Security Applications: Lessons of Real-World Deployment

JAMES PITA, HARISH BELLAMANE, MANISH JAIN, CHRIS KIEKINTVELD, JASON TSAI, FERNANDO ORDÓNÉZ, MILIND TAMBE
University of Southern California, CA, USA

1. INTRODUCTION

Game theory has played an important role in security settings. Stackelberg games [Fudenberg and Tirole 1991] in particular have recently gained a lot of attention for security applications [Basilico et al. 2009; Kiekintveld et al. 2009; Paruchuri et al. 2008; Pita et al. 2008; Pita et al. 2009]. In Stackelberg games a leader must commit to a strategy first, and then a follower selfishly optimizes its own reward, considering the action chosen by the leader. These games are well-suited to represent the challenges security forces face when allocating limited resources — security forces first commit to a randomized patrolling strategy to avoid predictability and the adversaries act after surveillance of this strategy. Indeed, these games have been at the heart of the deployed systems now in use by Los Angeles World Airport (LAWA) police, the United States Federal Air Marshals (FAMs), and soon to be used by the Transportation Security Administration (TSA). While Stackelberg games provide a strong foundation for creating systems to aid security officials in their scheduling and resource allocation tasks, there are many challenges that have been addressed in taking Stackelberg games from theory to practice. These important challenges include (i) efficiency of algorithms to find mixed (randomized) strategies for security forces that address both the scale of real-world problems as well as their complexity, (ii) evaluation of deployed real-world systems, (iii) knowledge acquisition (preference elicitation) and (iv) handling mixed-initiative interactions. The purpose of this writeup is to first give an overview of the systems we have deployed and then discuss these important challenges.

2. DEPLOYED SYSTEMS

The ARMOR (Assistant for Randomized Monitoring Over Routes) system [Pita et al. 2008] is in use by the LAWA police at Los Angeles International Airport (LAX) from August 2007. This system was designed to assist LAWA police in allocating checkpoints to inbound roads and canine units to airport terminals. ARMOR uses a Bayesian Stackelberg framework to optimally allocate resources based on security information provided by LAWA officials, and it also provides a mixed-initiative interface that allows LAWA officers to make adjustments based on specific intelligence they may have gathered on any particular day. Since its deployment, the police reports an increase in the number of arrests at the airport for offenses such as drug violations and concealed firearms.

Authors’ addresses: {jpita, bellaman, manishja, kiekintv, fordon, tambe, jasontts}@usc.edu
The IRIS (Intelligent Randomization In Scheduling) system [Tsai et al. 2009] is in use by the FAMs. The problem presented was how to assign the limited number of air marshals to different flights. While ARMOR has a limited number of roads and terminals to consider, IRIS has to consider thousands of flights and hundreds of personnel to assign in a Stackelberg game setting. There are also many scheduling constraints that must be adhered to along with locality constraints (an air marshal cannot fly out of an airport he is not located near). These scaling and scheduling issues proved to be major challenges for algorithms to find mixed strategies for FAMs (equilibrium strategies in a Stackelberg framework) that had to be overcome in order to produce a useful system. IRIS has been deployed in a pilot program in some international sectors by the FAMs since October 2009.

The GUARDS (Game-theoretic Unpredictable and Randomly Deployed Security) system is under development for the TSA. GUARDS will help to randomize a number of separate security activities, known as 'plays', designed to look for activities or problems at airports, again using the Stackelberg framework. GUARDS is being deployed at the Pittsburgh and LAX Airports and is undergoing evaluation.

3. LESSONS LEARNED

We now present lessons learned in algorithm development, evaluation of security systems, knowledge acquisition, and mixed-initiative environments.

In developing new algorithms, the key lesson learned is that speeding up the solutions to large games remains an important challenge. While ARMOR was based on newly developed algorithms for efficient solutions to Bayesian Stackelberg games [Paruchuri et al. 2008], there still remains the issue of combinatorial explosion in a standard normal-form representation of Stackelberg games created by the existence of many possible resources to schedule in the security policy. To overcome this obstacle in our current systems we have developed a more compact representation of the Stackelberg games of interest and a corresponding algorithm to solve for the optimal security allocation of resources given this representation known as ERASER-C (Efficient Randomized Allocation of SEcurity Resources Constrained) [Kiekintveld et al. 2009]. This compact representation and algorithm avoid the combinatorial explosion from multiple possible resources by taking advantage of the payoff structures in the Stackelberg games of interest [Kiekintveld et al. 2009].

Evaluation of real-world deployed security systems is an open issue that remains a difficult challenge. There are at least three key issues that make the evaluation of our systems difficult. First, there are security concerns with making evaluations of security policies publicly available making it difficult to obtain in depth evaluation from security forces. Second, there are ethical concerns in not providing the best security possible making it difficult to compare different systems (e.g. with and without ARMOR in place). Third, there are outside variables such as economic conditions, geopolitics, and number of travelers that make it difficult to evaluate whether our system is performing better than other approaches or whether its performance is due to outside variables. For example, comparing the number of arrests for a 15-months period before ARMOR at LAX checkpoints to a 12-months period after ARMOR, we see a five-fold increase in the number of arrests after ARMOR (to over 60). However, along with deploying ARMOR, the security forces also changed...
some of their procedures and this combined with possible changes in the economic conditions make it difficult to attribute this increase precisely to ARMOR. While these challenges still remain an issue, we rely on a multi-faceted evaluation to try overcome them. This includes gathering evidence from as many sources as possible, relying on expert evaluations from security officials, examining data from deployment, tests with human subjects and utilizing computer simulations to predict performance [Taylor et al. 2010; Pita et al. 2009].

Knowledge acquisition also remains a challenge. We need to be able to convert the knowledge of domain experts into actions and payoffs in a Stackelberg game framework. For instance, note that even for experts it is particularly difficult to estimate a terrorist’s possible actions and reward structure. We have turned to component-wise preference elicitation for some of our domains [Tsai et al. 2009], but finding a way to acquire knowledge efficiently still remains a bottleneck in our system development and a difficult challenge.

Finally, we find that mixed-initiative interfaces are important for some security settings where things are often dynamic and fluid. It is often difficult for a security force to adopt a system that does not allow them some flexibility to interact with and adjust schedules produced by the system. A major problem with these interactions is that a game theoretic model assumes the equilibrium policy will be strictly followed. Altering schedules can affect the proposed outcome of the Stackelberg game and handling these disturbances remains an open challenge. While the ARMOR system has a mixed-initiative interface, we found that security forces rarely used the mixed-initiative features.

There is a growing interest for security systems such as ARMOR, IRIS, and GUARDS in several other security agencies. Utilizing solutions to current research problems will help in addressing the new problems these agencies will present and in developing new operational systems.

REFERENCES


Tsai, J., Rathi, S., Kiekintveld, C., Ordóñez, F., and Tambe, M. 2009. IRIS - a tool for strategic security allocation in transportation networks. In AAMAS.