Altunay, Mine; Leyffer, Sven; Linderoth, Jeffrey T.; Xie, Zhen
Optimal response to attacks on the open science grid. (English) Zbl 1218.68065

Summary: Cybersecurity is a growing concern, especially in open grids, where attack propagation is easy because of prevalent collaborations among thousands of users and hundreds of institutions. The collaboration rules that typically govern large science experiments as well as social networks of scientists span across the institutional security boundaries. A common concern is that the increased openness may allow malicious attackers to spread more readily around the grid.

We consider how to optimally respond to attacks in open grid environments. To show how and why attacks spread more readily around the grid, we first discuss how collaborations manifest themselves in the grids and form the collaboration network graph, and how this collaboration network graph affects the security threat levels of grid participants. We present two mixed-integer program (MIP) models to find the optimal response to attacks in open grid environments, and also calculate the threat level associated with each grid participant. Given an attack scenario, our optimal response model aims to minimize the threat levels at unaffected participants while maximizing the uninterrupted scientific production (continuing collaborations). By adopting some of the collaboration rules (e.g., suspending a collaboration or shutting down a site), the model finds optimal response to subvert an attack scenario.

MSC:
68M99 Computer system organization
90C11 Mixed integer programming

Keywords:
cybersecurity; optimization; network security; attack propagation; multiobjective; integer optimization

Full Text: DOI