CS599: Security and Game Theory

Instructor: Milind Tambe

October 2012

Goal:
Provide students an in-depth understanding of the area of "Security Games" or use of game theory for security.

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 as well as to protect forests and wildlife, 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, 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.

My research group has been at the forefront of this research, and we are the first and currently the only research group that has led to 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 (LAX) since August 2007; in particular, it uses game theory to randomize allocation of police checkpoints and canine units. 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 and New York for planning patrols, and getting evaluated for a national deployment across all ports. There are many other applications being deployed by a variety of security agencies including the LA Sheriff's department, the TSA and others.

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, and 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 over the past 6 years. "Security games" is now a thriving area of research.

This CS599 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:

- "Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned" Milind Tambe, Cambridge University Press, 2011
- Key papers will be emailed out in advance.
- Some notes handed out during class

Schedule of Classes
CS 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: basic decision theory, basic linear programming
   Handout: Basic decision theory

2. Lecture 2: Chapter 1: Introduction and overview of security games

3. Lecture 3: Chapter 2: Introduction to problems of security: Erroll Southers or CREATE center

   Handout: Introduction to game theory
4. Lecture 4: Normal form games, Dominance, iterative dominance, Nash equilibrium; Mixed strategy Nash equilibrium, Stackelberg games, security games

Handout: Linear programming

5. Lecture 5: Chapter 8 (up to 8.4): Introduction to Linear Programming, Integer programming, solving security games, marginals, ERASER, Sampling
   Homework: Excel solver; 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: Continued with Bayesian games

   Students form teams to read the following chapters and present in class:
   Chapter 4: J. Pita, M. Jain, C. Western, P. Paruchuri, J. Marecki, M. Tambe, F. Ordonez, S. Kraus Deployed ARMOR Protection: The Application of a Game Theoretic Model for Security at the Los Angeles International Airport

   Chapter 5: J. Tsai, S. Rathi, C. Kiekintveld, M. Tambe, F. Ordonez IRIS: A tool for strategic security allocation in transportation networks

   Chapter 6: J. Pita, C. Kiekintveld, M. Tambe, E. Steigerwald, S. Cullen GUARDS - Game Theoretic Security Allocation on a National Scale

   Papers on other new applications developed for the US Coast Guard and the LA Sheriff's Dept respectively

8. Lecture 8: Student presentations in class (multiple teams).

   Handout: Introduction to MDPs
9. Lecture 9: Chapter 7, 8: MDPs, Basic approaches to solving Bayesian Stackelberg games: "Multiple LPs" (Contizer and Sandholm), DOBSS, ASAP, ORIGAMI, ERASER-C, Sampling

10. Lecture 10:Chapter 7, 8: continued

11. Lecture 11: Chapter 10: Emotions, behavioral game theory research

    R. Yang, C. Kiekintveld, R. John, F. Ordonez, M. Tambe Improving Resource Allocation Strategy Against Human Adversaries in Security Games In Proceedings of the International Joint Conference on Artificial Intelligence (IJCAI), July 2011

J. Pita, R. Maheswaran, M. Tambe, S. Kraus A Robust Approach to Addressing Human Adversaries in Security Games In Proceedings of the European Conference on Artificial Intelligence (ECAI), August 2012.

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

13. Lecture 13: Chapter 3: Guest lecture: US Coast Guard

    R. Yang, M. Tambe, F. Ordonez Computing Optimal Strategy against Quantal Response in Security Games In Proceedings of the International Conference on Autonomous Agents and Multiagent Systems (AAMAS), June 2012.
    E. Shieh, R. Yang, B. An, M. Tambe, C. Baldwin, J. DiRenzo, B. Maule, G. Meyer PROTECT: A Deployed Game Theoretic System to Protect the Ports of the United States In Proceedings of the International Conference on Autonomous Agents and Multiagent Systems (AAMAS)(Innovative applications track), June 2012.
14. Lecture 14: PROTECT, latest research on game theory for security US Coast Guard

15. Lecture 15: Chapter 12: Frontiers of security game theory research: Stackelberg vs Nash

Chapter 13: M.E. Taylor, C.Kiekintveld, M. Tambe Evaluating Deployed Decision Support Systems for Security: Challenges, Analysis and Approaches
16. Lecture 16: Student project ideas presentation, discussion and feedback

17. Lecture 17: Chapter 9: Column generation, application in solving large scale games such as for the FAMS

    M.P. Johnson, F. Fang, M. Tambe, H.J. Albers Patrol Strategies to Maximize Pristine Forest Area In Proceedings of the Conference on Artificial Intelligence (AAAI) (Computational Sustainability Track), July 2012.

18. Lecture 18: Spatio-temporal game theory: Protecting multiple mobile targets and with multiple patrollers; forest protection

19. Lecture 19: Results of Homework, Review before midterm

20. Lecture 20: Midterm I

21. Lecture 21: Cybersecurity (Guest lecture)

    O. Vanek, Z. Yin, M. Jain, B. Bosansky, M. Pechoucek, M. Tambe Game-theoretic Resource Allocation for Malicious Packet Detection in Computer Networks In

Proceedings of the International Conference on Autonomous Agents and Multiagent Systems (AAMAS), June 2012.

22. Lecture 22: Cyber applications, contagion:

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

    J. Tsai, T. Nguyen, M. Tambe Security Games for Controlling Contagion In Proceedings of the Conference on Artificial Intelligence (AAAI), July 2012.

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: Invited lecture: *Richard John (human behavior and game theory)*

26. Lecture 26: Final project presentations

27. Lecture 27: Invited lecture: LA Sheriff's dept or LAX airport

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.