

ARMOR: Assistant for Randomized Monitoring Over Routes

Milind Tambe and Fernando Ordonez
tambe@usc.edu, fordon@usc.edu

The ARMOR project is focused developing methods for creating randomized plans and processes for monitoring, inspection, patrolling, checking and so forth -- 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.

Brief Description:

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



ARMOR has been deployed at the Los Angeles International Airport to randomize checkpoint deployment and canine unit allocation(left); Police officers attending the six month evaluation of ARMOR called it a success, leading to its permanent deployment at LAX.

patrolling or monitoring is important, but randomization must provide distinct weights to different actions based on their complex costs and benefits. ARMOR focuses on a novel 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 agencies; 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. To that end, 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. This deployment has led to significant interest from the media and other potential users/customers, while simultaneously leading to novel research challenges.

Objectives:

- (a) *Scale up algorithms to solve Bayesian Stackelberg games:* Transitioning ARMOR to real-world domains has revealed key algorithmic challenges such as scaling up to very large domains. In particular, we wish to be able to handle domains where security agencies may have an order of magnitude more actions (e.g. it is a significantly larger infrastructure to protect, or have many more police patrol paths or units to consider, etc). This requires significant improvements to our base algorithms.
- (b) *Behavioral game theory:* We propose to conduct experiments enabling students at USC to play against ARMOR (using a benign game setting); experiments will test how students react against ARMOR under different experimental settings. We will analyze the data, provide new models and potentially provide improvements to ARMOR based on results of these experiments.

- (c) *Adapt algorithms to solve Bayesian Stackelberg games to address different observability conditions:* We have so far assumed that our adversaries can fully observe the actions of the security forces (whose actions are being randomized). However, in some domains this may not be so, e.g. there may be unmarked police vehicles on patrol creating uncertainty as to whether they are observed or not. We hope to improve ARMOR to include this condition.
- (d) *Los Angeles International Airport deployment:* In addition, we will continue to support and improve our application of ARMOR at the LA international airport.

Major Products and Customers:

- **Product s:** Our major product is the ARMOR software, which allows plans and schedules to be randomized. The ARMOR software consists of the core algorithm as well as the GUI to enter constraints, and other inputs to read data files useful to model the underlying game.
- **Customers:** ARMOR has been successfully transitioned to the police at the Los Angeles International Airport; they have been using it since AUGUST 2007. In addition, there is significant interest in ARMOR, and work has begun to support the Federal Air Marshals in randomizing placement of air marshals on international flights. In addition, we are beginning to interact with the Port of Long Beach, several branches of the TSA, LA sheriff's department, Port Authority of New York and New Jersey, DHS red team, and others.

Technical Approach:

- (a) *To address scale up of algorithms to solve Bayesian Stackelberg games:* A key technique we are investigating exploits the special structure of these games when deployed in security contexts that enable its decomposition. Clever decomposition could allow much larger games to be solved. We will prove the correctness of such decomposition and conduct experimental evaluation.
- (b) *Behavioral game theory:* We have initial data from students playing against ARMOR. We hope to continue detailed investigation with more experiments. Detailed analysis involves significant expertise in statistical analysis. We are beginning to collaborate with experts in the statistical arena to help us analyze this data.
- (c) *Adapt algorithms to solve Bayesian Stackelberg games to address different observability conditions:* So far, we have handled uncertainty about the terrorists, i.e. modeling different types of abilities of the terrorists. We hope to add uncertainty over actions of the security forces, leading to a more complex game to be solved.

Major Milestones and Dates:

1. Develop new algorithm that allows for an order of magnitude scale-up in security agency's actions --- May 2009
2. Conduct experiments with students, analyze data --- Oct 2008
3. Develop new algorithms in response to experimental results --- May 2009
4. Develop new algorithms that handle variable observability conditions --- May 2009