

ARMOR: Assistant for Randomized Monitoring Over Routes
Milind Tambe, Fernando Ordóñez, University of Southern California
 tambe@usc.edu, fordon@usc.edu

- 1. Overview.....1
- 2. Research Accomplishments2
 - 2.1. Minimizing information produced by security2
 - 2.2. Game-theoretic approach2
 - 2.3. Evaluating the performance of security versus human opponents.....2
 - 2.4. Speeding up solution methods.....3
- 3. Applied Relevance3
- 4. Collaborative Projects3
- 5. Research Products4
 - 5.1. Publications and Reports4
 - 5.2. Presentations5
 - 5.3. Models, Databases, and Software Tools and Products5
- 6. Education and Outreach Products5

1. Overview

The ARMOR project is focused on developing methods for creating randomized plans and processes for monitoring, inspection, patrolling, and security in general --- so that even if an attacker observes the plans, he/she cannot predict its progression --- thus providing risk reduction while guaranteeing a certain level of protection quality.

Security at major locations of economic or political importance is a key concern around the world, particularly given the threat of terrorism. Limited security resources prevent full security coverage at all times, which allows adversaries to observe and exploit patterns in selective patrolling or monitoring, e.g. they can plan an attack avoiding existing patrols. Hence, randomized patrolling or monitoring is important, but randomization must provide distinct weights to different actions based on their complex costs and benefits.

We have developed two different approaches depending on what is known about the adversary. If there is no information about the adversary we use a Markov Decision Process (MDP) to represent patrols and identify randomized solutions that minimize the information available to the adversary. When there is partial information about the adversary we decide on efficient patrols following novel game-theoretic methods, which require solving a Bayesian Stackelberg game.

The ARMOR system focuses on the game-theoretic method of providing such randomization of plans and processes. Casting the problem as a Bayesian Stackelberg game, it obtains randomized strategies for security agents; one of the fundamental advances in ARMOR then is to provide the fastest algorithms known-to-date to solve such games. ARMOR’s strength is its marriage of strong theoretical game-theoretic foundations with practical applications, and the virtuous cycle of theory and practice to benefit from each other.

The ARMOR software has been deployed successfully at the Los Angeles International Airport since August 2007 to determine where and when to place checkpoints, and where and when to deploy canine units. In addition, since May 2008, we have been working in adapting this system to randomize the scheduling of Federal Air Marshals to commercial flights. This deployment in real applications has led to significant interest from the media and other potential users/customers, and substantial research.

"This research was supported by the United States Department of Homeland Security through the Center for Risk and Economic Analysis of Terrorism Events (CREATE) under grant number 2007-ST-061-000001. However, any opinions, findings, and conclusions or recommendations in this document are those of the authors and do not necessarily reflect views of the United States Department of Homeland Security."



2. Research Accomplishments

2.1. Minimizing information produced by security

Our work has developed a series of models and algorithms to decide best patrolling strategies that can achieve a high level of coverage or reward while taking into account the presence of an adversary. We assume the adversary can observe and learn the patrolling strategy and use it to its advantage. This makes ineffective classical optimal patrolling strategies which can be predictable and new models must be developed. The first set of models developed assumes the security agents have no model of the adversary.

In this case, we use MDPs and POMDPs to model patrols of an agent/team of agents respectively. On these decision processes we obtain solutions that trade-off the reward and the randomness of the patrolling policy. We develop and implement efficient algorithms capable of obtaining the maximum reward solutions while maintaining certain level of randomness.

2.2. Game-theoretic approach

The second set of algorithms assumes that partial information of the adversary is known. In this case, we model the interaction between the security agent and criminal adversaries as a Bayesian Stackelberg game, where the security agent is the leader and decides on a patrolling strategy first with the adversary making a decision subsequently aware of the decision of the leader. We assume that the leader may be unsure about the adversary faced and represent this with a probability distribution over possible adversary types. While the optimal policy selection for a Bayesian Stackelberg game is known to be NP-hard, our solution approach based on an efficient Mixed Integer Linear Program (MILP) provides significant speed-ups over existing approaches in obtaining the optimal solution. The resulting policy randomizes the agent's possible strategies, while taking into account the probability distribution over adversary types.

2.3. Evaluating the performance of security versus human opponents

Existing algorithms for Stackelberg games efficiently find optimal solutions, but they critically assume that the follower plays optimally. Unfortunately, in real-world applications, agents face human followers who — because of their bounded rationality and limited observation of the leader strategy—may deviate from their expected optimal response. Not taking into account these likely deviations when dealing with human adversaries can cause an unacceptable degradation in the leader's reward, including in security applications where these algorithms have seen real-world deployment. To address this crucial problem, we introduce three new mixed-integer linear programs (MILPs) for Stackelberg games to consider human

followers, incorporating: (i) novel anchoring theories on human perception of probability distributions and (ii) robustness approaches for MILPs to address human imprecision. We rely on empirical validation to evaluate the effectiveness of the proposed methods. To that end, we consider two settings based on real deployed security systems, and compare 6 different approaches (three new with three previous approaches), in 4 different observability conditions, involving 98 human subjects playing 1360 games in total. The final conclusion was that a model which incorporates both the ideas of robustness and anchoring achieves statistically significant better rewards and also maintains equivalent or faster solution speeds compared to existing approaches.

2.4. Speeding up solution methods

The game-theoretic methods to determine optimal randomized security policies do not scale well in general. This problem is exacerbated when in addition the defender must coordinate different resources to deploy security assets, which may be subject to complex scheduling constraints.

Given a specific structure in the payoff matrices we can obtain a compact representation of the strategies and payoffs for Bayesian Stackelberg games, and introduce a new exact solution algorithm using this representation. This is possible whenever the payoff matrix is such that the reward obtained by the leader and the adversary of an attack on a target depends only on whether that target is protected or not. This value does not depend on which other targets are protected. This compact representation leads to exponential improvements in both representation size and solution time over the best known solution algorithms for generic Stackelberg games. We also extend the original algorithm to incorporate different types of resources with additional scheduling constraints, while still offering comparable performance improvements over previous algorithms.

3. Applied Relevance

To date we have deployed these enhanced patrolling strategies for scheduling checkpoints and K9 police patrols at the Los Angeles International Airport. In addition we are involved in a research collaboration with the Federal Air Marshals to randomize the scheduling of federal agents to commercial flights. We are also exploring the possibility of adapting ARMOR for the deployment of security patrols by the police of Chile as part of a research project funded by the Chilean government.

The idea of using randomness to thwart the objectives of adversaries could also be applied more broadly to any decision that a leader can make as a probability distribution over actions.

For our collaboration with Los Angeles World Airports (LAWA) police we have developed a computer system interface (ARMOR) to these algorithms to determine best vehicle checkpoint locations and patrol routes. The work with FAM is developing an assistant interface (IRIS) which codifies the specific structure of the problem domain.

4. Collaborative Projects

We have deployed the ARMOR-Checkpoints and ARMOR-K9 in collaboration with the Los Angeles World Airport (LAWA) police. This collaboration has involved extensive meetings with LAWA police personnel to calibrate the data and include specific constraints of each problem to the DOBSS model. We have provided LAWA police with alternative schedules of vehicle checkpoints and K-9 patrols obtained from the ARMOR software and have received feedback on

the ease of use and effectiveness of the recommendations. In February we handed over the ARMOR software to LAWA police.

We have had a close collaboration with Federal Air Marshals (FAM), including to date two visits to FAMs headquarters in Dulles, Virginia and one visit by FAM officials to USC. In addition we have had bi-weekly meetings to exchange ideas on the development of the scheduling assistant and progress of our research.

We have participated in the establishment of a Security Center in collaboration between the University of Chile and the Chilean Interior Minister. Among other projects this collaboration is aimed at facilitating a deployment of the ARMOR approach to police patrols in the city of Santiago.

In addition we have had inquiries from TSA, LA County Sheriff Department, and the NY/NJ Port Authority about ARMOR and its possible use.

5. Research Products

Research Products (Please detail below)		#
5a	# of peer-reviewed journal reports published	5
5a	# of peer-reviewed journal reports accepted for publication	1
5a	# of non-peer reviewed publications and reports	19
5a	# of scholarly journal citations of published reports	
5b	# of scholarly presentations (conferences, workshops, seminars)	
5b	# of outreach presentations (non-technical groups, general public)	
5c	# of products delivered to DHS, other Federal agencies, or State/Local	1
5c	# of patents filed	2
5c	# of patents issued	
5c	# of products in commercialization pipeline (products not yet to market)	1
5c	# of products introduced to market	

5.1. Publications and Reports

	Ref	Not Ref
1. Paruchuri, P., Pearce, J., Marecki, J., Tambe, T., Ordonez, F., Kraus, S., "Coordinating Randomized Policies for Increasing Security of Agent Systems," <i>Journal of Information Technology and Management (ITM)</i> , to appear	x	
2. Pita, J., Jain, M., Tambe, M., Ordonez, F., Portway, Western, C. Paruchuri, P., Kraus, S., "Using Game Theory for Los Angeles Airport Security," <i>AI Magazine</i> , to appear		x
3. Jain, M., Pita, J., Tambe, M., Ordonez, F., Paruchuri, P., Kraus, S., "Bayesian Stackelberg Games and Their Application for Security at Los Angeles International Airport," <i>SIGecom Exchanges</i> , 2008		x
4. Pita, J., Jain, M., Western, C., Paruchuri, P., Marecki, J., Tambe, M., Ordonez, F., Kraus, S., "Security via Randomization: A Game-Theoretic Model and its Application to the Los Angeles International Airport," in the proceedings of <i>IEEE Conference on Technologies for Homeland Security</i> , 2008		x
5. Paruchuri, P., Pearce, J., Marecki, J., Tambe, M., Ordonez, F., Kraus, S., "Efficient Algorithms to Solve Bayesian Stackelberg Games for Security Applications," in proceedings of the <i>National Conference on Artificial Intelligence (AAAI)</i> , NECTAR track, July 2008		x

6.	Marecki, J., Tambe, M., “Towards Faster Planning with Continuous Resources in Stochastic Domains,” in proceedings of the <i>National Conference on Artificial Intelligence (AAAI)</i> , July 2008		x
7.	Pita, J., Jain, M., Western, C., Paruchuri, P., Marecki, J., Tambe, M., Ordonez, F., Kraus, S., Deployed ARMOR, “Protection: The Application of a Game Theoretic Model for Security at the Los Angeles International Airport,” in proceedings of the <i>Seventh International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS)</i> , Industry Track, May 2008		x
8.	Paruchuri, P., Pearce, J., Marecki, J., Tambe, M., Ordonez, F., Kraus, S., “Playing Games with Security: An Efficient Exact Algorithm for Bayesian Stackelberg Games,” in proceedings of the <i>Seventh International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS)</i> , May 2008		x
9.	Schurr, N., Marecki, J., Tambe, M., “RIAACT: A Robust Approach to Adjustable Autonomy for Human-Multiagent Teams,” in proceedings of the <i>Seventh International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS)</i> , May 2008		x

5.2. Presentations

Tambe, M., “A Game Theoretic Approach for Security,” Risk Symposium, Santa Fe, 2008

5.3. Models, Databases, and Software Tools and Products

Date Delivered	Item	Agency Receiving Product	Agency POC	Commercialization Status (D-delivered, P-Pipeline, M-Market)
Feb 2008	ARMOR	LAWA Police	Srgt. Cruz	D - P

We delivered a working version of ARMOR to LAWA Police in February 2008, after the six month mark of the collaboration with them. Since then they have been using the software to decide the schedule of checkpoints and K9 patrols at the LAX airport. We are in the process of patenting the software and exploring collaborations for its commercialization.

6. Education and Outreach Products

Education and Outreach Initiatives	#
# of students supported (funded by CREATE)	
# of students involved (funded by CREATE + any other programs)	6
# of students graduated	4
# of contacts with DHS, other Federal agencies, or State/Local (committees)	
# of existing courses modified with new material	
# of new courses developed	
# of new certificate programs developed	
# of new degree programs developed	