Defense Strategies and Expected Capacity of High Performance Computing Infrastructures

Nageswara S. V. Rao
Oak Ridge National Laboratory
Oak Ridge, TN, USA
raons@ornl.gov

Chris Y. T. Ma
Hang Seng Management College
Hong Kong
chris.ytma@gmail.com

Neena Imam
Oak Ridge National Laboratory
Oak Ridge, TN, USA
imamn@ornl.gov

Fei He
Texas A&M University
Kingsville, TX, USA
fei.he@tamuk.edu

ABSTRACT

We consider high performance computing infrastructures consisting of multiple sites connected over a wide-area network. These sites house heterogeneous computing systems, network elements and local-area connections, and the wide-area network plays a critical, asymmetric role of providing the vital connectivity between them. We model this infrastructure as a recursive system of systems, wherein the basic systems at the finest levels are composed of discrete cyber and physical components. These components may be disabled by cyber and physical disruptions, and their reinforcements protect against them albeit at a cost. We utilize results from a game formulation based on (i) characterizing the disruptions between systems at each level of recursion using aggregate failure correlation functions, and within basic systems using the multiplier functions, and (ii) using utility functions expressed in terms of the number of basic system components attacked and reinforced. At Nash Equilibrium, we derive expressions for the expected capacity of the infrastructure given by the number of computing nodes that are operational and connected to the network.

CCS CONCEPTS

• Computing methodologies → Modeling; • Networks → Cyber-physical networks;

Keywords and phrases: high performance computing infrastructure, networked systems, composite utility functions, aggregated correlation function, game theory, Nash Equilibrium

1 INTRODUCTION

A Distributed High Performance Computing (HPC) infrastructure consists of supercomputer sites connected over a Wide-Area Network (WAN). The computing systems could be heterogeneous with custom computing nodes equipped with Graphical Processing Units (GPU), Multiple Integrated Core (MIC) systems, neuromorphic and

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

other accelerators. They are housed in facilities with climate controls provided by Heating, Ventilation and Air Conditioning (HVAC) systems. These computing systems are connected via Local Area Network (LAN) switches to border routers, which are in turn connected to WAN via physical fibers. A distributed HPC infrastructure with N sites connected over WAN is shown in Figure 1. The HVAC system consists of a physical cooling tower and a mobile app that controls its operations such as temperature settings. A successful operation of these infrastructures depends on complex interactions between various cyber and physical components, which can be disrupted by attacks or other incidental failures. Hence, the infrastructure providers are required to strategically reinforce the components by taking into account various cyber and physical parts and correlations among them.

The wide ranging complexities of site systems, in particular supercomputers, lead to correlations at multiple levels, which makes

ACM acknowledges that this contribution was authored or co-authored by an employee, contractor, or affiliate of the United States government. As such, the United States government retains a nonexclusive, royalty-free right to publish or reproduce this article, or to allow others to do so, for government purposes only.

ICDCN '19, January 4–7, 2019, Bangalore, India

© 2019 Association for Computing Machinery.

ACM ISBN 978-1-4503-6094-4/19/01...\$15.00

<https://doi.org/10.1145/3288599.3288625>

the existing approaches based on System of Systems (SoS) formulations [10] inadequate. We utilize the recent *Recursive SoS* (RSoS) formulations [9] to capture the multi-level correlations, wherein each system is recursively defined. The *basic systems* at (possibly different) finest levels are entirely composed of discrete cyber and physical components. This formulation enables the incorporation of different levels of details to match the varying complexities of sites. In particular, it generalizes the two-level characterizations in [7, 10] wherein all systems consist solely of cyber and physical components.

A variety of cyber and physical attacks can be launched on the components of such an infrastructure, and they can degrade its capacity, typically, measured by the total number of computing nodes available to users. The computing nodes are accessible to users over the network, which makes them vulnerable to cyber attacks. Physical attacks in the form of fiber cuts and cooling tower degradations represent different attack vectors that degrade this infrastructure; however, they require physical proximity access by attackers. In addition, incidental disruptions such as device failures may also propagate within and across systems at various levels. Component reinforcements may be put in place to protect against these attacks and incidental failures, including deploying special-purpose firewalls, replicating routers in fail-over configurations, and installing redundant fiber lines to sites and between wide-area network router locations. While such reinforced components can survive direct attacks, computing nodes may still be unavailable to users due to propagative effects of attacks on other components [4]. For instance, even if the supercomputers at a site are hardened against cyber attacks, they can all be made unavailable, for example, by cutting the fiber connections to the site with physical attacks, or by bringing down the HVAC system by a single cyber attack on control app. Non-reinforced components, on the other hand, will be disabled by direct attacks. The reinforcements and attacks incur costs to the provider and attacker, respectively, and their corresponding benefits depend not only on the components but also on various correlations, due to the propagation of disruptions within the sites and between sites over the network.

An RSoS S used to model an HPC infrastructure [9] 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 , $i = 1, 2, \dots, N_1$, each of which itself is a recursively defined RSoS. By recursively expanding all non-basic systems, we reach the basic systems S_i , $i = 1, 2, \dots, N_S$. Let y_i and x_i denote the number of components of a basic system S_i attacked and reinforced, respectively. 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 a basic or non-basic system $S = S_i^k$ at level k , and $P_I(S)$ denote the survival probability of entire RSoS S . The *aggregate failure correlation function* C_i^k is the failure probability of the “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 the rest of RSoS, which is denoted by $S_{-S_i^k}$. In addition, correlations among the components are characterized by simple product-form, first-order differential

Figure 2: HPC network system with multi-core and GPU computing nodes.

conditions on $P_I(S_i)$ of basic system S_i , $i = 1, 2, \dots, N_S$ using the *system multiplier functions* [8].

We consider a game wherein individual system components can be disrupted by the attacker, and can be reinforced by the provider to defend against the attacks [7, 10]. The costs of attacks and reinforcements of basic systems are denoted by $L_A(y_1, \dots, y_{N_S})$ and $L_D(x_1, \dots, x_{N_S})$, respectively. The provider minimizes the *utility function* given by the sum of two parts:

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

where the first part corresponds to reward and the second part corresponds to cost. At Nash Equilibrium (NE), the attacker and provider minimize their respective utility functions [1]. The *expected capacity* of HPC infrastructure is the expected number of available computing nodes, given by

$$N_I = \sum_{i=1}^N n_{(i,c)} P_{(i,c)},$$

where $n_{(i,c)}$ is the number of computing nodes at site i , and $P_{(i,c)}$ is the survival probability of its computing system. In this paper, we utilize the definitions and NE conditions from earlier works [9] to obtain estimates of N_I in terms of cost terms, correlation functions, system survival probabilities, and their partial derivatives.

The organization of this paper is as follows. In Section 2, we expand the HPC infrastructure model of [9]. In Section 3, we present system survival probabilities at NE from [9] and estimates for expected capacity. We present conclusions in Section 4.

2 DISTRIBUTED HPC INFRASTRUCTURE

A generic distributed HPC infrastructure shown in Figure 1 consists of N sites connected over a wide-area network, which is represented as system $N + 1$. Each HPC site houses a supercomputer of potentially different size and architecture, and its HVAC system is controlled by a mobile phone app. The computing system consists of a number of computing nodes connected over an interconnect,

This infrastructure model can be further refined by expanding each $S_{(k,c)}^3$ into system of computing nodes $S_{(k,c,p)}^4$ and interconnect basic system $S_{(k,c,i)}^4$. Then, $S_{(k,c,p)}^4$ can be further decomposed into $n_{(k,c)}$ basic systems $S_{(k,c,p_j)}^5$, $j = 1, 2, \dots, n_{(k,c)}$, each containing multi-core CPU and GPU components, as shown in Figure 4. As in the previous case, there are two basic systems at level 2 corresponding to the network, and $2N$ basic systems at level 4 corresponding to HVAC system. Additionally, there are N basic systems at level 4 corresponding to the interconnects of computing systems at all sites, and a total of $\sum_{k=1}^N n_{(k,c)}$ basic systems at level 5 that correspond to computing nodes. The components of basic systems in this expanded version are primarily subject to cyber disruptions since physical disruptions require access deep into the facilities, typically, racks that contain computing and interconnect components.

3 EXPECTED CAPACITY

Under the conditions of the asymmetric network and uncorrelated systems, and de-coupled reinforcement effects (see [7] for formal definitions), the correlation functions C_i^k at recursive level k and multiplier functions Λ_b are used to characterize NE conditions. 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 the product correlation function C_{Π_b} and product multiplier function Λ_{Π_b} , respectively, for $b = 1, 2, \dots, N_S$, are given by [9]

$$\hat{P}_{b,D} = \frac{\Delta_{\Pi_b} \frac{\partial C_b}{\partial x_b} + \frac{\partial C_{\Lambda_b}}{\partial x_b} + \frac{F_{G,L}^{D,b}}{L_{G,L}^D}}{\Delta_{\Pi_b} \frac{\partial C_b}{\partial x_b} - (1 - C_{\Pi_b}) \Lambda_b}$$

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

$$\tilde{P}_{b,D} = -\frac{1}{\Lambda_{\Pi_b}} \frac{F_{G,L}^{D,b}}{L_{G,L}^D},$$

where $L_{G,L}^D$ is the composite gain-cost and $F_{G,L}^{D,b}$ is the composite multiplier [7]. 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_{Π_b} , basic system multiplier function Λ_b , $L_{G,L}^D$ and $F_{G,L}^{D,b}$ [7].

When applied directly to a RSoS $\mathcal{S}$ that consists of only basic systems S_b (namely, with 0 level of recursion, or $m_b = 0$), this estimate provides a simpler expression derived for SoS than in [5]

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

wherein we have $\Delta_{\Pi_b} = 1$, $\Lambda_{\Pi_b} = \Lambda_b$, $C_{\Pi_b} = C_b$ and $\frac{\partial C_{\Lambda_b}}{\partial x_b} = 0$. 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.

Consider the computing system at site k , i.e., $b = (k, c)$. The survival probability of the computing system at site k is given by

$$\hat{P}_{(k,c);D} = \frac{\Delta_{\Pi_{(k,c)}} \frac{\partial C_{(k,c)}^3}{\partial x_{(k,c)}} + \frac{\partial C_{\Lambda_{(k,c)}}}{\partial x_{(k,c)}} + \frac{F_{G,L}^{D,(k,c)}}{L_{G,L}^D}}{\Delta_{\Pi_{(k,c)}} \frac{\partial C_{(k,c)}^3}{\partial x_{(k,c)}} - (1 - C_{\Pi_{(k,c)}}) \Lambda_{(k,c)}}.$$

Since the term $\Lambda_{(k,c)}$ appears in the denominator of $\hat{P}_{(k,c);D}$, $\hat{P}_{(k,c);D}$ decreases with the number of cyber attacks $y_{(k,c)}$, and increases with $[y_{(k,p)} - x_{(k,p)}]_+$, $[y_{(k,t)} - x_{(k,t)}]_+$, $[y_{(k,a)} - x_{(k,a)}]_+$ which are the numbers of attacks exceeding the reinforcements on fiber, HVAC cooling tower, and HVAC control app, respectively. The latter condition may appear counter-intuitive at the surface but note that it only characterizes the states that satisfy NE conditions.

Since the expected capacity of the HPC infrastructure is given by

$$N_I = \sum_{k=1}^N n_{(k,c)} P_{(k,c)} = \sum_{k=1}^N n_{(k,c)} P_I(S_{(k,c)}^3),$$

where $n_{(k,c)}$ is the number of computing nodes at site k , its estimate is given by

$$\hat{N}_I = \sum_{k=1}^N n_{(k,c)} \hat{P}_{(k,c);D}.$$

Thus, we have the estimate

$$\hat{N}_I = \sum_{k=1}^N \frac{n_{(k,c)} \left(\Delta_{\Pi_{(k,c)}} \frac{\partial C_{(k,c)}^3}{\partial x_{(k,c)}} + \frac{\partial C_{\Lambda_{(k,c)}}}{\partial x_{(k,c)}} + \frac{F_{G,L}^{D,(k,c)}}{L_{G,L}^D} \right)}{\Delta_{\Pi_{(k,c)}} \frac{\partial C_{(k,c)}^3}{\partial x_{(k,c)}} - (1 - C_{\Pi_{(k,c)}}) \Lambda_{(k,c)}},$$

where $\Delta_{\Pi_{(k,c)}} = (1 - C_1^1) (1 - C_{(k)}^2)$,

and $C_{\Pi_{(k,c)}} = 1 - (1 - C_{(k,c)}^3) (1 - C_1^1) (1 - C_{(k)}^2)$. Applying the condition that the failure of the computation components of different sites are uncorrelated and the asymmetric network condition [5, 6], we have $C_2^1 = 1$, $C_1^1 = 0$, $C_{(k)}^2 = 0$, and $C_{(k,c)}^3 = 0$ for $k = 1, \dots, N$. Hence, we have $\Delta_{\Pi_{(k,c)}} = 1$ and $C_{\Pi_{(k,c)}} = 0$, and the expected capacity of the HPC infrastructure is given by

$$\hat{N}_I = \sum_{k=1}^N \frac{n_{(k,c)} \left(\frac{\partial C_{(k,c)}^3}{\partial x_{(k,c)}} + \frac{\partial C_{\Lambda_{(k,c)}}}{\partial x_{(k,c)}} + \frac{F_{G,L}^{D,(k,c)}}{L_{G,L}^D} \right)}{\frac{\partial C_{(k,c)}^3}{\partial x_{(k,c)}} - \Lambda_{(k,c)}},$$

where $\frac{\partial C_{\Lambda_{(k,c)}}}{\partial x_{(k,c)}} = \frac{\partial C_{(k)}^2}{\partial x_{(k,c)}} (1 - P_I(S_{(k)})) + (1 - P_I(S_1^1)) \frac{\partial C_1^1}{\partial x_{(k,c)}}$.

Although C_2^1 , C_1^1 , $C_{(k)}^2$, and $C_{(k,c)}^3$ for $k = 1, \dots, N$ are constants, their partial derivatives with respect to $x_{(k,c)}$ could be non-zero, as other parameters change to keep them constant. The equation indicates that higher survival probability of each site and all the sites together leads to lower expected computation capacity of the HPC infrastructure, since $\frac{\partial C_{(k)}^2}{\partial x_{(k,c)}}$ and $\frac{\partial C_1^1}{\partial x_{(k,c)}}$ should be non-negative. The effects of attack and defense of the fiber and HVAC system on the expected computation capacity are captured by the $\Lambda_{(k,c)}$ term in the denominator. Since $\frac{\partial P_I(S)}{\partial x_b} = -\frac{F_{G,L}^{D,b}}{L_{G,L}^D}$, we have $\frac{F_{G,L}^{D,b}}{L_{G,L}^D} \leq 0$. If we have $\frac{\partial C_{(k,c)}^3}{\partial x_{(k,c)}} + \frac{\partial C_{\Lambda_{(k,c)}}}{\partial x_{(k,c)}} \leq -\frac{F_{G,L}^{D,(k,c)}}{L_{G,L}^D}$ and $\frac{\partial C_{(k,c)}^3}{\partial x_{(k,c)}} < \Lambda_{(k,c)}$, then the

effects of attack and defense of the fiber and HVAC system on the expected computation capacity are similar to those on the survival probability of a site discussed before, for instance, the capacity decreases with the number of cyber attacks $y_{(k,c)}$, and increases with $[y_{(k,p)} - x_{(k,p)}]_+$, $[y_{(k,t)} - x_{(k,t)}]_+$, and $[y_{(k,a)} - x_{(k,a)}]_+$. These observations may appear counter-intuitive at the surface but note that they only characterize the states that satisfy NE conditions.

The above expected capacity N_I of HPC infrastructure is based on counting the number of computing nodes at various sites based on the coarse RSoS model. It can be defined to reflect the number of CPU cores or GPU cores by suitably refining the basic computing system $S_{(k,c)}^3$ into $n_{(k,c)}$ nodes. Let $n_{(k,c,p_j,cpu)}$ and $n_{(k,c,p_j,gpu)}$ denote the number of CPU and GPU cores of the computing node $S_{(k,c,p_j)}^5$, $j = 1, 2, \dots, n_{(k,c)}$. Then the expected number of number of CPU cores is given by

$$N_I^{cpu} = \sum_{k=1}^N \left(\sum_{j=1}^{n_{(k,c)}} n_{(k,c,p_j,cpu)} P_{(k,c,j)} \right),$$

where $P_{(k,c,j)} = P_I(S_{(k,c)}^3)$ which represents the survival probability of computing system $S_{(k,c)}^3$ under the refined RSoS model with respect to computing node $S_{(k,c,p_j)}^5$. Using the refined RSoS model shown in Figure 4, we obtain

$$P_I(S_{(k,c)}^3) = P_I(S_{(k,c,p)}^4) + P_I(S_{-S_{(k,c,p)}^4}) - 1 + C_{(k,c,p)}^4 (1 - P_I(S_{(k,c,p)}^4)).$$

Then, using the next level of refinement, we obtain

$$P_I(S_{(k,c,p)}^4) = P_I(S_{(k,c,p_j)}^5) + P_I(S_{-S_{(k,c,p_j)}^5}) - 1 + C_{(k,c,p_j)}^5 (1 - P_I(S_{(k,c,p_j)}^5)).$$

Similarly, the expected number of GPU cores is given by

$$N_I^{gpu} = \sum_{k=1}^N \left(\sum_{j=1}^{n_{(k,c)}} n_{(k,c,p_j,gpu)} P_{(k,c,j)} \right).$$

Then, the estimates $\hat{N}_I^{cpu}$ and $\hat{N}_I^{gpu}$ can be obtained as above using the corresponding product multiplier and product aggregate correlation functions.

4 CONCLUSIONS

We consider a class of infrastructures with HPC sites connected over a wide-area network. By utilizing correlations at system- and component-level, we consider a formulation of ensuring the infrastructure survival as a game between an attacker and a provider, by using composite utility functions [7, 10]. We utilized the survival probability estimates at NE from previous works [9] to provide compact expressions for the expected capacity given by the number of operational and accessible computing nodes. They provide insightful information about the dependence of capacity on cost and correlation parameters as well as the number of reinforced and attacked components. In particular, by employing sub-models of sites, effects of parts of the system on the expected capacity can

be inferred. Such inferences can be extended to individual components of the sites; for example, it can be inferred that reinforcement of HVAC app nullifies the amplification effect due to co-location of the servers at sites. These results are obtained by applying the extensions of previous results on interconnected systems [2, 3] and cyber-physical infrastructures [11] to the multi-site HPC infrastructure. In particular, the RSoS formulation of [9] is expanded to HPC infrastructure by taking into account the details of computing systems and the asymmetric aspects of the network connectivity.

The RSoS models presented here can be further refined by taking finer details into account such as the specifics of interconnects. In particular, performance studies of our approach using more detailed models of HPC infrastructure would be of future interest. The formulation of this paper may be extended to include cases where targeted attacks and reinforcements of specific individual components are explicitly represented. It is of future interest to compare this formulation to ones whose utility functions explicitly utilize the 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.

Acknowledgments

This work is funded by the Mathematics of Complex, Distributed, Interconnected Systems Program and RAMSES project, 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] D. Fudenberg and J. Tirole. *Game Theory*. MIT Press, 2003.
- [2] K. Hausken. Strategic defense and attack of complex and dependent systems. *Reliability Engineering*, 95(1):29–42, 2009.
- [3] K. Hausken. Defense and attack for interdependent systems. *European Journal of Operational Research*, 256:582A–591, 2016.
- [4] H. Orojloo and M. A. Azgomi. A method for evaluating the consequence propagation of security attacks in cyber-physical systems. In *Future Generation Computer Systems*, Aug 2016.
- [5] 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.
- [6] 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.
- [7] 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.
- [8] 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.
- [9] N. S. V. Rao, C. Y. T. Ma, and F. He. On defense strategies for recursive system of systems using aggregated correlations. In *International Conference on Information Fusion*, 2018.
- [10] N. S. V. Rao, C. Y. T. Ma, F. He, D. K. Y. Yau, and J. Zhuang. Cyber-physical correlation effects in defense games for large discrete infrastructures. *Games*, 9(3):52, 2018.
- [11] 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.