ADVANCES IN GAME THEORY FOR SECURITY AND PRIVACY

EC17 Tutorial

Bo An, Fei Fang, Yevgeniy Vorobeychik

Overview

The Stackelberg Security Game (SSG) model has proven to be immensely successful in solving real-world security problems in which security agencies (defenders) allocate limited resources to protect important settings against human adversaries. The SSG model has also resulted in a rich body of research publications. We survey recent directions in the area of security games, focusing on new applications aiming to address societal concerns such as environmental sustainability, screening for security threats at airports, urban crime and cyber-security.

This tutorial will introduce a wide variety of game-theoretic modeling techniques and algorithms that have been developed in recent years for security problems. Introductory material on game theory and mathematical programming (optimization) will be included in the tutorial, so there is no prerequisite knowledge for participants. After introducing the basic security game framework, we will describe novel optimization methods for computing Stackelberg equilibrium, learning human behavior models, eliciting preferences, handling uncertainty/observations/capabilities, and repeated interaction. At the end we will highlight the many opportunities for future work in this area, including exciting new domains and fundamental theoretical and algorithmic challenges.

Target Audience

The primary target audience for this proposed tutorial are students and researchers who are interested in applications of game theory for social good and security. This tutorial should also be of interest to researchers in the topic of applied multi-agent systems research and human behavior. We also anticipate that this tutorial will appeal to industry participants interested in applied work, and to game theory practitioners who may be interested in learning more about the specific techniques employed in this important class of games. The last version of this tutorial was given at AAAI'14 and approximately 60 people attended.

What will the audience walk away with?

The primary tools the audience can learn are game theoretic models for security scenarios and exact/approximate algorithms to find solutions. The audience will also learn how concepts from behavioral game-theory have been applied and deployed in the context of security games. Although it is

not the primary objective of the tutorial, the audience can also obtain some foundational knowledge in algorithmic game theory.

Pre-requisites

The aim of the tutorial is to be self-contained. That is, the idea is to provide all the knowledge needed to understand the topics discussed in the tutorial. However, basic knowledge of game theory and optimization can be of considerable value.

Required facilities for the tutorial: none

The desired tutorial length: half day

Syllabus for a half day tutorial

- Motivations: Resource allocation and patrolling in security problems
  - Motivating domains: LAX, FAMS, robot patrolling, TSA, Coast Guard, LA Metro, wildlife protection etc.
  - Goal: provide algorithms to make good (optimal) security decisions
  - Why game theory?
- Introduction to game theory and solutions
  - Maximin and minimax strategies and their computation
  - General-sum games and Nash equilibrium
  - Bayesian games and Bayes-Nash equilibrium
  - Leader-follower (Stackelberg) games
  - Stackelberg equilibrium and its computation
  - Bayesian Stackelberg games
- Security games: Foundations and Scalable Algorithms
  - Definition and examples
  - Multiple resources and scheduling constraints
  - Representative algorithms and complexity
  - Column and constraint generation
  - Branch-and-bound and cutting-plane methods
  - Compact representations and uncertainty
- Learning and Human Behavior
  - Human behavior models such as Prospect Theory and Quantal Response Equilibrium
  - Learning human behavior in repeated settings
- Game Theory for Cyber Security
  - Games on Networks

    - Games with Attack Graphs and Plans
    - Cyber-deception Games
- Game Theory for Privacy-Preserving Data Sharing
    - Structured Data Sharing
    - Sharing Genomic Data
    - Sanitizing Unstructured Data
- General Discussion/Questions

Presenter Information

Bo An is a Nanyang Assistant Professor at the School of Computer Science and Engineering of the Nanyang Technological University. He received the Ph.D degree in Computer Science from the University of Massachusetts, Amherst and was a Postdoctoral Researcher at the University of Southern California. His research interests include artificial intelligence, multi-agent systems, game theory, and optimization. He has published over 50 referred papers at AAMAS, IJCAI, AAAI, ICAPS, KDD, JAAMAS, AIJ and IEEE Transactions. He is the recipient of the 2010 IFAAMAS Victor Lesser Distinguished Dissertation Award. He won an Operational Excellence Award from the Commander, First Coast Guard District of the United States. He won the Best Innovative Application Paper award at the 11th International Joint Conference on Autonomous Agents and Multi-Agent Systems and the Deployed Innovative Application Award at the 28th Annual Conference on Innovative Applications of Artificial Intelligence. He also won the 2012 INFORMS Daniel H. Wagner Prize for Excellence in Operations Research Practice. He is a member of the editorial board of Journal of Artificial Intelligence Research (JAIR) and the Associate Editor of Journal of Autonomous Agents and Multi-agent Systems (JAAMAS). He was elected to the board of directors of IFAAMAS.

- **Email:** boan@ntu.edu.sg
- **Affiliation:** Nanyang Technological University
- **Address:** N4-02b-55, Nanyang Avenue, Singapore 639798

Fei Fang is a Postdoctoral Fellow at the Center for Research on Computation and Society (CRCS), Harvard University and an Adjunct Assistant Professor at the Institute for Software Research at Carnegie Mellon University. She received her Ph.D. from the Department of Computer Science at the University of Southern California in June 2016. She received her bachelor degree from Tsinghua University in July 2011. Her research lies in the field of artificial intelligence and multi-agent systems, focusing on computational game theory with applications to security and sustainability domains. Her work has won the Innovative Application Award at Innovative Applications of Artificial Intelligence (IAAI'16), the Outstanding Paper Award in Computational Sustainability Track at the International Joint Conferences on Artificial Intelligence (IJCAI'15). Her work on "Protecting Moving Targets with Mobile Resources" has been deployed by the US Coast Guard for protecting the Staten Island Ferry in New York City since April 2013. Her work on designing patrol strategies to combat illegal poaching has

led to the deployment of PAWS application in a conservation area in Southeast Asia for protecting tigers.

- **Email:** feifang@cmu.edu
- **Affiliation:** Carnegie Mellon University
- **Address:** 110 Maxwell Dworkin, Harvard University, 33 Oxford Street, Cambridge, MA, 02138

Yevgeniy Vorobeychik is an Assistant Professor of Computer Science and Computer Engineering and Vanderbilt University. Previously, he was a Principal Member of Technical Staff at Sandia National Laboratories. Between 2008 and 2010 he was a post-doctoral research associate at the University of Pennsylvania Computer and Information Science department. He received Ph.D. (2008) and M.S.E. (2004) degrees in Computer Science and Engineering from the University of Michigan, and a B.S. degree in Computer Engineering from Northwestern University. His work focuses on game theoretic modeling of security and privacy, algorithmic and behavioral game theory and incentive design, optimization, complex systems, epidemic control, network economics, and machine learning. Dr. Vorobeychik has published over 100 research articles on these topics. Dr. Vorobeychik was nominated for the 2008 ACM Doctoral Dissertation Award and received honorable mention for the 2008 IFAAMAS Distinguished Dissertation Award.

- **Email:** yevgeniy.vorobeychik@vanderbilt.edu
- **Affiliation:** Vanderbilt University
- **Address:** 2301 Vanderbilt Place, Nashville, TN