{(N_S+1,c)} = L_N C_{(N_S+1,p)}$$

which reflects that a router attack will disrupt all its L_N connections. For the sites, we have the opposite given by

$$C_{(k,p)} = L_k C_{(k,c)}$$

which indicates that at site k the fiber disruption will disconnect all its servers. This multiplicative effect carries over to partial differentials since

$$\frac{\partial C_{(k,p)}}{\partial P_{(k,p)}} = L_k \frac{\partial C_{(k,c)}}{\partial P_{(k,p)}} \quad \text{and} \quad \frac{\partial C_{(k,p)}}{\partial P_{(k,c)}} = L_k \frac{\partial C_{(k,c)}}{\partial P_{(k,c)}}$$

for $k=1,2,\ldots,N_S$, and $L_{N_S+1}=1/L_N$. Based on Theorem 4.1, this multiplier effect in partial differentials will be reflected in $\hat{P}_{(k,p);D}$ and $\hat{P}_{-(k,p);D}$ in addition to correlations.

For illustration, we now consider that the attacker and provider choose components to attack and protect, respectively, according to the uniform distribution. Then, corresponding to the site cyber models $S_{(k,c)}$, $k=1,2,\ldots,N_S$, there are $[y_{(k,p)}-x_{(k,p)}]_+$ non-reinforced fiber connections, where $[x]_+=x$ for $x>0$, and $[x]_+=0$ otherwise. Then, for cyber model $S_{(k,c)}$ of site k, $k=1,\ldots,N_S$, we have

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

which interestingly does not depend on $x_{(k,c)}$. Since the term $\Lambda_{(k,c)}$ appears in the denominator, $\hat{P}_{(k,c);D}$ in Theorem 4.1 decreases with the number of cyber attacks $y_{(k,c)}$, and increases with $[y_{(k,p)}-x_{(k,p)}]_+$ which is the number of physical attacks exceeding the reinforcements. The latter condition may appear counter-intuitive at the surface but note that it only characterizes the states that satisfy NE conditions. An analogous dependence of $\hat{P}_{-i;D}=\hat{P}_{-(k,c);D}$ and $\hat{P}_{j;D}=\hat{P}_{(k,p);D}$ on the parameters $x_{(k,c)}$, $x_{(k,p)}$, $y_{(k,c)}$, and $y_{(k,p)}$ (shown in Theorem 4.1) is less direct since $\Lambda_{-(k,c)}$ and $\Lambda_{(k,p)}$, respectively, appear inside the square root but is qualitatively somewhat similar since they appear in the denominator.

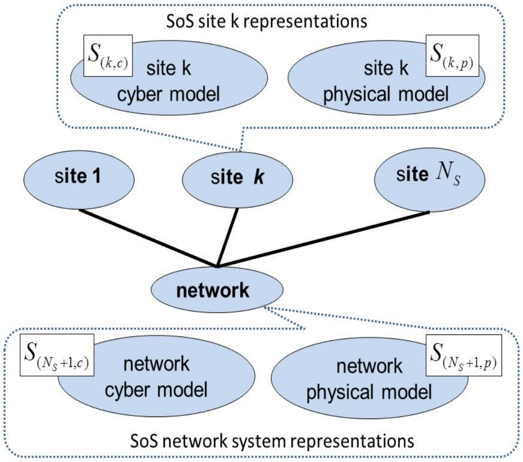

Fig. 3. SoS representation of cloud computing infrastructure.

VI. Conclusions

A class of system of systems each with discrete cyber and physical components are studied under the general disutility functions. The components of a system can be disrupted directly or indirectly by either a cyber or physical attack. They can be reinforced against such attacks by explicitly taking into account the correlations between the systems and also between the components within individual systems. These reinforcements entail certain costs which should be weighted against their benefits.

By formulating a game between an infrastructure provider and attacker, we derived Nash Equilibrium conditions in terms of the partial derivatives of cost terms, failure correlation functions and survival probabilities of component systems and their partial derivatives. We then estimated the sensitivity functions that indicate the dependence of the infrastructure survival probability on these quantities. We applied this approach to models of cloud computing infrastructures. These results extend previous results on interconnected systems [10], [11] and cyber-physical infrastructures [22] by using the general disutility functions, with the sum-form utility functions [20] and the product-form disutility functions [21] as specific examples. These results enable us to derive cost-centric strategies using a simple model of cloud computing infrastructures.

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. 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 infrastructures, 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 the 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] D. Fudenberg and J. Tirole. *Game Theory*. MIT Press, 2003.

[9] 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.

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

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

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

[13] 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.

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

[15] 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.

[16] 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.

[17] J. Moteff and P. Parfomak. Critical infrastructure and key assets: definition and identification. DTIC Document, 2004.

[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, 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.