Robustness of Cyber-Physical Network Infrastructures: A Game Theoretic Approach [1]

Math Project Title: Mathematics of Cyber-Physical Networks

Nageswara S. V. Rao
Oak Ridge National Laboratory
Oak Ridge, TN 37381

David K. Y. Yau
Purdue University
West Lafayette, IN 47907

Chris Y. T. Ma
Advanced Digital Sciences Center
Singapore, 138632

Fei He, Jun Zhuang
State University of New York at Buffalo
Buffalo, NY 14260

Abstract

The operation of a number of infrastructures, such as cloud computing and high-performance computing complexes, requires the continued functioning of cyber components such as computers, routers and switches, and also physical components such as fiber routes, cooling and power systems. While cyber attacks seem to get much public media attention, many infrastructure degradations have been due to physical factors such as back hoe incidents on fiber routes. The provider of these infrastructures is charged with initial provisioning and subsequent reinforcing of the infrastructure to defend against the degradations of both kinds. We consider a class of cyber-physical infrastructures modeled as discrete systems such that: (a) knowledge about the capabilities and locations of the infrastructure is available to the attacker, primarily from the information provided to 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 (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. These considerations lead to game theoretic models where information in items (a) and (b) is public, and that in items (c)-(d) is private.

The cyber and physical parts consist of components that may be individually attacked and defended, and the infrastructure requires a minimum number of both to function. The utility functions of the attacker and defender are sums of cost and system terms. Despite the probabilistic strategies, we show that the Nash Equilibrium (NE) for these games is deterministic in that underlying probabilities are either 0 or 1. If the costs depend only on the number of components, NE can be computed with polynomial complexity in the number of components for both infrastructure provisioning and reinforcement during operation. The performance degradations of the infrastructure at NE, including complete shutdown, depend on further details of reinforcement and attack strategies. We also incorporate the probabilities of successful attack and defense of components, and also the probabilities of their incidental failures. In the latter case, the attacker is at a certain advantage, but otherwise the game theoretic results remain qualitatively similar.

We analyze game theoretic models of cloud and high-performance computing infrastructures. In the former, computing servers are distributed at various sites over the Internet, and in the latter computing power is concentrated at specific supercomputing facilities. We apply the game theoretic methods to infer the conditions for the survival of these systems at NE, and derive expected performance levels under statistical independence conditions. Our results show that the cloud computing provider can hide and exploit the information about the distribution of servers at various sites to improve the expected performance against the attacker.

[1] 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.