sensors

MDPI

Article

Defense Strategies for Asymmetric Networked Systems with Discrete Components

Nageswara S. V. Rao [1,*,†], Chris Y. T. Ma [2,†], Kjell Hausken [3,†], Fei He [4,†], David K. Y. Yau [5,†] and Jun Zhuang [6,†]

[1] Computational Sciences and Engineering Division, Oak Ridge National Laboratory, Oak Ridge, TN 37831, USA
[2] Hang Seng Management College, Hong Kong; chris.ytma@gmail.com
[3] Faculty of Social Sciences, University of Stavanger, 4036 Stavanger, Norway; kjell.hausken@uis.no
[4] Department of Mechanical and Industrial Engineering, Texas A&M University, Kingsville, TX 78363, USA; fei.he@tamuk.edu
[5] Information Systems Technology and Design Clusteer, Singapore University of Technology and Design, Singapore 487372, Singapore; david.ky.yau@gmail.com
[6] Department of Industrial and Systems Engineering, University at Buffalo, Buffalo, NY 14260, USA; jzhuang@buffalo.edu
* Correspondence: raons@ornl.gov; Tel.: +1-865-574-7517
† These authors contributed equally to this work.

Received: 15 February 2018; Accepted: 26 April 2018; Published: 3 May 2018

Abstract: We consider infrastructures consisting of a network of systems, each composed of discrete components. The network provides the vital connectivity between the systems and hence plays a critical, asymmetric role in the infrastructure operations. The individual components of the systems can be attacked by cyber and physical means and can be appropriately reinforced to withstand these attacks. We formulate the problem of ensuring the infrastructure performance as a game between an attacker and a provider, who choose the numbers of the components of the systems and network to attack and reinforce, respectively. The costs and benefits of attacks and reinforcements are characterized using the sum-form, product-form and composite utility functions, each composed of a survival probability term and a component cost term. We present a two-level characterization of the correlations within the infrastructure: (i) the aggregate failure correlation function specifies the infrastructure failure probability given the failure of an individual system or network, and (ii) the survival probabilities of the systems and network satisfy first-order differential conditions that capture the component-level correlations using multiplier functions. We derive Nash equilibrium conditions that provide expressions for individual system survival probabilities and also the expected infrastructure capacity specified by the total number of operational components. We apply these results to derive and analyze defense strategies for distributed cloud computing infrastructures using cyber-physical models.

Keywords: networked systems; cyber-physical infrastructures; aggregated correlation functions; sum-form, product-form and composite utility functions

1. Introduction

Infrastructures for cloud computing, science experiments and computations and smart energy grid consist of complex, geographically-dispersed systems that are connected over long-haul networks. In these infrastructures, the communications network plays a critical, asymmetric role of providing the vital connectivity between the systems such as cloud computing sites, or supercomputers, or energy distribution centers. Network failures render the individual systems unreachable and in extreme cases can render the entire infrastructure unavailable. Such an infrastructure is represented by its constituent systems, S_i, $i = 1, 2, \ldots, N$, and the network connecting them is represented as a separate system S_{N+1}. The individual systems themselves are complex, consisting of several discrete cyber and physical components, which must be operational and connected to the network. The individual components of S_i may be disabled or disconnected, and S_i as a system may be disconnected, by cyber and physical attacks on the components. We formulate the problem of ensuring the infrastructure performance as a game between an attacker that launches cyber or physical attacks on the components and a provider that reinforces them to withstand the attacks. Since both attacks and reinforcements incur costs, the two players both weight the costs with expected benefits by minimizing utility functions. We derive Nash Equilibrium (NE) conditions that provide expressions for individual system survival probabilities and also the expected capacity specified by the total number of operational components. This paper extends and presents a unified view of the partial results presented in earlier conference papers on sum- and product-form utilities [1], composite utilities [2,3] and multi-site cloud infrastructures [4].

The components can be reinforced to survive direct attacks, but they can still be unavailable due to attacks on other components. For example, a super computer at a site may be hardened against cyber attacks, but can still be made unavailable by cutting fiber connections to the site. On the other hand, we consider that non-reinforced cyber and physical components will be disabled by direct cyber and physical attacks, respectively. Furthermore, in addition to within system S_i, the effects of attacks on its components may propagate to components of other systems S_j, $j \neq i$. Thus, both the correlations between components within individual systems and those between systems represent the propagation of disruptions across the infrastructure. The infrastructure provider is tasked with developing strategies to choose a number of components of each system to reinforce against the attacks by taking into account both types of correlations.

Let n_i denote the number of components of S_i, $i = 1, 2, \ldots, N+1$, of which y_i and x_i denote the number of components attacked and reinforced, respectively. Let P_i be the survival probability of S_i and P_I be the survival probability of the entire infrastructure. Furthermore, let S_{-i} denote the infrastructure without S_i and P_{-i} be its survival probability. The relative importance of S_i is captured by the aggregate failure correlation function C_i given by the failure probability of S_{-i} given the failure of S_i. Under the asymmetric network conditions, the specific role of the network is specified by two conditions: (a) $C_{N+1} = 1$ indicates that network failure will disrupt the entire infrastructure; and (b) $C_i = 0$, for $i = 1, 2, \ldots, N$, indicates that disruptions of individual systems are uncorrelated. The correlations between components of individual systems are captured by simple first-order differential conditions on P_i using the system multiplier functions that capture correlations within systems and also abstract the effects of system-level parameters [5]. This two-level characterization helps to conceptualize the basic correlations in infrastructures, such as cloud computing and smart grid infrastructures and provides insights into the needed defense strategies by naturally "separating" the system-level and component-level aspects.

A game between an attacker and a provider involves balancing 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, with the survival probability of the infrastructure. We consider that the provider minimizes the composite utility function given by:

$$\begin{aligned} U_D\,(x_1, \ldots, x_{N+1}, y_1, \ldots, y_{N+1}) = {} & F_{D,G}(x_1, \ldots, x_{N+1}, y_1, \ldots, y_{N+1}) G_D(x_1, \ldots, x_{N+1}, y_1, \ldots, y_{N+1}) \\ & + F_{D,L}(x_1, \ldots, x_{N+1}, y_1, \ldots, y_{N+1}) L_D(x_1, \ldots, x_{N+1}) \end{aligned}$$

where the first product term corresponds to the reward and the second product term corresponds to the cost. Within the product terms, $F_{D,G}$ and $F_{D,L}$ are the reward and cost multipliers, respectively, of the provider, and G_D and L_D represent the reward and cost terms, respectively, of keeping the infrastructure operational. Similarly, we consider that the attacker minimizes:

$$\begin{aligned} U_A\,(x_1,\ldots,x_{N+1},y_1,\ldots,y_{N+1}) = {} & F_{A,G}(x_1,\ldots,x_{N+1},y_1,\ldots,y_{N+1})G_A(x_1,\ldots,x_{N+1},y_1,\ldots,y_{N+1}) \\ & + F_{A,L}(x_1,\ldots,x_{N+1},y_1,\ldots,y_{N+1})L_A(y_1,\ldots,y_{N+1}) \end{aligned}$$

where $F_{A,G}$ and $F_{A,L}$ are the reward and cost multipliers, respectively, of the attacker, and G_A and L_A represent the reward and cost terms of disrupting the infrastructure operation, respectively. The expected capacity of the infrastructure is the expected number of available components, given by:

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

which reflects the part of the infrastructure that survives the attacks. In the example of the cloud infrastructure, it represents the number of operational servers that are available to users on average.

The composite utility function can be specialized to obtain sum-form and product-form utilities by using appropriate terms, as summarized in Table 1, and their choice represents different values in keeping the infrastructure operational:

(a) The sum-form utility function is given by:

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

which will be minimized by the provider. The scalar $g_D \geq 0$ represents the benefit of keeping the infrastructure operational such as income from an operational cloud computing infrastructure. Thus, the sum-form represents a weak coupling between gain and cost terms, since the effect of their minimization on the utility function is independent. For a provider, this form is used when explicit "gain" in keeping the infrastructure up can be identified and balanced against the cost.

(b) The product-form utility function is given by:

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

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 fails. Thus, the product-form represents a strong coupling between probability and cost terms, since the effect of minimization of one term gets multiplied by the other. This utility is used when the main goal of the provider is to keep the infrastructure up with the cost incurred, since there is no explicit "gain" term.

Table 1. Gain and cost terms and their multipliers for sum-form and product-form utilities of the provider.

	$F_{D,G}$	G_D	$F_{D,L}$	L_D
sum-form: U_{D+}	$[1 - P_I]$	g_D	1	L_D
product-form: $U_{D\times}$	0	0	$[1 - P_I]$	L_D

The Nash Equilibrium (NE) conditions based on the utility functions can used to estimate x_i's for the provider using various methods [6,7]. Our objective in this paper is to show that critical insights can be gained by deriving estimates of system survival probabilities and expected capacity explicitly in terms of various correlations, without relying on explicit solutions for x_i's. The differences in the goals of sum- and product-form utilities lead to qualitatively different defense strategies, which are derived separately in earlier works, and the corresponding expressions for the survival probabilities that are structurally different [5,8]. We show that under the asymmetric network conditions, NE conditions of this game lead to expressions for P_i's and N_I with the same structure. In particular, the estimates of P_i for sum-form and product-form utilities have the same expression in Theorem 3 except for one term, given by $\xi_i^{+} = \frac{1}{g_D}\frac{\partial L_D}{\partial x_i}$ and $\xi_i^{\times} = (1-P_I)\frac{\partial \ln L_D}{\partial x_i} = \frac{(1-P_I)}{L_D}\frac{\partial L_D}{\partial x_i}$. 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:

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

for $0 < P_I < 1$, which is an increasing function in both P_I and L_D; or, equivalently, we have, $P_I = 1 - L_D/g_D$. This similarity is striking since the sum-form and product-form utilities represent two quite different objectives.

The composite utility functions lead to simple expressions for P_i, $i = 1,2,\ldots,N$, and N_I at NE, which subsume the above cases. In general, the dependence of P_i on cost terms and aggregate correlation functions, as well as their partial derivatives, is presented in a compact form by using the composite gain-cost and composite multiplier terms (defined in Section 4). The expected capacity at NE is expressed in terms of cost term L_D and its derivative, the aggregate correlation functions C_i, $i = 1,2\ldots,N+1$, and the system multiplier functions, Λ_i, $i = 1,2\ldots,N+1$ (defined in Section 3.2). The expression provides critical information on the dependence of the expected capacity on system parameters, in particular C_i and Λ_i, and utility functions. Furthermore, by decomposing the system models into sub-models, such as cyber and physical sub-models, finer relationships can be inferred between system parameters, such as refined versions of C_i and Λ_i, and the expected capacity. We apply these results to a simplified model of cloud computing infrastructure with multiple server sites connected over a communications network.

The organization of this paper is as follows. We describe related work in Section 2. In Section 3, we describe the infrastructure model along with the aggregate correlation function and differential conditions on system survival probabilities. We present our game-theoretic formulation using sum-form, product-form and composite utility functions in Section 4 and derive NE conditions and estimates for the system survival probabilities and expected capacity. We apply the analytical results to a model of cloud computing infrastructure in Section 5. We present conclusions in Section 6.

2. Related Work

Critical infrastructures of power grids, cloud computing and transportation systems provide vital public and private services [9,10]. They depend on complex communications networks that connect the constituent systems, which by themselves consist of many disparate cyber and physical components [10]. The communications network plays a very critical role in these infrastructures [11], in some ways more so than the constituent systems, and its failure can significantly degrade the entire infrastructure [12,13]. 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 [14–16], which attempt to ensure continued infrastructure operations in the presence of evolving threats [17]. Partial differential equations and discrete component models have been used in several of these infrastructures to model the physical and cyber systems [18] 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 [19]; incomplete information games that account for partial knowledge about the system dynamics and attack models [20]; and multiple-target games that account for possibly competing objectives [21].

A comprehensive review of the defense and attack models in various game-theoretic formulations has been presented in [22]. Recent interest in cyber and cyber-physical systems led to the application of game theory to a variety of cyber security scenarios [16,23] and, in particular, for securing cyber-physical networks [24] with applications to power grids [11,25–27].

The system availability, reliability and robustness aspects can be explicitly integrated into the game formulations [14] 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 [28]. 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 [29]. 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 [5,8,29] 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 [30], and their two-level correlations have been studied using the sum-form utility functions in [5] and the product-form utility functions in [8]. 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 utility, on the other hand, represents a cost-centric priority, wherein the expected cost is to be minimized. The sum-form utility function [5] and the product-form utility function [8] 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 [8]. 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. These two utility functions are unified in [2], and the sum-form utility function has been studied under the asymmetric role of the communications network in [1].

The infrastructures for smart energy grids, cloud computing and intelligent transportation systems are composed of complex constituent systems that rely on communications networks. For wide-area operations, these networks play a critical asymmetric role of providing the vital connectivity needed for continued infrastructure operations. The asymmetric network correlations have been incorporated into multiple system infrastructures for sum-form and product-form utilities in [1], and these two works are unified in [3] by using the composite utility functions. The multi-site cloud computing infrastructure was discussed as an example for sum-form and product-form utility functions in [1] and composite utility functions in [3], wherein the network plays a critical asymmetric role. This model is further extended by including an HVAC system in [4], and also, additional details of NE conditions and capacity estimates are provided. In this paper, we consolidate these results and present a unified treatment of the sum-form, product-form and composite utilities under asymmetric network correlation conditions. For multi-site cloud infrastructures, we explicitly relate these utility functions and interpret the abstract definitions of correlation functions and system multiplier functions in terms of systems and their components.

3. Discrete System Models

We consider infrastructures with constituent systems consisting of discrete components [5,8] and connected over a communications network [1]. We first consider the correlations at the systems and network levels and then consider the correlations between the components of individual systems.

3.1. System-Level Correlations

The correlations between systems, including the network, in these infrastructures are characterized in terms of their survival probabilities as follows.

Condition 1. *Aggregate correlation function: Let C_i denote the failure probability of the rest of the infrastructure S_{-i} given the failure of S_i, and let C_{-i} denote the failure probability of S_i given the failure of S_{-i} such that:*

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

for $i = 1, \ldots, N + 1$. Then, the survival probability of the infrastructure is given by:

$$P_I = P_i + P_{-i} - 1 + C_i(1 - P_i) = P_i + P_{-i} - 1 + C_{-i}(1 - P_{-i})\,\square$$

The aggregate failure correlation function captures the interdependence of the 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 with 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 with the 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 the 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) ORsystems: The OR systems as modeled in [29] correspond to the special case $N = 2$ where the infrastructure consists of uncorrelated cyber and physical systems (denoted by $i = C$ and $-i = P$, respectively) that can be independently analyzed. For OR systems, the failure probabilities of S_i and S_{-i} are uncorrelated such that $C_i = C_{-i} = 0$, and hence, we have $P_{\bar{i}\cup\overline{-i}} = P_{\bar{i}} + P_{\overline{-i}}$ or equivalently $P_{\bar{i}\cap\overline{-i}} = 0$. Thus, we have $P_I = P_i + P_{-i} - 1$. We apply this condition next in Condition 2 for N systems considered in this paper.

The important asymmetric role of the communications network is characterized using the following condition.

Condition 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 $C_i = 0$, $i = 1, 2, \ldots, N$.* □

Part (i) of Condition 2 leads to $P_I = P_{-(N+1)}$, which indicates the role of the rest of infrastructure $S_{-(N+1)}$ without the network; namely, its survival probability is the same as that for server sites together. Part (ii) of Condition 2 leads to $P_I = P_i + P_{-i} - 1$, $i = 1, 2, \ldots, N$, which linearly depends on each of the failure probabilities of the constituent system S_i and the rest of infrastructure S_{-i}. It is important to note that although there are direct correlations between the site failures zero (Part (ii) above), these site failures are still indirectly related through the network. In particular, the failures of S_i and S_j, which are parts of $S_{-(N+1)}$, are correlated with the network via C_{N+1}; for example, they both become simultaneously unavailable when the wide-area network fails.

The effects of reinforcements and attacks on host sites and wide-area networks can be separated using the following two conditions:

(i) the first condition, $\frac{\partial P_{-i}}{\partial x_i} = 0$ for $i = 1, 2, \ldots, N$, indicates that reinforcing the server site S_i does not directly impact the survival probability of other sites or networks; and

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

While the reinforcements to individual server sites or networks are not directly reflected in other systems, their failures may still be correlated due to the underlying system structures as reflected in the aggregated correlation function of the network C_{N+1}. These system-level considerations for the provider are captured by the following condition, which is obtained by differentiating P_I in Condition 1 with respect to x_i and ignoring the terms corresponding to Parts (i) and (ii) above.

Condition 3. *De-coupled reinforcement effects: For P_I in Condition 1, we have for $i = 1, 2, \ldots, N+1$,*

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

for the provider. □

The condition captures the effect on the increment in P_I as a result of the change in the number of reinforced components x_i of S_i. It is the sum of (i) the increment in individual system survival probability P_i weighted by "non-correlation" term $(1 - C_i)$ and (ii) the increment in correlation C_i weighted by the failure probability $1 - P_i$ of S_i. For the sites S_i, $i = 1, 2, \ldots, N$, we have:

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

For the network S_{N+1}, we have:

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

Under Condition 2, C_i is constant, but its partial derivatives with respect to x_i could be non-zero, as other parameters change to keep it constant.

3.2. Component-Level Correlations

The system survival probabilities satisfy the following differential condition that specifies the correlations at the component level [5,31].

Condition 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:*

$$\frac{\partial P_i}{\partial x_i} = \Lambda_i(x_1, \ldots, x_{N+1}, y_1, \ldots, y_{N+1})P_i \qquad \text{and} \qquad \frac{\partial P_{-i}}{\partial x_i} = \Lambda_{-i}(x_1, \ldots, x_{N+1}, y_1, \ldots, y_{N+1})P_{-i}$$

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 $\Lambda_i < 1$. These system multiplier functions capture the underlying system structure including its parameters, in addition to the game variables x_i's and y_i's. For example, in the case of multi-site server infrastructure, Λ_i in Section 5.2 depends on the number of severs l_i at site i. This somewhat abstract condition enables us to capture such a structure in a generic manner and indeed is satisfied in two special cases studied extensively in the literature.

(a) Statistically independent components: The special case when component survival probabilities are statistically independent with and without reinforcements has been studied in [31]. Let $p_{i|R}$ and $p_{i|W}$ 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:

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

as in [31], or equivalently:

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

By differentiating the equation with respect to x_i, we obtain:

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

The condition for the faster than linear derivative is $\ln \left(\frac{p_{i|R}}{p_{i|W}} \right) > 1$ or equivalently $p_{i|R} > e p_{i|W}$, where e is the base of the natural logarithm. The condition that the survival probability of a reinforced component is higher than that of a non-reinforced component, but less than $e p_{i|W}$, namely, $e p_{i|W} > p_{i|R} > p_{i|W}$, corresponds to only the slower than linear derivative.

(b) Contest survival functions: The contest survival functions are to express P_i in [30] 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 the 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.

4. Game Theoretic Formulation

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

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

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

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

as the composite gain-cost term, wherein the gain G_D and cost L_D are "amplified" by the derivatives of their corresponding multiplier functions with respect to P_I. We then define:

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

as the composite multiplier term, wherein the gain multiplier $F_{D,G}$ and cost multiplier $F_{D,L}$ are "amplified" by the derivatives of their corresponding gain and cost terms with respect to x_i, $i = 1, 2, \ldots, N+1$, respectively. These two terms lead to the compact NE condition $\frac{\partial P_I}{\partial x_i} = -\frac{F_{G,L}^{D,i}}{L_{G,L}^{D}}$. These NE conditions can be used to solve for x_i's using available methods whose complexity depends on the details of gain and cost terms [14–16]. Indeed, different methods and trade-offs may be required to derive such solutions by exploiting the details of infrastructure [7]. We show in the next section that estimates for system survival probabilities and expected capacity can be obtained without explicitly solving for x_i's, and yet, they provide valuable qualitative insights about the infrastructure. Various terms of the composite utility function specialized to sum-form and product-form utilities are shown in Table 2, which are considered separately in Section 4.3.

Table 2. Gain and cost terms, their multipliers and other terms for sum-form and product-form utilities of the provider.

	$\boldsymbol{F_{D,G}}$	$\boldsymbol{G_D}$	$\boldsymbol{F_{D,L}}$	$\boldsymbol{L_D}$	$\boldsymbol{\frac{\partial F_{D,G}}{\partial P_I}}$	$\boldsymbol{\frac{\partial G_D}{\partial x_i}}$	$\boldsymbol{\frac{\partial F_{D,L}}{\partial P_I}}$	$\boldsymbol{L_{G,L}^{D}}$	$\boldsymbol{F_{G,L}^{D,i}}$
sum-form: U_{D+}	$[1-P_I]$	g_D	1	L_D	-1	0	0	$-g_D$	$\frac{\partial L_D}{\partial x_i}$
product-form: $U_{D\times}$	0	0	$[1-P_I]$	L_D	0	0	-1	$-L_D$	$[1-P_I]\,\frac{\partial L_D}{\partial x_i}$

4.1. OR Systems

The OR systems [31] constitute a sub-class of abstract infrastructures where simultaneous failures of two or more systems are extremely unlikely, namely their probability is zero. These abstract models are used to illustrate the simplifications that result from ignoring the correlations and are generally used for analysis purposes. Here, OR systems ignore the asymmetric role played by the communications network. These systems are simpler to analyze due to the absence of system-level correlation terms, and they serve as base study cases when the correlations can be ignored. Indeed, an estimate of P_i can be derived as a simple ratio of the 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 4 provides us an estimate for the survival probability of S_i as the ratio of the scaled gain-cost gradient and the 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 $\Lambda_i\,(x_1,\ldots,x_N,y_i,\ldots,y_N)$ and $\Theta_i\,(x_1,\ldots,x_N,y_i,\ldots,y_N)$, by Λ_i and Θ_i, respectively, to simplify the notation.

4.2. System Survival Probabilities and Expected Capacity

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

Theorem 1. *Survival probability estimates: Under Conditions 1, 3 and 4, estimates of the survival probability of system S_i, for $i = 1, 2, \ldots, N+1$, are given by:*

$$\hat{P}_{i;D} = \frac{\frac{\partial C_i}{\partial x_i} + \frac{F^{D,i}_{G,L}}{L^D_{G,L}}}{\frac{\partial C_i}{\partial x_i} - (1 - C_i)\Lambda_i}$$

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:

$$P_{-(N+1);D} = -\frac{1}{\Lambda_{-(N+1)}} \frac{F^{D,N+1}_{G,L}}{L^D_{G,L}}$$

Proof. Our proof is based on deriving NE conditions for the utility function. At NE, we have:

$$\frac{\partial P_I}{\partial x_i} = -\frac{F^{D,i}_{G,L}}{L^D_{G,L}}$$

Then, using the equation in Condition 3 and $\frac{\partial P_i}{\partial x_i} = \Lambda_i P_i$ from Condition 4, we have:

$$(1 - C_i)\Lambda_i P_{i;D} + (1 - P_{i;D})\frac{\partial C_i}{\partial x_i} = -\frac{F^{D,i}_{G,L}}{L^D_{G,L}} \tag{1}$$

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:

$$P_{i;D} = \frac{\frac{\partial C_i}{\partial x_i} + \frac{F^{D,i}_{G,L}}{L^D_{G,L}}}{\frac{\partial C_i}{\partial x_i} - (1 - C_i)\Lambda_i}$$

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 that 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 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, the NE condition is given by:

$$\frac{\partial P_I}{\partial x_{N+1}} = \frac{\partial P_{-(N+1);D}}{\partial x_{N+1}} = \Lambda_{-(N+1)} P_{-(N+1);D} = -\frac{F^{D,N+1}_{G,L}}{L^D_{G,L}}$$

which completes the proof. □

The system survival probability estimates $\hat{P}_{i;D}$ provide qualitative information about the effects of various parameters including aggregated correlation coefficient C_i, system multiplier functions Λ_i, composite gain-cost $L^D_{G,L}$ and composite multiplier $F^{D,i}_{G,L}$; note that the estimates may not necessarily lie within the range [0,1]. In particular, $\hat{P}_{i;D}$ (i) increases and decreases with $F^{D,i}_{G,L}$ and $L^D_{G,L}$, respectively, (ii) increases with Λ_i and (iii) depends both on C_i and its derivative for $i = 1, 2, \ldots, N$. For the network, $P_{-(N+1);D}$ is in a simpler form since $C_{N+1} = 1$.

We now consider that the asymmetric role played by the network described in Condition 2, namely its failure, renders entire infrastructure unavailable; also, failures of individual systems are uncorrelated with others. The following theorem provides a single, simplified expression for the expected capacity under these conditions.

Theorem 2. *Expected capacity under asymmetric network correlations: Under Conditions 1–4, the expected capacity is given by:*

$$N_I = \sum_{i=1}^{N} \left(-\frac{n_i}{\Lambda_i} \frac{F^{D,i}_{G,L}}{L^D_{G,L}} \right)$$

Proof. Under Part (ii) of Condition 2, Equation (1) in the proof of Theorem 1 simplifies to the equation:

$$\Lambda_i P_{i;D} = -\frac{F^{D,i}_{G,L}}{L^D_{G,L}}$$

for $i = 1, 2, \ldots, N$. Thus, we have $P_i = -\frac{1}{\Lambda_i} \frac{F^{D,i}_{G,L}}{L^D_{G,L}}$, which provides the expression for N_I. □

This condition indicates that lower $L^D_{G,L}$ and higher composite multiplier $F^{D,i}_{G,L}$ lead to lower expected capacity. Typically, the composite gain-cost $L^D_{G,L}$ is negative (e.g., $-g_D$ for sum-form) since it is minimized by the provider; thus, its lower value is more negative and has a higher magnitude. Furthermore, larger values of Λ_i also lead to lower expected capacity. In particular, the condition $\Lambda_i > 1$, called the faster than linear growth of $\frac{\partial P_i}{\partial x_i}$, leads to lower expected capacity. This seems counter-intuitive since faster improvement in P_i due to the increase in x_i leads to lower expected capacity, but note that it only characterizes the states that satisfy NE conditions.

4.3. Sum-Form and Product-Form Utility Functions

The NE conditions for sum-form and product-form utilities are derived by equating the corresponding derivatives to zero, which yields the following conditions, respectively:

$$\frac{\partial U_{D+}}{\partial x_i} = \frac{\partial P_I}{\partial x_i} g_D - \frac{\partial L_D}{\partial x_i} = 0 \quad \text{and} \quad \frac{\partial U_{D\times}}{\partial x_i} = -\frac{\partial P_I}{\partial x_i} L_D + (1 - P_I) \frac{\partial L_D}{\partial x_i} = 0$$

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

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 3. *Under Conditions 1, 3 and 4, estimates of the survival probability of system S_i, for $i = 1, 2, \ldots, N + 1$, are 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:

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

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 the sum-form, we have:

$$\frac{\partial P_I}{\partial x_i} = \frac{1}{g_D}\frac{\partial L_D}{\partial x_i} = \xi_i^+$$

Then, using the equation in Condition 3 and $\frac{\partial P_i}{\partial x_i} = \Lambda_i P_i$ from Condition 4, we have:

$$(1-C_i)\Lambda_i P^+_{i;D} + (1-P^+_{i;D})\frac{\partial C_i}{\partial x_i} = \frac{1}{g_D}\frac{\partial L_D}{\partial x_i} \tag{2}$$

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:

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

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

$$\frac{\partial P_I}{\partial x_i} = (1-P_I)\frac{1}{L_D}\frac{\partial L_D}{\partial x_i} = (1-P_I)\frac{\partial \ln L_D}{\partial x_i} = \xi_i^\times \tag{3}$$

Then, using the equation in Condition 3 and $\frac{\partial P_i}{\partial x_i} = \Lambda_i P_i$ from Condition 4, we have:

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

Then, we have:

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

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 that 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 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, the NE condition for the sum-form is given by:

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

Similarly, for the product-form, we obtain,

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

which completes the proof. □

The estimates $\hat{P}_{i;D}$ above provide sensitivity information about the corresponding survival probabilities with respect to various parameters; note that 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_i^A, which is proportional to the derivative term $\frac{\partial L_D}{\partial x_i}$ in both cases. The main difference is that $\xi_i^\times$ is an increasing function of P_I, whereas ξ_i^+ does not depend on P_I. Furthermore, the dependence on L_D is different for these two terms. Since $\xi_i^+ = \frac{1}{g_D} \frac{\partial L_D}{\partial x_i}$ and $\xi_i^\times = (1 - P_I) \frac{1}{L_D} \frac{\partial L_D}{\partial x_i}$, the role of g_D in the former is played by $L_D/(1 - P_I)$ 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 network failure renders the entire infrastructure unavailable, and the failure of individual systems is uncorrelated with others given by Condition 2. The following theorem provides a single, simplified expression for the expected capacity under these conditions.

Theorem 4. *Asymmetric network correlations: Under Conditions 1–4, the expected capacity is given by:*

$$N_I^A = \sum_{i=1}^{N} \left(n_i \frac{\xi_i^A}{\Lambda_i} \right)$$

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

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

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

Proof. Under Part (ii) of Condition 2, Equations (2) and (3) in Theorem 3 simplify to the same equation $\Lambda_i P_{i;D}^A = \xi_i^A$ for $A = +, \times$ and $i = 1, 2, \ldots, N$. Thus, we have $P_i^A = \frac{\xi_i^A}{\Lambda_i}$, which provides the expression for N_I^A. □

For the sum-form,

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

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

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

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

The expressions of N_I for the composite utility are simpler due to the generality of the composite gain-cost and composite multiplier, which are complex by themselves in that the sum-form and product-form are subsumed by them as indicated in Table 1. Typically, the composite gain-cost $L^D_{G,L}$ is negative (e.g., $-g_D$ for the sum-form) since it is minimized by the provider; thus, its lower value is more negative and has a higher magnitude. Furthermore, larger values of Λ_i also lead to lower expected capacity. In particular, the condition $\Lambda_i > 1$, called the faster than linear growth of $\frac{\partial P_i}{\partial x_i}$, leads to lower expected capacity. This seems counter-intuitive since faster improvement in P_i due to the increase in x_i leads to lower expected capacity, but note that it only characterizes the states that satisfy NE conditions.

5. Multi-Site Server 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 by using separate cyber and physical models for each site in [2]. Here, we expand this model to incorporate both cyber and physical aspects of the HVAC of a site, namely its mobile phone app and cooling tower located outside the facility. The sites are connected over a wide-area network S_{N+1}, as shown in Figure 1. The components of the network include routers, each of which manages l_{N+1} connections as shown in Figure 2.

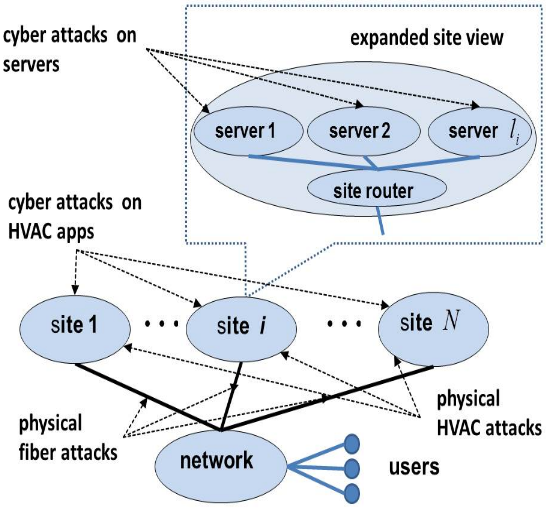

Figure 1. Cloud computing infrastructure with N server sites.

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 the servers are accessible to users. Meanwhile, routers are located at geographically-separated sites, and access to them is limited (to network administrators), so 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. Cutting the network fibers that connect server sites to routers will disconnect the entire site, making it inaccessible to the users. 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.

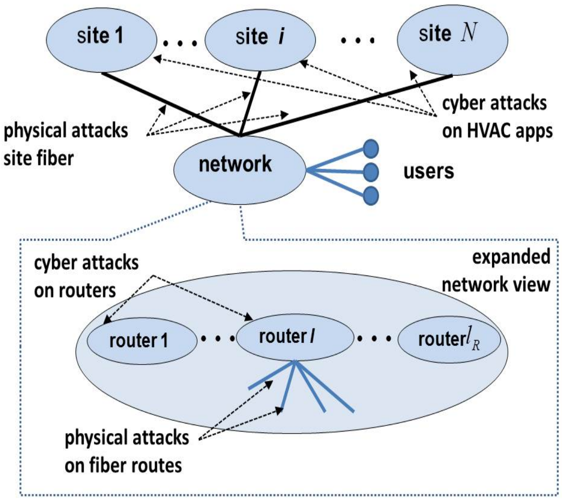

Figure 2. Network of a multi-site cloud server infrastructure.

5.1. System-Level Correlations

The cyber and physical aspects of a site S_i can be represented by using two finer sub-models $S_{(i,c)}$ and $S_{(i,p)}$ that correspond to the 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, respectively, as illustrated in Figure 3. Let $n_{(i,c)}$ and $n_{(i,p)}$ represent the cyber and physical components of S_i, which correspond to the number of components of $S_{(i,c)}$ and $S_{(i,p)}$, respectively, such that $n_i = n_{(i,c)} + n_{(i,p)}$. Let $x_{(i,c)}$ and $x_{(i,p)}$ denote the number of cyber and physical components that are reinforced, respectively, such that $x_i = x_{(i,c)} + x_{(i,p)}$. Similarly, $y_{(i,c)}$ and $y_{(i,p)}$ denote the number of cyber and physical components that are attacked, respectively, such that $y_i = y_{(i,c)} + y_{(i,p)}$. The relationships between these system-level models can be captured using refined versions of the aggregate correlation function as follows. For the wide-area 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 of its l_{N+1} connections, thereby illustrating the amplification effect of these cyber attacks. For the server sites, we have a similar effect due to physical fiber attacks denoted by label p_f reflected by:

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

which indicates that at site S_i, the fiber disruption will disconnect all of its l_i servers. Similarly, the cyber attack on the site's HVAC app denoted by label c_h leads to:

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

which indicates that at site S_i, the HVAC disruption will affect all of its l_i servers. In the limiting case, each component can be represented as a singleton sub-model $S_{i,j}$ such that $x_i = \sum_{j=1}^{n_i} x_{(i,j)}$ and

$y_i = \sum_{j=1}^{n_i} y_{(i,j)}$. Here, $x_{(i,j)} \in \{0,1\}$ and $y_{(i,j)} \in \{0,1\}$ indicate if the component represented by $S_{i,j}$ is reinforced and attacked, respectively.

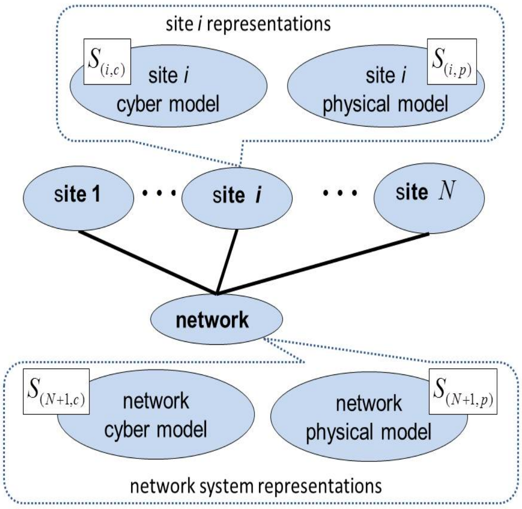

Figure 3. Representation of the cloud computing infrastructure.

5.2. Component-Level Correlations

We now consider a special case where the attacker and provider choose the components of a constituent system to attack and reinforce, respectively, according to a uniform distribution. 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 i as:

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

which reflects the additional lowering of the survival probability in inverse proportion to the level of cyber attack $y_{(i,c)}$. Under the independence of component attacks and reinforcements, the survival probability of the cyber sub-model $S_{(i,c)}$ is given by:

$$P_{(i,c)} = p_{(i,c)|R}^{x_{(i,c)}} p_{(i,c)|W}^{n_{(i,c)} - x_{(i,c)}} \tag{4}$$

which in turn provides:

$$\frac{\partial P_{(i,c)}}{\partial x_{(i,c)}} = P_{(i,c)} \ln \left(\frac{p_{(i,c)|R}}{p_{(i,c)|W}} \right)$$

Using the above formulae, for cyber model $S_{(i,c)}$ of site S_i, we have:

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

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

Under the statistical independence of cyber and physical attacks, for the cyber and physical sub-models, namely, $S_{(i,c)}$ and $S_{(i,p)}$, respectively, we have the following generalization of Equation (4):

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

or equivalently:

$$\ln P_i = n_{(i,c)} \ln p_{(i,c)|W} + x_{(i,c)} \ln\left(\frac{p_{(i,c)|R}}{p_{(i,c)|W}}\right) + n_{(i,p)} \ln p_{(i,p)|W} + x_{(i,p)} \ln\left(\frac{p_{(i,p)|R}}{p_{(i,p)|W}}\right)$$

By differentiating the equation with $x_{(i,c)}$, we obtain:

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

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 that the HVAC sub-model $S_{(i,h)}$ of site i is further decomposed into cyber and physical singleton sub-models represented by $S_{(i,c_h)}$ and $S_{(i,p_h)}$, respectively. Then, we have:

$$\Lambda_{(i,c_h)} = \ln\left(1 + \frac{y_{(i,c_h)}}{1 + l_i[y_{(i,c_h)} - x_{(i,c_h)}]_+}\right) \tag{5}$$

which corresponds to a cyber attack on and defense of the HVAC app. Similarly, we have:

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

which corresponds to a physical attack on and defense of the HVAC cooling tower.

5.3. Expected Capacity Estimates

We now consider the capacity of the infrastructure under x_i reinforcements and y_i attacks on components of S_i, which can be further partitioned into the corresponding values of sub-systems of S_i.

5.3.1. Sum-Form and Product-Form

Based on the estimates from Section 4.3, for the expected capacity N_I^A of the sub-models of S_i, the dependence on $y_{(i,c)}$ and $\left[y_{(i,p)} - x_{(i,p)}\right]_+$ is more direct, and it is qualitatively similar for both sum-form and product-form, since the term Λ_i appears in the denominator. Then, we obtain the following expected capacity estimates: for the sum-form,

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

and for the product form,

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

In both cases, the multipliers n_i, g_D and L_D are positive, and it is reasonable to assume the condition $\frac{\partial L_D}{\partial x_i} \geq 0$, as described above. Thus, the expected capacity decreases with the number of cyber attacks $y_{(i,c)}$. The opposite trend is true with respect to $\left[y_{(i,p)} - x_{(i,p)}\right]_+$, which implies no effect if the number of reinforced components is at least as large as the number of component attacks, and otherwise, the expected capacity increases with the difference. 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.

The term $\left(n_i \frac{\xi_i^A}{\Lambda_i}\right)$ that corresponds to site S_i can be further refined by decomposing into its sub-models, which provides insight into their individual effects. The impact of the HVAC control app at site i is reflected in its corresponding term:

$$\frac{\xi_i^A}{\ln\left(1 + \frac{y_{(i,c_h)}}{1+l_i[y_{(i,c_h)}-x_{(i,c_h)}]+}\right)}$$

obtained from Equation (5), which shows that reinforcing the app, that is $x_{(i,c_h)} = 1$, nullifies the amplification effect of l_i since $[y_{(i,c_h)} - x_{(i,c_h)}]+ = 0$ for both sum-form and product-form utility functions. Such an analysis can be carried out for other critical components of the sites to gain information on which components to reinforce for higher utility. In particular, reinforcing the site fiber routes will have a similar effect on nullification, but server reinforcements will have somewhat lesser impact.

5.3.2. Composite Utility Functions

We now obtain the following expected number of servers for the composite utility functions,

$$N_I = \sum_{i=1}^{N} \left(- \frac{n_i F_{G,L}^{D,i}}{L_{G,L}^{D} \ln\left(1 + \frac{y_{(i,c)}}{1+l_i\left[y_{(i,p)}-x_{(i,p)}\right]_+}\right)} \right)$$

In the equation, n_i is positive, and it is reasonable to assume that $-\frac{F_{G,L}^{D,i}}{L_{G,L}^{D}} \geq 0$, since $\frac{\partial P_I}{\partial x_i} = -\frac{F_{G,L}^{D,i}}{L_{G,L}^{D}}$ at NE, and the survival probability of entire infrastructure P_I does not decrease with x_i. Thus, the expected capacity decreases with $y_{(i,c)}$, and the opposite is true with respect to $\left[y_{(i,p)} - x_{(i,p)}\right]_+$, as discussed in the previous section. 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, also as in the previous section. As in sum-form and product-form utility functions, the term:

$$\left(-\frac{n_i}{\Lambda_i}\frac{F_{G,L}^{D,i}}{L_{G,L}^{D}}\right)$$

can be decomposed using sub-models of site i to assess the impacts of its parts, in particular its components. For the HVAC app at site i, we have the corresponding term:

$$\left(-\frac{F_{G,L}^{D,(i,c_h)}}{L_{G,L}^{D}\ln\left(1+\frac{y_{(i,c_h)}}{1+l_i\left[y_{(i,p_h)}-x_{(i,p_h)}\right]_+}\right)}\right)$$

which shows that reinforcing the HVAC app nullifies the amplification by factor l_i, even under the more general utility function since l_i does not appear in the dependent term $F_{G,L}^{D,(i,c_h)}$. Furthermore, such an analysis can be carried out for other components, and in a limiting case, each component can be modeled as a singleton sub-model, in which case their attack and reinforcement variables are Boolean.

The dependencies considered here for the sub-models are quite simple as a result of the statistical independence and uniform distributions of reinforcements and attacks. Even under such simple conditions, the detailed NE conditions are quite complex to characterize, but they do provide qualitative insights into the effects of underlying parameters.

6. Conclusions

We consider a class of infrastructures with multiple systems, wherein the communications network plays an asymmetric role by providing the critical connectivity between them. By utilizing correlations at the system- and component-level, we formulated the problem of ensuring the infrastructure survival as a game between an attacker and a provider, by using composite utility functions that generalize the sum-form and product-form utility functions. We derived Nash equilibrium conditions in terms of composite gain-cost and composite multiplier, which provide compact expressions for individual system survival probabilities and also the expected number of operational components. This paper presented a unified account of partial results that were separately developed for: sum-form utility functions [5] and under asymmetric network conditions [1]; product-form utility functions [8]; composite utility functions [2]; composite utility functions under asymmetric network conditions [3]; and detailed derivations for multi-site cloud server infrastructure [4]. These results extend previous results on interconnected systems [30,32] and cyber-physical infrastructures [31] by using the composite utility functions. We presented a comprehensive treatment of the three utility functions, including more illustrative details of the sum-form and product-form utility functions. For multi-site cloud infrastructures, we explicitly related the correlation functions and system multiplier functions to the infrastructure parameters, which in turn provided us insights into the estimates for system survival probabilities and the expected capacity. In particular, by employing sub-models of the sites, the effect of parts of the system on the expected capacity could be inferred by using the corresponding multiplier functions.

The formulation studied in this paper can be extended to include cases where targeted attacks and reinforcements of specific individual components are explicitly represented. The system models here incorporate the same level of detail in that they all consist of components, and it would be of future interest to incorporate varying levels of detail in them, for example by replacing components with the recursively-defined systems. The utility functions considered in this paper do not explicitly use the capacity term. Instead, they are driven by the infrastructure level considerations by using P_I, which in turn leads to expressions for the capacity that involve other terms that contribute to P_I. It is of future interest to compare this formulation to ones whose utility functions contain the expected capacity term in place of infrastructure survival probability terms. Another future direction is to consider the simultaneous cyber and physical attacks on multiple systems and components and sequential game formulations of this problem. Performance studies of our approach using more detailed models of cloud computing infrastructure, smart energy grid infrastructures and high-performance computing complexes would be of future interest.

Author Contributions: Conceptualization, N.R., K.H. and J.Z.; Methodology, N.R., and D.Y.; Formal Analysis, N.R., C.M. and F.H.; Investigation, N.R., C.M. and F.H.; Writing-Original Draft Preparation, N.R.; Writing-Review & Editing, C.M. and F.H.; Project Administration, N.R.; Funding Acquisition, N.R.

Acknowledgments: The authors thank the detailed and constructive comments of an anonymous reviewer that greatly improved the presentation of the results in this paper. 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 the U. S. Department of Defense, and performed at Oak Ridge National Laboratory managed by UT-Battelle, LLC, for the U.S. Department of Energy under Contract No. DE-AC05-00OR22725.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Rao, N.S.V.; Ma, C.Y.T.; Hausken, K.; He, F.; Yau, D.K.Y.; Zhuang, J. Game-Theoretic strategies for asymmetric networked systems. In Proceedings of the International Conference on Information Fusion, Xi'an, China, 10–13 July 2017.
2. Rao, N.S.V.; Imam, N.; Ma, C.Y.T.; Hausken, K.; He, F.; Zhuang, J. On defense strategies for system of systems using aggregated correlations. In Proceedings of the11th Annual IEEE International Systems Conference, Montreal, QC, Canada, 24–27 April 2017.
3. Rao, N.S.V.; Ma, C.Y.T.; Hausken, K.; He, F.; Yau, D.K.Y.; Zhuang, J. Defense strategies for asymmetric networked systems under composite utilities. In Proceedings of the IEEE International Conference on Multisensor Fusion and Integration for Intelligent Systems, Daegu, Korea, 16–18 November 2017.
4. Rao, N.S.V.; Ma, C.Y.T.; He, F. Defense strategies for multi-site cloud computing server infrastructures. In Proceedings of the International Conference on Distributed Computing and Networking, Varanasi, India, 4–7 January 2018.
5. Rao, N.S.V.; Ma, C.Y.T.; Hausken, K.; He, F.; Zhuang, J. Defense strategies for infrastructures with multiple systems of components. In Proceedings of the International Conference on Information Fusion, Heidelberg, Germany, 5–8 July 2016.
6. Fudenberg, D.; Tirole, J. *Game Theory*; MIT Press: Cambridge, MA, USA, 2003.
7. Rass, S.; König, S.; Schauer, S. On the Cost of Game Playing: How to Control the Expenses in Mixed Strategies. *Decision and Game Theory for Security*; Rass, S., An, B., Kiekintveld, C., Fang, F., Schauer, S., Eds.; Springer International Publishing: Cham, Switzerland, 2017; pp. 494–505.
8. Rao, N.S.V.; Ma, C.Y.T.; Hausken, K.; He, F.; Zhuang, J. Game-Theoretic strategies for systems of components using product-form utilities. In Proceedings of the IEEE International Conference on Multisensor Fusion and Integration for Intelligent Systems, Baden-Baden, Germany, 19–21 September 2016.
9. DHS. Critical Infrastructure Sectors. Available online: http://www.dhs.gov/critical-infrastructure-sectors. (accessed on 1 October 2015).
10. Lewis, T.G. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*; John Wiley & Sons: Hoboken, NJ, USA, 2014.
11. Chen, P.Y.; Cheng, S.M.; Chen, K.C. Smart attacks in smart grid communication networks. *IEEE Commun. Mag.* **2012**, *50*, 24–29. [CrossRef]
12. Brown, G.; Carlyle, M.; Salmeron, J.; Wood, K. Analyzing the vulnerability of critical infrastructure to attack and planning defenses. In *Tutorials in Operations Research: Emerging Theory, Methods, and Applications*; INFORMS, Catonsville, MD, USA, 2005; pp. 102–123, doi:10.1287/educ.1053.0018.
13. Rinaldi, S.M.; Peerenboom, J.P.; Kelly, T.K. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Syst.* **2001**, *21*, 11–25. [CrossRef]

14. Bier, V.M.; Azaiez, M.N. (Eds.) *Game Theoretic Risk Analysis of Security Threats*; Springer: Berlin, Germany, 2009.
15. Bu, S.; Yu, F.R. A game-theoretical scheme in the smart grid with demand-side management: Towards a smart cyber-physical power infrastructure. *IEEE Trans. Emerg. Top. Comput.* **2013**, *1*, 22–32. [CrossRef]
16. Manshaei, M.H.; Zhu, Q.; Alpcan, T.; Bacşar, T.; Hubaux, J.P. Game theory meets network security and privacy. *ACM Comput. Surv. (CSUR)* **2013**, *45*, 25. [CrossRef]
17. Sandler, T.; others. Terrorism & game theory. *Simul. Gaming* **2003**, *34*, 319–337.
18. Brown, G.; Carlyle, M.; Salmerón, J.; Wood, K. Defending Critical Infrastructure. *Interfaces* **2006**, *36*, 532–544. [CrossRef]
19. Jose, V.R.R.; Zhuang, J. Technology Adoption, Accumulation, and Competition in Multi-period Attacker-Defender Games. *Mil. Oper. Res.* **2013**, *18*, 33–47. [CrossRef]
20. Nikoofal, M.; Zhuang, J. Robust Allocation of a Defensive Budget Considering an Attackers Private Information. *Risk Anal.* **2012**, *32*, 930–943. [CrossRef] [PubMed]
21. Shan, X.; Zhuang, J. Cost of Equity in Homeland Security Resource Allocation In the Face of A Strategic Attacker. *Risk Anal.* **2013**, *33*, 1083–1099. [CrossRef] [PubMed]
22. Hausken, K.; Levitin, G. Review of Systems Defense and Attack Models. *Int. J. Performab. Eng.* **2012**, *8*, 355–366.
23. Shiva, S.; Roy, S.; Dasgupta, D. Game theory for cyber security. In Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, Oarkridge, TN, USA, 21–23 April 2010; p. 34.
24. Cardenas, A.A.; Amin, S.; Sastry, S. Secure control: Towards survivable cyber-physical systems. In Proceedings of the 28th International Conference on Distributed Computing Systems Workshops, Beijing, China, 17–20 June 2008; pp. 495–500.
25. Hahn, A.; Ashok, A.; Sridhar, S.; Govindarasu, M. Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid. *IEEE Trans. Smart Grid* **2013**, *4*, 847–855. [CrossRef]
26. Mo, Y.; Kim, T.H.J.; Brancik, K.; Dickinson, D.; Lee, H.; Perrig, A.; Sinopoli, B. Cyber–physical security of a smart grid infrastructure. *Proc. IEEE* **2012**, *100*, 195–209.
27. Pasqualetti, F.; Dörfler, F.; Bullo, F. Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design. In Proceedings of the IEEE Conference on Decision and Control and European Control Conference (CDC-ECC), Orlando, FL, USA, 12–15 December 2011; pp. 2195–2201.
28. Das, S.K.; Kant, K.; Zhang, N. (Eds.) *An Analytical Framework for Cyber-Physical Networks*; Morgan Kaufman: Burlington, MA, USA, 2012.
29. Rao, N.S.V.; Ma, C.Y.T.; Shah, U.; Zhuang, J.; He, F.; Yau, D.K.Y. On resilience of cyber-physical infrastructures using discrete product-form games. In Proceedings of the International Conference on Information Fusion, Washington, DC, USA, 6–9 July 2015.
30. Hausken, K. Defense and attack for interdependent systems. *Eur. J. Oper. Res.* **2016**, *256*, 582–591. [CrossRef]
31. Rao, N.S.V.; Ma, C.Y.T.; He, F.; Zhuang, J.; Yau, D.K.Y. Cyber-physical correlations for infrastructure resilience: A game-theoretic approach. In Proceedings of the International Conference on Information Fusion, Salamanca, Spain, 7–10 July 2014.
32. Hausken, K. Strategic defense and attack of complex and dependent systems. *Reliab. Eng.* **2009**, *95*, 29–42. [CrossRef]