Game Theory and Human Behavior: Challenges in Security and Sustainability

Rong Yang, Milind Tambe, Manish Jain,
Jun-young Kwak, James Pita, and Zhengyu Yin
{yangrong,tambe,manishja,junyounk,jpita,zhengyuy}@usc.edu

University of Southern California, Los Angeles, CA, 90089

Abstract. Security and sustainability are two critical global challenges that involve the interaction of many intelligent actors. Game theory provides a sound mathematical framework to model such interactions, and computational game theory in particular has a promising role to play in helping to address key aspects of these challenges. Indeed, in the domain of security, we have already taken some encouraging steps by successfully applying game-theoretic algorithms to real-world security problems: our algorithms are in use by agencies such as the US coast guard, the Federal Air Marshals Service, the LAX police and the Transportation Security Administration. While these applications of game-theoretic algorithms have advanced the state of the art, this paper lays out some key challenges as we continue to expand the use of these algorithms in real-world domains. One such challenge in particular is that classical game theory makes a set of assumptions of the players, which may not be consistent with real-world scenarios, especially when humans are involved. To actually model human behavior within game-theoretic framework, it is important to address the new challenges that arise due to the presence of human players: (i) human bounded rationality; (ii) limited observations and imperfect strategy execution; (iii) large action spaces. We present initial solutions to these challenges in context of security games. For sustainability, we lay out our initial efforts and plans, and key challenges related to human behavior in the loop.

Introduction

Many of today's critical national and global challenges involve interactions of large numbers of different agents (individuals, large and small corporations, government agencies). A key challenge in solving these problems is to model and analyze the strategic interactions among these multiple intelligent agents, with their different goals, strategies and capabilities. Game theory provides a fundamental tool to understand and analyze such challenges.

The goal of this paper is to point to some research issues in computational game theory as they relate to two such global challenges: security and sustainability. These are massive world challenges, and as such the paper only focuses on limited aspects of these challenges. The key thrust of the research issues we focus on is in the fusion of computational game theory and models of human behavior. More specifically, classical game theory makes assumptions on human behavior – such as perfect and infallible rationality, the ability to perfectly observe and perfectly execute strategies – that are not consistent with real-world scenarios. Indeed, it is well understood that humans are bounded in their computational abilities or may reach "irrational" decisions due to other reasons [15,2]. In both security and sustainability domains, many of the agents are humans, and it is therefore critical to integrate human behavior in the game-theoretic algorithms for these domains.

In security, many scenarios are naturally modeled as a game; much of our own research has focused on the use of Bayesian Stackelberg games for security resource allocation[12,17,16]. These games typically involve a defender who acts first by setting up a security policy and an adversary who may conduct surveillance and then react; in our work, given particular restrictions on payoffs in these games, they are often labeled as *security games*[16]. The research in this area mainly focuses on improving the allocation of security resources by more accurately modeling the human adversary's behavior [19,13,18]. We briefly discuss four key research challenges in this context. The first challenge comes from the basic assumption of classical game theory that all players are perfectly rational, which may not hold when dealing with human adversaries. It is therefore crucial to integrate more realistic models of human decision-making in security games to more accurately predict adversaries' response to defender's strategies. The second challenge is caused by uncertainties in security games that arise in particular due to human players: specifically, adversaries may not perfectly observe defender strategies, defenders may not perfectly execute their strategies, etc. Therefore, it is important to ensure a robust solution in designing defender's resource allocation strategies. The third challenge is modeling, particularly given that we face human adversaries with the capability to generate a very large number of potential threats in real security games. We create a new game-theoretic framework that allows for compact modeling of such threats. Finally, scalability is important as a result of growth in the number of defender strategies, the attacker strategies, and the attacker types. We need to develop efficient algorithms for computing optimal defender strategy of allocating defender resources.

In sustainability, we focus on energy as a key resource, and for providing a concrete scenario, outline our initial efforts using a multi-agent system to lower energy usage in an office building. This research once again requires that we not only model complex strategic interactions between individuals (humans and agents) and design successful mechanisms to influence the humans' behavior, but also ensure that our theoretical models are augmented by more realistic models of human behavior. While we outline just our initial steps, sustainability research in general will require further integration of game theory and human behavior as we consider the complex strategic interactions in the future of large and small energy producers and consumers, individuals, governments, utility companies and others.

In the following, we first discuss the challenges we face in applying game theory to real-world security scenarios, and outline our approaches to address these challenges. For sustainability, we describe a multi-agent system highlighting the challenges of applying game-theoretic framework to the domain.

Security

Stackelberg games are often used to model the interaction between defenders and adversaries (attackers) in security settings [12,16,17]. In such games, there is a defender, who plays the role of leader, taking action first, and a follower (attacker) who responds to the leader's actions. In particular, in Stackelberg security games, the defender decides on how to allocate their security resources taking into consideration the response of the adversary; the attacker conducts surveillance to learn defender's strategy and then launches an attack. The optimal defender strategy hence emphasizes randomized security allocation to maintain unpredictability in its actions. I In a Bayesian Stackelberg game, the defender faces multiple types of adversaries, who might have different preference and objectives. Computing the optimal defender strategy for Bayesian Stackelberg games, so as to reach a "strong Stackelberg Equlibrium" is known to be a NP-hard problem[1].

In this section, we first give a brief introduction to the actual deployed applications that we have developed for different security agencies based on fast algorithms for obtaining optimal defender strategies in Bayesian Stackelberg games. While these algorithms have significantly advanced the state of the art, new challenges arise as we continue to expand the role of these game-theoretic algorithms; we discuss these challenges next.

Background

ARMOR (Assistant for Randomized Monitoring Over Routes) was our first application of security games [12]. It is deployed at the Los Angeles International Airport (LAX) since 2007. ARMOR helps LAX police officers to randomize deployment of their limited security resources. For example, they have eight terminals but not enough explosive-detecting canine units to patrol all terminals at all times of the day. Given that LAX may be under surveillance by adversaries, the question is where and when to have the canine units patrol the different terminals. The foundation of ARMOR are algorithms for solving Bayesian Stackelberg games [11,12]; they recommend a randomized pattern for setting up checkpoints and canine patrols so as to maintain unpredictability.

IRIS (Intelligent Randomization In Scheduling) was designed to help the Federal Air Marchals Service (FAMS) to randomize allocations of air marshals to flights to avoid predictability by adversaries conducting surveillance, yet provide adequate protection to more important flights [17]. The challenge is that there are a very large number of flights over a month, and not enough air marshals to cover all the flights. At its backend, IRIS casts the problem it solves as a Stackelberg game and in particular as a security game with a special payoff structure. IRIS uses the Aspen algorithm [3], and is in use by FAMS since 2009.

GUARDS (Game-theoretic Unpredictable and Randomly Deployed Security) was developed in collaboration with the United States Transportation Security Administration (TSA) to assist in resource allocation tasks for airport protection at over four hundred United States airports [14]. In contrast with ARMOR and IRIS, which focus on one installation/applications and one security activity (e.g. canine patrol or checkpoints) per application, GUARDS reasons with multiple security activities, diverse potential threats and also hundreds of end users. The goal for GUARDS is to allocate TSA personnel to security activities conducted to protect the airport infrastructure. GUARDS again utilizes a Stackelberg game, but generalizes beyond security games and develops a novel solution algorithm for these games. GUARDS has been delivered to the TSA and is currently under evaluation and testing for scheduling practices at an undisclosed airport.

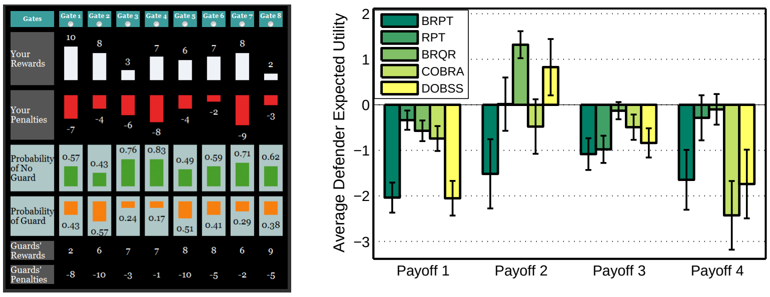
PROTECT (Port Resilience Operational/Tactical Enforcement to Combat Terrorism) is a pilot project we recently started in collaboration with the United State Coast Guard. PROTECT aims to recommend randomized patrolling strategies for the coast guard while taking into account (i) weights of different targets protected in their area of operation; (ii) adversary reaction to any patrolling strategy. We have begun with a demonstration and evaluation in the port of Boston and depending on our results there, we may proceed to other ports.

Challenges in Integrating Human Behavior Models

The first-generation security game applications mentioned above have been a significant step forward over previous methods in allocating security resources. However, to continue expanding the use of game-theoretic methods in security settings, we must address the human behavior within game-theoretic frameworks. While classical game theory makes assumption of perfect rationality, flawless observations and perfect executions, human decision makers may have bounded rationality, suffer from limited observation power and introduce error in execution of strategies [15]. They may also create new strategies that are not originally defined in the game model. To address such challenges, we must integrate realistic models of human bahavior into game-theoretic algorithms. To that end, in this section, we outline our initial research effort to tackle these challenges and point out key future challenges.

Human Decision Making

In order to address the assumption of perfect rationality of human adversaries, we focus on integrating more realistic models of human decision-making into the computational analysis of security problems. In this context, we have developed



Gates	Gate 1	Gate 2	Gate 3	Gate 4	Gate 5	Gate 6	Gate 7	Gate 8
Your Rewards	10	8	3	7	6	7	8	2
Your Penalties	-7	-4	-6	-8	-4	-2	-9	-3
Probability of No Guard	0.57	0.43	0.76	0.83	0.49	0.59	0.71	0.62
Probability of Guard	0.43	0.57	0.24	0.17	0.51	0.41	0.29	0.38
Guards' Rewards	2	6	7	7	8	8	6	9
Guards' Penalties	-8	-10	-3	-1	-10	-5	-2	-5

(a) Game Interface

(b) Average Defender Expected Utility

Fig. 1. Experiments with human subjects.

Cobra (Combined Observability and Rationality Assumption) [13] to address (i) the anchoring bias of human while interpreting the probabilities of several events; (ii) the bounded rationality they have in computing best response. Our most recent work in addressing human decision making [18] develops two new methods for generating defender strategies in security games based on using two well-known models of human behavior to model the attacker's decisions. The first is Prospect Theory (PT) [7], which provides a descriptive framework for decision-making under uncertainty that accounts for both, risk preferences (e.g. loss aversion) and variations in how humans interpret probabilities through a weighting function. The second model is Quantal Response Equilibrium (QRE) [10], which assumes that humans will choose better actions more frequently, but with some noise in the decision-making process that leads to stochastic choice probabilities. In this work, we develop new techniques to compute optimal defender strategies in Stackelberg security games under the assumption that the attacker will make choices according to either the PT or QRE model. More specifically, we present

- Brpt (Best Response to Prospect Theory), a mixed integer programming formulation, for computing the optimal leader strategy against players whose response follows a PT model;
- Rpt (Robust-PT), modifying BRPT method to account for uncertainty about the adversaries choice, caused by imprecise computation [15].
- Brqr (Best Response to Quantal Response), to compute the optimal defender strategy assuming that the adversary's response is based on quantal response model.

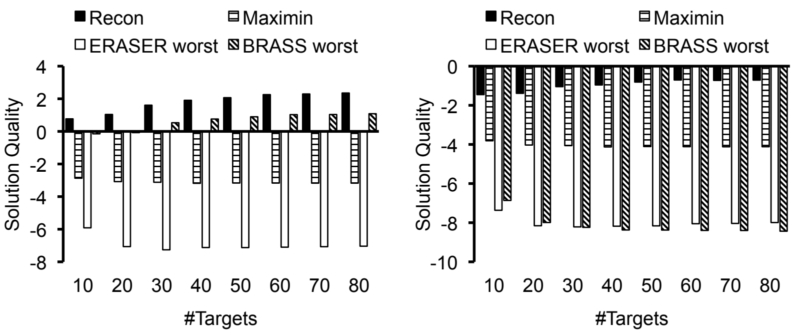
In order to validate the performance of different models, we conducted the intensive empirical evaluation of different models against human subjects in security games. An online game called "The Guard and the Treasure" was designed to simulate a security scenario similar to the ARMOR program for the Los Angeles International (LAX) airport [12]. Figure 1(a) shows the interface of the game. Subjects played the role of followers and were able to observe the leader's mixed strategy. In the game, subjects were asked to choose one of the eight gates to open (attack). We conducted experiment with college students at USC to compare our five models: COBRA, BRPT, RPT, BRQR and the perfect rationality baseline (DOBSS) in the experiment.

Fig. 1(b) displays average performance for the different strategies in each payoff structure. Overall, BRQR performs best, RPT outperforms COBRA, and BRPT and DOBSS perform the worst. BRPT and DOBSS suffer from adversary's deviation from the optimal strategy. In comparison, BRQR, RPT and COBRA all try to be address such deviations. BRQR considers some (possibly very small) probability of adversary attacking any target. In contrast, COBRA and RPT separate the targets into two groups, the ϵ-optimal set and the non-ϵ-optimal set, using a hard threshold. They then try to maximize the worst case for the defender assuming the response will be in the ϵ-optimal set, but assign less resources to other targets. When the non-ϵ-optimal targets have high defender penalties, COBRA and RPT become vulnerable when the targets that are identified as non-ϵ-optimal are actually preferred by the subjects.

Robustness to Uncertainties in Attacker's Observation and Defender's Strategy Execution

As mentioned earlier, attacker-defender Stackelberg games have become a popular game-theoretic approach for security with deployments for the LAX Police, the FAMS and the TSA. Unfortunately, most of the existing solution approaches do not model two key uncertainties of the real-world: there may be noise in the defender's execution of the suggested mixed strategy and/or the observations made by an attacker can be noisy. In our recent work [19], we provide a framework to model these uncertainties, and demonstrate that previous strategies perform poorly in such uncertain settings. This work provides three key contributions: (i) RECON, a mixed-integer linear program that computes the risk-averse strategy for the defender given a fixed maximum execution and observation noise, $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ respectively. RECON assumes that nature chooses noise to maximally reduce defenders utility, and RECON maximizes against this worst case; (ii) two novel heuristics that speed up the computation of RECON by orders of magnitude; (iii) experimental results that demonstrate the superiority of RECON in uncertain domains where existing algorithms perform poorly.

We compare the solution quality of RECON, ERASER, and COBRA under uncertainty: ERASER [6] is used to compute the SSE solution, and COBRA [13] is one of the latest algorithms that addresses attacker's observational error. Figure 2(a) and 2(b) present the comparisons of the worst-case utilities among RECON, ERASER and COBRA under two uncertainty settings: low uncertainty ($\boldsymbol{\alpha}$=$\boldsymbol{\beta}$=$\mathbf{0.01}$) and high uncertainty ($\boldsymbol{\alpha}$=$\boldsymbol{\beta}$=$\mathbf{0.1}$). MAXIMIN utility is provided as a benchmark. Here x-axis shows the number of targets and y-axis shows the defender's worst-case utility. RECON significantly outperforms MAXIMIN, ERASER and COBRA in both uncertainty settings. For example, in high uncertainty setting, for 80 targets, RECON on average provides a worst-case utility of -0.7, significantly better than MAXIMIN (-4.1), ERASER (-8.0) and COBRA (-8.4).



(a) Low uncertainty case ($\alpha = \beta = 0.01$).

(b) High uncertainty case ($\alpha = \beta = 0.1$).

Fig. 2. Worst Case Defender Utility Comparison.

While RECON provides the best performance when we compare worst-case utilities, a key challenge that remains open is to compare its performance with BRQR mentioned in the previous section, and perform such comparison against human subjects. These are key topics for future work.

Modeling Challenge

Security Circumvention Games (SCGs) are a modeling approach to address an adversary's potentially innumerable action space in security settings. While SCGs are motivated by an existing model of security games [20], SCGs make three new critical contributions to the security game model: (i) SCGs allow for defensive actions that consider heterogeneous security activities for each target, (ii) SCGs allow for multiple resources to be allocated to a target (i.e. targets are no longer covered or uncovered), and (iii) SCGs allow for heterogeneous threats on each target. For example, examining a security problem faced by the U.S. Transportation Security Administration (TSA), airports have ticketing areas, waiting areas, and cargo-holding areas. Within each of these areas, TSA has a number of security activities to choose from such as running perimeter patrols, screening cargo, and screening employees. TSA must both choose how many resources to assign to each area and which security activities to run. After observing the TSA's security policy, the attacker will choose which area to attack and what potential threat to execute. The key challenge is how to optimally allocate limited security resources between targets to specific activities, taking into account an attacker's response. SCGs provide the following additional key contributions: (i) a compact representation of the defender actions for efficiency; and (ii) an alternative approach for modeling attacker actions that avoids enumerating all possible threat scenarios. This attempt to avoid exhaustive enumeration of all possible threats is key in SCGs.

More specifically, SCGs create a list of potential threats that circumvent different combinations of specific security activities. By basing threats on circumventing particular combinations of security activities, we avoid the issue of enumerating all the possible potential threats. However, we also incorporate a cost to the attacker for circumventing more activities to capture the idea of causing maximal damage at minimal cost. Each individual security activity has a specific circumvention cost associated with it and more activities circumvented leads to a higher circumvention cost. This cost reflects the additional difficulty of executing an attack against increased security. This difficulty could be due to the need for additional resources, time, and other factors in executing an attack. Since attackers can now actively circumvent specific security activities, randomization becomes a key factor in the solutions leading to significant unpredictability in defender actions.

Addressing the Scalability Challenge

Real-world problems, like the FAMS security resource allocation problem, present trillions of action choices for the defender in security games. Such large problem instances cannot even be represented in modern computers, let alone solved using previous techniques. We provide new models and algorithms that compute optimal defender strategies for massive real-world security domains. In particular, we developed: (i) Aspen and Rugged, algorithms that compute the optimal defender strategy with a very large number of pure strategies for both the defender and the attacker [3,5]; (ii) a new hierarchical framework for Bayesian games that can scale-up to large number of attacker types and is applicable to all Stackelberg solvers [4]. Moreover, these algorithms have not only been experimentally validated, but Aspen has also been deployed in the real-world [6].

Scaling up in pure strategies: Aspen and Rugged provide scale-ups in real-world domains by efficiently analyzing the strategy space of the players. Both algorithms use strategy generation: the algorithms start by considering a minimal set of pure strategies for both the players (defender and attacker). Pure strategies are then generated iteratively, and a strategy is added to the set only if it would help increase the payoff of the corresponding player (a defender's pure strategy is added if it helps increase the defender's payoff). This process is repeated until the optimal solution is obtained.

Scaling up with attacker types: The overarching idea of our approach to scale up attacker types is to improve the performance of branch-and-bound while searching for the solution of a Bayesian Stackelberg game. We decompose the Bayesian Stackelberg game into many hierarchically-organized smaller games, where Each smaller game considers only a few attacker types. The solutions obtained for the restricted games at the child nodes of the hierarchical game tree are used to provide: 1. pruning rules, 2. tighter bounds, and 3. efficient branching heuristics to solve the bigger game at the parent node faster. Additionally, these algorithms are naturally designed for obtaining quality bounded approximations since they are based on branch-and-bound, and provide a further order of magnitude scale-up without any significant loss in quality if approximate solutions are allowed.

Sustainability

To illustrate the challenges in applying game theoretic framework to the field of sustainability, we very briefly discuss a multi-agent system that affects both occupant behaviors and the operation of devices related to energy use. We also consider occupants as active participants in the energy reduction strategy by enabling them to engage in negotiations with intelligent agents that attempt to implement more energy conscious occupant planning. This occupant planning is carried out using multi-objective optimization methods to model the uncertainty of agent decisions, interactions and even general human behavior models. In these negotiations, minimizing energy and minimizing occupant discomfort resulting from various conditions in the space as well as from the negotiation process itself are the considered objectives.

In such energy domains, multi-agent interaction in the context of coordination presents novel challenges to optimize the energy consumption while satisfying the comfort level of occupants in the buildings. First, we should explicitly consider uncertainty while reasoning about coordination in a distributed manner. In particular, we suggest Bounded-parameters Multi-objective Markov Decision Problems (BM-MDPs) to model agent interactions/negotiations and optimize multiple competing objectives for human comfort and energy savings. Second, human behaviors and their occupancy preferences should be incorporated into planning and modeled as part of the system. As human occupants get involved in the negotiation process, it also becomes crucial to consider practical noise in human behavior models during the negotiation process. As a result, our goal is to eventually allow our system to be capable of generating an optimal and robust plan not only for building usage but also for occupants.

In our initial implementation, we compare four different energy control strategies: (i) manual control that simulates the current building control strategy maintained by USC facility managers; (ii) reactive control that building device agents reactively respond to the behaviors of human agents; (iii) proactive control that building agents predict human agent's occupancy and behavioral pattern given the schedules of human agents; and (iv) proactive control with a simple MDP that explicitly models agent negotiations [8,9]. As shown in [8,9], the simulation results indicate that our suggested control strategies could potentially achieve significant improvements in energy consumption while maintaining a desired occupant comfort level. However, this initial implementation is just a first step and significant additional research challenges need to be addressed for the intelligent energy-aware system to increase occupants' motivation to reduce their consumption as practicals by providing building occupants with feedback, especially understanding how their own or other neighbors' behavior influences energy consumption and long-term changes during negotiations.

Conclusion

Game theory provides a fundamental mathematical framework to model many real world problems involving strategic interactions among multiple intelligent actors; furthermore, computational game theory allows to scale-up the problems we can handle within this framework. However, classical game theory makes a set of assumptions of the rationality of the players which may not hold when dealing with real human players, thus requiring us to address new challenges in incorporating realistic models of human behavior in our game-theoretic algorithms. In this paper, we discussed our research in addressing these challenges in the context of security and sustainability. In security, we explained key challenges we face in addressing real world security problems, and presented the initial solutions for these challenges. In sustainability, the main concerns is the usage of energy and how to efficiently exploit the available reserves. The goal is to optimize the negotiation between minimizing energy use and minimizing occupant discomfort. Overall, this fusion of computational game theory and realistic models of human behaviors not only is critical in addressing real-world domains, but also leads to a whole new set of exciting research challenges.

References

1. V. Conitzer and T. Sandholm. Computing the optimal strategy to commit to, 2006.
2. R. Hastie and R. M. Dawes. *Rational Choice in an Uncertain World: the Psychology of Judgement and Decision Making.* Sage Publications, Thounds Oaks, 2001.
3. M. Jain, E. Kardes, C. Kiekintveld, F. Ordóñez, and M. Tambe. Security games with arbitrary schedules: A branch and price approach. In *AAAI*, 2010.
4. M. Jain, C. Kiekintveld, and M. Tambe. Quality-bounded solutions for finite bayesian stackelberg games: Scaling up. In *AAMAS*, page *to appear*, 2011.
5. M. Jain, D. Korzhyk, O. Vanek, V. Conitzer, M. Pechoucek, and M. Tambe. A double oracle algorithm for zero-sum security games on graphs. In *AAMAS*, 2011.
6. M. Jain, J. Tsai, J. Pita, C. Kiekintveld, S. Rathi, M. Tambe, and F. Ordóñez. Software Assistants for Randomized Patrol Planning for the LAX Airport Police and the Federal Air Marshals Service. *Interfaces*, 40:267–290, 2010.
7. D. Kahneman and A. Tvesky. Prospect theory: An analysis of decision under risk. *Econometrica*, 47(2):263–292, 1979.
8. L. Klein, G. Kavulya, F. Jazizadeh, J. Kwak, B. Becerik-Gerber, P. Varakantham, and M. Tambe. Towards optimization of building energy and occupant comfort using multi-agent simulation. In *The 28th International Symposium on Automation and Robotics in Construction (ISARC)*, June 2011.
9. J. Kwak, P. Varakantham, M. Tambe, L. Klein, F. Jazizadeh, G. Kavulya, B. B. Gerber, and D. J. Gerber. Towards optimal planning for distributed coordination under uncertainty in energy domains. In *Workshop on Agent Technologies for Energy Systems (ATES) at AAMAS*, 2011.

10. R. D. McKelvey and T. R. Palfrey. Quantal response equilibria for normal form games. *Games and Economic Behavior*, 2:6–38, 1995.
11. P. Paruchuri, J. P. Pearce, J. Marecki, M. Tambe, F. Ordonez, and S. Kraus. Playing games for security: An efficient exact algorithm for solving bayesian stackelberg games. *In AAMAS*, 2008.
12. J. Pita, M. Jain, F. Ordonez, C. Portway, M. Tambe, C. Western, P. Paruchuri, and S. Kraus. Deployed armor protection: The application of a game theoretic model for security at the los angeles international airport. *In AAMAS*, 2008.
13. J. Pita, M. Jain, F. Ordonez, M. Tambe, and S. Kraus. Solving stackelberg games in the real-world: Addressing bounded rationality and limited observations in human preference models. *Artificial Intelligence Journal*, 174(15):1142–1171, 2010.
14. J. Pita, M. Tambe, C. Kiekintveld, S. Cullen, and E. Steigerwald. Guards - game theoretic security allocation on a national scale. *In AAMAS*, 2011.
15. H. Simon. Rational choice and the structure of the environment. *Psychological Review*, 63(2):129–138, 1956.
16. M. Tambe. *Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned*. Cambridge University Press, 2011.
17. J. Tsai, S. Rathi, C. Kiekintveld, F. Ordonez, and M. Tambe. Iris - a tool for strategic security allocation in transportation networks. *In AAMAS*, 2009.
18. R. Yang, C. Kiekintveld, F. Ordonez, M. Tambe, and R. John. Improving resource allocation strategy against human adversaries in security games. *In IJCAI*, 2011.
19. Z. Yin, M. Jain, M. Tambe, and F. Ordonez. Risk-averse strategies for security games with execution and observational uncertainty. *In AAAI*, 2011.
20. Z. Yin, D. Korzhyk, C. Kiekintveld, V. Conitzer, and M. Tambe. Stackelberg vs. Nash in security games: interchangeability, equivalence, and uniqueness. In *AAMAS*, 2010.