Planning and Learning in Security Games

F. M. DELLE FAVE, Y. QIAN , A. X. JIANG, M. BROWN and M. TAMBE
University of Southern California

We present two new critical domains where security games are applied to generate randomized patrol schedules. For each setting, we present the current research that we have produced. We then propose two new challenges to build accurate schedules that can be deployed effectively in the real world. The first is a planning challenge. Current schedules cannot handle interruptions. Thus, more expressive models, that allow for reasoning over stochastic actions, are needed. The second is a learning challenge. In several security domains, data can be used to extract information about both the environment and the attacker. This information can then be used to improve the defender's strategies.

Categories and Subject Descriptors: I.2.8 [**Artificial Intelligence**]: Problem Solving, Control Methods, and Search

General Terms: Algorithms, Experimentation, Security; Theory

Additional Key Words and Phrases: Artificial Intelligence, Game Theory

1. INTRODUCTION

In recent years, research in security games has produced a number of approaches that led to the deployment of real world applications for protecting critical infrastructure such as ports, airports and trains [Tambe 2011; Conitzer and Sandholm 2006]. In essence, three types of algorithms were developed: (i) scalable algorithms [Jain et al. 2011; Jain et al. 2013]; (ii) algorithms for games with boundedly rational attackers [Yang et al. 2011; Nguyen et al. 2013]; and (iii) algorithms robust against execution and observation uncertainty [Yin et al. 2011; Yin and Tambe 2012].

With an eye to the future, the deployment of these algorithms in the real world introduces two new important challenges. The first is a planning challenge. As will be described later, several security domains involve significant uncertainty. Hence, the schedules in these domains are often interrupted due to unexpected events. Furthermore, in the real world, a schedule's spatial and temporal constraints are typically continuous dimensions. Hence, more expressive models need to be derived to represent such schedules. In particular, models that allow for reasoning over stochastic actions and continuous dimensions.

The second challenge is a learning challenge. Thus far, data available in most domains has been principally used to define the game's matrices. However, in the newer domains, the planned schedules are frequently interrupted. Hence, the information about the locations and times of interruptions as well as the information about the actual interactions between attackers and defenders can also be used. The former can be used to represent the uncertainty of the environment, whereas the latter can be used to learn the attacker's behavior.

Against this background, we present in this letter our initial attempt to address

Authors' addresses: {dellefav,yundi.qian,jiangx,matthew.brown,tambe}@usc.edu

the challenges of planning and learning in the context of security games. In Section 2, we introduce the key concepts related to solving patrolling problems using security games. In Section 3, we present two critical real world problems in which addressing the challenges of planning and learning is the key priority to generate effective schedules. Finally, in Section 4, we discuss some future work and some possible research directions.

2. STACKELBERG GAMES FOR SECURITY PROBLEMS

Protecting critical infrastructure is a challenging task for police and security agencies around the world. Areas such as ports, airports, historical landmarks or locations of political and economic importance are key targets for illegal activities. Example of such activities include fare evasion, burglary and strategic terrorism. Unfortunately, the number of resources available to patrol these domains is typically limited. In addition, adversaries such as terrorists or criminals, will monitor any type of patrolling activity to find and exploit predictable patterns.

To address these shortcomings, game theory provides a method to allocate limited security resources in a selective and randomized fashion. The idea is to cast each problem as a security game, a specialization of a Bayesian Stackelberg game, where a defender (i.e., a security agency) and an attacker (i.e., a terrorist or a criminal) compete over the protection of a number of targets (e.g. buses, trains, forest or marine reserves). In essence, in a security game, if an attacker attacks a target that was covered (protected) by the defender, then the attacker has a worse payoff than if the attacker had attacked the same target when it was not covered. Given these properties, research in security games has produced a number of approaches which are currently being used in several ports and airports of the United States (see [Tambe 2011] for more details).

3. NEW DOMAINS IN SECURITY GAMES

This section presents two different patrolling domains and discusses the way in which they are modeled as security games.

3.1 Patrolling the Los Angeles Metro System

The Los Angeles metro system is a barrier-free transit system. For this reason, fare evasion is a well acknowledged problem for the Los Angeles Sheriff's Department (LASD), the agency responsible for its security. The TRUSTS system was developed to deter such fare evasion and proceeds in two phases [Yin et al. 2012]. First, the spatial and temporal constraints of the problem (e.g., patrol length and train schedules) are encapsulated within a transition graph. Second, the transition graph is used to define a Bayesian Stackelberg game between one defender (the LASD) and multiple types of attackers (the fare evaders).

Schedules produced by the system were deployed on different real world trials. The results showed that the model lacked in accuracy. Indeed, as discussed in Section 1, the schedules were often interrupted due to the uncertainty related to patrolling a metro system. For instance, officers out on patrol would need to arrest an unruly passenger or help out a lost tourist, throwing them off the carefully constructed schedule. In light of this, the original framework has been recently

extended to incorporate uncertainty [Jiang et al. 2013]. The idea is to generalize the transition graph (the first phase) to a Markov decision process (MDP), thus addressing the planning challenge discussed in Section 1. This MDP is then used to define a Bayesian Stackelberg following the second phase of the TRUSTS system described earlier. A pure strategy is produced by solving the game and sampling the randomized strategy. Within this setting, however, the approach produces a Markov strategy which corresponds to a mapping from states to actions. To visualize a schedule then, a mobile application has been developed and is currently being evaluated by the LASD.

3.2 Marine Resources and Forest Protection

The oceans and forests of the world provide a variety of vital natural resources, such as fish and fuelwood, whose unregulated extraction and consumption have become a key concern for security agencies around the world. As a consequence, the intelligent and unpredictable patrolling of these reserves has become a key research challenge within both these domains and security games have been considered as a promising solution concept. Thus far, research has progressed principally in the forest domain. Specifically, the problem is cast as a security game where the forest area is represented as a circular continuous space. Hence, as discussed in Section 1, solving this game requires reasoning over continuous dimensions. An optimal strategy then corresponds to a band patrol capable of maximizing the fully protected pristine area of the forest [Johnson et al. 2012]. In contrast, work on the fish domain has just started. The most interesting feature of this domain is the availability of significant amounts of data on the interactions with the attacker, which, as discussed in the previous section, can be used to improve the defender's strategies.

4. FUTURE CHALLENGES AND RESEARCH DIRECTIONS

The challenges of planning and learning pertain to all the domains discussed in Section 3. In all domains, schedules might be interrupted due to some unexpected events (e.g., writing a citation in a train line, boarding an illegal fisherman's boat). As a consequence, incorporating planning within security games is necessary to model stochastic decision making. In so doing, several issues need to be investigated: new game models and solutions need to be designed and the computational effort required to solve them needs to be evaluated.

Additionally, the introduction of a learning component in security games is necessary to exploit the available domain information. The idea is to extract information from the available data and use it to improve the quality and the effectiveness of the defender's strategies. As a consequence, several key learning challenges such as the amount of data necessary or the computational effort required to learn this information, become relevant to this research. We will consider these challenges in our future work.

REFERENCES

Conitzer, V. and Sandholm, T. 2006. Computing the optimal strategy to commit to. In *Conference on Electronic Commerce (EC)*.

Jain, M., Conitzer, V., and Tambe, M. 2013. Security scheduling for real-world networks. In *International Conference on Autonomous Agents and Multiagent Systems (AAMAS)*.

Jain, M., Tambe, M., and Kiekintveld, C. 2011. Quality-bounded solutions for finite bayesian stackelberg games: Scaling up. In *Int. Conf. on Autonomous Agents and Multiagent Systems*.

Jiang, A. X., Yin, Z., Zhang, C., Tambe, M., and Kraus, S. 2013. Game-theoretic randomization for security patrolling with dynamic execution uncertainty. In *International Conference on Autonomous Agents and Multiagent Systems (AAMAS)*.

Johnson, M. P., Fang, F., , and Tambe, M. 2012. Patrol strategies to maximize pristine forest area. In *Conference on Artificial Intelligence (AAAI)*.

Nguyen, T. H., Yang, R., Azaria, A., Kraus, S., and Tambe, M. 2013. Analyzing the effectiveness of adversary modeling in security games. In *Conf. on Artificial Intelligence (AAAI)*.

Tambe, M. 2011. *Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned*. Cambridge University Press.

Yang, R., Kiekintveld, C., Ordonez, F., Tambe, M., and John, R. 2011. Improving resource allocation strategy against human adversaries in security games. In *International Joint Conference on Artificial Intelligence (IJCAI)*.

Yin, Z., Jain, M., Tambe, M., and Ordonez, F. 2011. Risk-averse strategies for security games with execution and observational uncertainty. In *Conference on Artificial Intelligence (AAAI)*.

Yin, Z., Jiang, A., Johnson, M., Tambe, M., Kiekintveld, C., Leyton-Brown, K., Sandholm, T., and Sullivan, J. 2012. Trusts: Scheduling randomized patrols for fare inspection in transit systems. In *Conference on Innovative Applications of Artificial Intelligence (IAAI)*.

Yin, Z. and Tambe, M. 2012. A unified method for handling discrete and continuous uncertainty in Bayesian stackelberg games. In *International Conference on Autonomous Agents and Multiagent Systems (AAMAS)*.