1-1-2014

Game Theory for Security: New Domains, New Challenges

Milind Tambe

Follow this and additional works at: http://research.create.usc.edu/current_synopses

Recommended Citation
Game Theory for Security: New Domains, New Challenges
We develop and apply general methods for planning and scheduling the deployment of limited resources to serve real-world security applications, based on rigorous game-theoretic modeling based on real-world data and solutions algorithms for such games.

Project Technical Description
1. Theme Area: Risk Analysis – management of risks due to intelligent, adaptive adversaries
2. Principal Investigator: Milind Tambe
3. Institution: USC
4. Co-Investigators: None
5. Keywords: infrastructure protection, game-theoretic resource deployment, mathematical programming, learning

6. Brief Description:
Our research focuses on effective allocation of limited security resources using game theory, accounting for the capability of adversaries to observe and exploit security schedules and data collected from multiple and repeated interaction with adversaries. We make use of attacker-defender Stackelberg games, and apply machine learning (to learn from interactions) and advanced algorithms using game-theoretic analysis to find optimal security policies for the defender to implement. These policies account for the different characteristics of the targets, the intelligent response of an adversary, and evolve over time with data.

It is critical to note that this research provides a significant advance over our previous research. Nonetheless, our past work did lead to actual real-world deployments: Our successful deployments include, IRIS. IRIS has been deployed by the Federal Air Marshals Service (FAMS) since 2009. Another application, PROTECT, has been deployed by the US Coast Guard in Boston since 2011 and New York since 2012, and is headed for nationwide deployment. Finally, GUARDS is being evaluated by the TSA for deploying security resources for infrastructure protection. While our research significantly differs from these past efforts, nonetheless we expect our newer research to also lead to eventual deployments as with these other previous applications.

Our emphasis next year will be newer domains that lead to new research challenges in game theory for security. First, TRUSTS is being evaluated by the Los Angeles Sheriff’s Dept. (LASD); LASD is focused on patrols in Los Angeles Metro Rail system for randomized checking of fare evaders, as well as for suppression of crime. Towards that end, we have been building hand-held mobile device interfaces. These devices would enable large amounts of data collection. Second, our latest project has begun focusing on protection of US fisheries, aiding the US Coast Guard in their fishery protection mission. Our initial focus will be protecting US Fisheries from incursion by Mexican lanchas in Coast Guard district eight, which is near New Orleans.
These new applications bring completely new research challenges to the fore which we will outline below: but in essence these are more dynamic domains, with the possibility to collect large quantities of data (as with the handhelds mentioned above), often involving reasoning about continuous time and space and often requiring coordination of multiple defender resources. We propose several directions for improving our methodology in response to these challenges. In addition, we will continue working to evaluate and improve existing systems to better understand their strengths and seek additional opportunities for improvements.

7. Objectives:
This research will address these fundamental research challenges at the intersection of computational and behavioral game theory under uncertainty:

(a) Handling Dynamic Schedules: We will investigate newer approaches that allow dynamic schedules given defender execution uncertainty, e.g., LA Sheriff’s Dept. officers may interrupt schedules provided to them to arrest troublemakers and may need dynamic schedules. The US coast guard may board boats and thus their schedule may get interrupted while on a fishery mission. This opens a novel area of research where the defender schedules are prone to interruptions and change. Previous work did not allow for such interruptions and dynamic flexible schedules.

(b) Learning from Data via Repeated Interactions: Whereas our previous applications focus on counter-terrorism, we are exploring new domains on combating everyday crimes, including protection of fishery and marine resources, and mass transit such as train systems. A key feature of domains is the repeated interactions between players, and as a result it is possible to collect abundant data. This creates a number of opportunities and challenges that belongs to the intersection of game theory and machine learning, such as learning a better model of the defender’s ability to carry out patrols and features of the defender’s interactions with the environment and adversary, e.g., we may learn how quickly defender is able to check fare evaders, how frequently fare evaders need to be arrested, and so on. We may also learn about the challenge outlined in (a): how frequently is a patrol schedule interrupted?

(c) Adversary Behavior Modeling: Data from behavioral game theory experiments on security games via Amazon Mechanical Turk, from an Israeli military unit on problems similar to security domains have revealed that players often deviate from predictions of perfect rationality on their part, in predictable ways. Data from LASD using handheld devices on LA Metro trains, and on illegal fishery incursions may provide us similar data to further refine our models. A major challenge is developing computational models of these adversary behaviors and incorporating the models into new game-theoretic analysis methods.

(d) Coordination of multiple defender units: In many cases we are faced with highly heterogeneous defender units, potentially belonging to different agencies. For example, in New York for the US Coast Guard, we may potentially need to coordinate US Coast Guard boats, helicopter patrols and NYPD boat patrols. In this instance, we may have only uncertain information about NYPD boat patrols, but may need to ensure not only that the US Coast Guard activities coordinate own assets but also these NYPD patrols. This will require new solution concepts as well as newer algorithms to handle the massive scale of the coordination problem.
8. Interfaces to CREATE Projects:
This work will maintain a close interface with CREATE’s PortSec risk analysis and economics project in evaluating the security resource allocations, and CREATE’s adaptive adversary project.

9. Previous or current work relevant to the proposed project:
Above, we have discussed several previous applications and relevant research. While our previous work has been developing game theoretic applications, each has surpassed the last in terms of complexity of models of adversary behavior, scale of the problem, types and numbers of adversaries, and constraints accommodated. Newer domains TRUSTS and fisheries are more dynamic domains, with large amounts of data, often involving reasoning about continuous time and space and often requiring coordination of multiple defender resources, leading to significant new research challenges.

10. Major Deliverables, Research Transition Products and Customers:
• **Products:** As mentioned above, our previous research has resulted in several deployed software applications for homeland security agencies. Our current research will focus on the TRUSTS software for the LASD and new software for the US Coast Guard for protection of fish. As opportunities develop with Customs and Border Protection and other agencies, our research will also focus on those opportunities.

• **Customers:** Our previous customers include the FAMS service has been using IRIS since 2009; PROTECT has been in use by the US Coast Guard since 2011 in Boston and since 2012 in New York and will be deployed nationwide; GUARDS is under evaluation by the TSA. We expect our new software to be usable by the Los Angeles Sheriff’s department(TRUSTS) and the US Coast Guard (fisheries).

11. Technical Approach:
Our technical approach will be based on the following:

a) **Handling Dynamic Schedules using Robust Solution Methods:** For the problem of dynamic patrol scheduling given defender execution uncertainty, we will investigate newer approaches based on Markov Decision Processes (MDPs) that allow e.g., LA Sheriff’s Dept. officers to deploy dynamic schedules that are robust against interruptions in the schedule, such as arrests. Since transition probabilities in these MDPs may themselves be uncertain, our robust approaches must handle uncertainty over uncertainty of transitions.

b) **Learning from Data via Repeated Interactions:** We will investigate new learning approaches for the everyday-crime domains, by combining game theory and machine learning techniques. In particular, for the fishery-protection domain, the defender (Coast Guard) may be uncertain about the locations of the fish stock, whereas the adversary (illegal fishermen) may have better ideas of where the fishes are. Nevertheless, data from repeated interactions allow us to learn the locations of fish stock from observations about the fishing activity. We plan to model this interaction as a partially-observable Markov-decision process (POMDP) and leverage the specific structure of the domain to speed up the computation.
c) **Adversary Behavior Modeling**: Behavioral game theory and psychology offer various models to explain human decision-making in games. The Quantal Response model has provided significant advantages over perfect rationality model, but it leads to a non-convex and non-linear optimization problem, which is difficult to solve. In addition to exploring new algorithmic techniques for such optimization problems, we propose to investigate other models that simultaneously provide computational efficiency and realistic modeling of human behavior choices, incorporating ideas from current social sciences research, such as that of opportunistic crime. To decide the parameters of human behavior models, we will employ machine learning techniques to elicit the appropriate values for the parameters, using data from experiments on Amazon Mechanical Turk as well as real-world data from LASD using handheld devices on LA Metro trains. We will also explore approaches that borrow ideas from robust optimization and aim to produce strategies that are robust against errors in the parameters and forms of the behavioral models.

d) **Coordination of multiple defender units**: For the scheduling heterogeneous defender units belonging to the same security agency (e.g., the US Coast Guard), one issue not addressed in earlier research is the often nonlinear effectiveness of joint actions, i.e., multiple units protecting the same target at the same time (or within a close time window). This creates computational challenges for scaling up to larger number of units. We will investigate new game models to efficiently represent this type of utility functions as well as new algorithms that can efficiently handle the massive scale of real-world problem instances. In particular, we plan to exploit the submodular structure of utility functions and apply techniques from submodular optimization to yield approximate algorithms with theoretical guarantees on the solution quality. We also plan to adapt models and techniques from research on multiagent cooperative planning, including the Decentralized Markov Decision Process (Dec-MDP) model and relevant algorithms such as reward shaping.

At a meta level our approach continues to be one of building on our virtuous cycle of using theory and algorithm to inform practice, and using practical implementation to inform theory and research.

12. **References**

19. A Deployed Quantal Response Based Patrol Planning System for the US Coast Guard. Bo An, Fernando Ordonez, Milind Tambe, Eric Shieh, Rong Yang, Craig Baldwin, Joseph DiRenzo, Ben Maule, Garrett Meyer. Interfaces 2013