

**Project 17: Secure Multiagent Systems (Tambe)**

This research explores techniques for enhancing security for multiagent systems by optimizing randomization to achieve quality guarantees.

**Modeling Area:** Risk Management

**Principal Investigator:** Milind Tambe

**Institution:** University of Southern California

**Other Investigators:** Fernando Ordonez

**Student Research Assistants:** Praveen Paruchuri

**Brief Description:**

Security in multiagent systems is commonly defined as the ability of the system to deal with intentional threats from other agents. Our research focuses on domains where such intentional threats are caused by adversaries that are either totally unknown or can be associated with limited assumptions about them. In our earlier work we developed secure multiagent systems where the adversary's actions & payoffs are unknown. We proposed intentional policy randomization as a solution technique e.g. randomizing security check at airports etc. We are now extending this work to where the adversary's actions and payoffs are known but their types are unknown e.g., police patrolling where criminal activities can be listed but not which criminal occurs at which time. In such domains, the standard procedure is to model it as a Bayes-Nash game. However, solution to Bayes-Nash games is exponential as the number of adversaries increase. We focus on obtaining heuristic solutions with quality guarantees while optimizing the runtime properties. In particular, we develop secure policies for agent that guarantee a reward to within epsilon of the best Nash equilibrium while obtaining the solution faster using the mixed integer linear programming approaches we developed.



Patrol teams for airport security need optimal solutions

**Objectives:**

The key objective is to develop a modeling framework for providing security for multiagent systems acting in hostile environments where the enemy type is unknown.

**Major Products and Customers:**

The major product is a toolkit that gives secure policies for agents acting in real world like a patrolling unit providing security for a group of houses. In fact, we are planning on developing a toolkit for our campus DPS. Given the number of people patrolling and a map of the area to patrol we will generate a patrolling plan for each person in the patrolling team. The patrol team can then perform planned patrols while ensuring that they get the maximum possible reward.

**Interfaces to other CREATE Projects:**

Although the project being developed is aimed at the patrolling domain, the methods developed are general and will be of interest in many other security based applications.

**Technical Approach:**

Game theory provides algorithmic techniques to develop policies for agents acting in adversarial settings. Applications based on security typically need us to find the best possible plan to be followed. Bayes-Nash games are standard approach for generating policies for agents acting in adversarial domains where the adversary's action/rewards is known but has a probability distribution on their types. However, generating the Bayes-Nash equilibrium is hard and is an NP problem. Given the importance of quality of solution, we developed good heuristics that generate policies for the agent which are within epsilon of the optimal reward in a high-exponent polynomial time.

**Major Milestones and Dates**

1. Develop good heuristic solution for Bayes Nash game – November, 06
2. Basic model and collecting actual data for project with DPS – December, 06
3. Implementation of project and data collection – January, 07
4. Finalize analysis and prepare report – March/April, 07