Robustness of Cyber-Physical Network Infrastructures: A Game Theoretic Approach

Nagi Rao — Oak Ridge National Laboratory; **David Yau, Chris Ma** — Purdue University
Jun Zhuang, Fei He — State University of New York, Buffalo

Introduction

The operation of infrastructures for cyber services, such as network connectivity and computing capacity, requires the functioning of:

(i) *cyber components* such as computers, routers and switches, and
(ii) *physical components* such as fiber routes, cooling and power systems.

Their operation is cyber-physical in nature due to its dependence on both cyber and physical components. The components may be degraded by factors such as incidental weather-related power failures and device failures as well as deliberate cyber attacks on computers and physical attacks on fiber routes. While cyber attacks on computing systems and networks seem to get more public media attention, in many occasions the infrastructure degradations have been due to physical factors such as power blackouts and back hoe incidents on fiber routes

We consider a class of cyber infrastructures modeled as discrete systems of cyber and physical components, wherein the infrastructure is subject to incidental degradations and attacks targeting service interruptions. The provider is charged with reinforcing certain portions of the infrastructure to defend against the degradations of both kinds. These infrastructures are characterized by :

(a) knowledge about the capabilities and locations of the infrastructure is available to the attacker, primarily from the information provided to facility users;
(b) knowledge about incidental degradations is available to both parties, primarily from public sources;
(c) costs incurred by the defender and attacker are private information and not available to the other; and
(d) strategies used by the defender in choosing which parts to reinforce, and by the attacker in choosing which parts to attack are not revealed to the other.

Our contribution: Systematic analysis and design methods for achieving robustness of network and computing infrastructures using a game theoretic approach.

Cyber Infrastructures

A. UltraScience Net

USN is a wide-area network testbed that provides suites of 10Gbps connections of several thousands of miles in support of high-performance network tests USN infrastructure consists of the data-plane of two parallel OC192 connections with co-location sites at Oak Ridge, Chicago, Seattle and Sunnyvale.

B. Computer Infrastructure Models

We consider cloud and high-performance computing infrastructures that provide computing capabilities to users in two different ways:

- **Cloud Computing Infrastructures** (CCI) provide commodity computing capacity using servers distributed over the Internet, wherein the user is typically unaware of the location of servers that execute the task.
- **High-Performance Computing Infrastructures** (HPCI) make available supercomputers to users, who typically access specific systems, and these computers are typically connected over high capacity networks.

Cyber and Physical Attacks

We consider that the defender and attacker make Boolean choices of defending and attacking the cyber and physical part as a whole, respectively. The utility function of the attacker is a sum of:

(i) a cost term representing the cost of launching an attack, and
(ii) a system performance term representing benefit of rendering the system non-operational.

Based on Nash Equilibrium the following are the strategies of attacker and defender

Attacker: utility

$$U_A(P_A, Q_D) = P_A C^A Q_D^T + P_{SA} R^A Q_{SD}^T$$

will attack cyber or physical according to:

$$p_{s|c} > \frac{a_c}{2s(1-q_{scp})} \qquad p_{s|p} > \frac{a_p}{2s(1-q_{scp})}$$

probability of successful attacks

Defender: utility

$$U_D(P_A, Q_D) = P_A C^D Q_D^T - P_{SA} R^A Q_{SD}^T$$

will defend both cyber and physical parts under

$$q_{s|cp} > \frac{d_{cp}}{2s(p_{sc}+p_{sp})}$$

according to probability of successful defense

Component Attacks

Cyber and physical parts consist of components that can be individually attacker and defended: Rows and columns of gain matrices correspond to number of cyber and physical components.

Attacker: row represents number of cyber or physical components to be attacked

$$P_A = \left[p_{c1} p_{c2} \cdots p_{cn_c} p_{p1} p_{p2} \cdots p_{pn_p} p' \right]$$

cost term:

$$P_A C^A Q_D^T = \sum_{j=1}^{n_c n_p + 1} q_j \left(\sum_{l=1}^{n_c} p_{ci} c_{l,j} + \sum_{l=1}^{n_c} p_{pi} c_{n_c+l,j} \right)$$

system term

$$P_A R^A Q_D^T = \sum_{i=1}^{n_c+n_p+1} \sum_{j=1}^{n_c n_p+1} p_i s_{ij} q_j$$

Defender: column represents number of cyber and physical components to be defended.

$$Q_D = \left[q_{1:1} q_{1:2} \cdots q_{1:n_p} \cdots q_{n_c:1} q_{n_c:2} \cdots q_{n_c:n_p} q' \right]$$

Nash Equilibrium: Deterministic and polynomial time computable – provides high-level system status

$$\text{system state} = \begin{cases} \text{survive} & \text{if } [(x_c \geq k_c) \wedge (x_p \geq k_p)] \\ & \vee [(y_c < n_c - k_c) \wedge (y_p < n_p - k_p)] \\ \text{not} & \text{else if} \\ & [(x_c < k_c) \wedge (y_c > n_c + x_c - k_c)] \\ & \vee [(x_p < k_p) \wedge (y_p > n_p + x_p - k_p)] \\ \text{either} & \text{else} \end{cases}$$

Cyber Infrastructures

The gain matrices of the game are specified based on the infrastructure:

Defender cost: $d_{i,j} = d_{l,j_c;j_p} = j_c d_{dc} + j_p d_{dp}$

Attacker cost:

cyber $c_{i,j} = i c_{ac}$

physical $c_{i,j} = (i - n_c)^{\alpha} c_{ap}$

system matrix:

$$-s_{i,j} = \begin{cases} -2S & \text{if } [(y_c = 0) \wedge (y_p = 0)] \\ 2S & \text{else if} \\ & [(x_c < k_c) \\ & \wedge (y_c > n_c + x_c - k_c)] \\ & \vee [(x_p < k_p) \\ & \wedge (y_p > n_p + x_p - k_p)] \\ -S\left[1 + \frac{x_c - k_c}{x_c - k_c + y_c}\right] & \text{else if } y_p = 0 \\ -S\left[1 + \frac{x_p - k_p}{x_p - k_p + y_p}\right] & \text{else if } y_c = 0 \end{cases}$$

Cloud Infrastructure

Expected capacity of the cloud computing infrastructure under uniform and statistically independent attack and defense models: for n_s sites with n_{s_i} servers at site i

number of components attacked: $y_a; a = c, p$

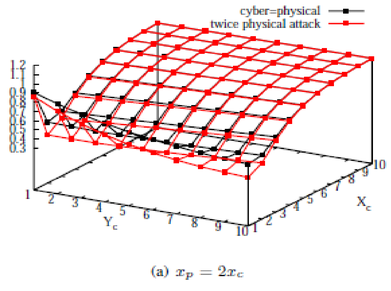
number of components defended: $x_a; a = c, p$

$$\left(\sum_{i=1}^{n_s} n_{s_i} \left[1 - \sum_{a=c,p} \left(\left[1 - \frac{1}{n_a} \right]^{x_a} \left[1 - \left(1 - \frac{1}{n_a} \right)^{y_a} \right] \right) \right] \right)$$

$$= \left(\sum_{i=1}^{n_s} n_{s_i} \right) \left[1 - \sum_{a=c,p} \left(\left[1 - \frac{1}{n_a} \right]^{x_a} \left[1 - \left(1 - \frac{1}{n_a} \right)^{y_a} \right] \right) \right]$$

$$= \left(\sum_{i=1}^{n_s} n_{s_i} \right) f_{U(n_c, n_p, x_c, x_p, y_c, y_p)}$$

Robustness fraction



(a) $x_p = 2x_c$

HPC Infrastructure

Under uniform and statistically independent attack and defense models, the expected number of supercomputers operational: for n_s sites

number of components attacked: $y_a; a = c, p$

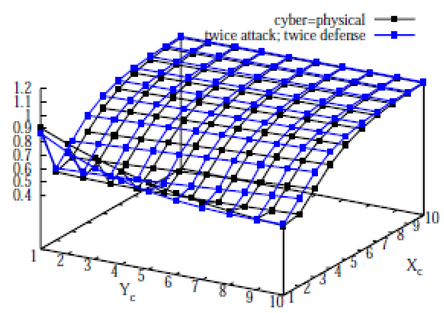
number of components defended: $x_a; a = c, p$

$$\hat{N}_{HPC} = \sum_{i=1}^{n_s} \left[1 - \sum_{a=c,p} \left(\left[1 - \frac{1}{n_a} \right]^{x_a} - \left(1 - \frac{1}{n_a} \right)^{x_a + y_a} \right) \right]$$

$$= n_s \left[1 - \sum_{a=c,p} \left(\left[1 - \frac{1}{n_a} \right]^{x_a} \left[1 - \left(1 - \frac{1}{n_a} \right)^{y_a} \right] \right) \right]$$

$$= n_s f_{U(n_c, n_p, x_c, x_p, y_c, y_p)}$$

Robustness fraction



(c) $x_p = 2x_c$ and $y_p = 2y_c$

Conclusions

We presented a systematic analysis and design framework for cyber infrastructures based on two game theoretic models that capture different levels of detail. We studied the strategic interactions between an attacker and a defender using this game-theoretic approach. When the utility function of the attacker and provider consist of sums of individual cost and system terms, NE is deterministic, and is polynomial-time computable under uniform costs. We utilized these results to design/reinforce USN network infrastructure and models of cloud and high-performance computing infrastructures.

Case	k_c	k_p	c_{ac}	c_{cp}	d_{dc}	d_{dp}	attack	defense	survival	residual capacity
A.	25	1	1	1	1	1	100 (c)	25(c), 1(p)	100% (both)	50.75 (both)
B.	25	1	1	10	10	1	100 (c)	25(c), 1(p)	100% (both)	50.75 (both)
C.	25	2	1	10	10	1	100 (c)	25(c), 2(p)	100% (both)	50.69 (both)
D.	25	1	10	1	10	1	1(p)	25(c), 1(p)	100% (both)	65.46 (prop), 58.26 (uni)
D'.	25	1	10	1	10	1	1(p)	25(c), 1(p)	100% (both)	57.26 (both)
E.	25	3	1	10	10	1	5(p)	25(c), 3(p)	100% (both)	66.10 (prop), 65.00 (uni)

TABLE I
SIMULATION OF 1000 SERVER CLOUD COMPUTING INFRASTRUCTURE; C AND P DENOTE CYBER AND PHYSICAL PARTS, AND PROP AND UNI DENOTE PROPORTIONAL AND UNIFORM STRATEGIES.

Publications

1. N. S. V. Rao, C. Y. T. Ma, J. Zhung, F. He, D. K. Y. Yau, Cloud computing infrastructure robustness: A game theory approach, International Conference on Computing, Networking and Communications,2012.
2. N. S. V. Rao, Y. Narahari, C. E. Veni Madhavan, D. K. Y. Yau, C. Y. T. Ma, An analytical Framework for cyber-physical networks, *in Securing Cyber-Physical Infrastructures: Foundations and Challenges*, Editors: S. Das, K. Kant and N. Zhang, 2011
3. N. S. V. Rao, C. Y. T. Ma, D. K. Y. Yau, On robustness of a class of cyber-physical network infrastructures, Workshop on Design, Modeling and Evaluation of Cyber Physical Systems, 2011.

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 performed at Oak Ridge National Laboratory managed by UT-Battelle, LLC for U.S. Department of Energy under Contract No. DE-AC05-00OR22725.

For further information

Please contact: Nagi Rao *raons@ornl.gov*.