Simulation-Based Strategic Analysis of Complex Security Scenarios

SAND2011-5408P

Sandia National Laboratories

Yevgeniy Vorobeychik, 8953; Joshua Letchford, 8953; Robet Armstrong, 8961

Early Career R&D Program

Problem

Defender wants to protect assets from attack.
Defense is expensive, so should be cost-effective.
Assets are interdependent: failure of one asset can lead to failures in others. The defender has an intrinsic value for each asset if it does not fail.

Attacker has an intrinsic value for each asset, can attack up to K targets, choosing these to maximize his total expected value.

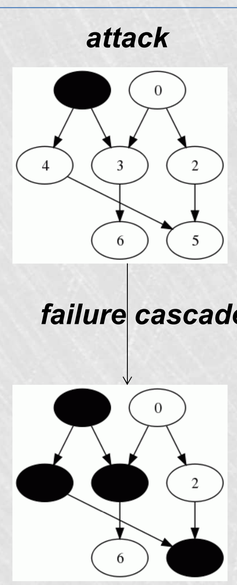
Example: (cyberdefense) Wish to secure a set of connected, interdependent resources, but too costly to maximally secure everything. Attacker will intelligently choose targets.

Approach

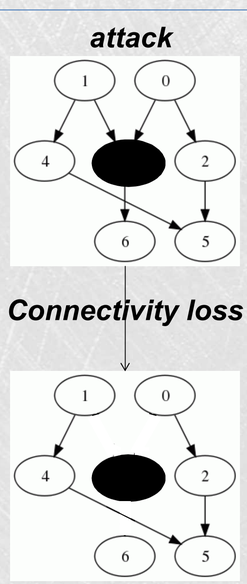
Combine simulation, optimization, and game theory

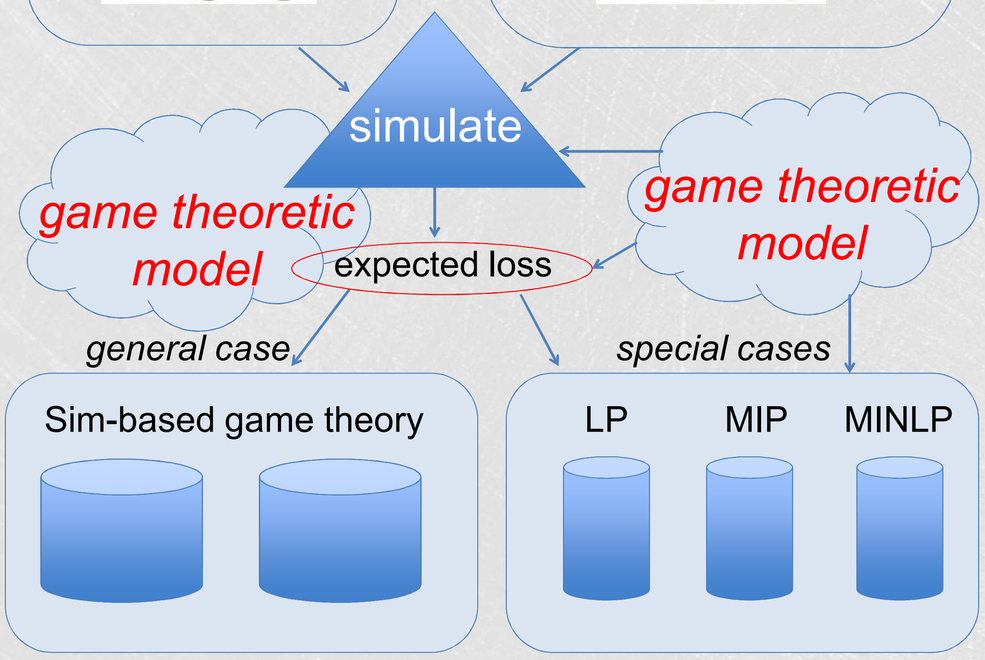
Failure Models

Cascading failures



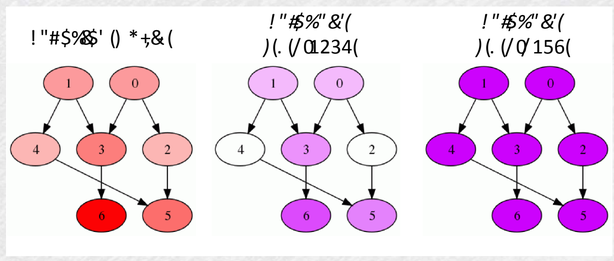
Degraded connectivity



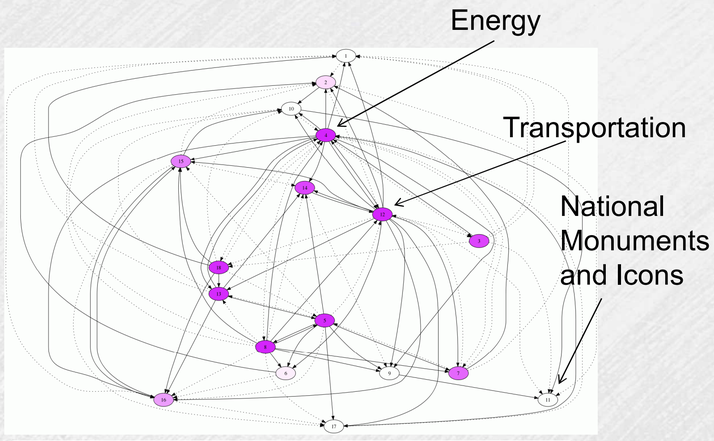


Results

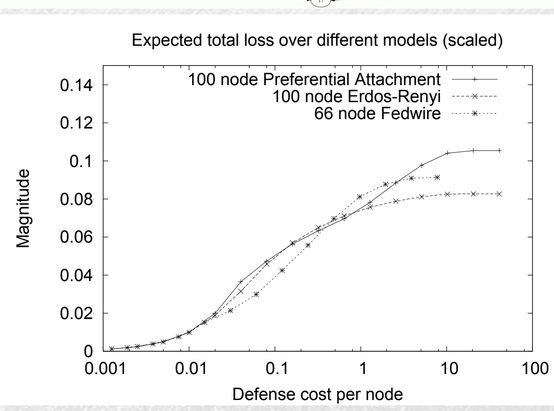
Supply chain defense



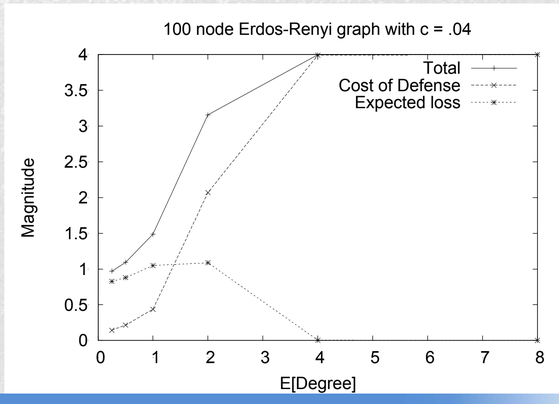
CIKR defense



For cost of defense low enough network topology does not matter



Density plays a major role: even relatively low density makes the network difficult to defend



Significance

Develop optimal defense strategies in settings with interdependent *assets:*

- *Cybersecurity*
- *Software project development (using data flow graph)*
- *Critical infrastructure defense (use a dependency graph)*
- *Supply chain security and integrity*
- *Energy grid security*
- *Transportation grid security*
- *Financial system security*
- *Optimal sequential monitoring strategies*
  network represents constraints on sequential strats

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000."

SAND 2010-xxxP

Sandia National Laboratories