Designing Better Strategies against Human Adversaries in Network Security Games

(Extended Abstract)

Rong Yang, Fei Fang, Albert Xin Jiang,
Karthik Rajagopal*, Milind Tambe, Rajiv Maheswaran
University of Southern California, Los Angeles, CA, 90089
{yangrong,feifang,jiangx,tambe,maheswar}@usc.edu, *{nkartr}@gmail.com

ABSTRACT

In a Network Security Game (NSG), security agencies must allocate limited resources to protect targets embedded in a network, such as important buildings in a city road network. A recent line of work relaxed the perfect-rationality assumption of human adversary and showed significant advantages of incorporating the bounded rationality adversary models in non-networked security domains. Given that real-world NSG are often extremely complex and hence very difficult for humans to solve, it is critical that we address human bounded rationality when designing defender strategies. To that end, the key contributions of this paper include: (i) comprehensive experiments with human subjects using a web-based game that we designed to simulate NSGs; (ii) new behavioral models of human adversary in NSGs, which we train with the data collected from human experiments; (iii) new algorithms for computing the defender optimal strategy against the new models.

Categories and Subject Descriptors

H.4 [**Computing Methodology**]: Game Theory

General Terms

Security, Algorithm

Keywords

Bounded Rationality, Network Stackelberg Games, Decision-making, Quantal Response

1. INTRODUCTION

Stackelberg Security Games (SSGs) have received great attention recently in solving real-world security problems, in which security forces (the leader) must allocate resources to protect one or more potential targets from being damaged by the attackers (the followers). Since the attackers can usually observe the defender's strategy before deciding on a plan of attack, the defender commits to a randomized strategy before the attacker chooses a strategy. Such attacker-defender Stackelberg game models have been used as the basis of many real-world deployed systems, including ARMOR, IRIS and GUARDS [6].

Appears in: *Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems – Innovative Applications Track (AAMAS 2012)*, Conitzer, Winikoff, Padgham, and van der Hoek (eds.), 4-8 June 2012, Valencia, Spain.

In this paper we focus on security games whose domains have structure that is naturally modeled as graphs. For example, in response to the devastating terrorist attacks in 2008 [2], Mumbai police deployed randomized checkpoints as one countermeasure to prevent future attacks [7]. This can be modeled as a Stackelberg game on a graph with intersections as nodes and roads as edges, where certain nodes are targets for attacks. The attacker chooses a path on the graph ending at one of the targets. The defender can schedule checkpoints on edges to try to catch the attacker before a target is reached. Previous studies [7, 8] model these games as Network Security Games.

A common assumption of these previous studies is that the attacker is perfectly rational (i.e. chooses a strategy that maximizes their expected utility). However, extensive experimental studies have shown that standard game-theoretic assumptions of perfect rationality are not ideal for predicting the behavior of humans in multi-agent decision problems, and various alternative models have been proposed [1, 5]. Recently, Yang *et al* [9] studied human behavior models of attackers in the setting of (non-networked) Stackelberg security games. They showed that defender strategies based on a quantal response model (an adaptation of Quantal Response Equilibrium (QRE) concept [5] to the Stackelberg setting) achieved promising performance when tested against human subjects, outperforming previous methods for security games as well as a behavior model based on Prospect Theory [4].

In this work, we initiate the study of human behavior models of adversaries in network security games. Compared to the non-networked domains, the network structure of this domain further complicates the decision process of the human adversaries, hence further motivating the need to relax assumptions of perfect rationality. Specifically, the attacker must choose a path in the graph where each edge is covered by the defender with some observed probability, and thus must reason about sequences of random events. Our goal is to explore any bias and/or heuristic behavior exhibited by human adversaries when facing such decision problems, and to design defender strategies that exploit such behavior. While it is generally accepted that humans tend to rely on heuristics when faced with complex problems (e.g., [3]), to the best of our knowledge, there are no existing studies that specifically addressed heuristic human behavior in the security domain.

We propose two behavior models for attackers in network security games. First, we adapted the quantal response model [9] to network security games. For the second model (which we call quantal response with heuristics), the attacker's behavior now depends on the values of several easy-to-compute *features* of the attacker's decision problem. Furthermore, we developed a web-based game that simulates the decision tasks faced by the attacker. We recruited hu-

man subjects to play the game, in order to collect data for training the model as well as evaluate the defender strategies that are computed based on the trained model.

2. METHODOLOGY

We consider a network security game the same as what is defined in [7], except that we now allow general-sum payoff structures.

Adversary Models: We propose two models of the adversary. In the first model, the adversary's mixed strategy is a quantal response (QR) to the defender's strategy: the probability that the adversary chooses path A_i is

$$\texttt{QR}: \quad q_i(\lambda \mid \boldsymbol{x}; \Gamma) = \frac{e^{\lambda U_i^a(\boldsymbol{x};\Gamma)}}{\sum_{A_k \in \mathcal{A}} e^{\lambda U_k^a(\boldsymbol{x};\Gamma)}} \tag{1}$$

where Γ denotes a given game sample, $\boldsymbol{x}$ is the defender's strategy, U_i^a is the adversary's expected utility of choosing path A_i, and $\lambda > 0$ is the parameter of the quantal response model [5] which represents the error level of the adversary's quantal response. In the second model, which we call Quantal Response with Heuristics (QRH), the probability that the adversary chooses path A_i is

$$\texttt{QRH}: \quad q_i(\mu \mid \boldsymbol{x}; \Gamma) = \frac{e^{\mu \cdot f_i(\boldsymbol{x})}}{\sum_{A_k \in \mathcal{A}} e^{\mu \cdot f_k(\boldsymbol{x})}} \tag{2}$$

where $\mu = \langle \mu_1, ..., \mu_m \rangle$ is a vector of coefficients of the model and given $\boldsymbol{x}$, $f_i(\boldsymbol{x}) = \langle f_{i1}(\boldsymbol{x}), .., f_{im}(\boldsymbol{x}) \rangle$ is a vector of m *features* for path A_i that influences the attacker's decision making. Since our focus for the QRH model is on simple heuristics, we use a set of five features for each path that are easy to compute for humans and thus could be used as a basis for heuristics: 1. number of edges; 2. minimum coverage on a single edge; 3. maximum coverage on a single edge; 4. sum of edge coverage; 5. average of edge coverage.

Model Training: We developed a web-based game which simulates the decision tasks faced by the attacker in network security games. Figure 1 displays the interface of the game. Players are

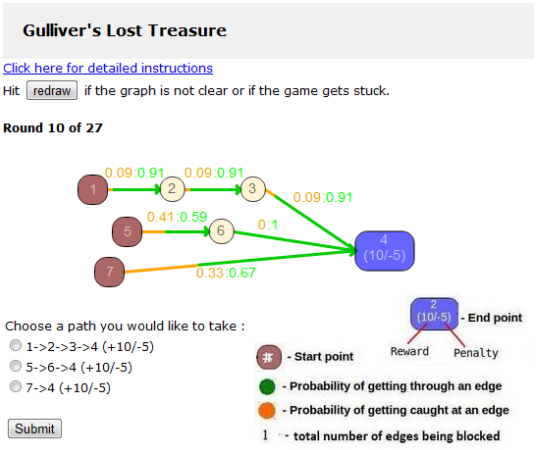

Figure 1: Game Interface (colored)

introduced to the game through a series of explanatory screens describing how the game is played. In the game, the web interface presents a graph to the subjects and specifies the source(starting) nodes and the target nodes in the graph. The subjects are asked to select a path from one of the source nodes to one of the target nodes. They are also told that the defender is trying to catch them by setting up checkpoints on the edges. The probability that there will be a check point on each edge is given to the subjects, as well as the reward for successfully getting through the path and the penalty for being caught by the defender. We posted the game as a Human Intelligent Task on Amazon Mechanical Turk (https://www.mturk.com) to collect data on how human subjects play the game and learned the parameters of both the QR model and the QRH model with the data using Maximum Likelihood Estimation.

Computing Defender Strategy: Given a QR/QRH model of the adversary, we have the following optimization problem to compute the corresponding defender's optimal strategy:

$$\max_{\boldsymbol{x},p} \sum_{A_i \in \mathcal{A}} q_i(\lambda \mid \boldsymbol{x}; \Gamma)((R_i^d - P_i^d)p_i + P_i^d) \tag{3}$$

$$\text{s.t.} \sum_{e \in E} x_e \leq M, \quad 0 \leq x_e \leq 1, \quad \forall e \in E \tag{4}$$

$$p_i = \sum_{e \in A_i} x_e, \quad \forall A_i \in \mathcal{A} \tag{5}$$

where $q_i(\lambda \mid \boldsymbol{x}; \Gamma)$ in Equation (3) is specified in Equation (1) and (2). The problem is a nonlinear and nonconcave. We use a heuristic algorithm based on local optimization with random restarts, similar to that used in [9] to solve the problem.

3. CONCLUSION

We presented an initial study of human behavior models of adversaries in network security games. In particular, we first proposed two behavior models, quantal response (QR) and quantal response with heuristics (QRH). In order to train our models and to evaluate their performances, we developed a web-based game that simulates the decision tasks faced by the attacker. We then trained the model with the data that we collected by posting the game on Amazon Mechanical Turk. Finally, we provided new algorithms to compute the defender optimal strategy against the new models.

4. ACKNOWLEDGMENTS

This research was supported by Army Research Office under the grant # W911NF-10-1-0185.

5. REFERENCES

[1] C. F. Camerer, T. Ho, and J. Chong. A cognitive hierarchy model of games. *QJE*, 119(3):861–898, 2004.

[2] R. Chandran and G. Beitchman. Battle for Mumbai ends, death toll rises to 195. *Times of India*, November 2008.

[3] G. Gigerenzer, P. Todd, and the ABC Research Group. *Simple Heuristics that make us smart*. Oxford University Press, 1999.

[4] D. Kahneman and A. Tvesky. Prospect theory: An analysis of decision under risk. *Econometrica*, 47(2):263–292, 1979.

[5] R. D. McKelvey and T. R. Palfrey. Quantal response equilibria for normal form games. *Games and Economic Behavior*, 2:6–38, 1995.

[6] M. Tambe. *Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned*. Cambridge University Press, New York, NY, 2011.

[7] J. Tsai, Z. Yin, J. Kwak, D. Kempe, C. Kiekintveld, and M. Tambe. Urban security: Game-theoretic resource allocation in networked physical domains. *In AAAI*, 2010.

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

[9] R. Yang, C. Kiekintveld, F. Ordonez, M. Tambe, and R. John. Improving resource allocation strategy against human adversaries in security games. *In IJCAI*, 2011.