How to Protect a City: Strategic Security Placement in Graph-Based Domains

(Extended Abstract)

Jason Tsai, Zhengyu Yin, Jun-young Kwak, David Kempe, Christopher Kiekintveld, Milind Tambe

University of Southern California, Los Angeles, CA 90089
{jasontts, zhengyuy, junyounk, dkempe, kiekintv, tambe} @usc.edu

ABSTRACT

We apply game-theoretic techniques to urban security deployment and propose new algorithms to efficiently solve real-world domains that are intractable with existing algorithms.

Categories and Subject Descriptors

I.2.11 [**Computing Methodologies**]: Artificial Intelligence—*Distributed Artificial Intelligence - Intelligent Agents*

General Terms

Algorithms, Performance, Experimentation, Security, Theory

Keywords

Game Theory, Stackelberg Games, Algorithms, Uncertainty, Security, Randomization, Patrolling, Risk Analysis

1. MOTIVATION

Protecting targets against potential attacks is an important problem for security forces worldwide. The general setting we study is as follows: An attacker assigns different values to reaching (and damaging or destroying) one of multiple targets. A defender is able to allocate resources (such as patrol cars or canine units) to capture the attacker before he reaches a target. In many of these situations, the domain has structure that is naturally modeled as a graph. For example, city maps can be modeled with intersections as nodes and roads as edges, where nodes are targets for attackers. In order to prevent attacks, security forces can schedule checkpoints on edges (e.g., roads) to detect intruders. For instance, in response to the devastating terrorist attacks in 2008 [1], Mumbai police deploy randomized checkpoints as one countermeasure to prevent future attacks [2]. The strategy for placing these checkpoints must necessarily be decided in advance of attack attempts, should account for targets of differing importance, and should anticipate an intelligent adversary who can observe the strategy prior to attacking.

In light of these requirements, game-theoretic approaches have been developed to assist in generating randomized security strategies in several real-world domains, including applications in use by the Los Angeles International Airport [11] and the Federal Air Marshals Service [9]. To account for the attacker's ability to observe deployment patterns, these methods model the problem as a Stackelberg game and solve for an optimal probability distribution over the possible deployments to ensure unpredictability.

Novel solvers for classes of security games have recently been developed [3, 11, 4]. However, these solvers take time at least polynomial in the number of actions of both players. In our setting, every path from an entry point to a target is an attacker action, and every set of r or fewer edges is a defender action. (r is the maximum number of checkpoints.) Since the attacker's actions grow exponentially with the size of the network, and the defender's actions grow exponentially with r, existing methods quickly become too slow when applied to large real-world domains. Therefore, our goal is to develop faster methods for these settings and evaluate them theoretically and empirically.

Cite as: How to Protect a City: Strategic Security Placement in Graph-Based Domains (Extended Abstract), Jason Tsai, Zhengyu Yin, Jun-young Kwak, David Kempe, Christopher Kiekintveld, Milind Tambe, *Proc. of 9th Int. Conf. on Autonomous Agents and Multiagent Systems (AAMAS 2010)*, van der Hoek, Kaminka, Lespérance, Luck and Sen (eds.), May, 10–14, 2010, Toronto, Canada, pp. 1453-1454
Copyright © 2010, International Foundation for Autonomous Agents and Multiagent Systems (www.ifaamas.org). All rights reserved.

2. RELATED WORK

Aside from the literature on Stackelberg games for security, our approach is also based on insights from network interdiction [12, 8, 5]. These are the special case of our model when there is a single target, or — equivalently — all targets have identical values. For such games, Washburn and Wood (1995) give an algorithm finding optimal strategies for both players based on Min-Cut computations. However, different target values can cause their algorithm to perform arbitrarily poorly, as we see in our experiments.

Two additional lines of work are somewhat related. Mavronicolas et al. (2008) define and analyze a network security game where each attacker can attack any node of the network, and the defender chooses a path to patrol to capture as many attackers as possible. Because the attacker is not restricted to paths, the types of results for this game are different from ours, and the focus in [10] is on understanding the impact of selfish behavior by defenders rather than optimal strategies. Hider-seeker games [3, 7] are also studied on graphs, but here, the attacker's goal is only to evade capture, not to reach any particular target.

3. PROBLEM DESCRIPTION

A graph-based security game models an attacker and a defender who take actions on a graph $G = (V, E)$, with $n = |V|$ nodes and $m = |E|$ edges. The attacker starts at one of the source nodes $s \in S \subseteq V$ *of his choosing* and travels along a path in an attempt to reach one of the targets $t \in T \subseteq V$. The attacker's pure strategies are thus all s-t paths P, denoted by $\mathcal{B}$, from some source s to some target t. The defender tries to capture the attacker before he reaches a target, by placing up to r resources on *edges* of the graph. The defender's pure strategies are subsets of r or fewer edges; we de-

note the set of all such sets by $\mathcal{L}$. Assuming that the defender plays $L \in \mathcal{L}$ and the attacker $P \in \mathcal{B}$, the attacker is captured whenever $P \cap L \neq \emptyset$, and succeeds in his attack when $P \cap L = \emptyset$.

Unsuccessful attacks always have a payoff of c for the defender, while successful ones have a penalty of $D(t)$. We make the natural restriction that $D(t) \leq c$. We also assume that the game is zero-sum, meaning that the attacker's payoff for a successful attack on target t is $-D(t)$, and $-c$ for an unsuccessful one. We stress here that targets may have vastly different payoffs associated with them, unlike in [12]. This distinction is crucial to model real security domains, and thus to bridge the gap between theory and practice.

In a world of increasingly sophisticated and determined attackers, a good defender strategy must take into account the fact that the attacker will observe and exploit patterns in the defender's behavior. Thus, the game is naturally modeled as a Stackelberg game, an approach also taken (for the same reasons) in past work in security settings [6, 9]. The defender is modeled as the *leader* and moves first, by selecting a mixed strategy $\lambda \in \Lambda$ that assigns a probability to each pure strategy $L \in \mathcal{L}$. The attacker is the *follower* and chooses a strategy after observing the defender's mixed strategy. There is always a pure-strategy best response for the attacker, so we restrict the attacker to pure strategies without loss of generality. Thus, the attacker's Stackelberg strategy is a function $f : \lambda \mapsto P$. For any pair of strategy profiles (λ, f), the expected rewards for the defender (R_D) and attacker (R_A) are given by:

$$R_D(\lambda, f) = p \cdot c + (1-p) \cdot D(t) \quad (1)$$

$$R_A(\lambda, f) = p \cdot -c + (1-p) \cdot -D(t) \quad (2)$$

where t is the target at the end of the path specified by $f(\lambda)$, and p the probability that the attacker is captured on the path to t given the defender's strategy λ. Although the optimal defender strategy is a Stackelberg Equilibrium, since our game is zero-sum, this is equivalent to a Maximin strategy. Unfortunately, as $\mathcal{L}$ has size $\Theta(m^r)$, and $\mathcal{B}$ has size exponential in n, existing methods for computing such strategies do not scale to realistic problem sizes.

4. SUMMARY OF FINDINGS

In this work, we develop an efficient procedure for generating checkpoint deployments based on two key ideas: (i) a polynomial-sized approximation of the strategy space solved using a linear program (marginal distribution); (ii) two efficient sampling techniques to map solutions back to the original space (joint distribution). To avoid the exponential strategy space over all possible combinations of checkpoint placements (the joint distribution), our methods operate on the marginal probabilities of edges, i.e., the total probability of placing a checkpoint on an edge. Our linear program, RANGER, efficiently solves for the optimal marginal distribution for the defender by upper-bounding the capture probabilities along paths by the sum of marginal probabilities.

To implement these solutions, we must sample the distribution or convert them into distributions over the joint actions (sets of r checkpoints). Our sampling algorithms efficiently generate joint distributions in the original problem space from RANGER's solution over marginal probabilities. We prove that under certain conditions, the actual capture probabilities of the joint distributions produced by our algorithms match the upper bound of RANGER, and necessarily yield *optimal* payoffs. *Radius Sampling* generates optimal joint distributions if certain conditions on the marginal distribution are met. *Comb Sampling* generates distributions which are optimal against an *approximating attacker* who calculates the expected value of an attack by summing the marginal probabilities in the path.

In addition to our theoretical results, we test our methods empirically. Our results show orders of magnitude improvement in runtime over previously known algorithms, making it possible to solve real-world problems. In randomly-generated small games where we could actually determine the optimal reward, our techniques provide optimal solutions in nearly all cases, despite optimality conditions not necessarily being met. We also evaluate the quality of our solutions on a model of the southern area of Mumbai, which was the subject of severe terrorist attacks in 2008. On this real-world domain, the algorithms provide superior rewards to other intuitive defense strategies that might be used in such a domain. In contrast, previously known, optimal algorithms are unable to solve the problem due to the immense size. Thus, although guarantees cannot be provided for the general case, experimentally, our techniques efficiently generate high-quality solutions in domains of interest.

5. ACKNOWLEDGEMENT

This research was supported by the United States Department of Homeland Security through the Center for Risk and Economic Analysis of Terrorism Events (CREATE) under grant number 2007-ST-061-000001. Any opinions, conclusions or recommendations herein are solely those of the authors and do not necessarily reflect views of the Department of Homeland Security.

6. REFERENCES

[1] Battle for Mumbai ends, death toll rises to 195. *Times of India*, 29 November 2008.

[2] S. A. Ali. Rs 18L seized in nakabandi at Vile Parle. *Times of India*, 4 August 2009.

[3] N. Basilico, N. Gatti, and F. Amigoni. Leader-follower strategies for robotic patrolling in environments with arbitrary topologies. In *AAMAS-09*, 2009.

[4] V. Conitzer and T. Sandholm. Computing the optimal strategy to commit to. In *ACM EC-06*, pages 82–90, 2006.

[5] K. J. Cormican, D. P. Morton, and R. K. Wood. Stochastic network interdiction. *Oper. Res.*, 46(2):184–197, 1998.

[6] N. Gatti. Game theoretical insights in strategic patrolling: Model and algorithm in normal-form. In *ECAI-08*, pages 403–407, 2008.

[7] E. Halvorson, V. Conitzer, and R. Parr. Multi-step Multi-senor Hider-Seeker Games. In *IJCAI*, 2009.

[8] E. Israeli and R. K. Wood. Shortest-path network interdiction. *Networks*, 40(2):97–111, 2002.

[9] C. Kiekintveld, M. Jain, J. Tsai, J. Pita, M. Tambe, and F. Ordóñez. Computing Optimal Randomized Resource Allocations for Massive Security Games. In *AAMAS-09*, 2009.

[10] M. Mavronicolas, V. Papadopoulou, A. Philippou, and P. Spirakis. A network game with attackers and a defender. *Algorithmica*, 51(3):315–341, 2008.

[11] P. Paruchuri, J. P. Pearce, J. Marecki, M. Tambe, F. Ordóñez, and S. Kraus. Playing games with security: An efficient exact algorithm for Bayesian Stackelberg games. In *AAMAS-08*, pages 895–902, 2008.

[12] A. Washburn and K. Wood. Two-person zero-sum games for network interdiction. *Operations Research*, 43(2):243–251, 1995.