Defense Strategies for Asymmetric Networked Systems Under Composite Utilities

Nageswara S. V. Rao*, Chris Y. T. Ma†, Kjell Hausken‡, Fei He§, David K. Y. Yau¶, Jun Zhuang‖

*Oak Ridge National Laboratory, Oak Ridge, TN, USA
†Hang Seng Management College, Hong Kong
‡University of Stavanger, Norway
§Texas A&M University, Kingsville, TX, USA
¶Singapore University of Technology and Design, Singapore
‖State University of New York at Buffalo, Buffalo, NY, USA

Abstract—We consider an infrastructure of networked systems with discrete components that can be reinforced at certain costs to guard against attacks. The communications network plays a critical, asymmetric role of providing the vital connectivity between the systems. We characterize the correlations within this infrastructure at two levels using (a) aggregate failure correlation function that specifies the infrastructure failure probability given the failure of an individual system or network, and (b) first-order differential conditions on system survival probabilities that characterize component-level correlations. We formulate an infrastructure survival game between an attacker and a provider, who attacks and reinforces individual components, respectively. They use the composite utility functions composed of a survival probability term and a cost term, and the previously studied sum-form and product-form utility functions are their special cases. At Nash Equilibrium, we derive expressions for individual system survival probabilities and the expected total number of operational components. We apply and discuss these estimates for a simplified model of distributed cloud computing infrastructure.

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

I. INTRODUCTION

Infrastructures for cloud computing, science experiments and computations, and smart energy grid, consist of complex systems connected over long-haul networks. In these infrastructures, the communications network plays a critical, asymmetric role of providing the vital connectivity between the systems which include cloud computing sites or supercomputers or energy distribution centers. Network failures render these systems unreachable, and in extreme cases can render the entire infrastructure unavailable. Such an infrastructure is represented by its constituent systems, \( S_i \), \( i = 1, 2, \ldots, N \), and the network is represented as a separate system \( S_{N+1} \) [14]. The individual systems themselves are complex, consisting of several discrete cyber and physical components, which must be operational and connected to the network. The individual components of \( S_i \) may be disabled or disconnected, and \( S_i \) as a system may be disconnected, by component cyber and physical attacks.

The components can be reinforced to survive direct attacks, but they may rendered unavailable by attacks to other components. For example, servers at a cloud computing site can be hardened against cyber attacks but they can all be made unavailable by cutting fiber connections to the site. On the other hand, non-reinforced components will always be disabled by direct attacks. The reinforcements and attacks incur costs to the provider and attacker, respectively. In networked systems, correlations between components and systems lead to the propagation of disruptions across the infrastructure. Thus, in addition to within system \( S_i \), the attack effects may propagate to components of other systems \( S_j, j \neq i \).

The infrastructure provider is tasked with developing strategies to choose a number of components to reinforce against attacks by taking into account various correlations. Game theory formulations are used in [14] to derive such defense strategies separately for sum-form and product-form utility functions. In this paper, we employ the complex utility functions [13] that generalize and unify both utility functions, and additionally explicitly account for the asymmetric role of the network in deriving the Nash Equilibrium (NE) conditions and defense strategies.

For \( S_i \), let \( n_i \) denote its number of components of which \( y_i \) and \( x_i \) denote the number of components attacked and reinforced, respectively. Let \( P_i \) be the survival probability of \( S_i \), and \( P_i \) be the survival probability of entire infrastructure. Also, let \( S_{-i} \) denote the infrastructure without \( S_i \), and \( P_{-i} \) be its survival probability. The relative importance of \( S_i \) is captured by the aggregate failure correlation function \( C_i \) [15] given by the failure probability of \( S_{-i} \) given the failure of \( S_i \). The asymmetric role of the network is specified by two conditions [14]: (a) \( C_{N+1} = 1 \) indicates that the network failure will disrupt the entire infrastructure, and (b) \( C_i = 0, \) for \( i = 1, 2, \ldots, N \), indicates that disruptions of individual systems are uncorrelated. The correlations between components of individual systems are captured by simple first-order differential conditions on \( P_i \) [15]. This two-level
characterization helps to conceptualize the basic correlations in infrastructures, such as cloud computing and smart grid infrastructures, and provides insights into the needed defense strategies by naturally “separating” the system-level and component-level aspects.

A game between an attacker and a provider involves balancing the costs of attacks and reinforcements of systems, given by $L_A(y_1, \ldots, y_{N+1})$ and $L_D(x_1, \ldots, x_{N+1})$, respectively, with the survival probability of the infrastructure. We consider that the provider minimizes the composite utility function given by

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

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

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

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

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

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

Using appropriate $F_{D,G}$ and $F_{D,L}$ terms, the composite utility function can be specialized as: (a) the sum-form utility function given by

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

which will be minimized by the provider, and the scalar $g_D \geq 0$ represents the benefit of keeping the infrastructure operational; and (b) the product-form utility function given by

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

which will be minimized by the provider; it represents the “wasted” cost to the provider since it is the expected cost under the condition that the infrastructure fails. The sum-form and product-form utility functions [14] reflect two different values attached to keeping the infrastructure operational: the sum-form represents a weaker coupling of probability and cost terms, whereas the product-form utility function is their product. In general, they lead to qualitatively different defense strategies that are derived separately, and the corresponding expressions for the survival probabilities appear to be structurally different. The composite utility functions lead to simpler expressions for $P_I$, on cost terms and aggregate correlation functions, and their partial derivatives, is presented in a compact form by using the composite gain-cost and composite multiplier terms (defined in Section IV). We apply these results to a simplified model of cloud computing infrastructure with multiple server sites connected over a communications network.

The organization of this paper is as follows. We briefly describe the related work in Section II. In Section III, we briefly describe the infrastructure model of [14] along with the aggregate correlation function and differential conditions on system survival probabilities. We present our game-theoretic formulation using composite utility functions in Section IV, and derive NE conditions and estimates for the system survival probabilities and expected capacity. We apply the analytical results to a model of cloud computing infrastructure in Section V. We present conclusions in Section VI.

II. RELATED WORK

Critical infrastructures of power grids, cloud computing, and transportation systems rely on communications networks for connecting their constituent systems. These infrastructures are under increasing cyber and physical attacks, which the providers must counter by applying defense measures and strategies. Game-theoretic methods have been extensively applied to develop the needed defense strategies [1], [2], [10]. A comprehensive review of the defense and attack models in various game-theoretic formulations has been presented in [9]. Recent interest in cyber and cyber-physical systems led to the application of game theory to a variety of cyber security scenarios [10], [19], and, in particular, for securing cyber-physical networks [3] with applications to power grids [4], [6], [11], [12].

The system survivability terms are integrated into discrete models of cyber-physical infrastructures in various forms under Stackelberg game formulations [5]. A subclass of these models using the number of cyber and physical components that are attacked and reinforced as the main variables has been studied in [18]. These models characterize infrastructures with a large number of components, and are coarser compared to the models that consider the attacks and reinforcements of individual cyber and physical components. Under these formulations, various forms of correlation functions are used to capture the dependencies amongst the constituent systems and their components [15], [16], [18].

Collections of systems with complex interactions have been studied using game-theoretic formulations in [8], and their two-level correlations have been studied using the sum-form
utility functions in [15] and the product-form utility functions in [16]. These two utility functions are unified in [13] and the sum-form utility function has been studied under the asymmetric role of communications network in [14]. In this paper, we unify these two works by using the composite utility functions and additionally explicitly account for the asymmetric network role.

III. DISCRETE SYSTEM MODELS

We consider infrastructures with constituent systems consisting of discrete components [15], [16], and connected over a communications network [14]. The correlations between systems, including the network, in these infrastructure are characterized in terms of their survival probabilities as follows.

**Condition 3.1: Aggregate Correlation Function:** [15], [16] Let \( C_i \) denote the failure probability of rest of the infrastructure \( S_{i-1} \) given the failure of \( S_i \), and let \( C_{-i} \) denote the failure probability of \( S_i \) given the failure of \( S_{-i} \) such that

\[
C_i(1 - P_i) = C_{-i}(1 - P_{-i}),
\]

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

\[
P_I = P_i + P_{-i} - 1 + C_i(1 - P_i) = P_i + P_{-i} - 1 + C_{-i}(1 - P_{-i}).
\]

Under the statistical independence of system failures we have \( C_i = 1 - P_{-i} \) since the failure probability of \( S_{-i} \) is not dependent on \( P_i \). Substituting in the above condition, we have \( P_I = P_i P_{-i} \) as expected. Generalizations of this condition include two interesting cases: (a) If \( C_i > 1 - P_{-i} \), the failures in \( S_{-i} \) are positively correlated to those in \( S_i \), indicating that they occur with a higher probability following the latter. (b) If \( C_i < 1 - P_{-i} \), failures in \( S_{-i} \) are negatively correlated to latter failures.

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

**Condition 3.2: Asymmetric Network and Uncorrelated Systems Conditions:** [14] The aggregated correlation functions of \( S_i, i = 1, 2, \ldots, N + 1 \) satisfy the conditions: (i) for the network \( S_{N+1} \), we have \( C_{N+1} = 1 \), and (ii) for the constituent systems, we have \( C_i = 0, i = 1, 2, \ldots, N \). \( \square \)

The part (i) leads to \( P_I = P_{-(N+1)} \) which indicates the role of rest of infrastructure \( S_{-(N+1)} \) without the network. The part (ii) leads to \( P_i = P_i + P_{-i} - 1, i = 1, 2, \ldots, N \) which linearly depends on each of failure probabilities of the constituent system \( S_i \) and rest of infrastructure \( S_{-i} \).

At the system-level, the effects of reinforcements and attacks can be separated using the following two conditions:

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

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

While the reinforcements do not directly encompass the correlations between the parts of infrastructure, their failures may still be correlated due to the underlying system structures as reflected in their aggregated correlation functions. These system-level considerations for the provider are captured by the following condition which is obtained by differentiating \( P_I \) in Condition 3.1 with respect to \( x_i \) and ignoring the terms corresponding to parts (i) and (ii) above.

**Condition 3.3: De-Coupled Reinforcement Effects:** For \( P_I \) in Condition 3.1, we have for \( i = 1, 2, \ldots, N + 1 \),

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

for the provider. \( \square \)

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

The system survival probabilities satisfy the following differential condition that specifies the correlations at the component level [15], [17].

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

\[
\frac{\partial P_i}{\partial x_i} = \Lambda_i(x_1, \ldots, x_N, y_1, \ldots, y_N) P_i
\]

\[
\frac{\partial P_{-i}}{\partial x_i} = \Lambda_{-i}(x_1, \ldots, x_N, y_1, \ldots, y_N) P_{-i}
\]

for \( i = 1, 2, \ldots, N + 1 \). \( \square \)

Expressions for \( \Lambda_i \) for two cases are derived in [14] when: (a) component failures of \( S_i \) are statistically independent, and (b) \( P_i \) is expressed using the contest survival functions.

IV. GAME THEORETIC FORMULATION

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

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

for \( i = 1, 2, \ldots, N + 1 \) for the provider. We define

\[
L_G^{D,L} = G_D \frac{\partial F_{D,G}}{\partial P_I} + L_D \frac{\partial F_{D,L}}{\partial P_I}
\]

as the composite gain-cost term, wherein the gain \( G_D \) and loss \( L_D \) are “amplified” by the derivatives of their corresponding multiplier functions with respect to \( P_I \). We then define

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

as the composite multiplier, wherein the gain multiplier \( F_{D,G} \) and cost multiplier \( F_{D,L} \) are “amplified” by the derivatives of their corresponding gain and cost terms with respect to \( x_i, i = 1, 2, \ldots, N + 1 \), respectively. These two terms lead
the compact NE condition \( \frac{\partial P_I}{\partial x_i} = \frac{F_{D,i}}{L_{G,L}} \). Various terms of the composite utility function specialized to sum-form and product-form utilities are shown in Table I.

### A. NE Sensitivity Functions

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

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

\[
\hat{P}_{i;D} = \frac{\partial C_i}{\partial x_i} + \frac{F_{D,i}}{L_{G,L}}
\]

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

\[
P_{-(N+1);D} = - \frac{1}{\Lambda_{-(N+1)}} \frac{F_{D,N+1}}{L_{G,L}}.
\]

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

\[
\frac{\partial P_I}{\partial x_i} = - \frac{F_{G,L}}{L_{G,L}}.
\]

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

\[
(1 - C_i) \Lambda_i P_{i;D} + (1 - P_{i;D}) \frac{\partial C_i}{\partial x_i} = - \frac{F_{D,i}}{L_{G,L}}.
\]

(1)

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

\[
P_{i;D} = \frac{\partial C_i}{\partial x_i} + \frac{F_{D,i}}{L_{G,L}}.
\]

for \( i = 1, 2, \ldots, N + 1 \).

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

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

Then, NE condition is given by

\[
\frac{\partial P_I}{\partial x_{N+1}} = \frac{\partial P_{-(N+1);D}}{\partial x_{N+1}} = \Lambda_{-(N+1)} P_{-(N+1);D} = - \frac{F_{D,N+1}}{L_{G,L}},
\]

which completes the proof. \( \square \)

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

We now consider that the asymmetric role played by the network described in Condition 3.2, namely, its failure renders entire infrastructure unavailable; also, failures of individual systems are uncorrelated with others. The following theorem provides a single, simplified expression for the expected capacity under these conditions.

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

\[
N_I = \sum_{i=1}^{N} \left( \frac{n_i F_{D,i}}{\Lambda_i L_{G,L}} \right)
\]

for \( i = 1, 2, \ldots, N \).

**Proof:** Using Equation (1) in the proof of Theorem 4.1, under part (ii) of Condition 3.2 simplifies to the equation

\[
\Lambda_i P_{i;D} = - \frac{F_{G,L}}{L_{G,L}}.
\]

for \( i = 1, 2, \ldots, N \). Thus, we have \( P_i = - \frac{1}{N} F_{G,L} \), which provides the expression for \( N_I \). \( \square \)

This condition indicates that lower \( L_{G,L} \) and higher composite multiplier \( F_{G,L} \) lead to lower expected capacity. Typically, the composite gain-cost \( L_{G,L} \) is negative (e.g. \( g_D \) for sum-form) since it is minimized by the provider; thus, its lower value is more negative and has a higher magnitude. Also, larger values of \( \Lambda_i \) also lead to lower expected capacity.

In particular, the condition \( \Lambda_i > 1 \), called the faster than linear growth of \( \frac{\partial P_i}{\partial x_i} \), leads to lower expected capacity. This seems counter-intuitive since faster improvement in \( p_i \) due to increase in \( x_i \) leads to lower expected capacity, but note that it only characterizes the states that satisfy NE conditions.
Results similar to Theorems 4.1 and 4.2 are presented in [14], where the term $\frac{F_{D,L}^i}{G_{L,i}}$ is replaced by a more specific term

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

where $A = +$ and $A = \times$ correspond to the sum-form and product-form utilities, respectively. Theorem 4.2 subsumes these results and is also applicable to more general cases.

V. DISTRIBUTED CLOUD COMPUTING INFRASTRUCTURE

A distributed cloud computing infrastructure consists of $N$ sites, each with $l_i$ servers at site $i$, $i = 1, 2, \ldots, N$, as shown in Figure 1. The sites are connected over a communication network $S_{N+1}$ which consists of a number of routers each managing $l_{N+1}$ connections. A variety of cyber and physical attacks on its components degrade the infrastructure in different ways. Cyber attacks on the servers may be launched remotely over the network since they are accessible to users. In contrast, routers are geographically separated with limited access primarily to network administrators, and cyber attacks on routers require different techniques compared to servers. Furthermore, physical attacks in the form of fiber cuts degrade this infrastructure, but they require a proximity access by an attacker. For example, fibers connecting server sites to gateway routers and in between wide-area routers may be physically cut, thereby making sites and portions of networks inaccessible to users. Various reinforcements against the attacks may be used by the provider including replicating servers and routers to support fail-over operations, and installing redundant fiber lines to the sites and between router locations. In this section, we consider a special case where the provider and attacker randomly chooses $x_i$ and $y_i$ components to reinforce and attack, respectively, according to uniform distribution [14].

A. System Models and Correlations

This infrastructure is represented by a collection of cyber and physical models of the sites and network [14]. The cyber and physical aspects of site $S_i$ is represented using $S_{i,c}$ and $S_{i,p}$ that correspond to cyber and physical models, respectively as illustrated in Figure 2. Similarly, the network $S_{N+1}$ is represented by $S_{(N+1,c)}$ and $S_{(N+1,p)}$, which are the cyber and physical models. Let $n_{i,c}$ and $n_{i,p}$ represent the number of cyber and physical components, respectively, of site $S_i$ such that $n_i = n_{i,c} + n_{i,p}$. Similarly, let $x_{i,c}$ and $x_{i,p}$ represent the number of cyber and physical components reinforced at site $S_i$ such that $x_i = x_{i,c} + x_{i,p}$, and let $y_{i,c}$ and $y_{i,p}$ represent the number of cyber and physical components attacked at site $S_i$ such that $y_i = y_{i,c} + y_{i,p}$. The relationships between these system-level models can be captured using the aggregate correlation functions as follows (described in detail in [14]). For the communications network,

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

which reflects that a cyber attack on a router will disrupt all its $l_{N+1}$ connections, and for server sites

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

for the number of cyber and physical components, respectively, of site $S_i$. Let

$$y_{i,c} = 1 - \frac{\ln L_{D,i}^G}{\partial x_{i,c}}$$

where $y_{i,c}$ is appropriately chosen, and $y_{i,c} = 0$ otherwise. Then, the survival probability of a non-reinforced server at site $i$ is approximated by

$$P_{i,c|R} = \frac{1 + l_i [y_{i,c} - x_{i,c}]}{1 + l_i [y_{i,c} - x_{i,c}]}$$.

Thus, for cyber model $S_{i,c}$ of site $S_i$ under the independence of component attacks, we have

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

The statistical independence of cyber and physical attacks leads to the following condition [14]

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

which enables us to approximate $\Lambda_i$ by $\Lambda_{i,c}$. In the estimate $\hat{P}_{i,D}$ in Theorem 4.1, $\Lambda_i$ is in the denominator with a negative sign since its multiplier $(1 - C_i)$ lies in the interval $[0, 1]$. When other terms are fixed, $\hat{P}_{i,D}$ depends linearly on the logarithm of the number of cyber attacks $y_{i,c}$ with a multiplication factor $a$, and inversely on the logarithm of $[y_{i,c} - x_{i,c}]^+$ which is the number of attacks exceeding the reinforcements. However, the exact relationship depends on the sign of $a$, which could be positive or negative based on other factors $G_{i,c}$, $P_{D,i}^{D,L}$, and $P_{G,L}^{D,L}$.}

B. Expected Capacity

Based on Theorem 4.2 we obtain the following expression for the expected number of servers

$$N_I = \sum_{i=1}^{N} \left( \frac{\frac{n_i F_{D,i}^{D,L}}{P_{G,L}^{D,L} \ln \left( 1 + \frac{y_{i,c}}{1 + l_i [y_{i,c} - x_{i,c}]} \right)} \right).$$
It is of future interest to compare this formulation to ones whose utility functions contain the expected capacity term in place of infrastructure survival probability terms. Another future direction is to consider the simultaneous cyber and physical attacks on multiple systems and components, and sequential game formulations of this problem. Performance studies of our approach using more detailed models of cloud computing infrastructure, smart energy grid infrastructures and high-performance computing complexes would be of future interest.

**REFERENCES**


