On Defense Strategies for Recursive System of Systems Using Aggregated Correlations

Nageswara S. V. Rao*, Chris Y. T. Ma†, Fei He‡
*Oak Ridge National Laboratory, Oak Ridge, TN, USA
†Hang Seng Management College, Hong Kong
‡Texas A&M University, Kingsville, TX, USA

***Abstract*—We consider a class of Recursive System of Systems (RSoS), wherein systems are recursively defined and the basic systems at finest level are composed of discrete cyber and physical components. This formulation captures the models of systems that are adaptively refined to account for their varied structure, such as sites of a heterogenous distributed computing infrastructure. The components can be disrupted by cyber or physical means, and can also be suitably reinforced to survive the attacks. We characterize the disruptions at each level of recursion using aggregate failure correlation functions that specify the conditional failure probability of RSoS given the failure of an individual system at that level. At finest levels, the survival probabilities of basic systems satisfy simple product-form, first-order differential conditions using the multiplier functions, which generalize conditions based on contest success functions and statistical independence of component survival probabilities. We formulate the problem of ensuring the performance of RSoS 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 basic system components attacked and reinforced. We derive sensitivity functions at Nash Equilibrium that highlight the dependence of survival probabilities of systems on cost terms, correlation functions, and their partial derivatives. We apply these results to a simplified model of distributed high-performance computing infrastructures.**

I. Introduction

Game-Theoretic formulations using *System of Systems* (SoS) have been used to develop reinforcement strategies for infrastructures with discrete components, such as cloud computing infrastructure and smart grid [11]. Typically, systems in these formulations have a similar structure, for example, characterized by first-order differential conditions on their survival probabilities [20]. Distributed heterogeneous infrastructures, with systems such as sites with customized servers with Graphical Processing Unit (GPU) and neuromorphic accelerators, require more adaptive characterizations to capture their varying structure. We present a *Recursive SoS* (RSoS) formulation wherein each system is recursively defined under a hierarchy such that the *basic systems* at (possibly different) finest levels are composed of discrete cyber and physical components. This formulation enables the incorporation of different levels of details to match the varying complexities of potentially heterogeneous systems. In particular, it generalizes the two-level characterizations in [23] wherein all systems are basic, namely, consist of cyber and physical components and do not capture the varying complexity levels. The components of basic systems may be disrupted by direct cyber or physical attacks, and in addition, may be made unavailable by attacks on other components, for example, network routers. The effects of disruption on a component may propagate to other components of its basic system, and also beyond to components of other basic systems. The provider can reinforce the components to withstand direct attacks, but must also account for inter and intra-system properties to ensure that components are *operational* as individual units and also be *available*, such as being connected to the network.

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.

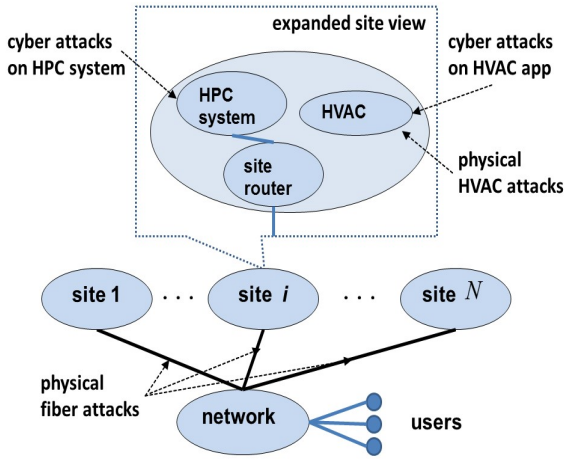

Fig. 1. HPC infrastructure with multiple supercomputer sites connected over a wide-area network.

We consider an RSoS $\mathcal{S}$ which is either (i) a *basic* system composed of discrete cyber and physical components, or (ii) consists of N_1 level-1 systems $S_i^1, i = 1, 2, \ldots, N_1$, each of which is a recursively defined RSoS. Thus, $\mathcal{S}$ can be expanded into an *RSoS tree* by recursively expanding each non-basic system S_i^1 into next level systems S_j^2's, and so on. Thus, for each non-basic system S, we can identify its *descendant* basic systems as the leaves of RSoS subtree rooted at S. Also, we identify the set of systems $\mathcal{S}^k$ at each level k of the tree, which consist of basic and non-basic systems at that level. By recursively expanding all non-basic systems, we obtain the basic systems $S_i, i = 1, 2, \ldots, N_S$, which correspond to the

leaves of RSoS tree located at possibly different depths. The effects of disruptions may propagate among the components of its basic system S_i, and also to other basic systems S_j, $j \neq i$, due to various correlations by propagating up the RSoS tree and then down. For example, consider a distributed High-Performance Computing (HPC) infrastructure with multiple sites connected over a wide area network shown in Figure 1. Consider a site with a supercomputer system with a Heating, Ventilation and Air Conditioning (HVAC) system controlled by a smart phone app; this site can be represented with five basic systems, namely, computing system, gateway router, fiber lines to the site, HVAC system's cooling tower and control app. A cyber attack on a supercomputer may bring it down, and a physical attack on fiber lines that connect the site to network may render it unavailable to users. A compromised phone app may increase the temperature of HVAC system to trigger a shutdown of supercomputer, which illustrates the propagation of disruptions. In an extreme case, the effects of component attacks may disrupt entire RSoS, for example, cyber attacks may bring down all routers of the wide-area network, thereby making all supercomputers unavailable. The RSoS provider is tasked with developing defense strategies to reinforce components of basic systems S_i's against attacks, by accounting for both component disruptions and their propagation within and among the systems at various levels of recursion.

Let y_i and x_i denote the number of components of basic system S_i attacked and reinforced, respectively, wherein a reinforced component survives a direct attack but may be disrupted indirectly. For a non-basic system S, let y_S and x_S represent the number of components attacked and reinforced, respectively, which are obtained by adding the corresponding values of its descendent basic systems. Let $P_I(S)$ denote the survival probability of basic or non-basic system $S = S_i^k$ at level k, and $P_I(\mathcal{S})$ denote the survival probability of entire RSoS $\mathcal{S}$. The *aggregate failure correlation function* C_i^k is the failure probability of "rest" of RSoS (namely, without S_i^k) given the failure of S_i^k at level k. Intuitively, it indicates the relative importance of S_i^k by capturing the fault propagation from it to rest of RSoS, which is denoted by $\mathcal{S}_{-S_i^k}$. In addition to the system-level characterization, correlations among the components are characterized by simple product-form, first-order differential conditions on $P_I(S_i)$ for basic system $S_i, i = 1, 2, \ldots, N_S$ using the system multiplier functions [24]. These conditions lead to simplified estimates of survival probabilities of systems at the Nash Equilibrium (NE), and subsume characterizations using the contest success functions and statistical independence conditions as special cases. This recursive characterization of correlations is natural to RSoS, for example, cloud computing and smart grid infrastructures [28], and leads to simplified analyses of NE conditions by "separating" system aspects into different hierarchical levels and from the basic components level.

The reinforcements and attacks on components entail respective costs to the provider and attacker, respectively. In developing defense strategies, the provider should weigh the costs against benefits in terms of keeping the infrastructure operational. This task requires taking into account system correlations at different system levels 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 basic systems are denoted by $L_A(y_1, \ldots, y_{N_S})$ and $L_D(x_1, \ldots, x_{N_S})$, respectively. The provider minimizes the *composite utility function* given by the sum of two parts [23]:

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

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 RSoS operational, respectively. Similarly, the attacker's composite utility function is given by

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

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 RSoS, respectively. At NE, the attacker and provider minimize their respective utility functions [8].

We derive NE conditions that show the dependence of $P_I(S_i)$ on cost terms, correlation functions, multiplier functions, system survival probabilities, and their partial derivatives. We also estimate the sensitivity functions of $P_I(S_i)$ 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 $P_I(S_i)$ 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 [27], [28] constitute a special RSoS class with one level of recursion. More generally, our RSoS formulation generalizes SoS formulation of composite utilities of [20], [23], which in turn subsumes the sum-form [22] and product-form [21] utilities.

The organization of this paper is as follows. We briefly describe previous works related to our formulation and results in Section II. In Section III, we describe RSoS model along with the aggregate correlation functions at recursion levels and differential conditions on survival probabilities of basic systems using the multiplier functions. We present a game-theoretic formulation in Section IV, and derive NE conditions and sensitivity estimates. We apply the analytical results to a

simple model of distributed HPC infrastructure in Section V. We present conclusions in Section VI.

II. Related Work

Critical networked infrastructures of smart grids, cloud and high performance computing, and transportation systems are vital to national security [3], [14], [17]. They can be viewed as systems of systems, which can be varied and heterogeneous but connected and interdependent. Game-theoretic methods have been extensively applied to capture the interactions between providers and attackers of such critical infrastructures [1], [4], [29], and to develop 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 [30]. 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], [31], and in particular for securing cyber-physical networks [5] with applications to power grids [6], [9], [16], [19].

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 [28]. 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 [24], product-form disutility functions [25] and composite utility functions [20], [23].

The sum-form utility [24] 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 utility [25], 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 [25]. 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 composite utility functions in [20], [23] generalize these two cases by using composite gain-cost term and gain-cost gradient term. The asymmetric role of the network in distributed SoS infrastructures has been studied under sum-form [22], product-form [21] and composite utilities [23], [23], and their detailed analysis is provided for multi-site cloud server infrastructure [26]. These asymmetric aspects of the network connectivity, however, are not addressed in this paper.

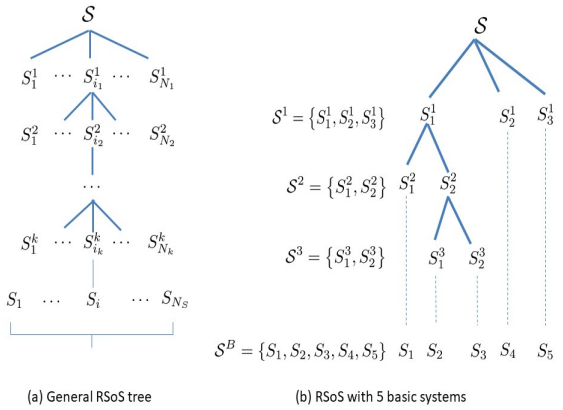

Fig. 2. RSoS tree (a) general case, (b) example.

III. Discrete System Models

RSoS $\mathcal{S}$ consists of systems $\mathcal{S}^1 = \{S_i^1 : i = 1, 2, \ldots, N_1\}$ at level 1, which are listed left to right. By considering the nodes of RSoS-tree at level k, the systems of level k are $\mathcal{S}^k = \{S_i^k, i = 1, 2, \ldots, N_k\}$ listed left to right for $k = 1, 2, \ldots, L$, where L is the deepest level. In general, systems of $\mathcal{S}^k$ could be non-basic or basic. The leaf nodes of RSoS tree consist of basic systems $\mathcal{S}^B = \{S_i, i = 1, 2, \ldots, N_S\}$ listed left to right, which could be at different depths. An example RSoS is shown in Figure 2 with 3, 2 and 2 systems at levels 1, 2 and 3, respectively. The basic systems $\mathcal{S}^B = \{S_1, S_2, S_3, S_4, S_5\}$ correspond to 2, 1 and 2 systems at levels 1, 2 and 3, respectively. Level 1 consists of one non-basic system S_1^1 and two basic systems $S_2^1 = S_4$ and $S_3^1 = S_5$; level 2 consists of one basic system $S_1^2 = S_1$ and one non-basic system S_2^2; and level 3 consists of two basic systems $S_1^3 = S_2$ and $S_2^3 = S_3$.

We capture the interactions between a system S_i^k and rest of RSoS $\mathcal{S}_{-S_i^k}$ of $\mathcal{S}$ in terms of their survival probabilities using the aggregate correlation function C_i^k and its companion function C_{-i}^k represented by the conditional failure probability of S_i^k given the failure of $\mathcal{S}_{-S_i^k}$ [24].

Condition 3.1: **Aggregate Correlation Function:** The probability that RSoS $\mathcal{S}$ with level-k systems $\mathcal{S}^k = \{S_i^k : i = 1, 2, \ldots, N_k\}$ is operational is given by

$$P_I(\mathcal{S}) = P_I(S_i^k) + P_I\left(\mathcal{S}_{-S_i^k}\right) - 1 + C_i^k\left[1 - P_I\left(S_i^k\right)\right],$$

where

$$C_i^k = C_{-i}^k \left(\frac{1 - P_I\left(\mathcal{S}_{-S_i^k}\right)}{1 - P_I(S_i^k)}\right)$$

is the aggregate failure correlation function of system S_i^k, $i = 1, \ldots, N_k$. $\square$

This definition can be recursively applied to express $P_I(S_i^k)$ in terms of $P_I(\cdot)$'s of descendants of S_i^k and the aggregate correlations corresponding to levels k and higher. In a special case where the failure of S_i^k leads to definite failure of rest of RSoS, we have $C_i^k = 1$ such that $P_I(\mathcal{S}) = P_I\left(\mathcal{S}_{-S_i^k}\right)$, that is, the survival probability of RSoS solely depends on $\mathcal{S}_{-S_i^k}$. Under the statistical independence of failures of S_i^k and $\mathcal{S}_{-S_i^k}$, we have $C_{-i}^k = 1 - P_I(S_i^k)$, since the failure probability of S_i^k does not depend on that of $\mathcal{S}_{-S_i^k}$. Consequently we have $P_I(\mathcal{S}) = P_I(S_i^k) P_I\left(\mathcal{S}_{-S_i^k}\right)$. A special class called OR systems corresponds to $C_i^k = 0$, and $C_{-i}^k = 0$ such that

$$P_I(\mathcal{S}) = P_I(S_i^k) + P_I\left(\mathcal{S}_{-S_i^k}\right) - 1.$$

These systems represent some of the simplest systems [24] to analyze due to the absence of correlations.

We now consider that the effects of reinforcements and attacks can be separated at each level such that $\frac{\partial P_I\left(\mathcal{S}_{-S_i^k}\right)}{\partial x_b} \approx 0$, where S_b is a descendant basic system of S_i^k. This condition indicates that reinforcing S_b of S_i^k does not directly impact the survival probability of rest of RSoS $\mathcal{S}_{-S_i^k}$, since S_b is not reachable through recursive expansion of other systems S_j^k, $j \neq i$. We capture such system-level considerations at each level for the provider using the following condition.

Condition 3.2: **De-Coupled Reinforcement Effects:** For $P_I(\mathcal{S})$ in Condition 3.1, we have for level-k systems S_i^k, $i = 1, 2, \ldots, N_k$,

$$\frac{\partial P_I(\mathcal{S})}{\partial x_b} \approx \left(1 - C_i^k\right) \frac{\partial P_I(S_i^k)}{\partial x_b} + \left(1 - P_I(S_i^k)\right) \frac{\partial C_i^k}{\partial x_b}$$

where S_b is a basic system of S_i^k. $\square$

This condition can also be recursively applied to express the right hand side in terms of $\frac{\partial P_I(S_b)}{\partial x_b}$ and $P_I(S_b)$ of the basic systems, and the correlations functions at levels i through L. We derive such expressions in Lemma 4.1 in the next section.

Since basic systems consist of components and cannot be further recursively expanded, their $P_I(\cdot)$'s depend on the correlations between the components, which are characterized using the multiplier functions defined next. We consider that the survival probabilities of basic systems satisfy the following differential condition, which was originally defined for cyber and physical sub-infrastructures [27].

Condition 3.3: **System Multiplier Functions:** The survival probability $P_I(S_b)$ of basic system S_b satisfies the following conditions: there exist *system multiplier function* Λ_b such that

$$\frac{\partial P_I(S_b)}{\partial x_b} = \Lambda_b(x_1, \ldots, x_N, y_1, \ldots, y_N) P_I(S_b)$$

for $b = 1, 2, \ldots, N_S$. $\square$

This condition characterizes the correlations between the components of basic systems. The system multiplier functions are defined for basic systems which can be at different levels, whereas Condition 3.2 is defined for systems at the same level k.

Condition 3.4: **Correlations and De-Coupled Reinforcement Conditions for Basic Systems:** For a basic system S_b of $\mathcal{S}$, the conditions corresponding to Conditions 3.1 and 3.2 are given by:

$$P_I(\mathcal{S}) = P_I(S_b) + P_I\left(\mathcal{S}_{-S_b}\right) - 1 + C_b\left[1 - P_I\left(S_b\right)\right],$$

where C_b is the aggregate failure correlation function of system S_b, and

$$\frac{\partial P_I(\mathcal{S})}{\partial x_b} \approx \left(1 - C_b\right) \frac{\partial P_I(S_b)}{\partial x_b} + \left(1 - P_I(S_b)\right) \frac{\partial C_b}{\partial x_b},$$

respectively, for $b = 1, 2, \ldots, N_S$. $\square$

IV. Game Theoretic Formulation

The provider's objective is to sustain infrastructure performance by reinforcing x_b components of the basic system S_b, which is determined by minimizing the corresponding utility function. Similarly, the attacker's objective is to disrupt the infrastructure by attacking y_b components of S_b, which is obtained by minimizing the corresponding utility function. NE conditions are derived by equating the corresponding derivatives of utility functions to zero, which yields [21]

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

for $b = 1, 2, \ldots, N_S$ for the provider. We define

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

as the *composite gain-cost* term, and

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

as the *gain-cost gradient* with respect to x_b, $b = 1, 2, \ldots, N_S$. Hence, at NE we have the following simplified condition on the partial derivative

$$\frac{\partial P_I(\mathcal{S})}{\partial x_b} = -\frac{F_{G,L}^{D,b}}{L_{G,L}^D}.$$

For the attacker, we similarly obtain

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

for $b = 1, 2, \ldots, N_S$. In this paper, we mainly concentrate on NE conditions for the provider, and the analysis approach is similar for the attacker.

A. NE Sensitivity Functions

We now derive estimates for the survival probability $P_I(S_b)$ of basic system S_b at NE using partial derivatives of the cost and failure correlation functions. For that purpose, we express the term $\frac{\partial P_I(\mathcal{S})}{\partial x_b}$ by recursively applying Condition 3.2, followed by Condition 3.3 for the corresponding S_b's, for $b = 1, 2, dots, N_S$.

Lemma 4.1: **Propagation of Correlations and Multiplier Functions:** Consider a basic system S_b obtained by recursive expansion of RSoS $\mathcal{S}$. Let the path from $\mathcal{S}$ to the leaf S_b consists of the sequence of recursively expanded systems $\mathcal{S}, S^1_{i_1}, S^2_{i_2}, ..., S^{m_b}_{i_{m_b}}, S_b$.

(i) By extending the correlation function and survival probability functions, with Condition 3.2 recursively applied to $\mathcal{S}$, we have

$$\frac{\partial P_I(\mathcal{S})}{\partial x_b} \approx (1 - C_{\prod_b}) \frac{\partial P_I(S_b)}{\partial x_b} + \Delta_{\prod_b} \left[(1 - P_I(S_b)) \frac{\partial C_b}{\partial x_b} + \frac{\partial C_{\Delta_b}}{\partial x_b} \right],$$

where $C_{\prod_b}$ is the *product aggregate correlation function* given by

$$C_{\prod_b} = 1 - (1 - C_b) \prod_{k=1}^{m_b} \left(1 - C^k_{i_k}\right),$$

and

$$\Delta_{\prod_b} = \prod_{k=1}^{m_b} \left(1 - C^k_{i_k}\right),$$

$$\frac{\partial C_{\Delta_b}}{\partial x_b} = \sum_{k=2}^{m_b} \left(\frac{\partial C^k_{i_k}}{\partial x_b} \left[1 - P_I(S^k_{i_k})\right] \prod_{j=1}^{k-1} (1 - C^j_{i_j}) \right) + \left[1 - P_I(S^1_{i_1})\right] \frac{\partial C^1_{i_1}}{\partial x_b}.$$

(ii) In terms of the *product multiplier function* $\Lambda_{\prod_b}$ of S_b given by

$$\Lambda_{\prod_b} = \frac{\partial P_I(\mathcal{S})}{\partial P_I(S^1_{i_1})} \frac{\partial P_I(S^1_{i_1})}{\partial P_I(S^2_{i_2})} \cdots \frac{\partial P_I(S^{m_b}_{i_{m_b}})}{\partial P_I(S_b)} \Lambda_b,$$

we have

$$\frac{\partial P_I(\mathcal{S})}{\partial x_b} = \Lambda_{\prod_b} P_I(S_b).$$

Proof: To show Part (i) we apply Condition 3.2 to $S^1_{i_1}, S^2_{i_2}, ..., S^{m_b}_{i_{m_b}}, S_b$ such that

$$\begin{aligned}
\frac{\partial P_I(\mathcal{S})}{\partial x_b} &\approx \left(1 - C^1_{i_1}\right) \frac{\partial P_I(S^1_{i_1})}{\partial x_b} + \left(1 - P_I(S^1_{i_1})\right) \frac{\partial C^1_{i_1}}{\partial x_b} \\
\frac{\partial P_I(S^1_{i_1})}{\partial x_b} &\approx \left(1 - C^2_{i_2}\right) \frac{\partial P_I(S^2_{i_2})}{\partial x_b} + \left(1 - P_I(S^2_{i_2})\right) \frac{\partial C^2_{i_2}}{\partial x_b} \\
\frac{\partial P_I(S^2_{i_2})}{\partial x_b} &\approx \left(1 - C^3_{i_3}\right) \frac{\partial P_I(S^3_{i_3})}{\partial x_b} + \left(1 - P_I(S^3_{i_3})\right) \frac{\partial C^3_{i_3}}{\partial x_b} \\
\cdots &\approx \cdots \\
\frac{\partial P_I(S^{m_b}_{i_{m_b}})}{\partial x_b} &\approx (1 - C_b) \frac{\partial P_I(S_b)}{\partial x_b} + (1 - P_I(S_b)) \frac{\partial C_b}{\partial x_b}.
\end{aligned}$$

Then by repeated substitution of the above equations, we obtain

$$\begin{aligned}
\frac{\partial P_I(\mathcal{S})}{\partial x_b} \approx\ & \left(1 - C_{\prod_b}\right) \frac{\partial P_I(S_b)}{\partial x_b} \\
&+ \left[1 - P_{\prod_b}(S_b)\right] \frac{\partial C_b}{\partial x_b} \\
&+ \sum_{k=2}^{m_b} \left(\frac{\partial C^k_{i_k}}{\partial x_b} \left[1 - P_I(S^k_{i_k})\right] \prod_{j=1}^{k-1} (1 - C^j_{i_j}) \right) \\
&+ \left[1 - P_I(S^1_{i_1})\right] \frac{\partial C^1_{i_1}}{\partial x_b},
\end{aligned}$$

where

$$1 - P_{\prod_I}(S_b) = [1 - P_I(S_b)] \prod_{k=1}^{m_b} \left(1 - C^k_{i_k}\right) = \Delta_{\prod_b} [1 - P_I(S_b)],$$

which provides the expression for $\frac{\partial C_{\prod_b}}{\partial x_b}$.

Part (ii) follows by applying the chain rule to $\frac{\partial P_I(\mathcal{S})}{\partial x_b}$ in terms of P_I's of $\mathcal{S}, S^1_{i_1}, S^2_{i_2}, ..., S^{m_b}_{i_{m_b}}, S_b$ and applying Condition 3.3. □

Qualitative information about the sensitivities of $P_I(S_b)$ to different parameters can be inferred using estimates derived in the following result.

Theorem 4.1: **Survival Probability Estimates:** Under Conditions 3.1, 3.2, 3.3, and 3.4, the estimates $\hat{P}_{b;D}$ and $\tilde{P}_{b;D}$ of the survival probability $P_I(S_b)$ of basic system S_b expressed in terms of $C_{\prod_b}$ and $\Lambda_{\prod_b}$, respectively, for $b = 1, 2, \ldots, N_S$, are given by

$$\hat{P}_{b;D} = \frac{\Delta_{\prod_b} \left[\frac{\partial C_b}{\partial x_b} + \frac{\partial C_{\Delta_b}}{\partial x_b} \right] + \frac{F^{D,b}_{G,L}}{L^D_{G,L}}}{\Delta_{\prod_b} \frac{\partial C_b}{\partial x_b} - (1 - C_{\prod_b}) \Lambda_b}$$

where S_b is a basic system under the condition: $C_b < 1$ or $\frac{\partial C_{\Delta_b}}{\partial x_b} \neq 0$ and

$$\tilde{P}_{b;D} = -\frac{1}{\Lambda_{\prod_b}} \frac{F^{D,b}_{G,L}}{L^D_{G,L}}.$$

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

$$\frac{\partial P_I(\mathcal{S})}{\partial x_b} = -\frac{F^{D,b}_{G,L}}{L^D_{G,L}}.$$

Then, using Part (i) of Lemma 4.1, we have

$$\begin{aligned}
\frac{\partial P_I(\mathcal{S})}{\partial x_b} &\approx (1 - C_{\prod_b}) \frac{\partial P_I(S_b)}{\partial x_b} + \Delta_{\prod_b} \left[(1 - P_I(S_b)) \frac{\partial C_b}{\partial x_b} + \frac{\partial C_{\Delta_b}}{\partial x_b} \right], \\
&= -\frac{F^{D,b}_{G,L}}{L^D_{G,L}}.
\end{aligned}$$

Then, by Condition 3.3 we have $\frac{\partial P_I(S_b)}{\partial x_b} = \Lambda_b P_I(S_b)$. Then, denoting estimate of $P_I(S_b)$ by $\hat{P}_{b;D}$, we have

$$(1 - C_{\prod_b})\Lambda_b \hat{P}_{b;D} + \Delta_{\prod_b}\left[1 - \hat{P}_{b;D}\right]\frac{\partial C_b}{\partial x_b} = -\left[\frac{F^{D,b}_{G,L}}{L^D_{G,L}} + \Delta_{\prod_b}\frac{\partial C_{\Delta_b}}{\partial x_b}\right].$$

Under the condition $C_b < 1$ or $\frac{\partial C_b}{\partial x_b} \neq 0$, we have

$$\frac{\partial C_b}{\partial x_b} - (1 - C_b)\Lambda_b \neq 0,$$

which provides the above expression for $\hat{P}_{b;D}$. The second estimate $\tilde{P}_{b;D}$ follows from Part (ii) of Lemma 4.1. □

The system survival probability estimate $\hat{P}_{b;D}$ of basic system S_b provides qualitative information about the effects of various parameters including the aggregated correlation coefficient $C_{\prod_b}$, basic system multiplier function Λ_b, composite gain-cost $L^D_{G,L}$ and composite multiplier $F^{D,b}_{G,L}$. We note that these estimates may not necessarily lie within range [0,1], and their main purpose here is to illustrate the dependencies of various terms while others are fixed. In particular, $\hat{P}_{b;D}$ (i) increases and decreases with $F^{D,b}_{G,L}$ and $L^D_{G,L}$, respectively, (ii) increases with Λ_b, and (iii) depends directly both on C_b and its derivative for $i = 1, 2, \ldots, N_S$, and indirectly on the corresponding correlations and derivatives at the levels of recursion.

The second estimate $\tilde{P}_{b;D}$ has a much simpler form but it subsumes correlations at all levels of recursion that correspond to S_b via its product multiplier function $\Lambda_{\prod_b}$, which depends on the partial derivatives of P_I's at successive levels as indicated in Part (ii) of Lemma 4.1.

When applied directly to RSoS $\mathcal{S}$ that consists of only basic systems S_b (namely, with 0 level of recursion, or $m_b = 0$) this theorem provides a simpler expression derived for SoS in [21]

$$\hat{P}_{b;D} = \frac{\frac{\partial C_b}{\partial x_b} + \frac{F^{D,b}_{G,L}}{L^D_{G,L}}}{\frac{\partial C_b}{\partial x_b} - (1 - C_b)\Lambda_b},$$

wherein we have $\Delta_{\prod_b} = 1$, $\Lambda_{\prod_b} = \Lambda_b$, $C_{\prod_b} = C_b$ and $\frac{\partial C_{\Delta_b}}{\partial x_b} = 0$. The added generality of the recursive formulation of RSoS still preserves the basic form of the estimate $\hat{P}_{b;D}$ valid for the simpler SoS formulation, albeit under the expanded definitions of product aggregate correlation and multiplier functions.

V. Distributed HPC Infrastructure

A distributed HPC infrastructure consisting of N sites connected over a wide-area network is shown in Figure 1. Each site houses a supercomputer of potentially different size and architecture, and its HVAC system is controlled by a mobile phone app. In particular, HVAC system itself consists of a physical cooling tower and the app that controls the temperature settings. In addition, the network connectivity to the site is provided by optical fibers, and thus each site is modeled by four basic systems, namely, two cyber and two physical systems as shown in Figure 3, which can be structured

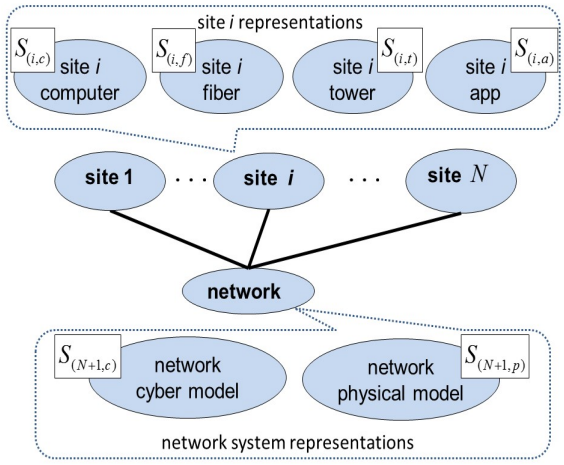

Fig. 3. Site and network systems of HPC infrastructure.

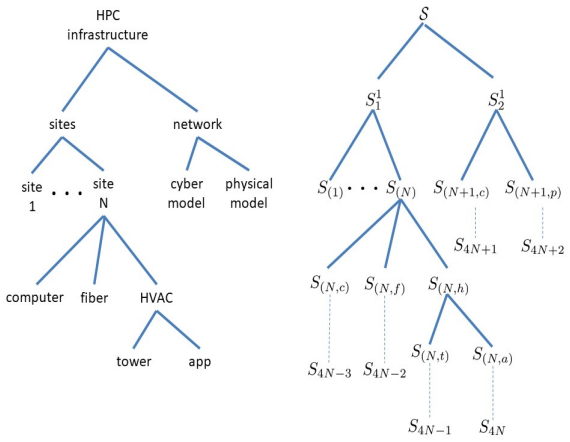

Fig. 4. RSoS tree representation of HPC infrastructure.

as a sub-tree. As systems, a site and network are structurally quite different and consist of different types of components, namely, computing and communications devices, respectively. An RSoS model of these sites connected over the network is represented by two systems at level 1, one representing all sites and the other representing the network as shown in Figure 4. At level 2, each site is represented as a non-basic system, and the network is represented by two basic systems that consist of its cyber and physical components, respectively. Then, at level 3, for each site we have two basic systems, namely, computing system and network fiber, whose models are not further refined, and one non-basic system namely, the HVAC system, which is further refined to level 4 cooling tower and app systems, as shown in Figure 4.

At a site, the computing system including its gateway router and mobile app can be brought down by (different) cyber attacks, and the communication fibers that connect the sites may be physically cut. These attacks may render the computing system at the site unavailable by directly disabling it, for example, crashing it or manipulating the app to increase the temperature to trigger a shutdown, or by disconnecting it from the network by crashing the gateway router via a cyber attack or physically disconnecting the fiber.

The communication network connects the sites, and each of its routers manages L_N connections as shown in Figure 5;

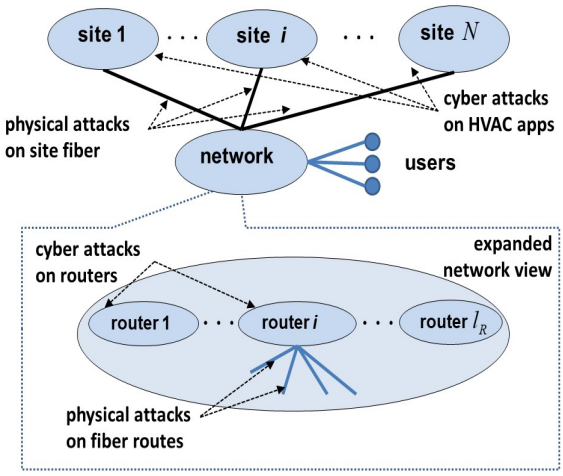

Fig. 5. Network of HPC infrastructure.

here, a cyber attack on a router will disconnect all its connections, whereas a fiber attack may disconnect one or some of them.

To reinforce the components of this infrastructure, some nodes of supercomputers and routers may be replicated, and redundant fiber lines may be installed. For simplicity of discussion, the site router is considered part of the computing system in terms of cyber attacks, and all sites are considered to be of similar structure, and the heterogeneity of RSoS is illustrated by modeling the communications network and sites at different levels of detail. More detailed system models are possible to capture finer details of computing system and site network; for example, the sites could vary in size and types of computing systems, such as generic clusters or custom-designed supercomputers. Similarly, the network infrastructure system models can be expanded to include the facilities that house wide-area network routers, along with various cyber components and facility HVAC systems with physical components.

This infrastructure is modeled by RSoS consisting of $3N$ systems at level 3 where $S^3_{(k,c)}$ $S^3_{(k,f)}$ and $S^3_{(k,h)}$ represent the computing system, fiber connection and HVAC system, respectively, of site k. At level 2, $S^2_{(N+1,c)}$ and $S^2_{(N+1,p)}$ represent the cyber and physical models of the communications network as illustrated in Figure 4. At level 4, for each site we have the cooling tower represented by $S^4_{(k,t)}$ and HVAC control app represented by $S^4_{(k,a)}$ for site k. In all, there are $4N+2$ basic nodes that constitute the leaves of RSoS tree, which correspond to the two systems at level 2, and $2N$ systems at each of levels 3 and 4.

Thus, in terms of the original indices, the basic systems can be identified as follows:

(i) *computing system and gateway router:* $S_{4(k-1)+1} = S^3_{(k,c)}$, for $k = 1, 2, \ldots, N$,
(ii) *physical site fiber connection:* $S_{4(k-1)+2} = S^3_{(k,f)}$, for $k = 1, 2, \ldots, N$,
(iii) *HVAC system:* $S_{4(k-1)+3} = S^4_{(k,t)}$, $S_{4(k-1)+4} = S^4_{(k,a)}$ for $k = 1, 2, \ldots, N$, and
(iv) *network:* $S_{4N+1} = S^2_{(N+1,c)}$ and $S_{4N+2} = S^2_{(N+1,p)}$.

The relationships between the aggregate correlation functions can be captured as follows (as described in [24]). For the communications network, we have

$$C^2_{(N+1,c)} = L_N C^2_{(N+1,p)}$$

which reflects that a router attack will disrupt all its L_N connections.

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 computing system models $S_b = S_{(k,c)}$, $k = 1, 2, \ldots, N$, 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 $S_b = S_{(k,c)}$ of site k, $k = 1, \ldots, N$, we have [22]

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

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. Now consider two basic systems $S_{b_1} = S_{(k,a)}$ corresponding to HVAC app of site k and $S_{b_2} = S_{(N+1,p)}$ corresponding to physical model of the network. Then, the product multiplier of the network cyber system is

$$\Lambda_{\prod_{b_2}} = \frac{\partial P_I(\mathcal{S})}{\partial P_I(S^1_2)} \frac{\partial P_I(S^1_2)}{\partial P_I(S_{(N+1,p)})} \Lambda_{(N+1,p)}.$$

The product multipler function of HVAC app of site k is

$$\Lambda_{\prod_{b_1}} = \frac{\partial P_I(\mathcal{S})}{\partial P_I(S^1_1)} \frac{\partial P_I(S^1_1)}{\partial P_I(S_{(N)})} \frac{\partial P_I(S_{(N)})}{\partial P_I(S_{(k,h)})} \frac{\partial P_I(S_{k,h})}{\partial P_I(S_{(k,a)})} \Lambda_{(k,a)},$$

which is more complex since S_{b_1} is at a deeper level. Similarly, the product aggregate correlation function of the network cyber model given by

$$C_{\prod_{(N+1,p)}} = 1 - (1 - C_{(N+1,p)})(1 - C^1_2)$$

is simpler than that of HVAC app given by

$$C_{\prod_{(k,a)}} = 1 - (1 - C_{(k,a)})(1 - C^1_1)(1 - C^2_{(k)})(1 - C^3_{(k,h)}).$$

These two product aggregate correlation functions depend on each other: (i) C^1_2 relates the network system S^1_2 to $\mathcal{S}_{-S^1_2}$ that subsume $S_{(N+1,p)}$ and $S_{(k,a)}$, respectively, and (ii) C^1_1 relates the site $S_{(k)}$ to $\mathcal{S}_{-S_{(k)}}$ that subsume $S_{(k,a)}$ and $S_{(N+1,p)}$, respectively.

VI. Conclusions

A class of system of systems is studied under composite utility functions, wherein the systems are recursively defined, and at the finest level, the basic systems consist of discrete cyber and physical components. This formulation enables adaptively-refined modeling of systems to account for their varied structure, such as the sites of a heterogenous distributed computing infrastructure. The components of a system can be disrupted directly or indirectly by cyber and physical attacks.

They can be reinforced against such attacks by explicitly taking into account the correlations between the systems at various levels of recursion and also between the components within individual basic systems. These reinforcements, however, incur certain costs which should be weighted against the benefits of the surviving components. We characterize the disruptions at each level of recursion using aggregate failure correlation functions that specify the conditional failure probability of RSoS given the failure of an individual system at that level. At finest levels, the survival probabilities of basic systems satisfy simple product-form, first-order differential conditions. By formulating a game between an infrastructure provider and attacker, we derived sensitivity functions at Nash Equilibrium that highlight the dependence of survival probabilities of systems on cost terms, correlation functions, and their partial derivatives. We applied this approach to a simplified model of a distributed HPC infrastructure. These results are recursive extensions of previous results on interconnected systems [10], [11] and cyber-physical infrastructures [27] with composite utility functions [20], of which the sum-form utility functions [24] and the product-form disutility functions [25] are special cases.

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. Also, it would be of future interest to address the asymmetric network conditions [21], [22] that characterize the important role of the wide-area network in certain infrastructures, wherein a complete network failure will incapacitate them entirely, for example, as in the case of multi-site cloud servers [26]. 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 system models with varying details 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. *European Journal of Operational Research*, 256:582591, 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, N. Imam, C. Y. T. Ma, K. Hausken, F. He, and J. Zhuang. On defense strategies for system of systems using aggregated correlations. In *11th Annual IEEE International Systems Conference*, 2017.

[21] N. S. V. Rao, C. Y. T. Ma, K. Hausken, F. He, D. K. Y. Yau, and J. Zhuang. Defense strategies for asymmetric networked systems under composite utilities. In *IEEE International Conference on Multisensor Fusion and Integration for Intelligent Systems*, 2017.

[22] N. S. V. Rao, C. Y. T. Ma, K. Hausken, F. He, D. K. Y. Yau, and J. Zhuang. Game-theoretic strategies for asymmetric networked systems. In *International Conference on Information Fusion*, 2017.

[23] N. S. V. Rao, C. Y. T. Ma, K. Hausken, F. He, D. K. Y. Yau, and J. Zhuang. Defense strategies for asymmetric networked systems with discrete components. *Sensors*, 18:1421, 2018.

[24] 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.

[25] 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.

[26] N. S. V. Rao, C. Y. T. Ma, and F. He. Defense strategies for multi-site cloud computing server infrastructures. In *International Conference on Distributed Computing and Networking*, 2018.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.