Computing Optimal Security Strategies for Interdependent Assets

Joshua Letchford
Duke University
Durham, NC
jcl@cs.duke.edu

Yevgeniy Vorobeychik
Sandia National Laboratories*
Livermore, CA
yvorobe@sandia.gov

Abstract

We introduce a novel framework for computing optimal randomized security policies in networked domains which extends previous approaches in several ways. First, we extend previous linear programming techniques for Stackelberg security games to incorporate benefits and costs of arbitrary security configurations on individual assets. Second, we offer a principled model of failure cascades that allows us to capture both the direct and indirect value of assets, and extend this model to capture uncertainty about the structure of the interdependency network. Third, we extend the linear programming formulation to account for exogenous (random) failures in addition to targeted attacks. The goal of our work is two-fold. First, we aim to develop techniques for computing optimal security strategies in realistic settings involving interdependent security. To this end, we evaluate the value of our technical contributions in comparison with previous approaches, and show that our approach yields much better defense policies and scales to realistic graphs. Second, our computational framework enables us to attain theoretical insights about security on networks. As an example, we study how allowing security to be endogenous impacts the relative resilience of different network topologies.

1 Introduction

Game theoretic approaches to security have received much attention in recent years. There have been numerous attempts to distill various aspects of the problem into a model that could be solved in closed form, particularly accounting for interdependencies of security decisions (e.g., Kunreuther and Heal [2003], Grossklags et al. [2008]). Numerous others offer techniques based on mathematical programming to solve actual instances of security problems. One important such class of problems is network interdiction [Cormican et al., 1998], which models zero-sum encounters between an interdictor, who attempts to destroy a portion of a network, and a smuggler, whose goal typically involves some variant of a network flow problem (e.g., maximizing flow or computing a shortest path).

Our point of departure is another class of optimization-based approaches in security settings: Stackelberg security games [Paruchuri et al., 2008]. These are two-player games in which a defender aims to protect a set of targets using a fixed set of limited defense resources, while an attacker aims to assail a target that maximizes his expected utility. A central assumption in the literature on Stackelberg security games is that the defender can commit to a probabilistic defense (equivalently, the attacker observes the probabilities with which each target is covered by the defender, but not the actual defense realization).

Much of the work on Stackelberg security games focuses on building fast, scalable algorithms, often in restricted settings [Kiekintveld et al., 2009, Jain et al., 2010, Shieh et al., 2012]. One important such restriction is to assume that targets exhibit independence: that is, the defender’s utility only depends on which target is attacked and the security configuration at that target. Short of that restriction, one must, in principle, consider all possible combinations of security decisions jointly for all targets, making scalable computation elusive. Many important settings, how-

* 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.