19th International Conference on Information Fusion
Heidelberg, Germany - July 5-8, 2016

Defense Strategies for Infrastructures with Multiple Systems of Components

Nageswara S. V. Rao*, Chris Y. T. Ma†, Kjell Hausken‡, Fei He§, Jun Zhuang¶
*Oak Ridge National Laboratory
†Advanced Digital Sciences Center
‡University of Stavanger, Norway
§Texas A&M University
¶State University of New York at Buffalo

***Abstract*—In several critical infrastructures correlations between the constituent systems represent certain vulnerabilities: disruptions to one may propagate to others and possibly to the entire infrastructure. The correlations between the systems are characterized in two ways in this paper: (i) the aggregate failure correlation function specifies the conditional failure probability of the infrastructure given the failure of an individual system, and (ii) the pairwise correlation function between two systems specifies the failure probability of one system given the failure of the other. The survival probabilities of individual systems satisfy first-order differential conditions that generalize the contest success functions and statistical independence conditions. We formulate a problem of ensuring the resilience of an infrastructure as a game between the provider and attacker; their utility functions are sums of infrastructure survival probability terms and cost terms, both expressed in terms of the numbers of system components attacked and reinforced. We derive Nash Equilibrium conditions and sensitivity functions that highlight the dependence of infrastructure resilience on the cost terms, correlation functions, and individual system survival probabilities. We apply these results to models of distributed cloud computing and energy grid infrastructures.**

I. Introduction

The operation of several critical infrastructures, including smart grids and cloud computing facilities, requires the continued functioning of a number of its constituent systems. For the smart grid, for example, these systems could be as diverse as Supervisory Control And Data Acquisition (SCADA) systems, power distribution systems, fiber plants, and cooling systems. Each system in turn may consist of several components, which may be disabled and/or disconnected by cyber and physical attacks. Disruptions due to such attacks may propagate among the components of a system and degrade its performance. Furthermore, these degradations may propagate to other systems and possibly to the entire infrastructure as a result of correlations between systems. To counter such degradations, the infrastructure providers are required to take into account the strategies of an attacker in the presence of such correlations between the systems and also among the components of individual systems.

We consider infrastructures that can be described by a collection of systems and their components, wherein the underlying cyber-physical interactions are characterized hierarchically between the systems and between the components within a system. Examples of such infrastructures include cloud computing infrastructures with multiple sites each with hundreds of servers, network infrastructures with multiple Point of Presence (POP) locations that house routers and switches of optical fiber connections, and power grid infrastructures with multiple SCADA and generation sites. We represent such an infrastructure with interconnected systems, S_i, $i = 1, 2, \ldots, N$, each in turn consisting of discrete components. The components of each system must be *operational* as individual units and also be *available* such as being connected to the network. These components are subject to individual attacks in that cyber (physical) attacks will disable cyber (physical) components that have not been reinforced. By reinforcement we mean defense, hardening, and investment to ensure the continued operation of components. In the case of a cloud computing infrastructure with multiple server sites, a cyber attack on a server may bring it down, and a physical attack on a fiber line may damage it permanently. In addition to these direct disruptions, correlations between the components may render the otherwise operational components unavailable by disconnecting them. For example, a physical attack on a fiber connection to a server site may disconnect all servers at that site from the network. The attacker's investment is y_i in attacking the system S_i, and provider's investment is x_i for reinforcing, namely, defending it. For example, y_i and x_i may be the number of components of S_i attacked and reinforced, respectively.

Let P_i denote the survival probability of S_i, and P_I denote the survival probability of the entire infrastructure. The survival probability equals one minus the failure probability. The *pairwise failure correlation function* $C_{i,j}(P_i, P_j)$ is the failure probability of S_i given the failure of S_j. The *aggregate failure correlation function* $C_i(P_i)$ is the failure probability of the "rest" of the infrastructure without S_i, given the failure of S_i. That is, $C_i(P_i) = C_{-i,i}(P_{-i}, P_i)$, where P_{-i} is the survival probability of the infrastructure without S_i, which is denoted by S_{-i}. These two correlation functions represent two different ways of characterizing the interdependencies within the infrastructure at the level of systems. To capture the interdependencies at the component level, we consider that P_i satisfies first-order differential conditions that involve x_i and y_i. These conditions generalize the contest success functions and statistical independence conditions used in game formulations for systems with discrete components.

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

(a) attacker has sufficient knowledge about the infrastructure to launch targeted attacks on individual components of

978-0-9964527-4-8

any system;
(b) cost of attacks and reinforcements of systems, denoted by $L_A(y_1, \ldots, y_N)$, and $L_D(x_1, \ldots, x_N)$, respectively, are not available to the other;
(c) strategies used by the provider in choosing which systems and how many of their components to reinforce, and by the attacker in choosing which systems and how many components to attack are not revealed to the other; and
(d) incidents and results of attacks on components will be known to the provider and attacker.

The information in items (a) and (d) is available to both players, and that in items (b)-(c) is private. The *provider utility function* is the sum of terms involving the system survival probability and cost given by

$$U_D = [P_I(x_1, \ldots, x_N, y_1, \ldots, y_N)]\, g_D - L_D(x_1, \ldots, x_N),$$

where g_D represents the reward of keeping the infrastructure operational. Similarly, the *attacker utility function* is

$$U_A = [1 - P_I(x_1, \ldots, x_N, y_1, \ldots, y_N)]\, g_A - L_A(y_1, \ldots, y_N),$$

where g_A represents the reward of disabling the infrastructure. The Nash Equilibrium (NE) of this game represents the attack and reinforcement actions, given by $(y_1, \ldots, y_N)$ and $(x_1, \ldots, x_N)$ respectively, that attempt to maximize the respective utility functions based on their information [6]. We derive NE conditions that highlight the dependence of P_I on cost terms, correlation functions and system survival probabilities, and their partial derivatives. We also estimate the sensitivity functions of P_I using the partial derivatives of $L_A(\cdot)$, $L_D(\cdot)$, P_i, and correlation functions, which indicate their relative importance.

These results extend previous results on interconnected systems in [7], [8] by (i) explicitly incorporating the interdependencies between the systems using two types of correlation functions, and (ii) utilizing the differential conditions of the P_i's to generalize the contest success functions. Also, these results extend earlier results on cyber-physical infrastructures [14], [15], which correspond to the special case $N = 2$ such that S_1 and S_2 correspond to cyber and physical sub-infrastructures, respectively. Together, these generalizations lead to finer modeling and analyses of cloud computing and smart grid infrastructures.

The organization of this paper is as follows. We briefly describe related work in Section II. In Section III, we present a discrete component model for these infrastructures, and discuss two types of correlation functions and differential conditions on system survival probabilities. We present a game-theoretic formulation in Section IV, and derive NE conditions and sensitivity estimates. We also describe two special cases, OR systems in Section IV-B and statistically independent conditions in Section IV-C, wherein the underlying correlation effects are somewhat simplified. We discuss NE conditions for applications of distributed cloud computing and smart grid infrastructures in Section V. We conclude this paper in Section VI.

II. Related Work

Critical infrastructures that support energy, cyber, and transportation systems are vital to national security, and they often rely on complex networked systems, which in turn consist of many disparate components [11]. Game-theoretic methods have been extensively applied to capture the interactions between providers and attackers of critical infrastructures [1]; they lead to strategies that ensure their continued operation in the presence of evolving threats. Several of these infrastructures are modeled using complex dynamic models of the underlying physical systems [2], in particular, using partial differential equations. In general, both game-theoretic formulations and their solutions are quite extensive for such infrastructures, including: multiple-period games that address multiple time-scales of system dynamics [10]; incomplete information games that account for partial knowledge about the system dynamics and attack models [13]; and multiple-target games that account for possibly competing objectives [16]. A comprehensive review of the defense and attack models in various game-theoretic formulations has been presented in [9]. In particular, game theory has been applied in a variety of cyber security applications[12], [17], and in particular for securing cyber-physical networks [3], [4].

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 power systems. Within this class, Stackelberg game formulations using discrete models of cyber-physical infrastructures have been studied in various forms [5], and a subclass of them is formulated using the number of cyber and physical components that are attacked and reinforced [15]. 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 [8] but the correlations between them are not explicitly accounted for. In this paper, we generalize these formulations by utilizing two types of correlation functions for infrastructures with N systems.

III. Discrete System Models

A distributed interconnected infrastructure consists of N constituent systems, S_1, S_2, $\ldots$, S_N, which can be functionally disabled or operationally disconnected through cyber or physical attacks on their components. In particular, cyber attacks in one system may render physical components in another system unavailable even if they are functional; for example, SCADA system attacks might disable power flows on the lines.

A. Aggregated Interactions

We next capture the interactions between the systems of the infrastructure in terms of their survival probabilities using the aggregate and pairwise failure correlation functions.

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

$$P_I = P_i + P_{-i} - 1 + \bar{C}_i\,(P_i)\,(1 - P_{-i}),$$

where $C_i(P_i) = \bar{C}_i(P_i)\frac{1-P_{-i}}{1-P_i}$ is the aggregate failure correlation function of system S_i, $i = 1, \ldots, N$. $\square$

The aggregate failure correlation function captures the interdependence of rest of the system S_{-i} on the failure of S_i, which can be illustrated using some specific cases. For example, in a cloud infrastructure where the fiber connections are represented by system S_F, we have $P_I = 1 - N_S(1-P_F)/K$, where K is a normalization constant. In this case, we have $C_F = N_S/K$, which shows that the fiber failure rate is amplified by N_S in rendering the servers unavailable. Under the statistical independence condition, we have $\bar{C}_i(P_i) = 1 - P_i$ so that $P_I = P_i P_{-i}$. In another case, when the failure of S_i leads to definite failure of rest of the infrastructure, we have $C_i(P_i) = 1$ such that $P_I = P_{-i}$, that is, the infrastructure survival probability solely depends on that of S_{-i}.

We now consider that the effects of reinforcements and attacks can be separated at the system level such that (i) $\frac{\partial P_{-i}}{\partial x_i} \approx 0$, which indicates that reinforcing S_i does not directly impact the survival probability of rest of the infrastructure, and (ii) $\frac{\partial P_i}{\partial x_j} \approx 0$ for $j \neq i$, which indicates that reinforcing S_j does not directly impact the survival probability of S_i. We capture such system-level considerations for the provider using the following condition.

Condition 3.2: For P_I in Condition 3.1, we have for $i = 1, 2, \ldots, N$, $j = 1, 2, \ldots, N$, $j \neq i$,

$$\frac{\partial P_I}{\partial x_i} \approx \left[1 + (1 - P_{-i})\frac{\partial \bar{C}_i}{\partial P_i}\right]\frac{\partial P_i}{\partial x_i}$$

$$\frac{\partial P_I}{\partial x_j} \approx \left[1 - \bar{C}_i(P_i) + (1 - P_{-i})\frac{\partial \bar{C}_i}{\partial P_{-i}}\right]\frac{\partial P_{-i}}{\partial x_j}$$

for the defender. $\square$

B. Pairwise Interactions

We now consider that the pairwise correlations between S_i and S_j are dominant, and correlations between three or more systems are negligible. In such a case, the inclusion exclusion principle provides the approximation

$$P_I = 1 - \left[\sum_{i=1}^{N}(1 - P_i) - \sum_{i=1}^{N-1}\sum_{j=i+1}^{N} P_{\bar{i}\cap\bar{j}}\right]$$

where $P_{\bar{i}\cap\bar{j}}$ is the joint failure probability of S_i and S_j. Then, we have $P_{\bar{i}\cap\bar{j}} = C_{i,j}(P_i, P_j)(1 - P_j)$, which leads to the following condition.

Condition 3.3: **Pairwise Correlation Function:** The probability that the infrastructure is operational is

$$P_I = \sum_{i=1}^{N} P_i - (N-1) + \sum_{i=1}^{N-1}\sum_{j=i+1}^{N} C_{i,j}(P_i, P_j)(1 - P_j),$$

where $C_{i,j}(P_i, P_j)$ is the pairwise failure correlation function of S_i and S_j. $\square$

The pairwise failure correlation functions capture the interdependence of failures of the S_i's. We denote the failure probability of system S_i by $P_{\bar{i}} = 1 - P_i$. The following are two illustrative forms of $C_{i,j}(P_i, P_j)$.

(a) *Statistical Independence:* Under statistical independence we have $C_{i,j}(P_i, P_j) = 1 - P_i$ so that $P_{i,j} = P_i P_j$, where $P_{i,j}$ is the survival probability of S_i and S_j. More generally, if $C_{i,j}(P_i, P_j) > 1 - P_i$, the failures in S_i are *positively correlated* to failures in S_j, that is, they occur with a higher probability following the latter, that is $P_{\bar{i}|\bar{j}} > P_{\bar{i}}$, or equivalently failure in S_j leads to a higher probability of failure in S_i. If $C_{i,j}(P_i, P_j) < 1 - P_i$, failures in S_i are *negatively correlated* to latter failures, that is $P_{\bar{i}|\bar{j}} < P_{\bar{i}}$.

(b) *OR Systems:* The OR systems as modeled in [15] correspond to the special case $N = 2$ where the infrastructure consists of cyber and physical systems (denoted by $i = C$ and $j = P$, respectively) that can be independently analyzed. For OR systems, the failure probability of cyber or physical sub-infrastructure is $P_{\bar{i}\cup\bar{j}} = P_{\bar{i}} + P_{\bar{j}}$ or equivalently $P_{\bar{i}\cap\bar{j}} = 0$. Thus, we have $P_I = P_{i,j} = P_i + P_j - 1$ and $C_{i,j}(P_i, P_j) = 0$.

We now consider that the effects of reinforcements and attacks can be separated at the system level such that $\frac{\partial P_i}{\partial x_j} \approx 0$ for $j \neq i$. Intuitively, this condition indicates that only direct impacts are dominant at the system level. For example, in cyber-physical infrastructures ($N = 2$), cyber reinforcements contribute to improving the cyber sub-infrastructure but not directly to improving the physical sub-infrastructure. We capture the pairwise system-level correlations for the defender using the following condition.

Condition 3.4: For P_I in Condition 3.3, we have

$$\frac{\partial P_I}{\partial x_i} \approx \left[1 + \sum_{\substack{j=1\\ j\neq i}}^{N}\left((1 - P_j)\frac{\partial C_{i,j}}{\partial P_i}\right)\right]\frac{\partial P_i}{\partial x_i}$$

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

$$\frac{\partial P_I}{\partial x_j} \approx \left[1 - C_{\Sigma_{i,j}} + (1 - P_j)\frac{\partial C_{\Sigma_{i,j}}}{\partial P_j}\right]\frac{\partial P_j}{\partial x_j}$$

for $j = 1, 2, \ldots, N$, where $C_{\Sigma_{i,j}} = \sum_{\substack{i=1\\ i\neq j}}^{N} C_{i,j}(P_i, P_j)$. $\square$

In the above condition, the first equation focuses on S_i since its reinforcement variable x_i directly affects its survival probability P_i. It is obtained by differentiating the equation in Condition 3.3 with respect to x_i and ignoring the $\frac{\partial P_j}{\partial x_i}$ terms. In this equation, while x_j does not directly affect P_I through $\frac{\partial P_i}{\partial x_j}$, the dependence is based on $\frac{\partial P_j}{\partial x_j}$ and the pairwise correlations. In the second equation, by anchoring on S_j, the sum effect of all pairwise correlations is captured by $C_{\Sigma_{i,j}} = \sum_{\substack{i=1\\ i\neq j}}^{N} C_{i,j}(P_i, P_j)$. Compared to the role of the aggregate correlation function $\bar{C}_i$ in Condition 3.2, this sum is more detailed in that it explicitly incorporates the pairwise correlations between S_j and S_i, $i = 1, 2, \ldots, N$, $i \neq j$. Note that S_{-i} used in Condition 3.2 is based on aggregating all systems except S_i, whose correlations are accounted for using $\bar{C}_i$. On the other hand, S_j used in Condition 3.4 does not correspond to the aggregation of all systems, but its correlations to all other systems are explicitly accounted for using $C_{\Sigma_{i,j}}$. This finer detail enables us to more

accurately characterize the infrastructures when their pairwise correlations are dominant. By following the above approach, it is possible to generalize the pairwise correlations to include correlations among three or more subsets of systems, which would lead to conditions that are more complex than above.

C. System Survival Probabilities

We consider that the system survival probabilities satisfy the following differential condition, which was originally defined for cyber and physical sub-infrastructures [14].

Condition 3.5: The survival probabilities P_i and P_{-i} of system S_i and S_{-i}, respectively, satisfy the following conditions: there exist functions h_i, h_{-i}, Λ_i, and Λ_{-i} such that

$$\begin{aligned}\frac{\partial P_i}{\partial x_i} &= h_i\left(P_i, x_1, \ldots, x_N, y_1, \ldots, y_N\right)\\ &= \Lambda_i(x_1, \ldots, x_N, y_1, \ldots, y_N)P_i\end{aligned}$$

$$\begin{aligned}\frac{\partial P_{-i}}{\partial x_i} &= h_{-i}\left(P_{-i}, x_1, \ldots, x_N, y_1, \ldots, y_N\right)\\ &= \Lambda_{-i}(x_1, \ldots, x_N, y_1, \ldots, y_N)P_{-i}\end{aligned}$$

for $i = 1, 2, \ldots, N$. □

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

(a) *Statistically Independent Components:* Let $p_{i|R}$ and $p_{i|N}$ denote the conditional survival probability of a component of S_i with and without reinforcement, respectively. Under the statistical independence condition of component failures, the probability that S_i survives the attacks is $P_i = p_{i|R}^{x_i} p_{i|N}^{N_i - x_i}$ [14], which in turn leads to

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

(b) *Contest Survival Functions:* The contest survival functions are to express P_i in [8] such that $P_i = \frac{\xi + x_i}{\xi + x_i + y_i}$, which in turn leads to

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

IV. Game Theoretic Formulation

The provider's objective is to make the infrastructure resilient by reinforcing x_i components of S_i, $i = 1, 2, \ldots, N$, to maximize the utility function

$$U_D = \left[P_I(x_1, \ldots, x_N, y_1, \ldots, y_N)\right] g_D - L_D(x_1, \ldots, x_N).$$

For uniform component reinforcement costs, we have $L_D\left(x_1, \ldots, x_N\right) = \sum_{i=1}^{N} c_{D,i} x_i$, where $c_{D,i}$ is the component reinforcement of S_i. The attacker's objective is to disrupt the infrastructure by attacking y_i components of S_i to maximize the utility function

$$U_A = \left[1 - P_I(x_1, \ldots, x_N, y_1, \ldots, y_N)\right] g_A - L_A(y_1, \ldots, y_N).$$

For uniform component attack costs, we use $C_A\left(y_1, \ldots, y_N\right) = \sum_{i=1}^{N} c_{A,i} y_i$, where $c_{A,i}$ is the component attack cost for S_i.

A. Nash Equilibrium Conditions

The Nash Equilibrium conditions are derived by equating the corresponding derivatives of the utility functions to zero, which yields

$$\frac{\partial U_D}{\partial x_i} = \frac{\partial P_I}{\partial x_i} g_D - \frac{\partial L_D}{\partial x_i} = 0$$

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

$$\frac{\partial U_A}{\partial y_i} = -\frac{\partial P_I}{\partial y_i} g_A - \frac{\partial L_A}{\partial y_i} = 0$$

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

B. OR Infrastructures

A special case where the probability of simultaneous failures of two or more systems is negligible constitutes the OR systems [14]. Here, the infrastructure will fail if any of the systems fails such that for any two systems S_i and S_j, we have $P_{\bar{i} \cup \bar{j}} = P_{\bar{i}} + P_{\bar{j}}$ or equivalently $P_{i,j} = P_i + P_j - 1$. Thus, the Condition 3.3 takes a much simpler form $P_I = \sum_{i=1}^{N} P_i - (N - 1)$, In these (theoretical) systems, the dependence of P_I on system parameters at NE is easier to derive and interpret, since it is determined entirely by the first equation in Condition 3.4 without involving $C_{i,j}(P_i, P_j)$, namely $\frac{\partial P_I}{\partial x_i} \approx \frac{\partial P_i}{\partial x_i}$. At NE, we have

$$\frac{\partial P_i}{\partial x_i} = \frac{1}{g_D} \frac{\partial L_D}{\partial x_i}.$$

Using Condition 3.5, an estimate for the survival probability of S_i is

$$\begin{aligned}&\tilde{P}_{i;D}\left(x_1, \ldots, x_N, y_1, \ldots, y_N\right)\\ &\qquad = \frac{\frac{\partial L_D}{\partial x_i}}{g_D \Lambda_i(x_1, \ldots, x_N, y_1, \ldots, y_N)},\end{aligned}$$

for $i = 1, 2, \ldots, N$. These estimates provide the sensitivity information of the survival probabilities of individual systems; in particular, the estimate for S_i depends only on the derivative Λ_i of the corresponding probability P_i. Although these estimates do not involve $C_{i,j}(P_i, P_j)$, the interactions between the systems may still be captured by the Λ_i's at the component level. In terms of cost and reward, the estimate $\tilde{P}_{i;D}$ is proportional to the cost derivative and inversely proportional to the reward term g_D. While being seemingly counter-intuitive, the multiplicative term g_D corresponds to a higher utility at a lower P_i value from among all NE solutions.

C. Statistical Independence of Systems

We consider that the failures of S_i and S_j are statistically independent such that $P_{ij} = P_i P_j$ and $C_{i,j}\left(P_i, P_i\right) = 1 - P_i$. At NE we have for $i = 1, 2, \ldots, N$, $j = 1, 2, \ldots, N$, $i \neq j$,

$$\left(2 - N - P_i + \sum_{k=1}^{N} P_k\right) \frac{\partial P_i}{\partial x_i} = \frac{1}{g_D} \frac{\partial L_D}{\partial x_i},$$

$$\left(2 - N - P_j + \sum_{k=1}^{N} P_k\right) \frac{\partial P_j}{\partial x_j} = \frac{1}{g_D} \frac{\partial L_D}{\partial x_j}.$$

We now substitute expressions for $\frac{\partial P_i}{\partial x_i}$ and $\frac{\partial P_j}{\partial x_j}$ based on Condition 3.5, and obtain the system of equations:

$$\left(2 - N - \bar{P}_{j;D} + \sum_{k=1}^{N} \bar{P}_{k;D}\right) \bar{P}_{j;D} = \frac{\frac{\partial L_D}{\partial x_j}}{g_D \Lambda_j (x_1, \ldots, x_N, y_1, \ldots, y_N)},$$

$$\left(2 - N - \bar{P}_{i;D} + \sum_{k=1}^{N} \bar{P}_{k;D}\right) \bar{P}_{i;D} = \frac{\frac{\partial L_D}{\partial x_i}}{g_D \Lambda_i (x_1, \ldots, x_N, y_1, \ldots, y_N)}.$$

Qualitatively, at NE, the survival probability estimates of systems S_i and S_j, namely, $\bar{P}_{i;D}$ and $\bar{P}_{j;D}$ have an inverse relationship, but their product is determined by $\Lambda_i(\cdot)$ and $\Lambda_j(\cdot)$ in a manner similar to the individual probabilities $\tilde{P}_{i;D}$ and $\tilde{P}_{j;D}$ of OR systems. However, unlike OR systems, statistical independence is not sufficient to decouple the estimates $\bar{P}_{i;D}$ and $\bar{P}_{j;D}$ so as not to involve pairwise correlations but depend solely on $\Lambda_i(\cdot)$ and $\Lambda_j(\cdot)$, respectively.

D. NE Sensitivity Functions

We now derive estimates for P_i and P_{-i} at NE using the partial derivatives of the cost and failure correlation function to obtain qualitative information about their sensitivities to different parameters from the provider's perspective.

Theorem 4.1: **Aggregate Correlation Function:** Under Conditions 3.1, 3.2, and 3.5, an estimate of the survival probability of rest of the infrastructure S_{-i}, for $\frac{\partial \bar{C}_i}{\partial P_{-i}} \neq 0$, $i = 1, 2, \ldots, N$, is

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

and, for $\frac{\partial \bar{C}_i}{\partial P_{-i}} = 0$, is

$$\hat{P}_{-i;D}(x_1, \ldots, x_N, y_1, \ldots, y_N) = \frac{\frac{\partial L_D}{\partial x_j}}{g_D \Lambda_{-i}\left[1 - \bar{C}_i\left(\hat{P}_{i;D}\right)\right]}.$$

An estimate of the survival probability of system S_i is

$$\hat{P}_{i;D}(x_1, \ldots, x_N, y_1, \ldots, y_N) = \frac{\frac{\partial L_D}{\partial x_i}}{g_D \Lambda_i \left[1 + (1 - \hat{P}_{-i;D})\frac{\partial \bar{C}_i}{\partial P_i}\right]}.$$

Proof: At NE, we have $\frac{\partial P_I}{\partial x_i} = \frac{1}{g_D}\frac{\partial L_D}{\partial x_i}$ and $\frac{\partial P_I}{\partial x_j} = \frac{1}{g_D}\frac{\partial L_D}{\partial x_j}$. By using the formulae in Condition 3.2, we have

$$\left[1 + (1 - P_{-i})\frac{\partial \bar{C}_i}{\partial P_i}\right]\frac{\partial P_i}{\partial x_i} = \frac{1}{g_D}\frac{\partial L_D}{\partial x_i}$$

$$\left[1 - \bar{C}_i(P_i) + (1 - P_{-i})\frac{\partial \bar{C}_i}{\partial P_{-i}}\right]\frac{\partial P_{-i}}{\partial x_j} = \frac{1}{g_D}\frac{\partial L_D}{\partial x_j}.$$

We now substitute expressions for $\frac{\partial P_i}{\partial x_i}$ and $\frac{\partial P_{-i}}{\partial x_j}$ based on Condition 3.5, and obtain the system of equations:

$$\left[1 + (1 - P_{-i})\frac{\partial \bar{C}_i}{\partial P_i}\right] P_i = \frac{\frac{\partial L_D}{\partial x_i}}{g_D \Lambda_i(x_1, \ldots, x_N, y_1, \ldots, y_N)}, \quad (1)$$

$$\left[1 - \bar{C}_i(P_i) + (1 - P_{-i})\frac{\partial \bar{C}_i}{\partial P_{-i}}\right] P_{-i} = \frac{\frac{\partial L_D}{\partial x_j}}{g_D \Lambda_{-i}(x_1, \ldots, x_N, y_1, \ldots, y_N)}. \quad (2)$$

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

The estimates $\hat{P}_{-i;D}$ and $\hat{P}_{i;D}$ provide sensitivity information for the corresponding probabilities P_{-i} and P_i, respectively, and are not always guaranteed to be within [0,1] range. Their main purpose is to provide qualitative information about the survival probability of S_i and the rest of the infrastructure S_{-i} based on the aggregate correlation function $\bar{C}_i$ between the two. Compared to OR systems, there are significant system-level interactions reflected in both $\hat{P}_{-i;D}(x_1, \ldots, x_N, y_1, \ldots, y_N)$ and $\hat{P}_{i;D}(x_1, \ldots, x_N, y_1, \ldots, y_N)$, namely, the survival probability of the infrastructure without S_i and that of S_i by itself, respectively. In particular, $\hat{P}_{-i;D}(x_1, \ldots, x_N, y_1, \ldots, y_N)$ depends on both $\bar{C}_i(\cdot)$ and its partial derivatives with respect to P_{-i}; while an increase in the former leads to a decrease in $\hat{P}_{-i;D}$, the effect of the latter depends on its sign and it can in some cases mitigate the decrease due to the former. Also $\hat{P}_{-i;D}$ depends on the partial derivative of L_D with respect to x_j; it also depends on the cost factor g_D and Λ_{-i} as expected. Its dependence on P_i is through the failure correlation function $\bar{C}_i(P_i)$. The qualitative behavior of $\hat{P}_{i;D}(x_1, \ldots, x_N, y_1, \ldots, y_N)$ is quite similar with respect to L_D. And, they both are affected by $\Lambda_i(\cdot)$ and $\Lambda_{-i}(\cdot)$, and each of them in turn depends on the number of component attacks and reinforcements in each system. Thus, the estimates $\hat{P}_{-i;D}$ and $\hat{P}_{i;D}$ reflect the correlations between S_{-i} and S_i explicitly $\bar{C}_i(P_i)$, as well as those captured by the survival probabilities of individual systems by themselves.

Theorem 4.1 utilizes $P_{\bar{i}|\overline{-i}} = \bar{C}_i(P_i)$, which captures the failure effects of the rest of the infrastructure S_{-i} on the system S_i. Alternatively, we can utilize $P_{\overline{-i}|\bar{i}} = C_i(P_i)$ which captures the failure effects of system S_i on rest of infrastructure S_{-i}.

We now consider the pairwise correlations in deriving NE conditions. We derive expressions for P_i and P_j in terms of the partial derivatives of cost and correlation functions,

which provide qualitative information about their sensitivities to different parameters.

Theorem 4.2: **Pairwise Correlation Function:** Under Conditions 3.3, 3.4, and 3.5, an estimate of the survival probability of system S_j, for $\frac{\partial C_{\Sigma_{i,j}}}{\partial P_j} \neq 0$, $i = 1, 2, \ldots, N$, $j = 1, 2, \ldots, N$, $i \neq j$, is

$$\hat{P}_{j;D}\left(x_1, \ldots, x_N, y_1, \ldots, y_N\right) = \frac{1 - C_{\Sigma_{i,j}} + \frac{\partial C_{\Sigma_{i,j}}}{\partial P_j}}{2\frac{\partial C_{\Sigma_{i,j}}}{\partial P_j}} \pm \sqrt{\left(\frac{1 - C_{\Sigma i,j} + \frac{\partial C_{\Sigma_{i,j}}}{\partial P_j}}{2\frac{\partial C_{\Sigma_{i,j}}}{\partial P_j}}\right)^2 - \frac{\frac{\partial L_D}{\partial x_j}}{g_D \Lambda_j \frac{\partial C_{\Sigma_{i,j}}}{\partial P_j}}},$$

and, for $\frac{\partial C_{\Sigma_{i,j}}}{\partial P_j} = 0$, is

$$\hat{P}_{j;D}\left(x_1, \ldots, x_N, y_1, \ldots, y_N\right) = \frac{\frac{\partial L_D}{\partial x_j}}{g_D \Lambda_j \left[1 - C_{\Sigma_{i,j}}\right]}.$$

An estimate of the survival probability of system S_i is

$$\hat{P}_{i;D}\left(x_1, \ldots, x_N, y_1, \ldots, y_N\right) = \frac{\frac{\partial L_D}{\partial x_i}}{g_D \Lambda_i \left[1 + \sum_{\substack{j=1 \\ j \neq i}}^{N} \left((1 - \hat{P}_{j;D}) \frac{\partial C_{i,j}}{\partial P_i}\right)\right]}.$$

Proof: Following along the lines of Theorem 4.1, we obtain the following expressions based on Conditions 3.4 and 3.5:

$$\left[1 + \sum_{\substack{j=1 \\ j \neq i}}^{N} \left((1 - P_j) \frac{\partial C_{i,j}}{\partial P_i}\right)\right] P_i = \frac{\frac{\partial L_D}{\partial x_i}}{g_D \Lambda_i(x_1, \ldots, x_N, y_1, \ldots, y_N)}, \quad (3)$$

$$\left[1 - C_{\Sigma_{i,j}} + (1 - P_j) \frac{\partial C_{\Sigma_{i,j}}}{\partial P_j}\right] P_j = \frac{\frac{\partial L_D}{\partial x_i}}{g_D \Lambda_j(x_1, \ldots, x_N, y_1, \ldots, y_N)}. \quad (4)$$

The expression for $\hat{P}_{j;D}$ is obtained by solving for P_j using quadratic Equation (3), and the expression for $\hat{P}_{i;D}$ follows from Equation (4). □

The estimates $\hat{P}_{i;D}$ and $\hat{P}_{j;D}$ provide qualitative information about the survival probabilities of S_i and S_j, respectively, by explicitly utilizing $C_{\Sigma_{i,j}}$, which in turn depends on $C_{i,j}(P_i, P_j)$ for $i = 1, 2, \ldots, N, i \neq j$. Note that the choices of i and j are arbitrary since the system indices can be re-labeled, but once indices are fixed such that $j > i$, the corresponding estimates are also fixed. The overall dependence of $\hat{P}_{i;D}$ and $\hat{P}_{j;D}$ on $C_{\Sigma_{i,j}}$, g_D and L_D is quite similar to the corresponding relationships described above for Theorem 4.1. One major difference, however, is that $\hat{P}_{i;D}$ and $\hat{P}_{j;D}$ depend on all pairwise correlations $C_{i,j}$ and their partial derivatives. In particular, $\hat{P}_{i;D}$ depends on each $1 - \hat{P}_{j;D}$, $j = 1, 2, \ldots, N$, $j \neq i$, which is multiplied by $\frac{\partial C_{i,j}}{\partial P_i}$ and summed in the denominator. In terms of other parameters, as in the case of Theorem 4.1, it similarly depends directly on $\frac{\partial L_D}{\partial x_i}$ and inversely on g_D and Λ_i. Then, $\hat{P}_{j;D}$ depends on each $\hat{P}_{i;D}$ through the pair sise correlation $C_{i,j}\left(\hat{P}_{i:D}, \hat{P}_{j;D}\right)$ through $C_{\Sigma_{i,j}} = \sum_{\substack{i=1 \\ i \neq j}}^{N} C_{i,j}(P_i, P_j)$. Moreover, it depends both on $C_{\Sigma_{i,j}}$ and its partial derivative $\frac{\partial C_{\Sigma_{i,j}}}{\partial P_j}$, and their net effect could be additive or otherwise depending on the sign of the latter. Also, it depends on $\frac{\partial L_D}{\partial x_j}$ and inversely on g_D and Λ_j in a qualitatively similar manner to $\hat{P}_{-i}$ in Theorem 4.1. In general, the relative values of pairwise correlations and their partial derivatives are reflected directly in these estimates.

V. Application Examples

We now describe simple models for cloud computing and energy grid infrastructures, and derive some estimates for the aggregate and pairwise correlation functions and $\Lambda_i(\cdot)$'s. Using these estimates, we discuss the implications of the sensitivity functions for the survival probabilities derived in Theorems 4.1 and 4.2; they depend on $\Lambda_i(\cdot)$'s and correlation functions, which depend on the systems and interactions between them, in addition to the cost terms and their differentials.

A. Distributed Cloud Computing Infrastructure

A distributed cloud computing infrastructure consists of N_S sites, with L_k servers at site k, $k = 1, 2, \ldots, N_S$. These sites are connected over a communication network wherein each router manages L_N connections. The servers and routers may be brought down by cyber attacks, and communication fiber routes to server sites and routers may be physically cut. The components may be reinforced by replicating the servers and routers, and by providing redundant, physically separate fiber routes. This infrastructure can be modeled using $2N_S + 2$ systems such that $S_{(k,c)}$ and $S_{(k,p)}$ represent the cyber and physical models of server site k, and $S_{(N_S+1,c)}$ and $S_{(N_S+1,p)}$ represent the cyber and physical models of the communications network. In terms of original indices, we have: $S_l = S_{(l,c)}$, for $l = 1, 2, \ldots, N_S$, $S_{N_S+1} = S_{(N_S+1,c)}$; $S_{N_S+1+l} = S_{(l,p)}$, for $l = 1, 2, \ldots, N_S$, and $S_{2N_S+2} = S_{(N_S+1,p)}$. The relationships between the aggregate correlation functions can be captured as follows. For the communications network, we have $C_{(N_S+1,c)} = L_N C_{(N_S+1,p)}$ which reflects that a cyber attack on a router will disrupt all its L_N connections. For site k, we have the opposite given by $C_{(k,p)} = L_k C_{(k,c)}, k = 1, 2, \ldots, N_S$, which indicates that a physical disruption of the fiber at site k will disconnect all its servers. This multiplicative effect carries over to partial differentials since $\frac{\partial C_{(k,p)}}{\partial P_{(k,p)}} = L_k \frac{\partial C_{(k,c)}}{\partial P_{(k,p)}}$ and $\frac{\partial C_{(k,p)}}{\partial P_{(k,c)}} = L_k \frac{\partial C_{(k,c)}}{\partial P_{(k,c)}}$ for $k = 1, 2, \ldots, N_S, N_S + 1$, and $L_{N_S+1} = 1/L_N$. Based on Theorem 4.1, this multiplier effect in partial differentials will be reflected in $\hat{P}_{(k,p);D}$, $\hat{P}_{(k,c);D}$, $\hat{P}_{-(k,p);D}$ and $\hat{P}_{-(k,c);D}$

in addition to the aggregate correlation functions $C_{(k,p)}$ and $C_{(k,c)}$.

We account for the pairwise correlations at site k by considering the corresponding cyber and physical models, namely $S_{(k,c)}$ and $S_{(k,p)}$ respectively. Since a physical fiber cut disconnects all servers at site k from the network, we have

$$C_{(k,c),(k,p)}\left(P_{(k,c)}, P_{(k,p)}\right) = L_k C_{(k,p),(k,c)}\left(P_{(k,p)}, P_{(k,c)}\right),$$

for $k = 1, 2, \ldots, N_S$, which indicates the multiplicative effect of physical attacks. The relationship for the communications network remains the same as above. Then, this multiplicative effect carries over to $C_{\Sigma_{i,j}}$ in Theorem 4.2. For example, by considering only the correlations between the corresponding cyber and physical models of the sites and network, we have the multiplicative effects carried over to $C_{\Sigma_{i,j}} = C_{\Sigma_{(k,c),(k,p)}}$, and hence to $\hat{P}_{(k,c);D}$ and $\hat{P}_{(k,p);D}$ for $k = 1, 2, \ldots, N_S + 1$. When correlations between all pairs $S_i = S_{(k_1,a_1)}$ and $S_j = S_{(k_2,a_2)}$ for distinct (k_1, a_1) and (k_2, a_2), where $k1 = 1, 2, \ldots, N_S + 1$, $k2 = 1, 2, \ldots, N_S + 1$, $a_1 \in \{c, p\}$ and $a_2 \in \{c, p\}$, we have $C_{\Sigma_{i,j}} = C_{\Sigma_{(k_1,a_1),(k_2,a_2)}}$, which indicates the propagation of the multiplicative effect throughout the infrastructure. In this general case, the correlations between cyber models and physical models are considered in addition to those between the cyber and physical models.

We now consider that the attacker and provider choose components according to the uniform distribution. Then, for the cyber model $S_{(k,c)}$ of site k, there are $[y_{(k,p)} - x_{(k,p)}]_+$ non-reinforced fiber connections, where $[x]_+ = x$ for $x > 0$, and $[x]_+ = 0$ otherwise. Then, the probability that a cyber-reinforced component survives $y_{(k,p)}$ fiber attacks is approximated by

$$p_{(k,c)|R} = \frac{f_{(k,c)}}{1 + L_k[y_{(k,p)} - x_{(k,p)}]_+},$$

where the normalization constant $f_{(k,c)}$ is appropriately chosen such that $0 \leq f_{(k,c)} \leq 1$. If a cyber component is not reinforced, it can be brought down by a direct cyber attack, or indirectly through a fiber attack. Thus, we approximate the survival probability of a cyber component at site k as

$$p_{(k,c)|N} = \frac{f_{(k,c)}}{1 + y_{(k,c)} + L_k[y_{(k,p)} - x_{(k,p)}]_+},$$

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

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

which does not depend on $x_{(k,c)}$, $k = 1, \ldots, N_S$. Then, since the $\Lambda_{(k,c)}$ appears in the denominator, $\hat{P}_{(k,c);D}$ in both Theorems 4.1 and 4.2 decreases with the number of cyber attacks $y_{(k,c)}$ and increases in proportion to $[y_{(k,p)} - x_{(k,p)}]_+$ which is the number of attacks exceeding the reinforcements. The latter condition may appear counter intuitive at the surface but note that it is applicable to only the states that satisfy NE conditions. An analogous dependence of $\hat{P}_{-(k,c);D}$ in Theorem 4.1 on the parameters $x_{(k,c)}$, $x_{(k,p)}$, $y_{(k,c)}$, and $y_{(k,p)}$ is less direct since the corresponding $\Lambda_{(k,c)}$ appears inside the square root but is qualitatively similar since it is in the denominator. When we consider only the cyber-physical correlations of the sites, the dependence of $\hat{P}_{(k,p);D}$ in Theorem 4.2 on $\Lambda_{(k,c)}$ is qualitatively similar.

B. Power Grid Infrastructure

We consider a simplified model of a power grid infrastructure controlled by a (cyber) network of N_S SCADA system sites, such that site k controls the power flow on L_k lines. A SCADA system at site i may be disabled by a direct cyber attack, which will disrupt the power flow on all its L_k lines. Unlike the cloud computing infrastructure, the impacts of cyber attacks are amplified by the L_k's. The SCADA systems are connected to a communication network as in the previous case. This infrastructure can be modeled using $2N_S+2$ systems such that $S_{(k,c)}$ and $S_{(k,p)}$ represent the cyber and physical models of SCADA site k, and $S_{(N_S+1,c)}$ and $S_{(N_S+1,p)}$ represent the cyber and physical models of the communications network. By using the reasoning analogous to the cloud computing infrastructure, we have $C_{(k,c)} = L_k C_{(k,p)}, k = 1, 2, \ldots, N_S$ which indicates that a cyber attack on site k would disrupt the power flow on all L_k lines. Also, these multiplicative effects will be reflected in the partial derivatives and in $\hat{P}_{(k,c);D}$, $\hat{P}_{(k,p);D}$, $\hat{P}_{-(k,c);D}$ and $\hat{P}_{-(k,p);D}$.

For SCADA site k, we consider the pairwise correlations between its cyber and physical models, namely $S_{(k,c)}$ and $S_{(k,p)}$, respectively. Following along the lines of previous example, we have

$$C_{(k,p),(k,c)}\left(P_{(k,p)}, P_{(k,c)}\right) = L_k C_{(k,c),(k,p)}\left(P_{(k,c)}, P_{(k,p)}\right),$$

for $i = 1, 2, \ldots, N_S, N_S + 1$, and $L_{N_S+1} = L_N$, which indicates the multiplicative effect of cyber attacks. As in the previous example, this multiplicative effect carries over to $C_{\Sigma_{i,j}} = C_{\Sigma_{(k,c),(k,p)}}$ and hence to $\hat{P}_{(k,c);D}$ and $\hat{P}_{(k,p);D}$ when only correlations between the cyber and physical models are considered.

We then estimate the survival probability of reinforced power lines that can be disconnected by $y_{(k,c)}$ cyber attacks on site k, as

$$p_{(k,p)|R} = \frac{f_{(k,p)}}{1 + L_k[y_{(k,c)} - x_{(k,c)}]_+},$$

where $0 \leq f_{(k,p)} \leq 1$ is appropriately chosen. Each power line can be directly disrupted by physical means such that it can be brought down if not reinforced, and a component is more likely to be unavailable if there are more physical attacks, namely, higher $y_{(k,p)}$. Thus, an attack on a SCADA system at site k will have an amplified effect on power lines compared to direct physical attacks such that

$$p_{(k,p)|N} = \frac{f_{(k,p)}}{1 + y_{(k,p)} + L_k[y_{(k,c)} - x_{(k,c)}]_+}$$

provides an estimate of the survival probability of a non-reinforced power line. Using the above formulae, for physical model $S_{(k,p)}$ for site k, we have

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

for which does not depend on $x_{(k,p)}$, for $k = 1, 2, \ldots, N_S, N_S + 1$. Similar to the cloud computing infrastructure, $\hat{P}_{(k,p);D}$ decreases with the number of physical

attacks $y_{(k,p)}$ and increases with the cyber attacks in excess of the cyber reinforcements, namely $[y_{(k,c)} - x_{(k,c)}]_+$.

In general compared to the previous example, the roles of cyber and physical models are reversed for the sites in this case, but those of the communications network are quite similar. The overall qualitative dependencies of the survival probability estimates (provided by Theorems 4.1 and 4.2) on the number of components attacked and reinforced in the individual systems are quite similar.

More general models with additional cyber and physical component types are considered for both cloud computing and energy grid infrastructures in [14], [15]. In particular, local area network devices at the server sites are considered for the former, and smart meters and line sensors are considered for the smart grid infrastructures. The overall analysis of this section can be directly extended to those more detailed component models.

VI. Conclusions

We studied a class of infrastructures consisting of a number of systems each of which is composed of discrete components that can be disrupted by either cyber or physical attacks. The components can be reinforced against such attacks by taking into account the interactions between the systems and also between the components within the systems. We characterized the interactions between the systems in these infrastructures at two levels: (i) the aggregate failure correlation function specifies the conditional failure probability of the infrastructure given that of an individual system, and (ii) the pairwise correlation function between two systems specifies the failure probability of one given that of the other. The survival probabilities of individual systems satisfy simple first-order differential conditions that characterize component correlations within the systems; these conditions generalize the contest success functions and statistical independence conditions. By formulating a game between an infrastructure provider and attacker, we derived Nash Equilibrium conditions in terms of the partial derivatives of cost terms, failure correlation functions and survival probabilities of component systems and their partial derivatives. We then estimated the sensitivity functions that indicate the dependence of the infrastructure survival probability on these quantities. We applied these results to analyze simplified models of cloud computing and energy grid infrastructures.

These results extend previous results on interconnected systems in [7], [8] by (i) explicitly incorporating the interdependencies between the systems using two types of correlation functions, and (ii) utilizing the differential conditions to generalize the contest success functions. Also, these results enable us to analyze in more detail the cyber-physical infrastructures studied in [14], [15]. In particular, these generalizations enable us to consider more detailed models of the correlations between various systems in cloud computing and energy grid infrastructures.

Several extensions of this formulation could be pursued in future studies, including the cases where the effects of attacks and reinforcements of specific individual components are explicitly accounted for. Another future direction is to consider simultaneous cyber and physical attacks. It would be interesting to study sequential game formulations of this problem, and cases where different levels of knowledge are available to each party. Applications of our approach to more detailed models of cloud computing infrastructure, smart energy grid infrastructures and high-performance computing complexes would be of future interest. It would also be of future interest to explore the applicability of this overall method to continuous models, wherein partial differential equations are used for describing the dynamics of individual systems or the entire infrastructure.

Acknowledgments

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.

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] 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.

[4] 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.

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

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

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

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

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

[10] 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.

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

[12] 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.

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

[14] 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.

[15] 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.

[16] X. Shan and J. Zhuang. Cost of equity in homeland security resource allocation in the face of a strategic attacker. *Risk Analysis*, 33(6):1083–1099, 2013.

[17] 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.