Proposal

ISE599: Security and Game Theory

Instructor: Milind Tambe

August 2015

Goal:
Provide students an in-depth understanding of the area of “Security Games” or use of game theory for security, with applications in infrastructure security, cybersecurity, green security and security against urban crime.

Motivation
Security remains a global challenge: limited security resources must be deployed to protect ports, airports, and other critical national infrastructure, to suppress crime in urban areas, to protect forests and wildlife, to reduce cyber crime and to curtail the illegal flow of drugs, weapons and money. Security challenges also include protection of networks including cyber, rail, road or maritime transportation networks, wildlife smuggling networks, blocking contagion of radicalism in social networks, and others. Yet, given limited security resources, these resources cannot be everywhere all the time, raising a crucial question of how to best use them.

Game theory provides a sound mathematical approach to deploy limited security resources to maximize their effectiveness. There has thus been a very significant focus on game theory for security and publications focused on this topic have seen a very rapid increase. This course is intended to provide students an introduction to this growing area of game theory for security, including an in-depth understanding of key research challenges.

While early work on game theory for security was often focused on small 2-by-2 games, we pioneered a new era of “security games” by focusing on massive games that could be solved by exploiting computational advances. Security games is a new area that combines computational and behavioral game theory, machine learning, planning under uncertainty, and many insights from other fields including criminology. Indeed, my research group has been at the forefront of this research, and we have built a wide range of actual deployed applications of game theory for security. Our first application, ARMOR, deployed game theory in practice at the Los Angeles International Airport
In 2007; in particular, it used game theory to randomize allocation of police checkpoints and canine units.

There are many applications that have followed. Our second application, IRIS, is used by the Federal Air Marshal Service to deploy air marshals on US air carriers and has been in use since 2009. A third application, PROTECT, for the US Coast Guard is in use in the ports of Boston, New York, Los Angeles, Houston for planning patrols, and potentially moving to other ports. There are many other applications being deployed by a variety of security agencies including the LA Sheriff’s department, the TSA and others. In addition to infrastructure security, security games research has now led to security resource allocation and patrol planning software being tested by wildlife security organizations, including Panthera, WWF and others, in countries ranging from Malaysia to Uganda. Security games research has also led to innovations in allocation of police against urban crime. In fact, USC’s own DPS started using security games based software starting June of 2015. There is now a startup ARMORWAY that builds on this work.

This set of applications and associated algorithms has caused an explosion of interest in applying game theory for security. Indeed, these applications are leading to real-world use-inspired research in the emerging research area of “security games”; specifically, the research challenges posed by these applications include scaling up security games to large-scale problems, handling significant adversarial uncertainty, dealing with bounded rationality of human adversaries, machine learning based on adversary behavior data in wildlife or urban crime, and many other interdisciplinary challenges. Several research groups in many different universities in the US and elsewhere are now pursuing this research, as evidenced by the increasing numbers of papers focused on game theory for security. “Security games” is now a major thriving area of research.

This ISE599 course is intended to provide students with an in-depth understanding of “Security games” --- this growing, thriving area of research. The syllabus will include a combination of:

- Key papers will be emailed out in advance.
- Some notes handed out during class
- A few invited lectures from key security experts
Schedule of Classes
ISE 599: Security and Game Theory

*italics* indicates homework reading for students. Chapter numbers refer to chapters of “Security and Game Theory”

1. Lecture 1: Course intro, syllabus, goals, key concepts: use of game theory for security, with applications in infrastructure security, cybersecurity, green security and security against urban crime. Introduction to basic decision theory.

   *Handout: Basic decision theory*

2. Lecture 2: Introduction and overview of security games: What they are, what are their applications, what are some key scientific challenges, who is doing research in this area,…

   **Introduction to game theory and security games**

3. Lecture 3: Introduction to basic game theory, Normal form games, Dominance, iterative dominance, Nash equilibrium; Mixed strategy Nash equilibrium, *Handout: Introduction to game theory*

4. Lecture 4: Introduction to linear programming techniques zero sum games, Stackelberg games, zero sum and non-zero-sum, Nash vs Stackelberg, Security games

   *Handout: Linear programming*


5. Lecture 5: Efficient solution techniques for security games, “Multiple LPs” (Conitzer and Sandholm), DOBSS, ERASER, Sampling

   *Homework: Excel solver and its use in linear programming/MIP; other tools*


Handout: Bayesian games; games of incomplete and imperfect information

6. Lecture 6: Extensive form games, Subgame perfect Nash equilibrium, Bayesian games, games of incomplete information and imperfect information, Harsanyi transformation, …

7. Lecture 7: Student presentations in class

There are a very large number of applications of security games. Lectures 7 and 8 will be for students to read papers on these applications and present that work in class. Depending on the number of students enrolled we may need one or two lectures. I am assuming two lectures (Lectures 7 and 8)

8. Lecture 8: Student presentations in class

Behavioral game theory and security games

9. Lecture 9: Behavioral game theory research

Handout: Behavioral game theory


10. Lecture 10: Yang et al IJCAI’11, Pita et al ECAI 12, Quantal response

11. Lecture 11: Continued with security games and behavioral game theory research

12. Lecture 12: Guest lecture: US Coast Guard

13. Lecture 13: Student project ideas presentation, discussion and feedback

Large-scale Security Games: Challenge of scale up:

14. Lectures 14: Column generation, application in solving large scale games such as for the FAMS

15. Lecture 15: Continuation of scale up

*Handout: Column generation, double oracle*

*M. Jain, C. Kiekintveld, E. Kardes, F. Ordonez, M. Tambe Security games with arbitrary schedules: A branch and price approach Proceedings of the National Conference on Artificial Intelligence (AAAI), July 2010*


16. Lecture 16: Results of Homework, Review before midterm

17. Lecture 17: Midterm

18. Lecture 18: Spatio-temporal game theory

*F. Fang, A. Jiang, M. Tambe Protecting Moving Targets with Multiple Mobile Resources In Journal of Artificial Intelligence Research (JAIR), 48:583-634, 2013*

**Green Security Games**
19. Lecture 19: Green Security: challenges and applications

_F. Fang, P. Stone and M. Tambe When Security Games Go Green: Designing Defender Strategies to Prevent Poaching and Illegal Fishing_ In _International Joint Conference on Artificial Intelligence (IJCAI), July, 2015_

20. Lecture 20: Green security continued

**Cybersecurity, information asymmetry and game theory**

21. Lecture 21: Cybersecurity (Guest lecture)


22. Lecture 22: Cyber applications

**Game theory and contagion of beliefs, fighting radicalism**

23. Lecture 23: Double oracle approach for solving large scale games


24. Lecture 24: Security games for controlling contagion of beliefs, ideas, with applications in health and security; Tsai et al, AAAI’12

25. Lecture 25: Final project presentation from students or invited lecture

26. Lecture 26: Final project presentations

27. Lecture 27: Invited lecture: Erroll Southers

28. Lecture 28: Final Quiz

**Schedule of Assignments and Exams**

- Paper presentation, discussion:(5%)
• Homework I: (15%)
• Midterm project ideas and discussion: (5%)
• Homework II: (10%)
• Midterm: (25%)
• Project: (30%)
• Final quiz: (10%)

**Homework assignments must be done individually; only the project can be done in a team.**

**Statement for Students with Disabilities**
Any student requesting academic accommodations based on a disability is required to register with Disability Services and Programs (DSP) each semester. A letter of verification for approved accommodations can be obtained from DSP. Please be sure the letter is delivered to me (or to TA) as early in the semester as possible. DSP is located in STU 301 and is open 8:30 a.m.–5:00 p.m., Monday through Friday. Website and contact information for DSP:
http://sait.usc.edu/academicsupport/centerprograms/dsp/home_index.html, (213) 740-0776 (Phone), (213) 740-6948 (TDD only), (213) 740-8216 (FAX) ability@usc.edu.

**Statement on Academic Integrity**
USC seeks to maintain an optimal learning environment. General principles of academic honesty include the concept of respect for the intellectual property of others, the expectation that individual work will be submitted unless otherwise allowed by an instructor, and the obligations both to protect one’s own academic work from misuse by others as well as to avoid using another’s work as one’s own. All students are expected to understand and abide by these principles. SCampus, the Student Guidebook, (www.usc.edu/scampus or http://scampus.usc.edu) contains the University Student Conduct Code (see University Governance, Section 11.00), while the recommended sanctions are located in Appendix A.

**Emergency Preparedness/Course Continuity in a Crisis**
In case of a declared emergency if travel to campus is not feasible, USC executive leadership will announce an electronic way for instructors to teach students in their residence halls or homes using a combination of Blackboard, teleconferencing, and other technologies.